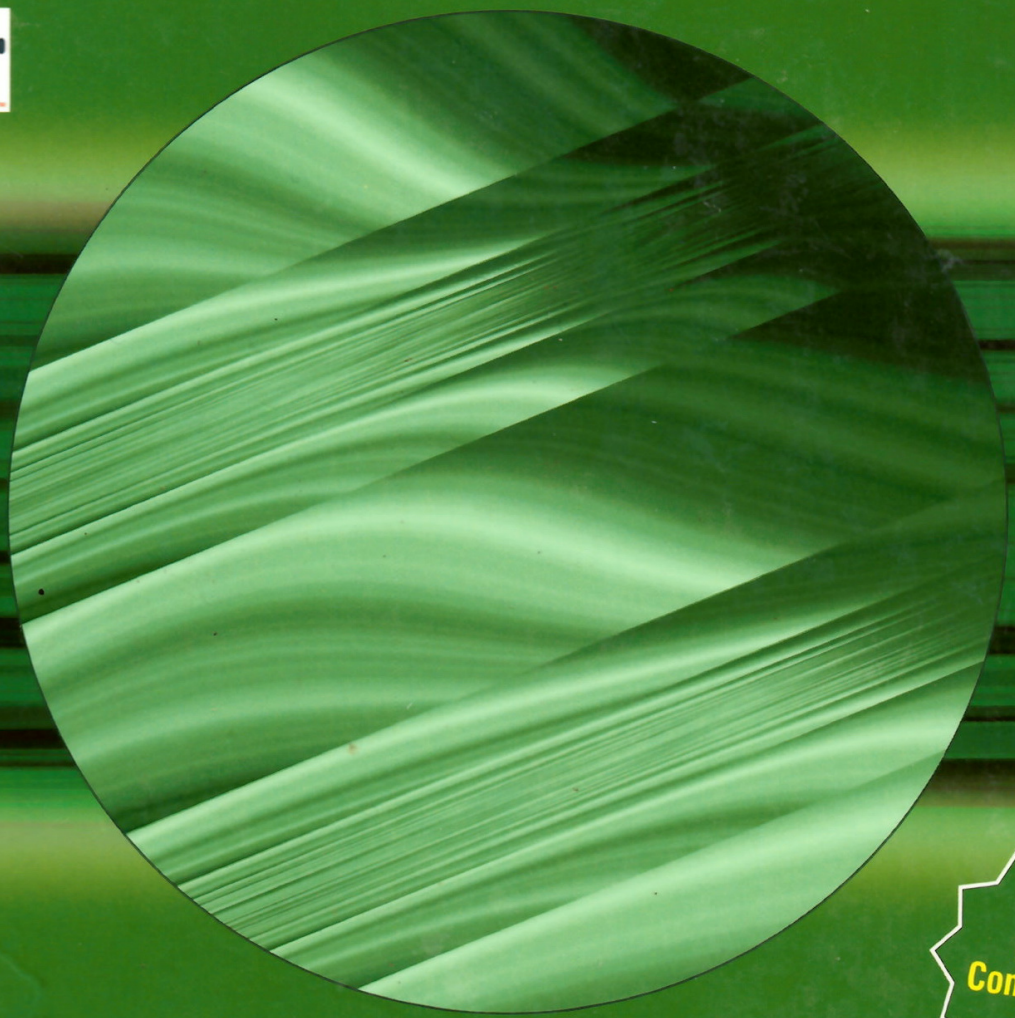
Marco Aurélio Filippetti

CCNA 4.1

Guia Completo de Estudo



Autor Consagrado

Novos Exercícios
100% Focado no Novo Exame (640-802)
Laboratórios voltados para o Dynamips

Visual Books

Cisco CCNA 4.1

(Exame 640-802)

Guia de Estudo Completo

Livraria Técnica VITÓRIA
Eletrônica - Eletricidade - Informática, etc.
Fone: (11) 3223-7872 - (11) 3361-7744
site: www.litec.com.br - e-mail: litec@litec.com.br
Rua Vitória, 374 - CEP 01210-001 - S. Paulo - SP
REF: R$:

* No site da editora está disponível para download um simulado do exame Cisco CCNA.
Acesse: <www.visualbooks.com.br>.

Marco Aurélio Filippetti

Cisco CCNA 4.1

(Exame 640-802)

Guia de Estudo Completo

Visual Books

Copyright© 2008 by Marco Aurélio Filippetti
Copyright© 2008 by Editora Visual Books

Nenhuma parte desta publicação poderá ser reproduzida sem autorização prévia e escrita da Editora Visual Books. Este livro publica nomes comerciais e marcas registradas de produtos pertencentes a diversas companhias. O editor utiliza essas marcas somente para fins editoriais e em benefício dos proprietários das marcas, sem nenhuma intenção de atingir seus direitos.

1a. Reimpressão - Julho de 2009

Editor Responsável: Laura Carvalho
Design da Capa: Henrique Citadini
Fechamento de Capa: Julio Winck
Diagramação/Design: Visual Books Editora
Revisão: Visual Books Editora
Realização Editorial: Visual Books Editora

Dados Internacionais de Catalogação na Publicação (CIP)
(Michele Beck Schröer - CRB 14/1059)

F483c Filippetti, Marco Aurélio
CCNA 4.1 - Guia Completo de Estudo. / Marco Aurélio Filippetti. - Florianópolis: Visual Books, 2008.

480 p.; il. ; 23cm.
ISBN: 978-85-7502-238-2

1. Comunicação entre computadores. 2. Redes de computadores. 3. CCNA 4.1. I. Título.

CDU 004.7

Direitos reservados por:
Visual Books Editora Ltda.
Rua Tenente Silveira, 209, sl 3 - Centro
Florianópolis - SC - 88.010-300
Tel: (48) 3222-1125 Fax: (48) 3324-2886

Serviço ao cliente: atendimento@visualbooks.com.br
HomePage: www.visualbooks.com.br

Dedico este livro à minha amada esposa Juliana que segue apoiando meus projetos com uma paciência quase infinita e sem hesitação.

Ao meu filho João Pedro, minha alegria de viver.

Aos meus pais, por tudo o que me proporcionaram e pelo constante apoio.

A toda a equipe da Visual Books por acreditarem e fazerem acontecer - uma vez mais!

Um agradecimento especial a todos os leitores das edições anteriores e do blog que mantenho, pelas sugestões, dicas e erratas enviadas!

Este livro é para todos vocês!

Sobre o Autor

Marco Aurélio Filippetti nasceu em 1974 e teve sua iniciação no mundo da informática ainda jovem, quando ganhou seu primeiro computador, um saudoso Sinclair TK-85. Hoje, Marco é especialista em Sistemas Computacionais e Engenharia de Telecom pela Universidade da Califórnia (Berkeley), possui os títulos *Cisco CQS Security Specialist*, CCIP e CCDP, *ITIL Foundations*, e é Mestre em Engenharia da Computação pelo Instituto de Pesquisas Tecnológicas de São Paulo (IPT).

Profissionalmente, o autor passou pela KPMG, T-Systems do Brasil, AT&T e atuou como Engenheiro Sênior na extinta Vivax (adquirida em 2006 pela Net), onde ajudou a implementar o sistema autônomo (ASN19090) da empresa. Em 2001, foi ainda sócio-fundador da Netceptions Consulting, uma renomada empresa de consultoria e treinamento em redes. Atualmente, trabalha como Engenheiro de Vendas Sênior para a British Telecom, em São Paulo.

O autor escreveu diversos artigos para revistas especializadas como *Security Hacker* e *ComputerWorld*, foi palestrante em eventos de âmbito nacional, como o ENIE - NetCom e mantém um movimentado blog focado nas certificações Cisco desde setembro de 2007 <http://blog.ccna.com.br>.

Pelo curso preparatório CCNA oferecido pela Netceptions, no período de 11/2001 a 02/2004, passaram mais de 300 pessoas das mais diversas empresas, e o índice de satisfação com o curso atingiu uma média de 95%, ainda hoje, esse nível de satisfação é considerado um dos maiores do mercado.

Atualmente, a metodologia de ensino desenvolvida pelo autor é levada para as salas de aula de cursos de graduação de algumas das mais renomadas faculdades de São Paulo, onde leciona nas cadeiras de Projetos de Redes e Gerência de Redes.

Apresentação

Uma vez mais, meu "MUITO OBRIGADO" a todos os leitores que adquiriram uma cópia desta edição e / ou das edições anteriores do livro. Sem vocês, leitores, eu não estaria aqui hoje, apresentando a 3ª edição deste livro.

Muito mudou desde o lançamento da 1ª edição, em janeiro de 2002. O exame Cisco CCNA ficou mais abrangente e mais difícil. O mercado tornou-se mais exigente, e mais do que nunca, reconhece o valor de um portador da certificação Cisco.

A motivação de formular uma 3ª edição deste livro não foi somente de adequá-lo às exigências do novo exame (640-802), mas também de complementar informações já existentes, de forma que este seja, de fato, o mais completo material sobre a certificação Cisco CCNA já escrito por um autor brasileiro. É ambicioso, sim, mas perfeitamente factível. Basta dedicação, e vontade.

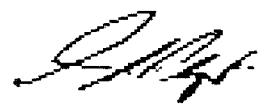
Dentre os tópicos adicionados nesta 3ª edição, encontram-se: maior aprofundamento em redes sem-fio, segurança de redes e IPv6. Além disso, foram retirados os tópicos que tratavam de ISDN e switches 1900, já que estes não são mais abordados no novo exame. Também foram incluídas novas ilustrações e exemplos, e novos exercícios - mais ao estilo do novo exame.

Eu acredito piamente que o material que encontra-se em suas mãos é de excelente qualidade, e abrange 100% do que lhe será cobrado no novo exame Cisco CCNA (exame 640-802). Use-o como guia para seus estudos com a certeza de que ele fará a diferença, assim como as edições passadas fizeram para muitos leitores.

Obrigado aos que participaram enviando sugestões, erratas e elogios. Vocês foram essenciais no trabalho de complementação e melhoria deste material, acreditem. Este livro é para vocês. Espero, mais do que nunca, que seus objetivos sejam atingidos. E que apreciem a leitura deste livro tanto quanto eu apreciei escrevê-lo.

Aproveito para deixar aberto um novo canal de comunicação com vocês, através do e-mail <ccna@ccna.com.br>, ou do blog que mantenho, que pode ser acessado no endereço: <http://blog.ccna.com.br>.

Um grande e caloroso abraço,



Marco A. Filippetti

Sumário

Apresentação 9

1 Introdução 19
1.1 Um Resumo da História da Cisco Systems 19
1.2 Sobre a Certificação Cisco Certified Network Associate - CCNA 20
1.2.1 Por que Tornar-se um CCNA? 21
1.2.2 Perguntas Freqüentes 22
1.2.3 Sobre o Exame 640-802 27
1.2.4 Estatísticas Aproximadas sobre o Novo Exame 27
1.2.5 Questões Típicas 29
1.2.6 Dicas Importantes 30

2 O Modelo OSI 33
2.1 Tópicos Abordados 33
2.2 Histórico 33
2.3 O Modelo de Camadas OSI 39
2.3.1 A Camada de Aplicação 42
2.3.2 A Camada de Apresentação 43
2.3.3 A Camada de Sessão 44
2.3.4 A Camada de Transporte 44
2.3.4.1 Controle de Fluxo 44
2.3.4.2 Confirmação (Acknowledgement) 47
2.3.5 A Camada de Rede 47
2.3.6 A Camada de Enlace de Dados 49
2.3.6.1 Switches e Bridges na Camada de Enlace 50
2.3.7 A Camada Física 51
2.3.7.1 Redes Ethernet 52
2.3.7.2 Os Conceitos Half-duplex e Full-duplex Ethernet 53
2.3.7.3 Endereçamento Ethernet 53
2.3.7.4 O Padrão Ethernet na Camada Física 55
2.3.7.5 Cabos e Conectores em uma Rede Ethernet 57
2.3.7.6 Cabos e Conectores em uma Rede Geograficamente Distribuída (WAN) 59
2.4 Encapsulamento de Dados 61
2.5 O Modelo de Três Camadas Cisco 62

3 Redes Sem-fio (Wireless Networks) 71
3.1 Tópicos Abordados 71
3.2 Introdução 71
3.3 Comparação entre Ethernet LAN e Wireless LAN 72
3.4 Tecnologias Wireless 72
3.5 Modos de Operação WLAN 75
3.6 Transmissão Sem-fio 76

3.7 Classes de Codificação Sem-fio 77
3.8 Interferência 79
3.9 Área de Cobertura, Velocidade e Capacidade 79
3.10 Implementação WLAN 80
3.10.1 Verificação da Operação da Rede Cabeada 80
3.10.2 Instalação e Configuração do AP 81
3.10.3 Configuração dos Detalhes WLAN no AP 81
3.10.4 Configuração do Cliente WIFI 82
3.10.5 Verificação do Funcionamento da WLAN 82
3.10.6 Segurança de Redes Wireless 83
3.11 Padrões de Segurança WLAN 85
3.11.1 Wired Equivalent Privacy (WEP) 85
3.11.2 Cisco Interim Solution 86
3.11.3 Wi-Fi Protected Access (WPA) 86
3.11.4 IEEE 802.11i e WPA-2 87

4 Switching e VLANs 91

4.1 Tópicos Abordados 91
4.2 Comutação na Camada de Enlace 91
4.2.1 Processo de Aprendizagem de Endereços 93
4.2.2 Processos de Encaminhamento e Filtragem 94
4.2.3 Esquemas de Inibição de Loops 95
4.2.3.1 A Solução: O Protocolo Spanning Tree (STP) 96
4.2.3.1.1 Como Determinar o Switch-Raiz 97
4.2.3.1.2 Determinação da Porta Designada 97
4.2.3.1.3 Modos de Operação das Portas de um Switch 97
4.2.3.2 Definição de Convergência 98
4.2.3.3 Exemplo de Funcionamento do Protocolo Spanning Tree 98
4.2.4 Tipos de Comutação 100
4.2.5 Spanning Tree PortFast 102
4.2.6 Spanning Tree UplinkFast 102
4.2.7 Spanning Tree BackboneFast 102
4.2.8 Rapid Spanning Tree Protocol (802.1w) 103
4.2.9 EtherChannel 103
4.3 Virtual LANs (VLANs) 103
4.3.1 Redução do Tamanho dos Domínios de Broadcast 104
4.3.2 Melhor Gerenciabilidade e Aumento de Segurança da Rede Local (LAN) 105
4.3.2.1 Comunicação Inter-VLANS 106
4.3.3 Tipos de Associações VLAN 107
4.3.3.1 Associação Estática 107
4.3.3.2 Associação Dinâmica 107
4.3.4 Identificação de VLANs 108
4.3.5 Frame Tagging 109
4.3.6 Métodos de Identificação de VLANs 110
4.3.7 Roteamento entre VLANs 111

4.3.8 O Protocolo VTP (Virtual Trunk Protocol) 112
4.3.8.1 Modos de Operação VTP 113
4.3.8.2 VTP Pruning 114
5 TCP/IP 127
5.1 Tópicos Abordados 127
5.2 Introdução 127
5.3 O Modelo DoD - TCP/IP 128
5.4 Estudo das Camadas do Modelo DoD (TCP/IP) 129
5.4.1 A Camada de Aplicação 129
5.4.2 A Camada de Transporte 130
5.4.2.1 Portas Lógicas 134
5.4.3 A Camada Internet 135
5.4.3.1 Portas Lógicas IP 138
5.4.3.2 ICMP 139
5.4.3.3 O Protocolo de Resolução de Endereço ARP (Address Resolution Protocol) 139
5.4.3.4 O Protocolo de Resolução de Endereço Reverso RARP (Reverse Address Resolution Protocol) 140
5.4.4 A Camada de Acesso à Rede (Network Access Layer) 141
5.4.4.1 Barramento 141
5.4.4.2 Estrela (Topologia Utilizada por Ethernet, Fast Ethernet e LocalTalk) .. 141
5.4.4.3 Árvore (Topologia Mista) 142
5.4.4.4 Anel Cabeado em Estrela (Topologia Utilizada por Token Ring) 143
5.4.4.5 Anel (Topologia Utilizada por FDDI) 143
5.5 Endereçamento IP 144
5.5.1 Determinação dos Intervalos 147
5.5.1.1 Classe A de Endereços 148
5.5.1.1.1 Endereços Reservados, Privativos ou Ilegais 149
5.5.1.1.2 Classe A - Endereços Válidos 149
5.5.1.2 Classe B de Endereços 150
5.5.1.2.1 Classe B - Endereços Válidos 150
5.5.1.3 Classe C de Endereços 150
5.5.1.3.1 Classe C - Endereços Válidos 151
5.5.2 Subnetting 151
5.5.2.1 Passos para uma Bem-sucedida Implementação de Sub-redes 152
5.5.2.1.1 Máscaras de Rede ou de Sub-rede (Subnet Masks) 152
5.5.2.1.2 Definição de Sub-redes de Classe C 153
5.5.2.2 Uso da Sub-rede "0" e da Sub-rede "All-One" (Ip Subnet-zero) 161
5.5.3 Sub-redes de Tamanho Variável (VLSM) 163
5.5.4 Classless Interdomain Routing (CIDR) 168
5.5.5 Sumarização 169
5.6 IP version 6 (IPv6) 172
5.6.1 Principais Motivações para a Migração do IPv4 para IPv6 173
5.6.2 Novidades nas Especificações do IPv6 173
5.6.3 Formato do Datagrama IPv6 174

5.6.4 Fragmentação e Determinação do Percurso 175
5.6.5 Múltiplos Cabeçalhos 175
5.6.6 Endereçamento 176
5.6.7 Estruturas de Endereços de Transição 177
5.6.8 Endereços IPv6 Especiais 178
5.6.9 Autoconfiguração 178
5.6.10 Protocolos de Apoio ao IPv6 178
5.6.11 Migração para IPv6 178
5.6.11.1 Dual Stacking 179
5.6.11.2 Tunelamento 6to4 (6to4 Tunneling) 179

6 Configuração Básica de Roteadores Cisco 189
6.1 Tópicos Abordados 189
6.2 O Sistema Cisco IOS (Internetwork Operating System) 189
6.2.1 A Rotina de Inicialização de um Router Cisco 193
6.2.2 A Interface de Comando (CLI) 195
6.2.2.1 Conectando-se (Logging in) a um Router 195
6.2.2.2 Estudo dos Diferentes Prompts do CLI 197
6.2.2.3 Recursos de Ajuda 199
6.2.2.4 Comandos de Edição Avançados 200
6.2.2.5 Reunindo Informações Básicas sobre o Router 202
6.2.2.6 Configuração de Senhas 202
6.2.2.7 Outros Comandos de Console 205
6.2.2.8 O Processo de Criptografia de Senhas 205
6.2.2.9 Utilização do Recurso Pipe 206
6.2.2.10 Configuração de Banners (Mensagens) 207
6.2.2.11 Configuração de Interfaces em um Router 208
6.2.2.12 Ativando (No Shut) e Desativando (Shut) uma Interface 210
6.2.2.13 Configuração de Endereçamento IP em Interfaces 211
6.2.2.14 Configurando Hostnames, Descrições e Salvando Configurações .. 213
6.2.2.15 Verificação da Configuração 214
6.2.2.16 Cisco Secure Device Manager (SDM) 216

7 Roteamento IP 231
7.1 Tópicos Abordados 231
7.2 O Processo de Roteamento 233
7.2.1 Configuração do Router 2621A 238
7.2.2 Configuração do Router 2501A 239
7.2.3 Configuração do Router 2501B 239
7.2.4 Configuração do Router 2501C 241
7.3 Roteamento IP 241
7.3.1 Roteamento Estático 242
7.3.1.1 Configuração de Roteamento Estático no Router 2621A 243
7.3.1.2 Configuração de Roteamento Estático no Router 2501A 244
7.3.1.3 Configuração de Roteamento Estático no Router 2501B 245
7.3.1.4 Configuração de Roteamento Estático no Router 2501C 246
7.3.1.5 Análise das Tabelas de Roteamento 246

7.3.2 Roteamento Default 247
7.3.3 Roteamento Dinâmico 250
7.3.3.1 Distâncias Administrativas (Administrative Distances) 251
7.3.3.2 Protocolos Baseados no Algoritmo Distance Vector 253
7.3.3.2.1 Estudo de uma Rede Baseada em Protocolos Distance Vector 254
7.3.3.2.2 Loops de Roteamento (Routing Loops) 256
7.3.3.2.3 Mecanismos Existentes para Minimizar a Ocorrência de Loops 257
7.3.3.2.4 Características do Protocolo RIP 258
7.3.3.2.5 Temporizadores do Protocolo RIP (RIP Timers) 259
7.3.3.2.6 Configurando RIP 260
7.3.3.2.7 Limitando a Propagação do RIP 261
7.3.3.2.8 RIP e Updates Inteligentes 261
7.3.3.2.9 RIP Versão 2 (RIPv2) 262
7.3.3.2.10 Verificação das Configurações RIP 263
7.3.3.2.11 Características do Protocolo IGRP 264
7.3.3.2.12 Temporizadores do Protocolo (IGRP Timers) 264
7.3.3.2.13 Configurando IGRP 265
7.3.3.2.14 Balanceando Carga (Load Balancing) com IGRP 265
7.3.3.2.15 Verificação das Configurações IGRP 266
7.3.3.3 Protocolos Baseados no Algoritmo Link State - O Protocolo OSPF 267
7.3.3.3.1 Designated Router/Backup Designated Router 272
7.3.3.3.2 Formação da Árvore SPF (SPF Tree) 273
7.3.3.3.3 Configurando OSPF em uma Rede Cisco 274
7.3.3.3.4 Configuração do Protocolo OSPF 274
7.3.3.3.5 Verificando a Configuração OSPF 275
7.3.3.3.6 Uso de Interfaces Loopback em Redes OSPF 278
7.3.3.3.7 Identificando Problemas em Redes OSPF 279
7.3.3.4 Protocolos Híbridos - O Protocolo EIGRP da Cisco 279
7.3.3.4.1 O Processo de Descoberta dos Routers Vizinhos 280
7.3.3.4.2 Reliable Transport Protocol (RTP) 282
7.3.3.4.3 Diffusing Update Algorithm (DUAL) 283
7.3.3.4.4 Conceito de Redes Descontíguas 283
7.3.3.4.5 Métricas EIGRP 284
7.3.3.4.6 Configuração EIGRP 285
7.3.3.4.7 Verificação EIGRP 285
7.4 Traduzindo Endereços com NAT (Network Address Translation) 287
7.5 Sumarização de Rotas Usando EIGRP e OSPF 291
7.6 Sumarização de Rotas Usando RIPv2 293

8 Gerenciamento de uma Rede Cisco 303

8.1 Tópicos Abordados 303
8.2 Componentes Físicos e Lógicos de um Roteador Cisco 303
8.2.1 O Configuration Register 304
8.2.1.1 Conversão Binário - Hexadecimal 307
8.2.1.2 Verificação do Valor do Configuration Register 308
8.2.1.3 Alterando o Configuration Register 308

8.3 Recuperação de Senhas 309
8.3.1 Routers da Série 2600 e de Outras Séries Mais Novas 309
8.3.2 Routers da Série 2500 e Mais Antigos 310
8.4 Procedimentos de Backup e Recuperação do Sistema IOS 311
8.5 Recuperação de uma Imagem IOS Armazenada em um Servidor TFTP .. 313
8.6 Procedimento de Backup dos Arquivos de Configuração (Startup-config e Running-config) 314
8.7 O Protocolo CDP (Cisco Discovery Protocol) 316
8.7.1 Obtenção dos Valores dos Timers CDP e Informações sobre Holdtime . 316
8.7.2 Obtenção de Informações sobre o Tráfego de Dados em Interfaces via CDP 318
8.8 Configuração do Telnet (Terminal Virtual) 319
8.8.1 Monitorando Conexões Telnet 320
8.9 Resolução de Hostnames 321
8.9.1 Configurando Routers para Lidar com Broadcasts e Multicasts 323
8.10 Configuração do Serviço DHCP em um Roteador Cisco 323
8.10.1 Monitorando o DHCP 325

9 Segurança de Redes 333
9.1 Tópicos Abordados 333
9.2 Segurança de Redes 333
9.2.1 Práticas para Mitigação dos Riscos 338
9.2.1.1 Firewalls e o Cisco Adaptative Security Appliance (ASA) 338
9.2.1.2 Anti-X 339
9.2.1.3 Ferramentas de Detecção e Prevenção de Intrusão 339
9.2.1.4 Cisco Security Agent (CSA) 340
9.2.1.5 SSH (Secure Shell) 340
9.2.1.6 Virtual Private Networks (VPNs) 341
9.3 Listas de Acesso 342
9.3.1 Listas de Acesso IP Padrão 344
9.3.1.1 Listas de Acesso IP Padrão – Exemplo de Aplicação 347
9.3.1.2 Listas de Acesso no Controle de Acessos via VTY (Telnet) 348
9.3.2 Listas de Acesso IP Estendidas 348
9.3.2.1 Outro Exemplo de Lista IP Estendida 349
9.3.3 Listas IP Nomeadas (Named ACLs) 350
9.3.4 Incluindo Descrições em ACLs 351
9.3.5 Outros Tipos de ACLs 352
9.3.6 Monitorando Listas de Acesso IP 352

10 Protocolos WAN 361
10.1 Tópicos Abordados 361
10.2 Terminologia WAN 362
10.3 Tipos de Conexão WAN 362
10.4 Estudo dos Protocolos WAN 363
10.4.1 O Protocolo HDLC 365
10.4.2 O Protocolo PPP 366
10.4.2.1 As Opções Disponíveis ao Protocolo LCP 367

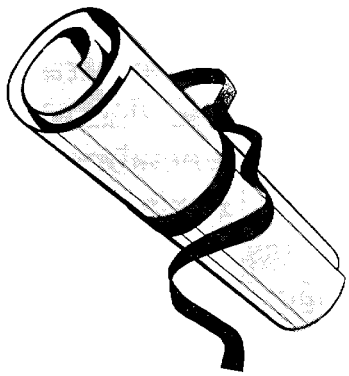
10.4.2.2 Estabelecimento de uma Sessão PPP 367
10.4.2.3 Os Métodos de Autenticação Utilizados pelo PPP 368
10.4.2.4 Configurando Autenticação PPP 369
10.4.2.5 Verificação e Monitoramento PPP 369
10.4.3 O Protocolo Frame-Relay 370
10.4.3.1 Configuração do Frame-Relay em Routers Cisco 373
10.4.3.2 DLCI - Data Link Connection Identifiers 374
10.4.3.3 Local Management Interface (LMI) e suas Mensagens 375
10.4.3.4 O Benefício Proporcionado por Subinterfaces 376
10.4.3.5 Criação de Subinterfaces 377
10.4.3.6 Mapeamento Frame-Relay 379
10.4.3.7 Esquemas de Controle de Congestionamento Empregados pelo Frame-Relay 380
10.4.3.8 Commited Information Rate (CIR) 381
10.4.3.9 Monitorando Frame-Relay em Routers Cisco 381

11 Configuração de Switches 387
11.1 Configuração de Switches Catalyst 2900 387
11.2 Recursos do Switch 2950 388
11.2.1 Slots GBIC (Gigabit Interface Converter) 389
11.2.2 Conexão à Porta Console 390
11.2.3 Inicialização do Switch 390
11.2.3.1 Rotina de Inicialização 392
11.2.4 Definindo Senhas de Modo Privilegiado e Usuário 393
11.2.5 Configuração do Hostname 393
11.2.6 Configuração do Endereço IP 394
11.2.7 Configuração de Interfaces (Portas) 394
11.2.7.1 Configuração de Descrições nas Interfaces 395
11.2.7.2 Configuração da Velocidade e do Modo Duplex da Porta 395
11.2.8 Verificação da Conectividade IP 396
11.2.9 Apagando a Configuração de um Switch 396
11.2.10 Gerenciamento da Tabela de Endereços MAC 397
11.2.10.1 Configuração de Endereços MAC Estáticos 398
11.2.10.2 Configuração de Segurança em Portas 398
11.2.11 Utilizando o Comando Show Version 400
11.2.12 Configuração de VLANs 401
11.2.12.1 Configuração de Portas de Transporte (Trunk Links) 402
112.12.2 Verificação de Links de Transporte 403
11.2.12.3 Configuração dos Modos STP 404
11.2.12.4 Configuração Etherchannel 404
11.2.12.5 Configuração de Roteamento dot1q 405
11.2.12.6 Configuração do Modo VTP na Linha 2900 406
11.3 Recuperação de Senhas com Switches 2950 407

Referências 419

Glossário 421

Apêndice A - Laboratórios 429
Apêndice B - Comandos para Prática 451
Apêndice C - Estudo de Casos 457
Apêndice D - A Interface do Exame 640-802 475



1 Introdução

1.1 Um Resumo da História da Cisco Systems

No começo dos anos 80, Len e Sandy Bosack, que trabalhavam em diferentes departamentos de computação na Universidade de Stanford (Califórnia - Estados Unidos), estavam tendo problemas em fazer seus sistemas se comunicarem. Para solucionar esse problema, eles criaram, em sua própria casa, um *gateway server* que permitia que duas máquinas utilizando sistemas e arquiteturas diferentes se comunicassem através do protocolo IP. Em 1984, era fundada a Cisco Systems.

Acredita-se que o nome Cisco (inicialmente grafado com "c" minúsculo) foi originado de um erro de despachante na incorporação da empresa. O nome deveria ser *San Francisco Systems*, porém, parte da documentação teria sido extraviada no processo, deixando legível apenas "cisco Systems".

A Cisco iniciou suas atividades comercializando um pequeno servidor *gateway* comercial - o que mudaria o conceito de redes para sempre. O primeiro produto foi chamado de *Advanced Gateway Server* (AGS). Depois vieram o *Mid-range Gateway Server* (MGS) e o *Compact Gateway Server* (CGS). Em 1993, surgiu o impressionante router 4000 e, logo em seguida, as linhas 7000, 2000 e 3000, que ainda são utilizadas.

A Cisco rapidamente tornou-se líder mundial em infra-estrutura para Internet e em soluções para conectividade ponta a ponta. Para manter-se líder, era preciso a criação de um programa de treinamento para formação de técnicos aptos a gerenciarem a infra-estrutura instalada. Surgiu, então, o programa *Cisco Career Certifications*, com a certificação *Cisco Certified Internetwork Expert*. Isso mesmo! Pode parecer

estranho, mas o CCIE foi a base para todas as outras certificações oferecidas hoje pela empresa, e não vice-versa. Hoje, existem seis diferentes focos (ou especializações), sendo o CCNA a base para todos eles (veja tabela 1.1). Com exceção do CCDA e o CCDP, todas as certificações são focadas no pós-venda, ou seja, essencialmente, no suporte técnico, configuração e atualização de redes já existentes. Já as certificações em design (CCDA e CCDP) são focadas no pré-venda, ou seja, no planejamento e desenho de redes. Isso não quer dizer que um profissional certificado CCNA não saiba planejar uma rede, ou que um profissional certificado CCDA não saiba suportar a rede que ele próprio desenhou. Apesar de o CCNA não ser pré-requisito para a obtenção do CCDA, sua obtenção é altamente recomendada.

Foco	Associate	Associate +	Professional	Expert (CCIE)
Routing & Switching	CCENT/CCNA		CCNP	CCIE Routing & Switching
Design	CCDA		CCDP	CCDE
Network Security	CCNA	CCNA Security	CCSP	CCIE Security
Service Provider	CCNA		CCIP	CCIE Service Provider
Storage Networking	CCNA		N/A	CCIE Storage Networking
Voice	CCNA	CCNA Voice	CCVP	CCIE Voice
Wireless		CCNA Wireless		

Tabela 1.1: Certificações e focos disponíveis hoje.
Fonte: Cisco Systems.

1.2 Sobre a Certificação Cisco Certified Network Associate – CCNA

A certificação CCNA é a base da pirâmide de certificações oferecidas pela Cisco hoje. É o primeiro passo a ser dado em direção à conquista do carimbo *Cisco Certified Internetwork Expert* (CCIE), uma das certificações em TI mais respeitadas atualmente.

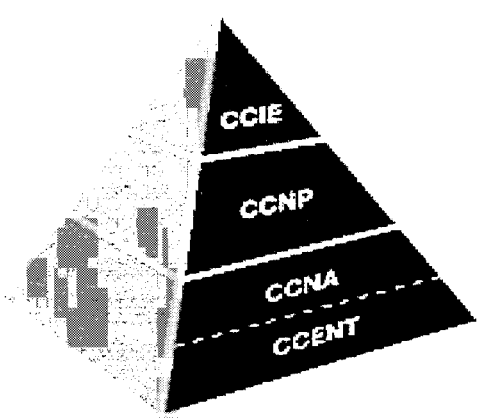


Figura 1.1: Pirâmide de certificação.

Muito requisitados pelo mercado atual, profissionais que satisfazem os requisitos mínimos exigidos pela Cisco e obtêm a certificação CCNA têm a certeza de que serão valorizados. Um CCNA, em teoria, deve ser capaz de implementar, configurar, gerenciar e prestar suporte a redes de pequeno-médio porte (sejam LANs, MANs ou WANs).

Em meados de 2007, a Cisco percebendo que a certificação CCNA encontrava-se em um nível um pouco elevado para uma certificação de entrada, criou a certificação CCENT (*Cisco Certified Entry Networking Technician*), que desde novembro de 2007 passou a ser a certificação base da Cisco.

Para obter o CCNA, o candidato continua com a opção de realizar somente um exame (agora o exame 640-802) ou de realizar dois exames separadamente: 640-822 (ICND1) e o 640-816 (ICND2). Sendo aprovado no exame ICND1, o candidato já obtém o status de CCENT. Se aprovado também no ICND2, ele recebe a chancela de CCNA. Em junho de 2008, a Cisco lançou três especializações para o CCNA: CCNA Security, CCNA Voice e CCNA Wireless. As especializações CCNA Security e CCNA Voice são pré-requisitos para as certificações de nível Professional CCSP e CCVP.

Já está em desenvolvimento a certificação CCIE focada em Wireless, e tudo indica que a Cisco vai lançar em breve uma certificação Professional focada em Wireless.

1.2.1 Por que Tornar-se um CCNA?

Os estudos e a prática necessários à obtenção da certificação CCNA invariavelmente melhorarão seu entendimento geral na área de *internetworking*[1], indo muito além da mera interação com os produtos Cisco.

A linha de certificação Cisco se diferencia de outras certificações populares, como MCSE/MCP da Microsoft ou Network+ da CompTIA que englobam uma variedade de tópicos de forma mais detalhada, sendo, portanto, mais difíceis de se obter. Outro fator interessante de ser mencionado é que, apesar de a certificação em questão ser oferecida por um fabricante específico (Cisco, no caso), os conhecimentos necessários para obtê-la podem ser aplicados em praticamente qualquer tipo de rede de dados. Esse é um dos principais motivos que faz do certificado Cisco CCNA ser, ainda hoje, tão valorizado pelo mercado.

Muitos pensam que a certificação CCNA perdeu força, e que o mercado hoje não a vê com os mesmos olhos de alguns anos atrás. Isso é um grande engano. Já prestei consultoria para várias empresas, e todas - sem exceção - ainda adotam o fato de o candidato possuir ou não a certificação como um grande diferencial na seleção. Portanto, não se engane: o CCNA, hoje, é um forte um balizador de mercado.

---

[1] *Internetwork* é o termo utilizado para definir uma "rede de redes", basicamente, uma grande rede espacialmente distribuída.

Ao optar pela linha de certificações Cisco, você está optando pela melhor formação profissional na área de transmissão de dados.

1.2.2 Perguntas Freqüentes

1) O que mudou no exame CCNA da versão 640-801 para a 640-802?

A versão 640-801, segundo a Cisco, foi aposentada em 06 de Novembro de 2007, sendo substituída pela versão 640-802. Apesar do anúncio, postado no site da Cisco desde meados de 2007, a versão 640-801 continua disponível para agendamento no site da VUE (veja figura 1.2), porém, somente em português (e alguns outros idiomas). Isso ocorre devido a Cisco ainda não ter traduzido a nova versão do exame para o português até o início de 2008. A vantagem em se fazer a versão 640-801 é que os novos tópicos não fazem parte dela, e a opção pelo idioma português.

A nova versão (640-802) manteve praticamente inalterado o conteúdo de sua predecessora, com algumas inclusões e exclusões: o novo formato abrange com maior nível de detalhes redes sem fio (Wireless), cobra um entendimento bastante básico da versão 6 do protocolo IP (IPv6) e inicia a cobrança de questões de segurança. Por outro lado, o exame deixa de cobrar ISDN, o que é uma novidade muito bem-vinda. De resto, o conteúdo é o mesmo. Assim como seu antecessor, o novo formato é bastante interativo e, por conseqüência, tende a valorizar o candidato melhor preparado.

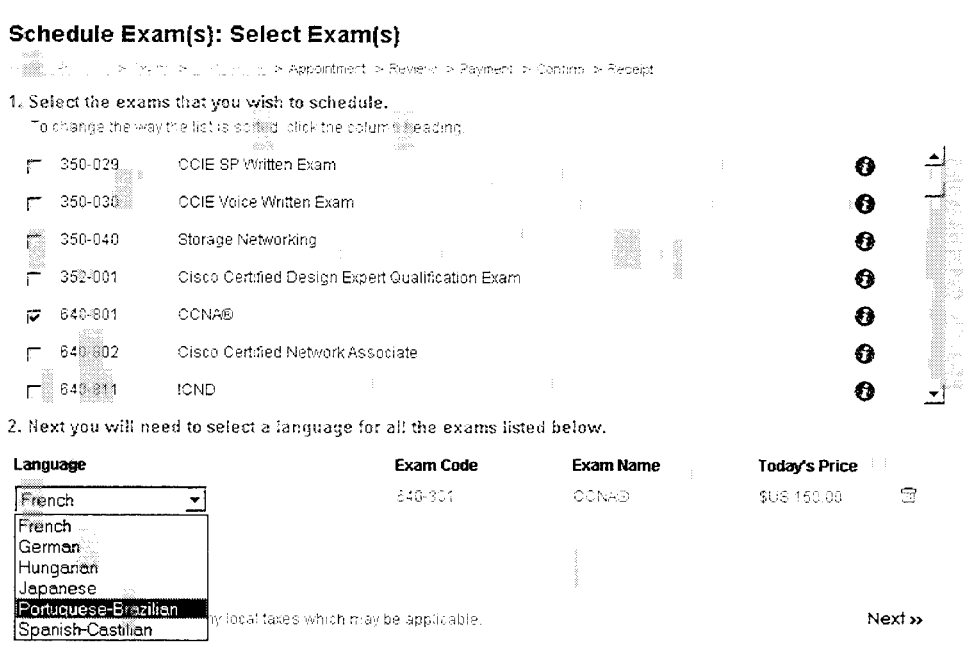


Figura 1.2: Tela do site da VUE mostrando que a versão 640-801 em português ainda encontrava-se disponível (acessado em fevereiro de 2008).

As chances de aprovação dos candidatos que se preparam apenas com base em *"braindumps"* (ex. *Testking*) foi drasticamente reduzida - objetivo principal da Cisco - elevando o nível geral do exame.

Resumindo: não basta decorar, tem que entender. O exame CCNA não valoriza tanto a prática e a experiência do candidato, porém, como o novo formato apresenta algumas das questões de forma interativa - por vezes simulando um roteador real em operação (veja exemplo no Apêndice D) - praticar os comandos vistos com o auxílio de programas simuladores (ou mesmo com *routers* reais) é de grande ajuda, tanto para o sucesso no exame, quanto para seu futuro profissional na área.

2) Qual a vantagem de ser certificado? Como o mercado encara profissionais com a certificação Cisco CCNA?

Em um mercado extremamente competitivo como o atual, a escolha de uma certificação globalmente reconhecida e procurada, como é o caso do CCNA, pode fazer muita diferença na obtenção de um bom emprego, ou mesmo na busca de uma promoção e, conseqüentemente, de um melhor salário.

O mercado para profissionais com conhecimentos comprovados em redes de dados é imenso e, financeiramente, bastante atrativo. CCNAs atuam configurando e operando LANs e WANs roteadas e LANs comutadas, entendem a fundo e são capazes de configurar redes IP, protocolos de roteamento, portas seriais, Frame-Relay, IP, Ethernet e listas de acesso, são freqüentemente procurados para efetuar otimização de performance de redes e são capazes de configurar acesso remoto LAN-to-LAN, requerido por novas áreas e aplicações como e-commerce, B2B, VoIP, redes convergentes etc.

3) Existem pré-requisitos para que eu possa me certificar? Quais são eles?

Não existem, formalmente, pré-requisitos para que um indivíduo se torne um CCNA. Em teoria, qualquer um com muita vontade e persistência e que tenha acesso ao material de estudo correto pode tornar-se um CCNA com menos de quatro semanas de estudo dirigido. Não é necessária experiência prática, tampouco estar atuando na área. No entanto, o nível de detalhamento exigido pela Cisco é alto, o que garante que grande maioria dos aprovados no exame realmente conheçam profundamente a teoria por trás do transporte de dados, mesmo sem possuir qualquer experiência na área. Por esse motivo, a certificação CCNA não é mais considerada como *entry-level* (que agora passa a ser o CCENT).

4) Como e onde me certifico? Quanto custa o exame?

Para tornar-se um CCNA, basta ser aprovado em um exame, o 640-801 (enquanto disponível), ou o novo 640-802 da Cisco. Discutiremos detalhes deste exame mais adiante. A Cisco ainda abre uma segunda opção: é possível "quebrar" o exame em 2 partes, sendo assim, seria necessário realizar 2 exames para se certificar (640-822 ICND1 e 640-816 ICND2). O interessante deste caminho é que, sendo aprovado no primeiro exame (640-822), o candidato já adquire o primeiro carimbo da Cisco, a recém-criada certificação CCENT (*Cisco Certified Entry Networking Technician*).

Eu, particularmente, não recomendo. É mais barato e mais prático partir diretamente para a 640-802 e obter o status de CCNA (muito mais reconhecido e valorizado pelo mercado do que o novo e desconhecido CCENT). Para candidatar-se ao exame basta inscrever-se em um dos centros autorizados VUE espalhados pelo Brasil, lembrando que a Cisco não mais utiliza os serviços da Prometric.

Para encontrar o centro mais próximo, ou mesmo para efetuar sua inscrição online, visite o website <http://www.vue.com>. O custo para se fazer o exame foi reajustado pela Cisco em junho/2008 e passou de US$ 150 para "salgados" US$ 250.

5) Preciso participar de algum curso antes? Estudar por conta própria é suficiente? Alguma sugestão?

Não, você não precisa participar de nenhum curso para estar apto a prestar o exame CCNA. No entanto, algumas firmas especializadas oferecem uma excelente preparação para ele. Estudar por conta própria pode ser o suficiente se você possui bastante força de vontade, disciplina e interesse pelo assunto. Se você não se encaixa nesse perfil, talvez inscrever-se em um curso seja o melhor caminho.

Outra solução para aqueles que não possuem todas as qualidades citadas pode ser a formação de um grupo de estudos, pois o ambiente proporcionado acaba exigindo mais disciplina e dedicação.

6) Preciso saber inglês para estudar ou realizar o exame CCNA?

Até a data da publicação deste material não havia uma versão em português do exame 640-802. Este quadro deve mudar em breve, uma vez que o exame 640-801 oferece versões em outros idiomas (inclusive português).

Mesmo já existindo a versão em português do exame 640-802, quando você estiver lendo este livro, é altamente recomendável que você possua, pelo menos, o chamado "inglês técnico", por duas boas razões:

I. O exame em português tem menos tempo para ser concluído que o em inglês (90 minutos contra 120 minutos), e algumas traduções no exame em português são, literalmente, "tristes", às vezes até incompreensíveis, o que pode levá-lo à confusão e conseqüente perda de questões;

II. Se você deseja se tornar um profissional competente na área de redes (ou qualquer outra área relacionada com Tecnologia da Informação), você vai ter que saber inglês e ponto final. A maioria da bibliografia técnica atualizada existente hoje na área encontra-se em inglês, os comandos e linguagens de programação são baseados no idioma inglês, isso só para citar alguns poucos motivos! Não há escapatória. Se você não entende nada de inglês, meu conselho é que invista nisso o mais rápido possível.

7) E quanto à parte prática? Preciso ter contato com routers e switches?

Apesar de não ser imprescindível, é recomendado o contato com equipamentos reais. O exame CCNA não tem como foco a parte prática e, sim, a teórica. Alguns programas simulam uma sessão console com routers e switches com um bom nível de realismo e detalhamento, como o excelente RouterSim, da Boson Software <www.boson.com>. Um software desses sai bem mais em conta que um router real (em torno de US$90), e chega a disponibilizar cenários com diversos routers, switches e até mesmo PCs (dependendo da versão do software utilizado). Existem ainda outras opções para praticar. Empresas como a *CCOnlineLabs.com* <www.cconlinelabs.com> e a *Network Learning* <www.ccbootcamp.com> disponibilizam o acesso a "racks" com diversos equipamentos Cisco, via Telnet. O problema é que o serviço é pago e, para os padrões brasileiros, os preços ainda são um tanto quanto "salgados". Uma alternativa que está se tornando bastante popular é a utilização de um software que "emula" um ou mais roteadores Cisco em seu PC. Este software chama-se *Dynamips / Dynagen* <http://dynagen.org/>. O Apêndice "A" deste livro trata desse software com detalhes.

Alguns cursos usam como diferencial o fato de possuírem um laboratório estado da arte para o curso CCNA (há os que alegam ter investido milhares de dólares na sua montagem). Esses cursos realmente colocam o candidato em contato com laboratórios muito bons e completíssimos. Porém, em um curso focado na formação CCNA, o participante dificilmente utilizará mais de 5% dos recursos disponíveis. Esses labs são, na verdade, concebidos tendo-se em mente cursos bem mais avançados, ou mesmo a realização de testes internos à própria

empresa. Uma vez montados, acabam sendo aproveitados no curso CCNA (por que não?). O custo de se implementar e manter uma estrutura dessas é imenso, e quem acaba pagando por isso são os participantes dos cursos. Tais firmas costumam cobrar valores abusivos por seus cursos e, não raro, tal investimento não propicia o retorno esperado para o participante. Com a quantia investida você poderia, por exemplo, montar um grupo de estudos com seus colegas e ratear o custo dos equipamentos necessários para a montagem de um bom lab. Vocês teriam um lab à sua disposição 24 horas por dia e, "de quebra", poderiam recuperar 100% do capital investido com a venda desses equipamentos após o uso (ou poderiam mantê-los caso desejem prosseguir para outras etapas, como o CCNP ou mesmo o CCIE).

8) Fui aprovado! Isso significa garantia de emprego?

Antes de qualquer coisa, não se iluda! Essa é a mais importante dica a ser dada. Passar no exame é um grande passo, mas não é tudo. É apenas uma pequena trilha conquistada em um longo caminho. Sim, isso mesmo! Não pense que inúmeras empresas se atirarão aos seus pés, implorando-lhe que trabalhe para elas.

A verdade é: possuir a certificação lhe abrirá muitas portas que antes se encontravam fechadas. Ela não garante, porém, que a tarefa de atravessá-las seja fácil e "indolor". Se você já possui experiência, atravessar essas portas será uma tarefa relativamente fácil. Caso não tenha experiência na área, seja humilde. Ofereça-se para trabalhos e cargos que talvez não sejam tão nobres, mas que lhe garantirão a tão necessária experiência. Procure pôr em prática toda a teoria assimilada durante seus estudos. E não se esqueça: continue sempre em frente. Parar na certificação CCNA é comparável a completar apenas o segundo grau. Isso não irá lhe garantir um bom emprego e ascensão. Obtida a certificação CCNA, mantenha-se no caminho. Prossiga para o próximo nível - o nível superior - e obtenha as certificações CCNP ou CCDP (ou CCIP!). Caso deseje ainda mais, aposte num doutorado e prossiga para o último passo: o invejado e procurado CCIE. Nesse mercado, ser uma pessoa dinâmica e estar sempre atualizado é de extrema importância.

Em tempo, não se esqueça de investir em sua formação acadêmica! Pegando carona em uma analogia muito inteligente que li outro dia: "Imagine que seu CV é visto como uma refeição pelo RH das empresas: as certificações são o molho, a experiência profissional é a carne e o diploma universitário é o prato. Qualquer combinação que você tente fazer não será atrativa sem o prato, pois ninguém apreciará uma refeição servida diretamente em cima da mesa. Da mesma forma, um prato

servido apenas com o molho não será atrativo pois a experiência profissional não pode ser substituída por uma certificação."

9) O que recebo quando passo no exame? Por quanto tempo meu título é válido?

O candidato sabe, no momento em que finaliza a última questão, se foi aprovado ou não. Se na tela aparecer um *Congratulations*, você sabe que passou. Ao ser aprovado no exame, você automaticamente passa a desfrutar do título CCNA. Não é necessário aguardar o certificado oficial (este lhe será enviado pela Cisco posteriormente, e demora, em média, de dois a quatro meses para chegar). O protocolo que é impresso no próprio local do exame já é o suficiente para comprovar seu novo status, que pode também ser comprovado pelo site da própria Cisco. Portanto, sem neuras quanto a aguardar o certificado!

O CCNA é válido por três anos. Antes do fim deste período, ou você faz uma prova de nível superior (ex.: uma das quatro do CCNP) ou renova o próprio CCNA.

1.2.3 Sobre o Exame 640-802

As questões da Cisco para o exame CCNA caem em uma das quatro categorias:

1. Planejamento e Design;
2. Implementação e Operação;
3. Resolução de Problemas;
4. Tecnologias.

Portanto, não há razão para se intimidar apenas porque você não possui conhecimentos profundos e/ou experiência no sistema Cisco IOS. Uma vez que você domine as duas primeiras categorias de questões, questões específicas sobre Cisco IOS não serão um problema. Experiência prática ajuda muito, mas não é essencial para ser bem-sucedido na prova CCNA. O grau de conhecimento exigido pode ser alcançado por meio do uso de simuladores e de um PC comum.

1.2.4 Estatísticas Aproximadas sobre o Novo Exame

- O exame é composto de 50 a 60 questões, a maioria apresentada no formato de múltipla escolha (algumas questões podem ser do tipo Verdadeiro ou Falso). A nova versão segue adotando questões interativas nos formatos arraste e solte (relacional), preencha os espaços

(normalmente digitação de uma linha de comando IOS, bastante simples) e configuração de cenários, onde são apresentadas determinadas situações (bem simples, como "configure a interface Ethernet do roteador A com o endereço IP xxx.yyy.zzz.nnn") nas quais o examinado deve digitar linhas de comando como se estivesse configurando um router real para obter o resultado esperado (um simulador da interface do exame pode ser acessado no endereço <http://www.cisco.com/warp/public/10/wwtraining/certprog/testing/simulation/tutorial.html>);

- É necessário acertar cerca de 85% das questões para ser aprovado;
- Não havia versões do exame 640-802 em outros idiomas que não o inglês e o japonês até a data em que este livro foi desenvolvido, mas esse quadro pode mudar em breve;
- Deveriam ser disponibilizados 120 minutos (para a versão em inglês) para a execução do exame, porém já foram registrados casos em que apenas 90 minutos foram concedidos. Portanto, prepare-se para a pior hipótese. Para a versão em português, quando ela for disponibilizada, prepare-se para algo em torno de 74 minutos;
- A nova versão (802), assim como sua antecessora, valoriza muito as questões no formato estudo de caso;
- Prepare-se para ver muitas questões sobre *subnetting*. Entretanto, muitas delas não deverão ser apresentadas no formato direto, como no exame antigo (ex.: "Quantas sub-redes válidas a máscara NNN.XXX.YYY.ZZZ pode criar?"). Em seu lugar, um diagrama de rede é apresentado ilustrando uma série de dispositivos (routers, switches e PCs) e seus respectivos endereços IP. Uma máscara de rede também é dada (em formato decimal, ou apenas citando o número de "bits" que foram reservados de um determinado endereço IP) e as perguntas são do tipo "Este PC não consegue acessar a Internet. Por quê?" ou ainda "O usuário X não consegue acessar o servidor Y. Por quê?". Esteja muito bem preparado com relação ao tópico *subnetting*. Sem dúvida, esse é um tópico eliminatório (pratique, e muito!);
- Outra questão de estudo de caso muito comum: um diagrama de rede é apresentado, seguido da pergunta: "O que há de errado com a rede ilustrada?".

1.2.5 Questões Típicas

- Diferenças entre bridges, switches e hubs;
- Configuração de senhas (*enable, enable secret, console, Telnet, user* etc.);
- Configuração de roteamento EIGRP, OSPF, IGRP ou RIP em um router (dentro de uma topologia de três routers). Existem vários comandos habilitados no simulador de IOS que a prova utiliza. Para verificar quais estão disponíveis, digite "?" e observe: os comandos em cinza estão desabilitados e os comandos em preto estão habilitados para uso;
- Conversão de um número em binário para decimal e hexadecimal (essa questão pode cair em forma dissertativa ou de "arraste e solte"!);
- Cálculo de subnets, número de hosts possíveis, número de hosts válidos, número de redes possíveis etc. Normalmente o exame se concentra em redes de classe "C" para questões desse tipo;
- Questões envolvendo listas de acesso proliferaram no novo formato, esteja preparado;
- Saiba configurar NAT (pode cair um exercício de laboratório sobre esse assunto);
- Estude a fundo *Frame-Relay*. Essa é uma tecnologia muito popular e a Cisco segue cobrando esse tema. Saiba as definições de LMI, DLCI, PVC, SVC etc.;
- Saiba interpretar descrições de estado de interfaces (ex.:"O que significa *Interface serial 0 is administratively down, line protocol is down*?");
- Modos de comutação (*store-and-forward* e *fragment-free*, principalmente!);
- Eis uma pergunta interessante de que se deve saber a resposta: "Se a NVRAM, a RAM e a FLASH de um roteador estiverem limpas, por onde ele deverá iniciar?";
- Eis um exemplo interessante de uma questão atípica: "Suponha que você faça uma série de alterações nas configurações de seu router e, em seguida, faça o backup delas para a NVRAM. Momentos mais tarde, você reinicia o router e percebe que nenhuma das alterações feitas está ativa. Qual seria uma possível causa?" Uma das respostas,

por exemplo, pode ser que o registrador do router não estava configurado para iniciar pela NVRAM;

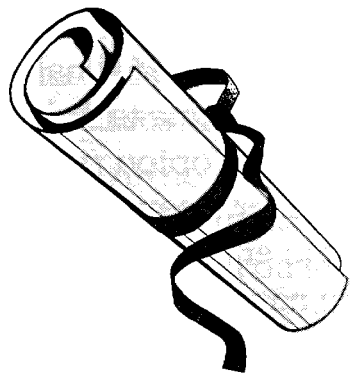
- OSPF é parte do escopo do exame, assim como EIGRP (esse último podendo aparecer com maior incidência). O mais importante sobre esses protocolos é conhecer suas métricas e características. Deve-se saber, por exemplo, que o protocolo OSPF utiliza algoritmos baseados no estado do link (*"link-state"*), assim como se deve saber que RIP e IGRP são exemplos de protocolos de roteamento que utilizam algoritmos baseados em *distance-vector*;
- Muitas das questões têm relação com o modelo OSI, portanto, estude-o muito bem;
- Deve-se conhecer o modelo de três camadas proposto pela Cisco;
- Saiba configurar VTP em um switch 2950, assim como endereço IP de gerenciamento e *default gateway*. É provável que uma das questões com simuladores seja baseada nisso;
- Atente para os novos tópicos cobrados (wireless, segurança e IPv6), especialmente os 2 primeiros.

1.2.6 Dicas Importantes

- Quando você se deparar com questões que envolvam comandos Cisco IOS, preste muita atenção no modo de configuração em que eles são executados. Ex.: USER ">", PRIVILEGED "#", GLOBAL CONFIG "(config)#", CONFIG-IF "(config-if)#" etc.;
- Quando você se deparar com questões que exijam a digitação de comandos, procure digitá-los por extenso, e não em sua forma abreviada (ex.: interface no lugar de int), e não se esqueça de salvar suas configurações no simulador;
- Espere deparar-se com informações sobre sub-redes no formato 192.252.144.0 /24 (24 bits utilizados para definição da porção de rede, ou 255.255.255.0);
- Grande parte das questões com mais de uma alternativa correta apresentarão o número de respostas desejado (ex.: "Qual das três opções abaixo..");
- Não é permitido marcar a questão ou retornar a uma questão já respondida (ao contrário de muitos programas

simuladores). Portanto, pense bastante e tenha muita calma antes de responder cada uma. Lembre que uma questão respondida afobadamente pode significar a diferença entre ser aprovado e fracassar;

- Não tente decorar todas as suas anotações na véspera do exame. Procure relaxar e estar descansado. Isso é muito importante para um exame exaustivo como é o CCNA;
- Procure chegar ao local do exame com antecedência de 20 a 30 minutos. Isso permite que você tenha algum tempo para relaxar, ou mesmo para lidar com algum contratempo;
- Não se esqueça de levar consigo toda a documentação exigida para apresentação ao encarregado pela aplicação do teste. Você pode ser impedido de realizar o exame caso falhe nesse quesito;
- Alguns centros que aplicam o teste não permitem ao candidato levar nenhum material para a sala de exame, incluindo lápis, caneta, borracha, papel (nem mesmo em branco - nesse caso, eles lhe fornecerão o material necessário), calculadoras, nem mesmo a carteira. Portanto, esteja preparado para lidar com esse tipo de situação;
- Finalmente, não se dê por vencido caso seja reprovado. Isso acontece com muitos candidatos que tentam o exame pela primeira vez. É um exame difícil, não é vergonha nenhuma ser reprovado na primeira tentativa. Lembre-se de que você pode refazer o teste quando se sentir mais preparado, podendo repeti-lo quantas vezes quiser (a não ser pelo seu custo, US$250!).



2 O Modelo OSI

2.1 Tópicos Abordados

- Benefícios Proporcionados pela Arquitetura em Camadas;
- Análise Individual das Camadas do Modelo ISO/OSI;
- A Interatividade entre as Camadas;
- A Camada de Transporte e o Mecanismo de Controle de Fluxo de Dados;
- A Camada de Rede e uma Visão Geral de Roteamento de Pacotes;
- Redes Ethernet;
- A Camada Física, Cabos e Conectores;
- O Processo de Encapsulamento de Dados;
- O Modelo de Três Camadas Proposto pela Cisco.

2.2 Histórico

Antes de iniciarmos, devemos entender os conceitos por trás de uma rede de dados: como os dados são formatados, organizados, transmitidos, recebidos, interpretados e, finalmente, como são utilizados. O objetivo deste capítulo é exatamente responder essas questões de forma clara e concisa.

Quando as primeiras redes de dados surgiram, computadores de um mesmo fabricante podiam tipicamente comunicar-se entre si. Por exemplo, empresas escolhiam ou uma solução IBM ou uma solução DEC[1] - nunca ambas, por uma questão de compatibilidade.

---

[1] *Digital Equipment Corp.* (hoje, a HP).

Obviamente, os usuários finais e mesmo os fabricantes de componentes não estavam muito à vontade com esse cenário por uma série de razões. Eis um exemplo clássico: vamos supor que uma grande multinacional XYZ, que adota a IBM como fornecedora exclusiva para seu parque tecnológico, adquirisse uma empresa regional B que, em sua história, optou pela DEC como fornecedor de tecnologia. Como fazer para integrar a parte adquirida à parte existente? Sem nenhum tipo de padronização entre os fabricantes, a integração era um verdadeiro pesadelo - quando não impossível. Casos como esse foram o suficiente para deixar muitos consumidores insatisfeitos a ponto de exigirem uma solução para esse impasse: que os fabricantes chegassem a um acordo, e que compatibilizassem de alguma forma suas tecnologias.

No início da década de 80, a ISO[2], juntamente com representantes dos diversos fabricantes existentes, criou um grupo de trabalho para resolver o problema. Algum tempo depois, em 1984, surgia o primeiro resultado desse esforço: o Modelo de Referência OSI[3]. O modelo OSI foi criado com o intuito de padronizar a comunicação de dados e de permitir a interoperabilidade - independentemente de marca (fabricante) ou sistema utilizado, ou seja, compatibilizar hardware[4] e software (protocolos) envolvidos, de alguma forma, com o transporte de dados. O modelo vinha exatamente como uma resposta às perguntas lançadas no início deste capítulo. Na verdade, ia mais longe, buscando a padronização da forma como os dados são formatados, organizados, transmitidos, recebidos, interpretados e (por que não?) utilizados. O modelo apresentava cada uma dessas fases através de "camadas", e em cada uma delas quais as regras (protocolos) a serem seguidas por todos os fabricantes - de software ou de hardware, de modo que o processo de comunicação de dados ocorresse de forma transparente.

O modelo OSI é um modelo de referência, ou seja, ele especifica todos os processos requeridos para que a comunicação de dados ocorra e divide esses processos em grupos lógicos, chamados *layers* (camadas). Sua adoção, contudo, não é obrigatória. Isso significa que um determinado fabricante tem a liberdade de desenvolver um protocolo que não se ajuste ao modelo, por exemplo. Esse protocolo é, então, chamado de "proprietário" e poderá ter problemas de compatibilidade com os demais existentes. Quando um sistema de comunicação de dados é baseado nesse tipo de modelo, sua estrutura é tida como uma "arquitetura em camadas".

---

[2] *International Organization for Standardization.*

[3] *Open Systems Interconnection* - Norma ISO 7498, publicada em 1984.

[4] A idéia inicial do projeto era padronizar apenas interfaces físicas.

O modelo OSI de fato resolvia grande parte dos problemas encontrados pela falta de padronização existente na época, porém, como tudo na vida, ele não era perfeito. O modelo OSI possui pontos fortes e pontos fracos, os quais serão apresentados mais adiante.

O governo americano, a princípio, tentou "forçar" a adoção do modelo homologado (OSI), através da imposição do GOSIP[5]. O governo brasileiro, através da lei de informática, não ficou atrás, e também tentou impor esse modelo. Todas as tentativas forçadas de imposição do modelo OSI fracassaram e, lentamente, este foi sendo preterido em prol de outros modelos, mais flexíveis e funcionais.

É interessante mencionar, no entanto, que o Modelo de Referência OSI não foi o primeiro independente de fabricantes em sua linha, apesar de ter sido o mais bem estruturado e aclamado de sua época. Um outro modelo já circulava havia algum tempo, porém, sem o endosso de um órgão forte e respeitado como a ISO. Era o modelo "informal" TCP/IP. Informal porque não era estruturado, como o OSI, nem possuía um órgão - como a ISO - controlando-o. O modelo TCP/IP era e ainda é muito mais flexível que o OSI, e também muito mais simples de ser implementado. O modelo foi idealizado e desenvolvido na Universidade da Stanford, na Califórnia, e testado com sucesso em 1974 pela dupla Bob Kahn e Vinton G. Cerf[6]. Na verdade, não era um "modelo" em seus primórdios, mas um conjunto de protocolos - cujo membro principal era o TCP[7].

A motivação para o desenvolvimento do modelo TCP/IP foi uma RFP[8] lançada pelo Departamento de Defesa Americano[9], que buscava um modo eficiente e confiável de mover dados, mesmo sob o advento de um holocausto nuclear. Muitas propostas foram apresentadas, porém apenas algumas se mostraram viáveis, sendo o TCP/IP uma delas. Por fim, em 1976, o Departamento de Defesa Americano acabou adotando o modelo TCP/IP como modelo de referência para a ARPANET[10]. É por esse motivo que alguns autores ainda se referem ao modelo TCP/IP por "modelo DoD". As figuras 2.1 e 2.2 ilustram bem o que o Departamento de Defesa Americano buscava, e como o problema foi solucionado.

---

[5] *Government OSI Profile*: definia o conjunto de protocolos a ser suportado pelos produtos adquiridos pelo governo americano.

[6] Os dois também foram oficialmente os primeiros a usar o termo "Internet", em seu documento sobre o protocolo TCP.

[7] *Transmission Control Protocol.*

[8] *Request For Proposal* (um pedido de proposta - equivalente a uma licitação).

[9] *DoD - Department of Defense.*

[10] *Advanced Research Projects Agency Network.*

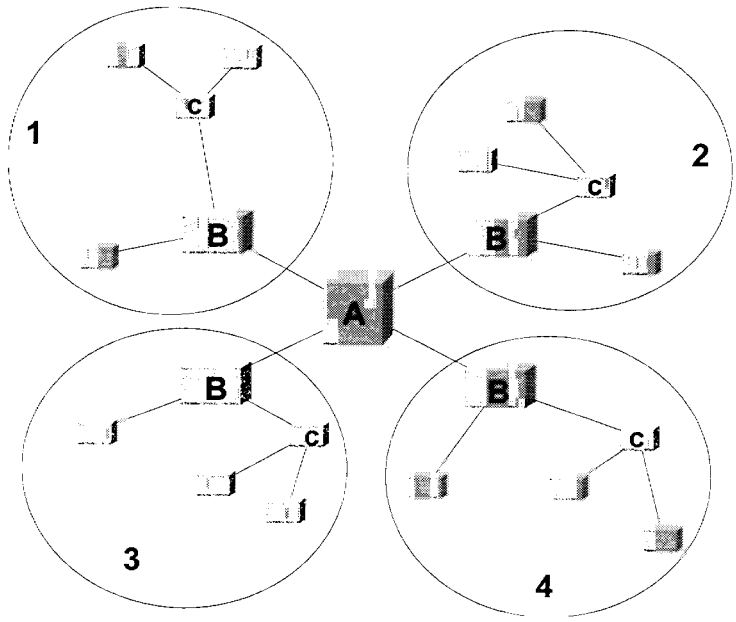


Figura 2.1: Modelo gráfico de uma Internetwork não redundante.

A figura 2.1 ilustra como era a estrutura da rede de dados existente na época anterior à encomenda de um modelo mais eficiente e redundante. Como se pode observar, essa rede era fortemente hierarquizada, e podemos notar seus "nós" de rede de nível 1 (representados pela letra "B") diretamente conectados ao ponto central (representado pela letra "A"), "nós" de nível 2 diretamente conectados aos de nível 1 e assim sucessivamente.

Essa era a estrutura original da Internet em seus primórdios, conhecida por DARPA Net[11]. Obviamente a DARPA Net não possuía muitas ramificações, e não era oferecida aos usuários comuns. Era basicamente uma rede militar de pesquisa, cuja infra-estrutura fora baseada no sistema telefônico existente. Portanto, a DARPA Net tinha sua operação baseada no chaveamento (comutação) de circuitos, tecnologia esta que, devido à sua natureza atípica, era extremamente ineficiente para a transmissão de dados.

Os problemas no desenho inicial da DARPA Net eram muitos, mas o principal era, sem dúvida, a total falta de inteligência da rede e redundância. Por exemplo, se o nó primário do backbone (representado pela letra "A" na figura 2.1) sofresse alguma "pane", a rede instantaneamente seria dividida em quatro sub-redes distintas e incomunicáveis (representadas na figura pelas áreas 1 a 4). Os militares não podiam aceitar essa vulnerabilidade, principalmente com a Guerra Fria e a constante ameaça de um holocausto nuclear (que graças aos céus, nunca veio). Além do problema apresentado, existiam outros,

[11] *U.S. Defense Advanced Research Projects Agency Network.*

como o constante risco de sobrecarga no nó principal, o que limitava enormemente a escalabilidade desse modelo.

Para resolver esse problema, o Departamento de Defesa Americano lançou um desafio aos grandes centros de pesquisa: desenvolver um modelo de rede que fosse redundante e, até certo ponto, independente. Ou seja, se houvesse uma guerra nuclear e alguns pontos dessa rede fossem colocados abaixo, essa rede deveria manter-se inteiramente operacional com os pontos restantes. Essa era a condição básica. Uma das propostas então apresentadas foi a ilustrada na figura 2.2.

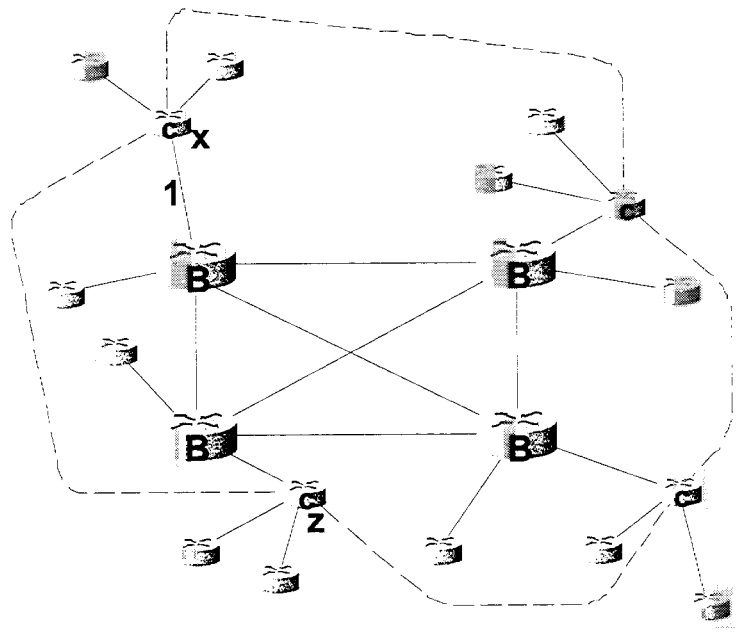


Figura 2.2: Modelo redundante de Internetwork - Internet atual.

No modelo proposto (figura 2.2), a função do nó central ("A" na figura 2.1) deixou de existir devido ao surgimento de relações de paridade entre os pontos de nível superior (roteadores de backbone, representados pela letra "B"). Observamos também que agora existem caminhos alternativos para ir de um quadrante a outro, através de conexões alternativas entre roteadores terciários ("C"). Para entender melhor o conceito, imagine que a conexão física localizada acima, à esquerda (identificada pelo número 1), fosse desfeita por algum motivo. Observe que os pontos imediatamente adjacentes ("C" e "B") continuam mantendo conectividade (entre si e com o restante da rede), uma vez que o ponto "x" (e seus dependentes imediatos) pode chegar até qualquer outro ponto da rede através de "z". Problema resolvido em parte. Com um cenário complexo como esse, era necessária a implementação de um conjunto de protocolos que fosse capaz de fazer essa rede funcionar. A proposta apresentada não

tratava meramente de uma mudança física na rede existente, mas de uma profunda mudança conceitual. Algo totalmente novo: a transição de uma rede baseada na comutação de circuitos (rede telefônica, para todos os efeitos) para uma baseada na comutação de pacotes de dados (datagramas). Assim, surge como resposta ao problema o conjunto de protocolos chamado TCP/IP[12].

A título de curiosidade, a figura 2.3 mostra como a rede de um provedor de acesso nível 1, nos EUA, encontra-se fisicamente estruturada - mostrando o que acabamos de ver na figura 2.2.

Figura 2.3: Estrutura atual de um provedor nível 1 (Tier 1).

Para o exame CCNA, é especialmente importante compreender os modelos OSI e TCP/IP do mesmo modo como a Cisco os enxerga. É com esse foco que analisaremos ambos neste livro.

Outro importante ponto que veremos neste capítulo é o modelo de três camadas proposto pela Cisco para auxiliar no desenho, implementação e gerenciamento de redes diversas. Entendendo esse modelo, você será capaz de eficientemente construir, manter e identificar problemas (*troubleshooting*) em redes com praticamente qualquer nível de complexidade ou porte.

Diferentes tipos de dispositivos e protocolos são definidos em cada uma das camadas do modelo OSI. É de extrema importância o entendimento dos diferentes tipos de cabos e conectores utilizados para interconectar esses equipamentos a uma rede. Neste capítulo, o cabeamento dos dispositivos de rede será discutido em conjunto com

[12] *Transmission Control Protocol/Internet Protocol.*

as tecnologias e protocolos de redes locais como o padrão Ethernet. Também lhes serão apresentados alguns exemplos de conectores WAN e conexões de routers e switches via emulação terminal (console). Veremos também como os dados são encapsulados à medida que descendem ou ascendem no modelo OSI.

2.3 O Modelo de Camadas OSI

Como já mencionado, quando as primeiras redes de dados surgiram, computadores de um mesmo fabricante podiam tipicamente comunicar-se entre si. Por exemplo, empresas empregavam ou uma solução IBM ou uma solução DEC (*Digital Equipment Corp.*, hoje HP), nunca ambas.

O modelo de camadas OSI foi criado com o intuito de se quebrar essa barreira na comunicação de dados e permitir a interoperabilidade, independentemente da marca (fabricante) ou sistema utilizado, ou seja, era uma tentativa de se estabelecer um padrão que fosse seguido pelos fabricantes de hardware e também pelos desenvolvedores de software.

O modelo OSI é um modelo de referência, ou seja, ele define de que forma dados gerados por uma aplicação em uma determinada máquina devem ser transmitidos através de um meio específico para uma aplicação em uma outra máquina. Trata-se de um modelo conceitual, estruturado em sete camadas, cada qual definindo processos e regras para a operação de uma rede de dados. O modelo foi especificado pela Organização Internacional para Padronização (ISO) em 1984 e, ainda hoje, é considerado o modelo arquitetural primário para redes de computadores.

O modelo OSI, basicamente, divide as tarefas inerentes à transmissão de informação entre máquinas em rede em sete grupos ou "camadas". A vantagem imediata dessa divisão é a geração de grupos menores e, portanto, mais facilmente gerenciáveis, em detrimento de apenas um pesado e complexo grupo. Uma vez definidas as sete camadas, tarefas (ou grupos de tarefas) são associadas a elas. Cada camada é razoavelmente independente das demais, permitindo, por exemplo, que tarefas associadas a uma camada possam ser implementadas ou modificadas sem que as demais tenham que sofrer qualquer tipo de alteração.

Basicamente, as sete camadas do modelo OSI podem ser subdivididas em duas categorias: superiores e inferiores (figura 2.4).

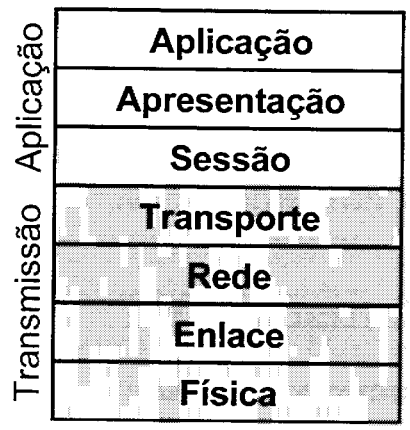


Figura 2.4: Subdivisão do Modelo OSI.

As camadas superiores do modelo OSI lidam com assuntos relacionados às aplicações e, geralmente, são apenas implementadas em software. A camada mais elevada, a chamada "Aplicação", é a mais próxima do usuário final. Tanto os usuários quanto os processos inerentes à camada de Aplicação interagem com softwares que possuem algum componente de comunicação.

É interessante ressaltar que o modelo OSI apenas fornece a arquitetura sugerida para a comunicação entre computadores. O modelo em si não é o que faz a comunicação ocorrer. O que a torna possível são os protocolos de comunicação. Esses protocolos implementam as funções definidas em uma ou mais camadas do modelo OSI.

Atualmente existe uma grande variedade de protocolos de comunicação, definidos nas mais diversas camadas do modelo OSI. Protocolos desenhados para gerenciar redes locais (LAN), por exemplo, atuam basicamente nas duas primeiras camadas do modelo (Enlace e Física), definindo como a comunicação de dados deve ocorrer nos diversos meios físicos possíveis.

Já os protocolos desenhados para atuar em redes geograficamente dispersas (WAN) são definidos nas últimas três camadas do modelo (Rede, Enlace e Física), e também são responsáveis por definir como a comunicação de dados deve ocorrer nos diversos meios físicos disponíveis para esse tipo de rede.

Existem ainda os protocolos de roteamento. Esses são protocolos definidos na camada 3 (Rede) e são responsáveis pelo gerenciamento da troca de informações entre os seus dispositivos (notadamente, roteadores), possibilitando a eles a seleção de uma rota apropriada para o tráfego de dados.

Finalmente, temos os protocolos de camada superior. Esses são os protocolos definidos nas quatro camadas superiores (Transporte, Sessão, Apresentação e Aplicação), e geralmente têm a função de

suportar os protocolos de camada inferior. Protocolos dependem de outros para realizar suas tarefas eficientemente. A maioria dos protocolos de roteamento, por exemplo, utiliza o suporte oferecido pelos protocolos de camada superior para gerenciar o modo como as informações são transportadas. Esse conceito de interdependência entre camadas é a base de tudo que o modelo OSI representa.

É interessante salientar que não há uma imposição, ou seja, fabricantes podem optar por não seguir o modelo à risca e, mesmo assim, conseguir alcançar uma interoperabilidade com outros fabricantes somente em determinadas camadas. A Cisco, por exemplo, desenvolveu protocolos de roteamento proprietários que coexistem em perfeita harmonia com protocolos padronizados pelo modelo em outras camadas (ex.: o protocolo IGRP da Cisco funciona sobre o protocolo IP). Esta é uma das grandes vantagens do modelo: flexibilidade.

Em suma, as principais vantagens em se adotar um modelo de referência em camadas seriam:

- Divisão de complexas operações de rede em camadas individualmente gerenciáveis (é mais fácil focar numa parte que no todo);
- Possibilidade de se alterar elementos de uma camada sem ter de alterar elementos de outras;
- Definição de um padrão, possibilitando a interoperabilidade entre os diversos fabricantes.

Camada	Descrição	Nome da PDU
Aplicação	**Application Layer** - Provê a interface com o usuário	
Apresentação	**Presentation Layer** - Trata da semântica, compressão / descompressão, criptografia e tradução dos dados	
Sessão	**Session Layer** - Gerencia o "diálogo" entre as portas lógicas e mantém a separação dos dados de diferentes aplicações	
Transporte	**Transport Layer** - Provê a comunicação confiável (ou não) e executa checagem de erros antes da retransmissão dos segmentos.	Segmento / Segment
Rede	**Network Layer** - Define e gerencia o endereçamento lógico da rede (ex. IP)	Pacote / Packet / Datagram
Enlace	**Data-link Layer** - Acomoda os pacotes em "quadros" através do processo de encapsulamento. Detecta erros, porém, não os corrige.	Quadro / Frame
Física	**Physical Layer** - Responsável pela movimentação dos bits entre as pontas e pela definição das interfaces, especificações elétricas e de pinagem dos cabos.	"bits"

Figura 2.5: O Modelo de Camadas OSI e as respectivas PDUs.

Para o exame CCNA, e para qualquer aspirante a um cargo relacionado a redes de dados, este talvez seja um dos capítulos mais importantes (nunca é demais chamar a atenção para esse ponto). A figura 2.5 ilustra o modelo de referência OSI, um resumo das funções de cada camada e as PDUs (*Protocol Data Units)* das quatro camadas inferiores (as mais importantes para nossos objetivos). É vital que você memorize cada uma dessas camadas e um resumo de suas funções, exatamente como na figura 2.5.

No exame não faltarão questões do tipo: "Qual o nome dado à PDU na camada de rede?" Resposta: Pacote ou Datagrama. Se você pretende fazer o exame em inglês, é aconselhável que você se acostume aos termos utilizados nessa língua. Por exemplo, o termo para camada de rede, em inglês, é *Network Layer*, e assim por diante. Neste livro, a grande maioria dos termos traduzidos para o português apresentam a notação original (em inglês) ao lado.

Para facilitar o processo de memorização das camadas que compõem o modelo OSI, criei duas frases: uma para os nomes das camadas em português e outra para os nomes em inglês. Sinta-se à vontade para criar sua própria frase, caso julgue necessário. Lembre-se: as frases a seguir ilustram a inicial de cada camada, partindo da mais alta (Aplicação/*Application*) e indo para a mais baixa (Física/*Physical*). Ei-las:

"**A**manhã **A**o **S**air do **T**rabalho **R**esolverei **E**ntrar na **F**aculdade (*port.*)"
(***A**plicação* | ***A**presentação* | ***S**essão* | ***T**ransporte* | ***R**ede* | ***E**nlace de Dados* | ***F**ísica*)

"**A**manhã **P**rovavelmente **S**erei **T**ransportado **N**uma **D**eterminada **P**erua (*ing.*)"
(***A**pplication* | ***P**resentation* | ***S**ession* | ***T**ransport* | ***N**etwork* | ***D**ata-Link* | ***P**hysical*)

Vamos agora verificar cada uma das camadas detalhadamente, focando no que o exame CCNA poderá cobrar do candidato.

2.3.1 A Camada de Aplicação

É nessa camada que ocorre a interação micro-usuário. A camada de aplicação é responsável por identificar e estabelecer a disponibilidade da aplicação na máquina destinatária e disponibilizar os recursos para que tal comunicação aconteça. Exemplos de aplicações e serviços existentes nessa camada são: navegadores e servidores Web (*Netscape, Apache, MS Explorer), e-mails gateways, Sistemas Electronic Data Interchange (EDI), Bulletin Board Systems* (BBS), servidores de banco de dados (MS-SQL, MySQL, Oracle), servidores X-window, entre muitos outros.

É interessante perceber que, em uma rede moderna, a relação cliente-servidor está quase sempre presente - sim, mesmo nas modernas redes *peer-to-peer* (P2P). Quando você está usando um *web-browser* - como o Internet Explorer, por exemplo - você está usando uma aplicação cliente. A aplicação servidora seria o programa *web-server* - como o Apache - que está rodando na máquina destino. Portanto, quando digita um endereço WWW em seu browser, você está basicamente solicitando, através de uma aplicação cliente - seu browser -, dados armazenados em uma máquina remota que está rodando uma aplicação servidora - o Apache, no caso.

Mas como fica essa relação no caso de redes P2P? Nada muda. Peguemos como exemplo o conhecido *Napster*. O software funciona simultaneamente como cliente e servidor. Ele atua como cliente quando você está fazendo uma solicitação à outra máquina (download), mas também age como servidor quando sua máquina está respondendo a uma solicitação de uma máquina remota (upload). Portanto, a relação cliente-servidor é mantida. Veremos melhor como isso funciona mais adiante.

2.3.2 A Camada de Apresentação

A camada de apresentação responde às solicitações de serviço da camada de aplicação e envia solicitações de serviço para a camada imediatamente inferior (sessão). Diferentemente das camadas inferiores, preocupadas em mover os bits de forma confiável de um ponto a outro, essa camada preocupa-se com a sintaxe e a semântica dos dados transmitidos. Por exemplo, após receber dados da camada de aplicação, pode ser necessário converter esses dados de seu formato original para um formato compreendido e aceitável por outras camadas do modelo, garantindo assim uma transmissão mais eficiente. Exemplos de formatações incluem PostScript, ASCII, EBCDIC, ASN.1, entre outras.

A camada de apresentação possui outras funções além de formatar e interpretar dados. Estas incluem compressão de dados e segurança da informação transmitida. Tarefas como compressão, descompressão, encriptação e decriptação, portanto, também encontram-se associadas a ela. Alguns padrões definidos nessa camada que estão relacionados a processos de compressão são TIFF, PICT, GIF, QuickTime, MPEG, JPEG, entre outros.

As funções de compressão e segurança, entretanto, não são exclusivas à camada de apresentação.

2.3.3 A Camada de Sessão

A camada de sessão é responsável pelo estabelecimento, gerenciamento e finalização de sessões entre a entidade transmissora e a entidade receptora. Ela basicamente mantém os dados de diferentes aplicações separados uns dos outros. Alguns exemplos de protocolos dessa camada são: *Network File System* (NFS), *Structured Query Language* (SQL), *Remote Procedure Call* (RPC), *AppleTalk Session Protocol* (ASP), entre outros.

2.3.4 A Camada de Transporte

Os serviços definidos na camada de transporte são responsáveis pela segmentação e reconstrução de fluxos de dados provenientes de camadas superiores. Eles provêm comunicação ponto a ponto e podem estabelecer uma conexão lógica entre a aplicação origem e a aplicação destino em uma rede.

A camada de transporte também é responsável pela disponibilização de mecanismos para multiplexar[13] fluxos de dados de camadas superiores e pelo estabelecimento e finalização (quebra) dos circuitos virtuais (lógicos). Essa camada mascara os detalhes de qualquer informação relacionada à rede das camadas superiores, promovendo uma transmissão de dados de modo bastante transparente.

2.3.4.1 Controle de Fluxo

A integridade dos dados é assegurada pela camada de transporte mantendo-se o controle do fluxo de dados e permitindo aos usuários a requisição de um transporte de dados confiável entre as pontas. Os mecanismos de controle de fluxo previnem que o computador origem "inunde" os buffers[14] do computador destino, o que resultaria em perda de dados. Para que essa comunicação seja confiável, é preciso que uma comunicação orientada à conexão seja estabelecida, e que os protocolos envolvidos assegurem-se do seguinte:

- Os segmentos transmitidos são confirmados (*acknowledged*) ao serem recebidos;
- Qualquer segmento não confirmado é retransmitido;

---

[13] O termo "multiplexar" vem do inglês *multiplexing*, e significa transmitir diversas informações simultaneamente usando-se o mesmo meio ou canal. O processo implica que as informações multiplexadas podem ser, posteriormente, extraídas em um meio ou canal particular.

[14] Buffer: Memória de acesso rápido destinada ao armazenamento temporário de pequenas quantidades de dados.

- Os segmentos são reconstituídos em sua seqüência original, uma vez recebidos pelo computador destinatário;
- Uma gerência do fluxo de dados é mantida a fim de evitar congestionamento, sobrecarga e perda de dados.

A figura 2.6 ilustra o funcionamento desse mecanismo.

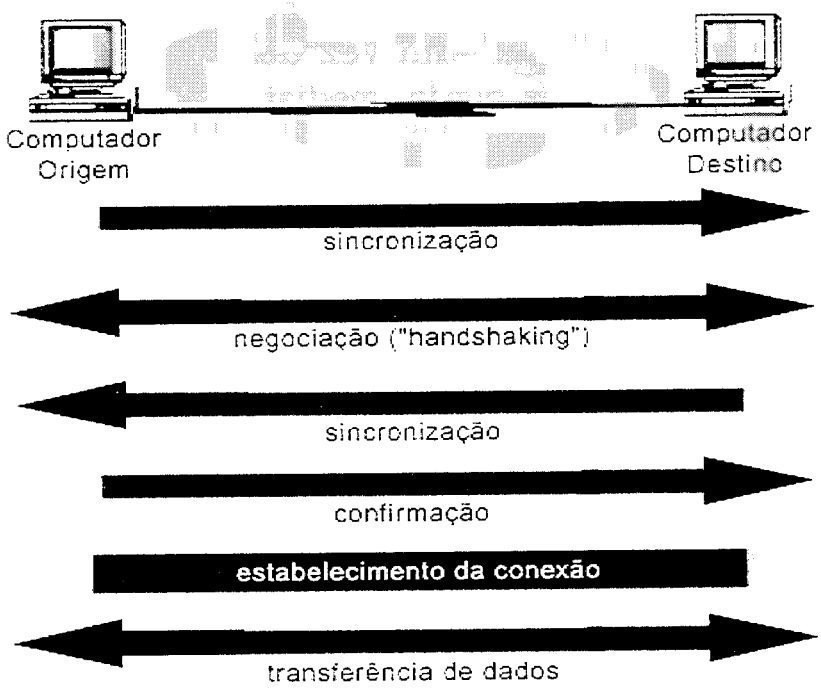


Figura 2.6: Operação do Controle de Fluxo.

Enquanto dados estão sendo transmitidos entre dois dispositivos, ambos verificam periodicamente a conexão estabelecida para assegurar-se de que os dados estão sendo enviados e recebidos apropriadamente.

Durante uma transmissão, congestionamentos de dados podem ocorrer devido à heterogeneidade das máquinas presentes em uma rede (ex.: computadores de alta velocidade geram dados mais rapidamente do que a infra-estrutura de rede pode transmiti-los ou máquinas mais lentas, processá-los) ou porque muitos computadores passam a transmitir simultaneamente datagramas para um mesmo gateway ou destino. No último caso, o gateway ou destino pode vir a ficar congestionado, mesmo que nenhuma das fontes, por si só, seja a causadora do problema. Podemos fazer uma analogia com um estreitamento em uma estrada. Normalmente, o problema não é apenas um carro, mas a quantidade de carros naquela estrada.

Quando uma máquina recebe um fluxo de datagramas maior do que pode processar, ela direciona o excedente para uma memória chamada buffer. Esse processo, conhecido como "bufferização", resolve

o problema apenas se o fluxo de dados possuir uma característica não-contínua, uma transmissão em "rajada". Entretanto, se o fluxo for ininterrupto, a memória buffer eventualmente se esgotará, a capacidade de recebimento da máquina será excedida e, como conseqüência, qualquer datagrama adicional será descartado.

Graças às funções desempenhadas pela camada de transporte, congestionamentos de rede originados por uma "inundação" de dados podem ser bem gerenciados. Em vez de simplesmente descartar datagramas - ocasionando a perda imediata de dados - a camada de transporte pode enviar ao transmissor um sinal de que não está pronto (*not ready*), fazendo com que ele aguarde antes de enviar mais dados. Após o receptor ter processado os datagramas armazenados em sua memória buffer, ele envia um sinal de transporte (*ready*), indicando que está pronto para receber e processar mais dados. A máquina transmissora, ao receber esse sinal, retoma a transmissão de onde havia parado.

Em uma comunicação confiável, orientada à conexão, datagramas devem ser entregues ao seu destino na exata ordem em que são transmitidos; do contrário, um erro de comunicação ocorre. Se qualquer segmento for perdido, duplicado ou corrompido durante o processo, um erro de comunicação também ocorrerá.

A resposta a esse problema seria a confirmação, pela máquina receptora, do recebimento de cada datagrama. Entretanto, a taxa de transmissão de dados seria extremamente baixa se a máquina transmissora tivesse de esperar por uma confirmação antes de enviar cada segmento. Portanto, uma vez que exista tempo, o transmissor envia segmentos antes de finalizar o processamento de cada confirmação.

A quantidade de dados que a máquina transmissora é capaz de enviar antes de receber a confirmação do(s) segmento(s) anteriormente enviado(s) é chamada de janela (*window*).

O processo chamado *windowing* controla a quantidade de informação transferida entre as máquinas participantes. Enquanto alguns protocolos quantificam a informação observando o número de pacotes, o TCP realiza essa quantificação contando o número de bytes. A figura 2.7 ilustra o comportamento de duas janelas: uma de tamanho 1 e outra de tamanho 2. Quando uma janela de tamanho 1 é configurada, a máquina transmissora aguarda a confirmação de cada segmento enviado antes de transmitir o próximo. Já em uma janela configurada com tamanho 2, a máquina transmissora pode enviar até 2 segmentos antes de receber uma confirmação.

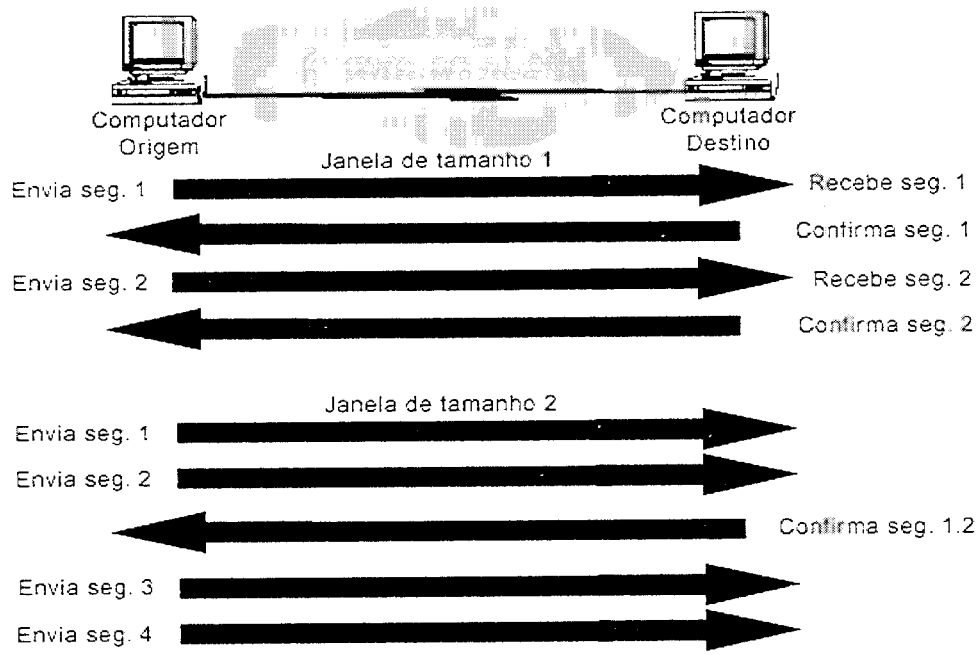


Figura 2.7: O processo de windowing.

2.3.4.2 Confirmação (*Acknowledgement*)

Uma conexão confiável garante a total integridade dos dados transmitidos entre dois pontos. Existe a garantia de que esses dados não serão duplicados ou perdidos. O método que torna isso possível é conhecido como "confirmação positiva com retransmissão" ou, em inglês, *positive acknowledgement with retransmition*. Essa técnica implica no envio de uma mensagem de confirmação pela máquina destino de volta para a máquina origem quando o recebimento dos dados for realizado com sucesso. Podemos fazer uma analogia ao serviço de correio registrado: assim que o destinatário recebe uma carta registrada, ele assina um protocolo que é enviado de volta ao remetente, garantindo a ele que a correspondência enviada chegou ao seu destino.

2.3.5 A Camada de Rede

A camada de rede é responsável pelo roteamento dos dados através da *internetwork* e pelo endereçamento lógico dos pacotes de dados, ou seja, pelo transporte de tráfego entre máquinas que não se encontram diretamente conectadas. Roteadores ou "routers" - também chamados de dispositivos de camada 3 (*layer 3 devices*) - são definidos nessa camada e provêm todos os serviços relacionados ao processo de roteamento.

Quando um pacote é recebido em uma determinada interface de um router, o endereço IP de destino é checado. Se o pacote não for destinado ao router em questão, este irá verificar se o endereço de

destino se encontra em sua tabela de roteamento (*routing table*), uma base de dados que fica armazenada na memória RAM do router e que pode ser estática ou dinamicamente formada.

Existem basicamente dois tipos de pacotes definidos na camada de rede: pacotes de dados (*data packets*) e pacotes de atualização (*router update packets*). No primeiro tipo, os pacotes são usados para transporte de dados pela *internetwork*, e os protocolos usados para suportar tal tráfego são conhecidos como protocolos roteados (*routed protocols*). Exemplos de protocolos roteados são o IP e o IPX.

O segundo tipo de pacote é utilizado para o transporte de atualizações sobre routers vizinhos e sobre os caminhos (*paths*) disponíveis para alcançá-los. Protocolos usados para gerenciar essa tarefa são chamados de protocolos de roteamento (*routing protocols*). Exemplos de protocolos de roteamento são RIP, EIGRP, OSPF, BGP, entre outros. Os pacotes de atualização são utilizados na formação e manutenção das tabelas de roteamento de cada router. As tabelas de roteamento formadas, armazenadas e utilizadas pelos routers incluem informações como endereços lógicos (*network addresses*), interface de saída (*exit interface*) e métrica (*metric*), que é a distância ou custo relativo até uma determinada rede remota.

Uma das mais importantes características dos routers é que eles segregam (quebram) os chamados "domínios de broadcast" (*broadcast domains*), ou seja, mensagens de broadcast não atravessam um router, o que já não ocorre com switches e hubs, que simplesmente as propagam (veremos mais adiante o porquê). Routers também quebram os chamados "domínios de colisão" (*collision domains*), o que switches também fazem (mas não hubs!). Dizer que routers quebram domínios de colisão significa dizer que cada interface de um router é considerada uma rede isolada e, como tal, necessita de um número de identificação (endereçamento) exclusivo. Cada dispositivo deverá utilizar o mesmo endereço de rede designado à interface a que se encontra conectado.

Considerando-se o exame CCNA, os pontos mais relevantes sobre routers são que eles:

- Não propagam mensagens de *broadcast* ou de *multicast*;
- Utilizam o endereço lógico no cabeçalho de camada de rede para determinar o router vizinho para qual o pacote deve ser enviado;
- Podem utilizar listas de acesso, criadas por um administrador, para gerenciar a segurança dos pacotes entrantes ou saintes;

- Podem prover funções de camada de Enlace (*bridging*) se necessário e, simultaneamente, efetuar roteamento de pacotes na mesma interface;
- Possibilitam a comunicação entre Virtual LANs (VLANs);
- Podem prover Qualidade de Serviço (*Quality of Service - QoS*) para tipos específicos de tráfego de dados.

2.3.6 A Camada de Enlace de Dados

A camada de Enlace assegura que os dados sejam transmitidos ao equipamento apropriado e converte os dados vindos da camada superior (Rede) em bits, tornando possível a transmissão através de meios físicos, como cabos, definidos na camada física. A camada de Enlace formata a mensagem em frames e adiciona um cabeçalho customizado contendo o endereço de hardware (MAC address) das máquinas transmissora e destinatária. Essa informação adicionada forma uma espécie de cápsula envolvendo a mensagem original, de modo análogo aos módulos lunares do projeto Apollo, no qual módulos úteis apenas a alguns estágios da viagem são descartados à medida que esses estágios são completados.

O padrão 802.2 (*Logical Link Control - LLC*) é utilizado em conjunto com outros padrões IEEE, adicionando funcionalidade ao padrão existente.

É importante entender que à camada de Rede (onde os routers são definidos) não importa a localização física das máquinas, mas a localização lógica das redes. A camada de Enlace de Dados (onde switches e bridges são definidos), sim, é responsável pela identificação de cada máquina (endereçamento físico) em uma rede local.

Para um host enviar dados a outro através de um router, a camada de Enlace se utiliza do endereço de hardware ou MAC address.

A camada de Enlace IEEE Ethernet possui duas subcamadas:

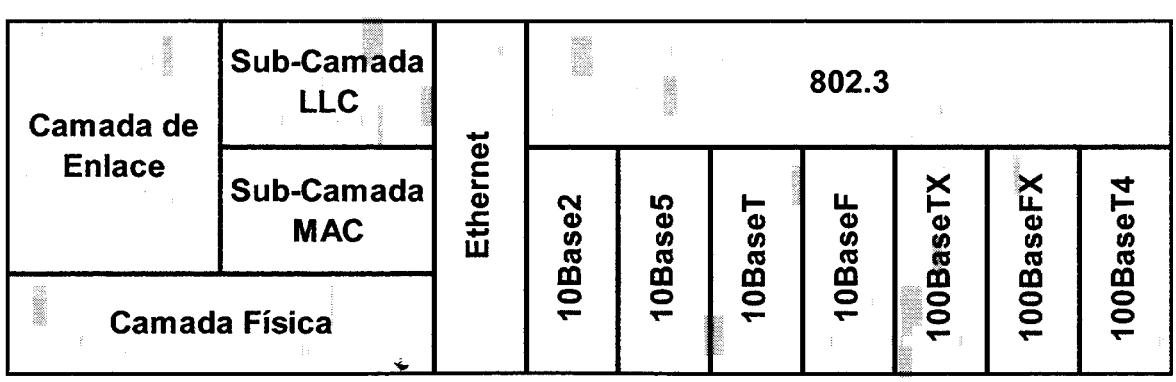


Figura 2.8: Subdivisão da camada de Enlace e especificações LAN (Ethernet).

- **Logical Link Control (subcamada LLC) 802.2**: Responsável pela identificação de protocolos da camada de Rede e seu encapsulamento. Um cabeçalho LLC diz à camada de Enlace o que fazer com um pacote uma vez que o frame é recebido. Por exemplo, assim que um host recebe um frame, ele analisa o cabeçalho LLC para entender para qual protocolo da camada de Rede (IP, IPX etc.) ele é destinado. A subcamada LLC também pode ajudar no controle de fluxo e seqüenciamento de bits;
- **Media Access Control (subcamada MAC)**: Define como os pacotes são alocados e transmitidos no meio físico. O endereçamento físico é definido nessa subcamada, assim como a topologia lógica. Disciplina da linha, notificação de erros (não a correção), entrega ordenada de frames, e controle de fluxo opcional também podem ser utilizados nessa subcamada.

2.3.6.1 Switches e Bridges na Camada de Enlace

Switches e bridges são dispositivos definidos na Camada de Enlace de Dados, que operam analisando os frames que cruzam a rede. O dispositivo de Camada 2 (seja ele um switch ou uma bridge) adiciona o endereço do hardware transmissor (endereço MAC) a uma tabela-filtro, formando uma base de dados que mapeia a porta que recebeu o frame para o endereço de hardware (MAC address) gravado na interface do dispositivo que o transmitiu.

Depois da formação da tabela-filtro, o dispositivo de camada 2 apenas enviará frames para o segmento onde o endereço de hardware destino está localizado. Isso é chamado de *transparent bridging*. Quando a interface de um switch recebe um frame e o endereço do hardware (MAC address) de destino é desconhecido, o switch propaga esse frame para todos os dispositivos conectados a cada uma de suas portas (esse processo é conhecido como *broadcast*). Se o dispositivo desconhecido responder a essa transmissão, o switch atualiza sua tabela mapeando a respectiva porta ao endereço de hardware daquele dispositivo.

Todos os dispositivos que recebem essa transmissão (*broadcast*) são considerados em um mesmo *domínio de broadcast*. Dispositivos de camada de Enlace propagam mensagens do tipo *broadcast*, ou seja, não há uma "quebra" desses domínios. Apenas dispositivos de camada 3 (Rede), como routers, são capazes de realizar essa segmentação. Essa é uma importante diferença entre dispositivos de camada 2 e camada 3 e, como tal, deve ser lembrada.

Os pontos mais importantes a saber sobre switches e bridges são:

- Filtram a rede utilizando endereços de hardware (MAC addresses);
- Switches são considerados *hardware-based bridges*, uma vez que utilizam um hardware especial (ASICs - *Application Specific Integrated Circuits*) dedicado ao processamento de frames, ou seja, o processamento dos switches é realizado diretamente no hardware, enquanto que nas bridges o processamento é realizado via software. Por esse motivo, switches são mais eficientes e possuem uma maior densidade de portas do que bridges;
- O maior benefício de se utilizar switches em lugar de hubs é que cada porta do switch é um domínio de colisão próprio, enquanto o hub cria um grande domínio de colisão, sem segmentação;
- Outro grande benefício é que os dispositivos conectados a um switch podem transmitir simultaneamente, uma vez que cada segmento possui seu próprio domínio de colisão.

2.3.7 A Camada Física

Na camada Física, a interface entre *Data Terminal Equipment* (DTE) e *Data Circuit-Terminating Equipment* (DCE) é identificada. Os DCEs são, normalmente, localizados nos provedores de serviço, enquanto os DTEs costumam ser dispositivos que se conectam aos DCEs, normalmente sendo encontrados nas instalações físicas do cliente. Routers podem ser tanto DCEs quanto DTEs, dependendo do contexto. Os serviços disponíveis para um DTE são geralmente acessados via modem ou via CSU/DSU (*Channel Service Unit /Data Service Unit*).

Os hubs (ou repetidores) são definidos nessa camada. Hubs são, na verdade, repetidores com múltiplas portas. Sua função se resume a receber um sinal, amplificá-lo e repassá-lo para todas as suas portas ativas, sem qualquer exame dos dados no processo. Isso significa que todos os dispositivos conectados ao hub estão dentro de um mesmo domínio de colisão e de *broadcast*.

Hubs criam uma topologia física em forma estrela em que ele é o dispositivo central. Todos os dispositivos são bombardeados com dados toda vez que algum dispositivo conectado a ele realize uma transmissão.

2.3.7.1 Redes Ethernet

Ethernet é um método de acesso ao meio por contenção (*contention media access method*) que permite que todos os dispositivos (hosts) em uma rede Ethernet compartilhem a mesma largura de banda de um link. Ethernet é muito popular devido à sua descomplicada implementação, consolidação no mercado, escalabilidade, baixo custo e facilidade de atualização para novas tecnologias (como Gigabit e 10 Gigabit Ethernet). O padrão Ethernet utiliza especificações das camadas de Enlace e Física.

Redes Ethernet utilizam uma técnica de acesso chamada de *Carrier Sense Multiple Access with Collision Detect* (CSMA/CD), o que permite aos dispositivos o compartilhamento homogêneo da largura de banda, evitando que dois dispositivos transmitam simultaneamente em um mesmo meio (figura 2.9). A técnica CSMA/CD foi a solução encontrada para o problema de colisões que ocorriam quando pacotes eram simultaneamente transmitidos de diferentes dispositivos em um mesmo meio.

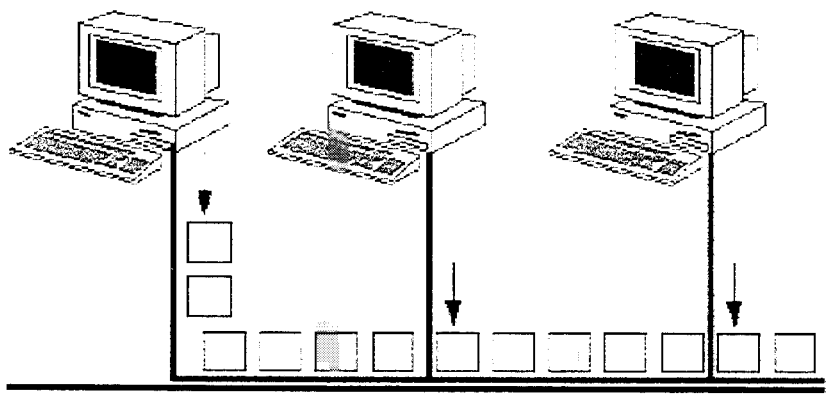


Figura 2.9: Funcionamento do mecanismo Carrier Sense Multiple Access with Collision Detect.

O funcionamento do mecanismo CSMA/CD é relativamente simples. Observe a figura 2.9 no intervalo de tempo entre o término da transmissão de um pacote e a geração de novos, outros hosts podem utilizar o meio de comunicação para enviar seus próprios pacotes. Quando um host deseja transmitir através da rede, ele primeiramente verifica se há presença de sinal no meio (cabo). Caso não seja constatada a presença de sinal (nenhum outro host transmitindo), o host inicia, então, sua transmissão. O host constantemente monitora o meio e, caso seja detectado outro sinal dele, um sinal de congestionamento é enviado, ocasionando uma pausa na transmissão de dados pelos outros hosts. Os hosts respondem ao sinal de congestionamento esperando um determinado intervalo de tempo antes de tentarem novamente o envio de dados. Após 15 tentativas sem sucesso (15 colisões), um *time-out* ocorrerá.

2.3.7.2 Os Conceitos "Half-duplex" e "Full-duplex" Ethernet

Half-duplex Ethernet é definido no padrão original Ethernet (IEEE 802.3) e utiliza apenas um par de cabos com sinal fluindo em ambas as suas direções, o que significa que colisões podem ocorrer (e normalmente ocorrem). *Half-duplex Ethernet* - tipicamente 10Base-T - atinge um pico de 60% de eficiência. Entretanto, em uma grande rede Ethernet 10Base-T será obtido, no máximo, de 3 a 4Mbps. Não é possível a rede *Half-duplex Ethernet* transmitir a taxas superiores a 10Mbps.

Full-duplex Ethernet utiliza dois pares de cabos. Não há colisões, uma vez que ela disponibiliza um par para a transmissão e outro, independente, para a recepção de dados. Teoricamente, é possível obter uma taxa de transferência da ordem de 100Mbps em ambas as direções, o que resulta em uma taxa agregada de 200Mbps - supondo-se 100% de eficiência.

O padrão Ethernet na camada de Enlace é responsável pelo endereçamento Ethernet, tipicamente chamado de endereço de hardware ou *MAC address*. É também responsável pelo encapsulamento dos pacotes recebidos da camada de Rede e pela preparação deles para transmissão pela rede local, através do método do acesso ao meio por contenção.

2.3.7.3 Endereçamento Ethernet

O esquema de endereçamento Ethernet utiliza o chamado endereço MAC (*Media Access Control*), que se encontra gravado no hardware de cada dispositivo de rede (como as placas de rede ["*NICs*"], por exemplo). O endereço MAC é uma seqüência de 48 bits (6 bytes [1 byte = 8 bits]) escrita em formato canônico, o que garante que todos os endereços MAC sejam gravados no mesmo formato, ainda que se tratando de dispositivos de diferentes fabricantes ou plataformas. A figura 2.10 ilustra como é feita a divisão dos 48 bits para endereçamento. É importante salientar que dois endereços MAC nunca deverão ser iguais.

A porção do Identificador Organizacional Único (*Organizationally Unique Identifier* - OUI) é definida pelo IEEE (Instituto de Engenheiros Elétricos e Eletrônicos), que o indica a uma determinada organização ou fabricante. O fabricante, por sua vez, designa um endereço administrativo global de 24 bits (porção *Vendor Assigned*), que é uma seqüência numérica exclusiva aos produtos daquele fabricante. O bit 46 será 0 no caso de ser um bit globalmente designado pelo fabricante, ou 1, no caso de ser um bit localmente gerido pelo administrador de rede.

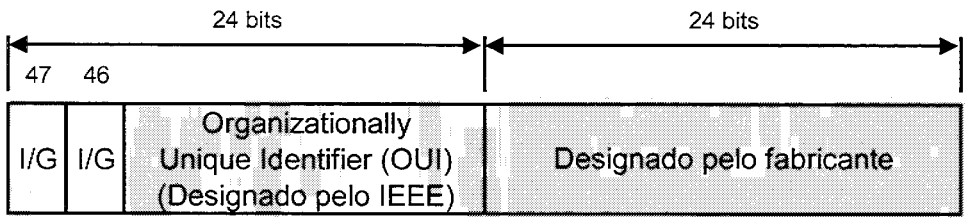


Figura 2.10: Esquema de endereçamento Ethernet.

A camada de Enlace de Dados é responsável pelo encapsulamento dos dados em "quadros" (frames). Frames são necessários para transmitir os dados passados pela camada de Rede (pacotes) através de um tipo de acesso ao meio. Existem três tipos de acesso: por contenção (Ethernet), passagem de *token* (*Token Ring* e FDDI) e *pooling* (*Mainframes* IBM e 100VGAnyLAN). Para efeitos do exame CCNA, apenas Ethernet será estudado mais detalhadamente. A figura 2.11 ilustra o formato dos dois tipos de frame Ethernet existentes na subcamada MAC.

Nota: *Não entraremos em muitos detalhes sobre os dois tipos de frames (SAP e SNAP), encontrados na subcamada LLC.*

Frame Ethernet

Preamble	Endereço Destino	Endereço Origem	Type	Dados	CRC
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 - 1474 bytes	4 Bytes

Frame IEEE 802.3

Preamble	SFD	Endereço Destino	Endereço Origem	Length	Cabeçalho 802.2 + Dados	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1474 bytes	4 Bytes

Figura 2.11: Tipos de frame Ethernet definidos na subcamada MAC.

- **Preâmbulo (*Preamble*)**: Seqüência alternada de 1 e 0 que provê um clocking de 5MHz no início de cada pacote, permitindo ao recipiente "travar" a cadeia de bits sendo recebida. O preamble usa um campo de sincronização (SFD) para indicar à estação receptora que a porção contendo dados da mensagem irá na seqüência;
- **Start Frame Delimiter (SFD)**: Seqüência alternada de 0 e 1, enquanto que o campo de sincronização é uma seqüência de 1s. O preamble e o campo SFD possuem, juntos, 64 bits (8 bytes) de extensão;
- **Endereço Destino (*Destination Address*)**: Transmite um campo de 48 bits utilizando o último bit significante (*Last Significant Bit* – LSB) primeiro. O campo DA é utilizado pelas

estações receptoras para determinar se o pacote a caminho é destinado àquela estação. O endereço de destino (DA) pode ser um endereço específico, um endereço broadcast ou um endereço multicast;

- **Endereço Origem (*Source Address*)**: Endereço de 48 bits fornecido pelo NIC da estação transmissora. Também utiliza o último bit significante primeiro. Endereços *broadcast* ou multicast são ilegais nesse campo;
- **Lenght** ou **Type**: Eis uma diferença entre os dois tipos de frame: o frame Ethernet utiliza o campo *Lenght* para registro do tamanho do campo de dados, enquanto o frame Ethernet_II (802.3) utiliza o campo *Type* para identificação do conteúdo do campo de dados;
- **Dados (Data)**: O campo *Data* contém os dados transmitidos à camada de Enlace pela camada de Rede, ou seja, trata-se do pacote de dados. O tamanho pode variar de 46 a 1474 bytes. Note que, no caso do frame IEEE 802.3, o campo *Data* encapsula o frame 802.2 (LLC), visando a identificação do protocolo de camada de Rede;
- **Frame Check Sequence (FCS)**: Campo no final do frame, utilizado para o armazenamento do *Cyclic Redundant Check* (CRC) - checagem baseada em algoritmos matemáticos para verificação da integridade dos frames transmitidos. Identifica frames corrompidos, porém não os corrige.

É importante notar que o frame IEEE 802.3, por si só, não seria capaz de identificar o protocolo de camada superior (Rede). O IEEE definiu a especificação 802.2 LLC (*Logical Link Control*) que incorpora essa e outras funções. Por esse motivo, o frame IEEE 802.3 encapsula um frame 802.2 LLC em seu campo de dados (vide figura 2.11).

2.3.7.4 O Padrão Ethernet na Camada Física

10Base2	185 metros (thinnet)
10Base5	500 metros (thicknet)
10BaseT	100 metros (CAT3, par trançado sem blindagem - UTP)
100BaseTX	100 metros (GAT5, 6, 7 par trançado sem blindagem - UTP)
100BaseFX	400 metros (65.2/125µ Fibra Multimodo
1000BaseCX	25 metros (Par trançado blindado - STP)
1000BaseT	100 metros (CAT5 - 4 pares trançados sem blindagem - UTP)
1000BaseSX	260 metros (62.5/50µ Fibra Multimodo)
1000BaseLX	10 Km (9µ Fibra Monomodo)

Cada uma das notações anteriores define uma interface de conexão (*Attachment Unit Interface* - AUI) diferente. Tais notações são de extrema

valia na identificação de informações importantes. Eis o significado da sintaxe utilizada:

[taxa máxima de transmissão] [tipo de transmissão] [comprimento máximo do cabo]
Ex: 10Base2 = [10Mbps] [Baseband] [aprox. 200 metros (185 metros)]

Os padrões Ethernet empregam sinalização banda base (daí o "Base" existente nas notações). A transmissão se faz por meio de pacotes que ocupam a banda de freqüência do canal (figura 2.12). Nenhum padrão Ethernet existente faz uso de técnicas de multiplexação de dados, o que exigiria o uso de sinalização banda larga.

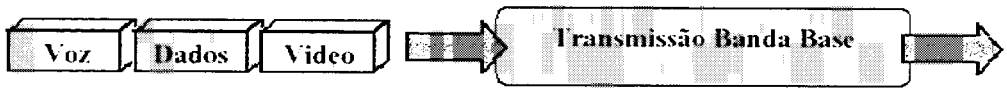


Figura 2.12: Transmissão banda base (utilizada no padrão Ethernet).

Os padrões 10Base2, 10Base5 e 10BaseT são os originais, definidos pelo padrão 802.3 do IEEE (*Institute of Electrical and Electronic Engineers*). Cada um deles define uma interface de conexão (*Attachment Unit Interface* - AUI), que permite a transferência bit a bit da camada de Enlace para a camada física. Isso permite que o MAC mantenha-se constante e ao mesmo tempo suportando novas tecnologias.

A interface original - AUI - entretanto, não suportava transmissões a 100Mbps devido às altas freqüências envolvidas. O padrão 100BaseT Ethernet precisava de uma nova interface, e as especificações 802.3u vieram a definir um novo padrão, chamado *Media Independent Interface* (MII), permitindo taxas de até 100Mbps, 4 bits por vez. O padrão *Gigabit Ethernet* utiliza um outro padrão de interface, chamado de *Gigabit Media Independent Interface* (GMII), permitindo transferências a 1000Mbps, 8 bits por vez.

***Nota**: Os padrões existentes para Gigabit Ethernet são IEEE 802.3ab (1000BaseT - par metálico) e IEEE 802.3z (1000BASE-SX - Fibra).*

É importante entender e saber diferenciar as várias velocidades de acesso à mídia que o padrão Ethernet disponibiliza. Entretanto, é igualmente importante conhecer os requerimentos de cada tipo de conector para cada tipo de implementação antes de se tomar uma decisão. EIA/TIA (*Electronic Industry Association/Telecom Industry Association*) são grupos que padronizam e definem as especificações físicas para o padrão Ethernet. EIA/TIA especifica que o padrão Ethernet utilize um conector registrado (*Registered Jack* - RJ), com uma seqüência 4-5 (por isso a sigla RJ-45) em um cabo não-blindado composto por pares metálicos trançados (*Unshielded*

Twisted Pair - UTP). A seguir, listamos os tipos de conectores e topologias disponíveis para os principais padrões Ethernet:

10Base2	Utiliza barramento lógico e físico, com conector AUI
10Base5	Utiliza barramento lógico e físico, com conector AUI
10BaseT	Topologias estrela e barramento lógico, conector RJ-45
100BaseTX	Topologias estrela e barramento lógico, conector RJ-45 MII
100BaseFX	Topologia Ponto-a-Ponto, conector ST ou SC

2.3.7.5 Cabos e Conectores em uma Rede Ethernet

O conector UTP, chamado de RJ-45, é transparente e permite que se vejam os oito fios coloridos que se conectam aos seus pinos. Esses fios são trançados (*twisted*) em quatro pares. Quatro fios (dois pares) carregam a voltagem e são chamados de *tip*. Os dois restantes são aterrados e conhecidos como *ring*. O conector RJ-45 é "crimpado" na ponta do cabo e a pinagem do conector é numerada de 1 a 8 (figura 2.13).

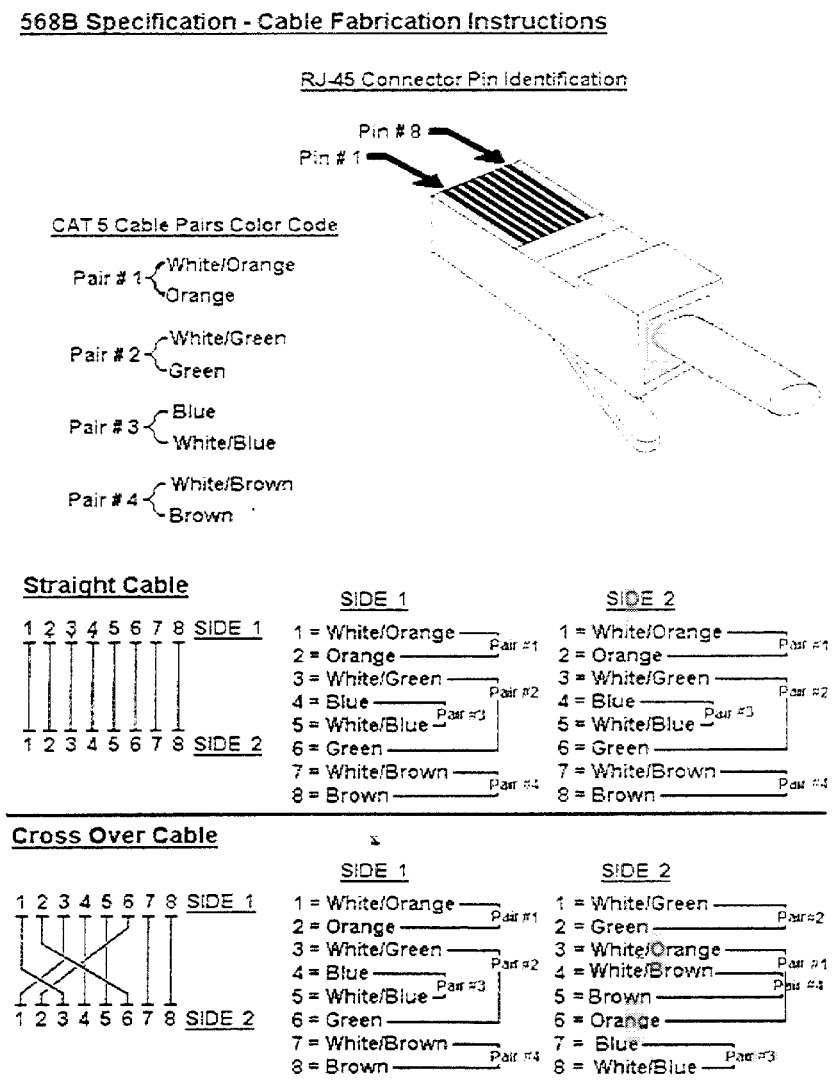


Figura 2.13: Diagramação dos cabos RJ45 Ethernet Crossover e Straight-Through[15].

[15] Fonte: <http://redvip.homelinux.net/varios/rj45/RJ45wiring.jpg>.

Os cabos UTP possuem pares trançados de fios metálicos em seu interior para eliminar o efeito *crosstalk*. A proteção aos sinais digitais vem da torção dos fios. Ao se trançar os cabos, os campos eletromagnéticos gerados pelo fluxo de eletricidade nos fios se anulam, reduzindo, assim, a interferência eletromagnética causada. Quanto mais torções por polegada, mais distante, supostamente, o sinal pode viajar sem interferência, porém uma maior quantidade de fios é necessária, o que encarece muito o cabo. Cabos UTP categorias 5 e 6, por exemplo, têm muito mais torções por polegada que cabos categoria 3, e são, portanto, considerados de melhor qualidade, uma vez que estão menos sujeitos à interferência eletromagnética e são mais caros.

Os modos de se medir a ocorrência de *crosstalk* em redes Ethernet são (saiba isso!):

- **Near End Crosstaltk (*NEXT*)**: É medida a partir da ponta transmissora do cabo;
- **Far End Crosstalk (*FEXT*)**: É medida a partir da ponta final do cabo;
- **Power Sum NEXT (*PSNEXT*)**: Um teste matemático que simula a energização dos quatro pares de fios simultaneamente, garantindo que o nível de ruído e interferência não seja superior ao aceitável. A medida PSNEXT é mais adotada em redes *GigabitEthernet*, já que estas usam, de fato, os quatro pares de fios do cabo UTP.

Diferentes tipos de cabos são necessários na implementação de uma rede. Deve-se saber, por exemplo, quando utilizar cabos do tipo *Straight-Through* ou *Crossover* (figura 2.13):

- Cabos *Straight-Through* devem ser utilizados na conexão de um router a um hub ou switch, um servidor a um hub ou switch, uma workstation a um hub ou switch;
- Cabos *Crossover* devem ser utilizados na conexão de uplinks entre switches, hubs a switches, hub a outro hub, router a outro router, dois computadores (*back-to-back*, ou seja, sem o intermédio de outro dispositivo).

***Dica**: Para saber quando usar um cabo crossover ou straight-through, lembre-se que o primeiro é para conexões entre equipamentos definidos na mesma camada (ex.: Camada 1 – Camada 1, Camada 2 – Camada 2), e o segundo é usado em conexões entre dispositivos definidos em camadas diferentes (ex.: Camada 1 – Camada 2, Camada 1 – Camada 3). As exceções seriam conectar um PC (Camada 1) a um router (Camada 3) ou um Switch (Camada 2) a um Hub (Camada1). Nesses casos, um crossover seria necessário.*

2.3.7.6 Cabos e Conectores em uma Rede Geograficamente Distribuída (WAN)

As conexões seriais (normalmente utilizadas nas comunicações WAN - *Wide Area Network*) disponibilizadas pelos produtos Cisco suportam praticamente qualquer tipo de serviço WAN. As conexões mais encontradas são linhas privativas/dedicadas (LPs) utilizando os encapsulamentos HDLC (*High Level DataLink Control*), PPP (*Point-to-Point Protocol*), ISDN (*Integrated Services Digital Network*) ou *Frame-Relay*. As velocidades de transmissão mais comuns variam de 2400bps a 1.544Mbps (T1).

- **Transmissão Serial**: Conectores seriais WAN utilizam transmissão serial (bit a bit) sobre um canal apenas. Transmissões paralelas podem ser feitas em até 8 bits por vez. Todas as WANs usam transmissão do tipo serial, sem exceção. Roteadores Cisco utilizam um conector serial de 60 pinos (DB60), proprietário (exclusivo) da Cisco. O tipo de conector encontrado na outra ponta vai depender do provedor de serviço ou dos requerimentos do dispositivo localizado na outra ponta. As diferentes terminações disponíveis são EIA/TIA-232, EIA/TIA-449, V.35 (usados na conexão de CSU/DSU), X.21 (usados em redes X.25/Frame-Relay) e EIA-530. Conexões seriais são descritas em freqüência ou em ciclos por segundo (Hertz). A quantidade de dados que podem ser transportados nessas freqüências é chamada de "largura de banda" (*bandwidth*), ou seja, *bandwidth* é a quantidade de dados, em bits por segundo, que uma conexão serial é capaz de transportar;
- **DTE/DCE**: Routers são, por definição, dispositivos DTE, e se conectam a um dispositivo DCE, como, por exemplo, um CSU/DSU (*Channel Service Unit/Data Service Unit*). Os CSU/DSU, então, são conectados a um *demarc* (*demarcation location*, tipicamente uma tomada RJ-45 fêmea na parede), sendo essa a última responsabilidade do provedor. Tudo o que se encontra nas instalações do contratante de serviço, até o *demarc*, é definido como *Customer Premise Equipment* (CPE);
- **Interfaces Modulares e Fixas**: Alguns routers Cisco possuem interfaces fixas, outros, modulares. Os routers de interface fixa, como a antiga série 2500, não podem ter suas interfaces trocadas ou atualizadas. Se você necessitar de

uma nova interface, por exemplo, terá de comprar um novo router. Entretanto, routers mais recentes como os das séries 1700, 1800, 2600 ou 2800 possuem interfaces modulares, permitindo a adição, troca ou atualização das interfaces disponíveis. São, portanto, mais customizáveis e preservam o investimento. Routers da série 1700, por exemplo, são capazes de disponibilizar várias portas seriais, interfaces FastEthernet e até permitem adicionar módulos de voz;

- **ISDN (RDSI)**: O padrão ISDN-BRI (*Basic Rate Interface*) é definido por dois canais B (*Bearer*) de 64Kbps e um canal D (*Data*) de 16Kbps, usado para sinalização e sincronização de dados. Routers que suportam ISDN-BRI vêm com uma interface U ou uma interface S/T. A diferença entre os dois é que a interface U já é uma interface de dois fios padrão ISDN, enquanto a interface S/T possui quatro fios e precisa ser conectada a um terminal de rede do tipo 1 (NT1) para convertê-la em dois fios, seguindo as especificações do padrão ISDN;
- **Conexões Via Console**: Os produtos Cisco (routers e switches) são comercializados com cabos e conectores de console, permitindo a conexão, configuração, verificação e monitoração do produto. O cabo utilizado na conexão entre um produto Cisco e o terminal (normalmente um PC comum) é o cabo *rollover*, com conectores RJ-45. A pinagem de um cabo *rollover* é a seguinte: 1-8;2-7;3-6;4-5;5-4;6-3;7-2;8-1. Como você pode perceber, basta pegar um cabo *Straight-Through*, cortar uma das pontas, invertê-lo e crimpá-lo ao novo conector. Geralmente, um conector DB9 será utilizado para conectar um produto Cisco ao terminal. A maioria dos produtos Cisco suporta conexões console via conectores RJ-45, entretanto, algumas séries ainda utilizam conectores DB25. A maioria dos routers possui uma porta AUX, que é uma porta auxiliar normalmente utilizada para conexão a um modem. Conexões estabelecidas ao router via portas de console ou AUX são tidas como gerenciamento *out-of-band* (OOB), uma vez que a configuração do router é realizada fora da rede. Já uma conexão a um router via Telnet é considerado como gerenciamento *in-band*. Para conectar-se ao um router Cisco via porta Console ou via modem, basta utilizar um programa emulador terminal como o HyperTerminal, que acompanha o Windows.

2.4 Encapsulamento de Dados

Quando um dispositivo transmite dados através de uma rede para outro dispositivo, esses dados são encapsulados e "embrulhados" com informações específicas a cada camada do modelo OSI pela qual passam.

Cada camada do dispositivo transmissor comunica-se apenas com sua camada "irmã" no dispositivo receptor. Para se comunicar e trocar informações, cada camada usa o que chamamos de *Protocol Data Units* (PDUs). Essas PDUs contêm informações específicas de controle anexadas à medida que os dados atravessam cada camada do modelo, geralmente anexadas ao cabeçalho *(header)* do pacote de dados, podendo também ser anexada ao seu final *(trailer)*.

Essas informações são anexadas aos dados através de um processo conhecido como encapsulamento, que ocorre em cada uma das camadas do modelo. Cada PDU tem um nome específico, dependendo da informação que seu cabeçalho carrega. Essa informação apenas pode ser interpretada pela camada "irmã", no dispositivo receptor, quando é retirada, e os dados são repassados para a camada imediatamente superior.

O processo se repete até que o pacote de dados atinja as camadas superiores do modelo (Sessão, Apresentação e Aplicação), quando podem ser interpretados e utilizados. A figura 2.14 ilustra esse processo, camada a camada.

Observe que, na camada de enlace, além do cabeçalho (composto pela soma de cabeçalhos das camadas imediatamente superiores), encontramos um *trailer*. Esse anexo contém o campo FCS (*Frame Check Sequence*), que detecta se os dados foram corrompidos durante o processo de transmissão pela camada física (bits).

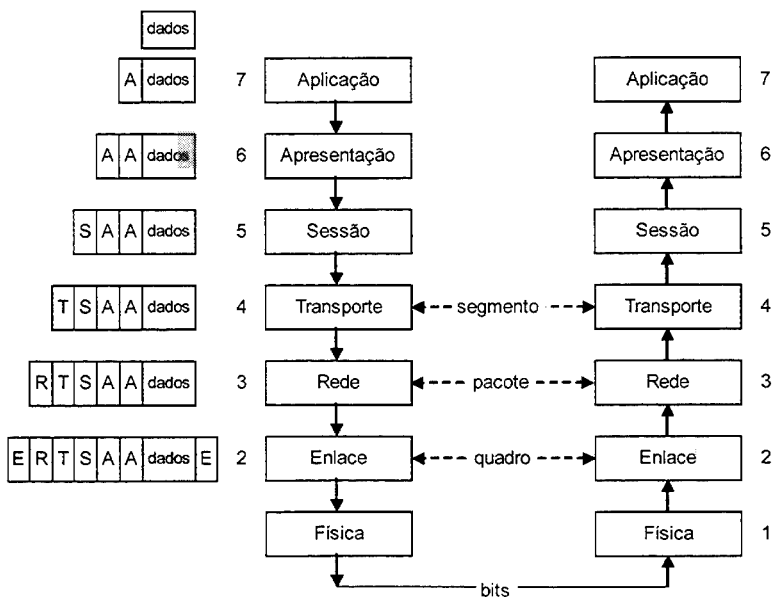


Figura 2.14: O processo de encapsulamento de dados no modelo OSI.

2.5 O Modelo de Três Camadas Cisco

Sistemas hierárquicos nos ajudam a entender melhor onde deve ser alocado cada recurso, como cada recurso se encaixa e interage com os outros e quais funcionalidades vão onde. Eles trazem ordem e compreensão para o que seriam, de outro modo, sistemas muito complexos.

Grandes redes podem ser extremamente complexas, envolvendo múltiplos protocolos, configurações detalhadas e diversas tecnologias diferentes. A hierarquização auxilia na sumarização de uma vasta gama de detalhes em um modelo mais descomplicado e compreensível.

O modelo de três camadas foi criado pela Cisco para auxiliar projetistas e administradores de redes em tarefas como desenho, implementação e gerenciamento de uma rede hierárquica escalável, confiável e custo-efetiva. A Cisco define três camadas hierárquicas, como nos mostra a figura 2.15. É importante entender e aceitar o conceito de "manter o tráfego de dados local, no local" ao se planejar uma rede hierárquica.

Note, na figura, que os uplinks (conexões entre as camadas) têm sua banda aumentada, conforme se avança no modelo. Isso é interessante pois, conforme se sobe na hierarquia, mais se concentra o tráfego de dados. Por isso, é necessário planejar com atenção para evitar o surgimento de "gargalos". Observe também, que as conexões entre as camadas são redundantes, o que aumenta a disponibilidade da rede.

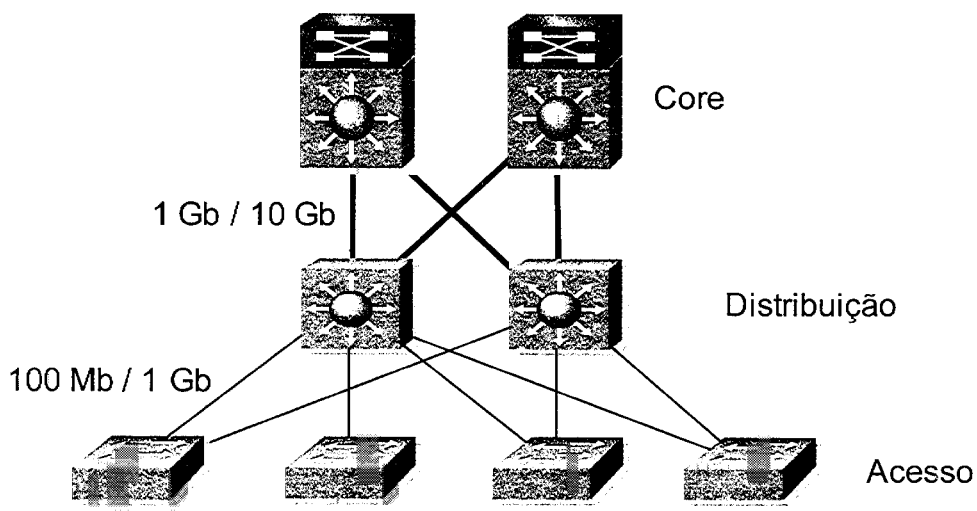


Figura 2.15: Ilustração do modelo hierárquico de três camadas proposto pela Cisco.

Core Layer (Camada Principal): A camada principal é o "coração" da rede. Responsável pelo transporte de grandes volumes de dados, de forma simultaneamente rápida e confiável. Se ocorrer uma falha em

qualquer dispositivo ou processo nessa camada, todos os usuários serão afetados. Portanto, tolerância à falha é um fator crítico nessa camada. Nela encontraremos dispositivos de rede como switches *Layer-3* e/ou routers de alto desempenho (dependendo do tamanho e arquitetura da rede em questão). Como nesta camada ocorre a agregação dos links de toda a rede, largura de banda também é um fator crítico. Eis uma lista do que **não** deve ser feito na camada principal:

- Implementação de processos ou dispositivos que retardem o tráfego de dados, incluindo a implementação de listas de acesso, roteamento entre VLANs e filtragem de pacotes. De um modo geral, nesta camada não deve ocorrer a manipulação de dados, ou seja, do modo como os pacotes ou frames chegam, eles devem ser encaminhados, o mais confiável e rápido possível;
- Implementação de processos ou dispositivos que suportem o acesso a grupos de trabalho;
- Expansão do core pela simples adição de dispositivos. Se a performance tornar-se um fator crítico no core, seu upgrade deve ser a opção à sua expansão.

Distribution Layer (Camada de Distribuição): Também referida como Camada de Grupos de Trabalho (*Workgroup Layer*), sua função principal é prover o roteamento entre VLANs, filtragem de dados (por meio da implementação de Firewalls, Listas de Controle de Acesso ou outros mecanismos) e quaisquer outros recursos necessários pelos grupos de trabalho. É função desta camada prover o tratamento e manipulação do tráfego, se necessário, ANTES que ele chegue ao Core da rede. É nesta camada que devem ser implementadas políticas de acesso à rede. Dispositivos de rede comuns à camada de distribuição são switches layer-3 e/ou routers. Eis uma lista de funções que encontram-se disponíveis nessa camada:

- Implementação de ferramentas como listas de acesso, filtragem de pacotes e *queuing*;
- Implementação de políticas de segurança e acesso à rede, incluindo *firewalls* e *address translation services*;
- Redistribuição entre protocolos de roteamento, incluindo roteamento estático;
- Roteamento entre VLANs;
- Definição de domínios *broadcast* e *multicast*.

Access Layer (Camada de Acesso): A camada de acesso controla o acesso de grupos e usuários aos recursos da rede. Grande parte dos recursos de que os usuários precisarão estarão disponíveis localmente. Os dispositivos de rede mais comumente encontrados nessa camada são os switches de camada 2 e hubs. Alguns processos que devem ser considerados na camada de acesso:

- Implementação contígua de políticas de acesso à rede e segurança;
- Criação de diferentes domínios de colisão;
- Conectividade dos grupos de trabalho com a camada de distribuição.

Ao se planejar uma LAN, é importante ter em mente as diferentes tecnologias Ethernet disponíveis. Seria, sem dúvida, maravilhoso implementar uma rede rodando gigabit Ethernet em cada desktop e 10 gigabit Ethernet entre switches, mas embora isso venha a acontecer algum dia, seria muito difícil justificar o custo de uma rede com esse perfil nos dias de hoje.

Utilizando-se um "mix" das diferentes tecnologias Ethernet disponíveis hoje, é possível a criação de uma rede eficiente a um custo justificável. Eis algumas sugestões de onde utilizar cada tipo de tecnologia em uma rede hierárquica:

- Implementação de switches 10/100Mbps na Camada de Acesso para promover uma boa performance a um custo baixo. Links de 100/1000Mbps podem ser usados em clientes e servidores que demandem largura de banda mais elevada. Nenhum servidor deve rodar abaixo de 100 Mbps, se possível. É interessante implementar uplinks de 1Gbps conectando as camadas de Acesso e Distribuição, para evitar "gargalos";
- Implementação de FastEthernet ou mesmo GigabitEthernet nos switches entre as camadas de acesso e distribuição. A utilização de 10 Mbps pode gerar "gargalos";
- Implementação GigabitEthernet nos switches entre a camada de distribuição e o core. Deve haver uma preocupação em implementar as mais rápidas tecnologias disponíveis entre os switches do core. A adoção de links redundantes nos switches presentes entre a camada de distribuição e a central é recomendável para contingência e balanceamento de carga.

Questões de Revisão – O Modelo OSI

1. Qual camada do modelo Cisco é responsável pela segmentação de domínios de colisão?

a) Física
b) Acesso
c) Central
d) Rede
e) Distribuição
f) Enlace de Dados

2. PDUs (Protocol Data Units) na camada de rede do modelo OSI são chamados de:

a) Central
b) Frames
c) Pacotes
d) Segmentos
e) Acesso
f) Distribuição
g) Transporte

3. Em qual camada do modelo Cisco os domínios de Broadcast são definidos?

a) Central
b) Rede
c) Física
d) Distribuição
e) Acesso
f) Transporte

4. PDUs na camada de Enlace de Dados recebem o nome de:

a) Frames
b) Pacotes
c) Datagramas
d) Transporte
e) Segmentos
f) Bits

5. O processo de segmentação do fluxo de dados ocorre em qual camada do modelo OSI?

a) Física
b) Enlace
c) Rede
d) Transporte
e) Distribuição
f) Acesso

6. Para qual das seguintes interconexões você NÃO precisaria de um cabo Ethernet crossover?

a) Conexão de uplinks entre switches.
b) Conexão de um roteador a um switch.
c) Conexão de um hub a um hub.
d) Conexão entre hubs e switches.

7. Qual informação a camada de Enlace usa para identificar um host na rede local?

a) Endereço lógico da rede
b) Número da porta TCP
c) Endereço de Hardware
d) Default gateway

8. Em qual camada encontram-se definidos os roteadores no modelo OSI?

a) Física
b) Transporte
c) Enlace de Dados
d) Rede

9. Em qual camada do modelo OSI "0s" e "1s" são convertidos em sinal elétrico?

a) Física
b) Transporte
c) Enlace de Dados
d) Rede

10. As Bridges são definidas em qual camada do modelo OSI?

a) Física
b) Transporte
c) Enlace de Dados
d) Rede

11. Qual camada do modelo proposto pela Cisco provê a segmentação de redes Ethernet?

a) Acesso
b) Física
c) Rede
d) Distribuição
e) Central
f) Transporte
g) Enlace de Dados

12. Qual mecanismo é adotado pela camada de Transporte para evitar o esgotamento do buffer na máquina destino?

a) Segmentação
b) Encapsulamento
c) Envio de mensagens de reconhecimento (ACKs)
d) Controle de fluxo
e) Envio de BPDUs

13. Qual camada do modelo OSI preocupa-se com a semântica dos dados?

a) Aplicação
b) Apresentação
c) Sessão
d) Transporte
e) Enlace de Dados

14. Os roteadores podem prover quais das seguintes funções (escolha todas que se aplicam)?

a) Quebra de Domínios de Colisão
b) Quebra de Domínios de Broadcast
c) Endereçamento lógico de rede
d) Filtragem da rede através da análise de endereços físicos

15. Roteadores são tipicamente aplicados em qual camada do modelo proposto pela Cisco?

a) Acesso
b) Enlace de Dados
c) Central
d) Distribuição
e) Rede

16. Quantos bits definem um endereço de hardware?

a) 6 bits b) 16 bits c) 46 bits d) 48 bits

17. Qual das seguintes não é uma vantagem de se adotar um modelo em camadas?

a) Dividir uma complexa operação de rede em um conjunto de operações menores, com gerenciamento simplificado.
b) Permitir que ocorram mudanças em uma camada sem que todas as outras tenham de ser alteradas.
c) Permitir que ocorram mudanças em todas as camadas sem que uma tenha de ser alterada.
d) Definir uma interface padrão permitindo a integração entre equipamentos de diversos fabricantes.

18. Quais são as três opções que usam cabeamento metálico par-trançado?

a) 100BaseFX
b) 100BaseTX
c) 100VG-AnyLAN
d) 10BaseT
e) 100BaseSX

19. O que o termo "Base" significa em 10BaseT?

a) Cabeamento de banda-larga que transmite uma série de sinais digitais ao mesmo tempo e na mesma linha.
b) Cabeamento de banda-básica que transmite uma série de sinais digitais ao mesmo tempo e na mesma linha.
c) Cabeamento de backbone que transmite apenas um sinal digital por vez na linha.
d) Cabeamento de banda básica que transmite apenas um sinal digital por vez na linha.

20. Se em uma rede temos dois hubs de 12 portas 10/100 cada, quantos domínios de broadcast e quantos domínios de colisão essa rede possui?

a) 24 e 1 c) 1 e 12 e) 1 e 24
b) 12 e 12 d) 1 e 1

21. Se em uma rede temos dois switches de 12 portas 10/100 cada, quantos domínios de broadcast e quantos domínios de colisão essa rede possui?

a) 24 e 1 c) 1 e 12 e) 1 e 24
b) 12 e 12 d) 1 e 1

Respostas das Questões de Revisão – O Modelo OSI

1. **B**. A camada de acesso é onde os usuários obtêm acesso à rede e onde a Cisco recomenda Switches para quebra de domínios de colisão.

2. **C**. PDUs são usados para definir dados em cada camada do modelo OSI. PDUs na camada de rede são chamadas de pacotes.

3. **D**. Os roteadores, por definição, quebram domínios de broadcast. Esses dispositivos (routers) são definidos na camada de distribuição do modelo proposto pela Cisco.

4. **A**. PDUs na camada de Enlace são chamadas de frame (quadro).

5. **D**. A camada de Transporte recebe um grande fluxo de dados das camadas superiores e os quebram em partes menores, chamadas segmentos.

6. **B**. Cabos Ethernet crossover são requeridos para conexão de switches a switches, hubs a hubs e hubs a switches.

7. **C**. Os endereços MAC, também chamados de endereços de hardware, são usados para identificar hosts individualmente em uma rede local.

8. **D**. Roteadores são definidos na camada de Rede do modelo OSI.

9. **A**. A camada Física é responsável pela transformação dos binários em sinal digital e por seu transporte de uma mídia (cabo) ao outro lado.

10. **C**. As bridges e os switches quebram domínios de colisão e ambos são definidos na camada de Enlace de Dados.

11. **A**. A camada de Acesso é usada para prover acesso aos usuários e hosts à rede, e os switches são usados na segmentação de redes Ethernet nessa camada.

12. **D**. Controle de fluxo é um recurso que evita o esgotamento dos buffers em um dispositivo. Ainda que esse recurso possa ser aplicado em diversas camadas, a camada de Transporte é a que oferece o melhor esquema de controle de fluxo no modelo.

13. **B**. A camada de Apresentação do modelo OSI provê essa funcionalidade.

14. **A, B, C, D**. A palavra-chave dessa questão é "pode". Routers podem prover todas as funcionalidades listadas.

15. **D**. A Cisco sugere o uso de roteadores na camada de distribuição e switches nas duas outras camadas. Não se trata de uma regra rígida, entretanto. Essa apenas é a melhor resposta.

16. **D**. O endereço de hardware possui uma extensão de 48 bits (6 bytes).

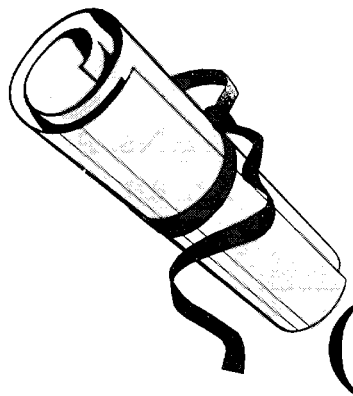
17. **C**. Na verdade, uma das grandes vantagens de um modelo em camadas é que ele permite efetuar alterações em apenas uma camada do modelo, sem ter de se preocupar com as outras.

18. **B, C , D**. 100BaseTX usa par trançado metálico, assim como 100VGAnyLAN e 10BaseT. FX e SX utilizam fibra ótica.

19. **D**. A técnica de sinalização baseband (banda básica) utiliza a totalidade da banda disponível pelo meio físico na transmissão, tornando-o ineficiente. Já a técnica de sinalização broadband (banda-larga) transmite uma série de sinais simultaneamente através do meio físico, tornando-o mais eficiente.

20. **D**. Uma rede baseada em hubs não é uma rede segmentada, em nenhum nível. Trata-se de um grande domínio de broadcast e colisão.

21. **E**. Em uma rede comutada, cada porta de um switch é um domínio de colisão distinto, porém, ainda temos apenas um domínio de *broadcast*. Nesse caso, temos 24 portas, portanto, 24 domínios de colisão.



3 Redes Sem-fio (Wireless Networks)

3.1 Tópicos Abordados

- Principais Tecnologias;
- Modos de Operação;
- Tipos de Serviço;
- Transmissão Sem-fio;
- Classes de Codificação Sem-fio;
- Interferência;
- Implementação WLAN;
- Segurança WLAN.

3.2 Introdução

Nunca a comunicação sem fio esteve tão presente na vida do usuário final como atualmente. Seja através do acesso à Internet via celular, seja na transmissão infravermelho entre palmtops e/ou laptops, na comunicação *bluetooth*[1] entre PCs e periféricos ou no acesso a redes IP via *WI-FI*[2]. Além disso, novas tecnologias já aparecem prometendo revolucionar ainda mais a comunicação de dados sem fio, como é o caso do *WIMAX*[3].

---

[1] Norma que define um padrão global de comunicação sem-fio que possibilita a transmissão de voz e dados entre diferentes equipamentos por meio de um link por rádio-freqüência.

[2] *Wireless Fidelity*: Meio de acesso sem-fio de alta velocidade.

[3] *Worldwide Interoperability for Microwave Access*: Tecnologia sem-fio que permite velocidades de até 130Mbps com alcances de até 45Km.

3.3 Comparação entre Ethernet LAN e Wireless LAN

Existem muitas semelhanças entre Ethernet e Wireless LANs. Ambas permitem a troca de frames entre elementos de rede, ambas são definidas pelo IEEE (802.3 para Ethernet e 802.11 para Wireless), ambas possuem cabeçalhos e *trailers* (apêndices), sendo que o cabeçalho contém os endereços MAC de origem e de destino, ambas implementam métodos para determinar quando um dispositivo pode ou não transmitir.

A maior diferença está no modo como os dados são transmitidos. Em redes Ethernet, os frames são transmitidos por meio da geração de sinais elétricos em um cabo metálico (ou de sinais luminosos em um fibra-óptica). Já redes Wireless utilizam ondas de rádio para a transmissão de frames. Logicamente existem muitas outras diferenças, algumas sendo "efeitos colaterais" de se utilizar a tecnologia Wireless.

Por exemplo, o padrão Ethernet prevê a transmissão de dados em *full duplex* (FDX). Em redes wireless, entretanto, se 2 (ou mais) dispositivos enviarem ondas de rádio em um mesmo espaço, e em uma mesma freqüência, a interferência tornará ambas as ondas ininteligíveis.

Por este motivo, redes wireless devem operar preferencialmente em modo *half-duplex* (HDX). Para definir arbitrariamente a freqüência a ser utilizada por cada transmissão, WLANs utilizam o algoritmo CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*) para reforçar a transmissão em HDX e evitar ao máximo a incidência de colisões.

3.4 Tecnologias Wireless

Vale ressaltar que tudo o que é necessário saber sobre tecnologias de acesso sem-fio para o exame CCNA 640-802 pode ser encontrado neste livro.

A figura 3.1, ilustra as tecnologias de acesso sem-fio mais comuns e suas respectivas velocidades e alcances.

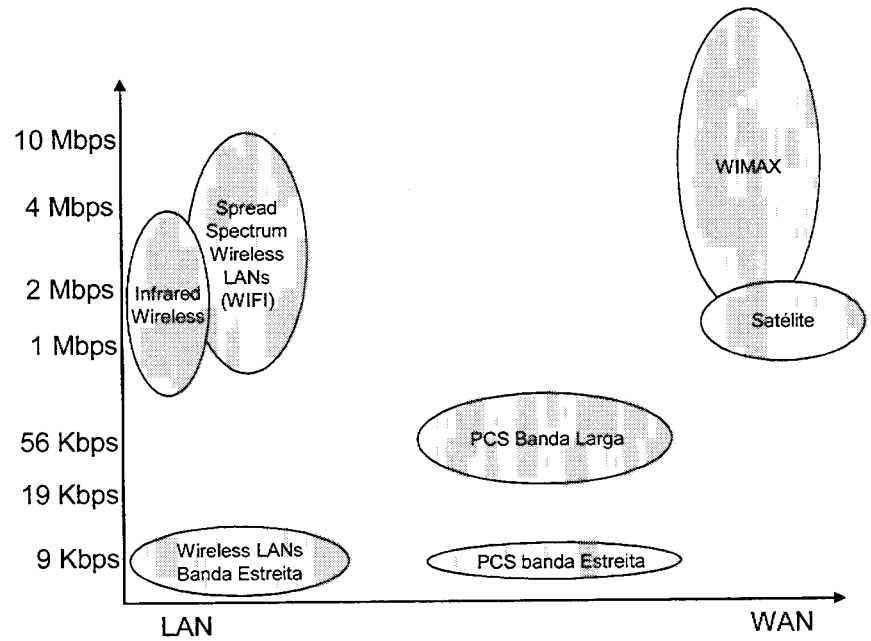


Figura 3.1: Comparação entre as tecnologias Wireless atuais.

Em seguida, discutiremos cada uma das tecnologias ilustradas.

- **Infrared Wireless LANs:** Essa tecnologia é bastante comum para transferência entre PCs ou PDAs, desde que eles se encontrem fisicamente próximos e que não existam barreiras físicas entre o transmissor e o receptor - uma limitação tecnológica da transmissão por infravermelho. Vale aqui citar o exemplo do controle remoto de televisão (que opera usando a mesma tecnologia). Ele não funciona se algo estiver bloqueando a transmissão (tente mudar de canal debaixo das cobertas) ou se o aparelho de TV estiver muito distante (mais de 10 metros, aproximadamente). As vantagens dessa tecnologia são o baixo custo e a velocidade de transmissão, que vem aumentando gradualmente. Atualmente, essa tecnologia é capaz de atingir velocidades de até 4Mbps. Bastante razoável, portanto. A desvantagem é a necessidade de proximidade física entre as pontas e a incapacidade de transpor barreiras físicas;
- **Wireless LANs Banda Estreita:** Tecnologia de transmissão via ondas de rádio, inadequada para os requerimentos atuais. Vantagens: baixo consumo de energia, distância coberta. Desvantagens: Necessidade de se usar equipamentos proprietários, baixa velocidade de transmissão, necessidade de permissão para usar a freqüência de rádio necessária;

- **Spread Spectrum Wireless LANs**: Aqui encontram-se as famosas redes WIFI. A figura 3.2 ilustra os padrões existentes hoje e suas principais características;

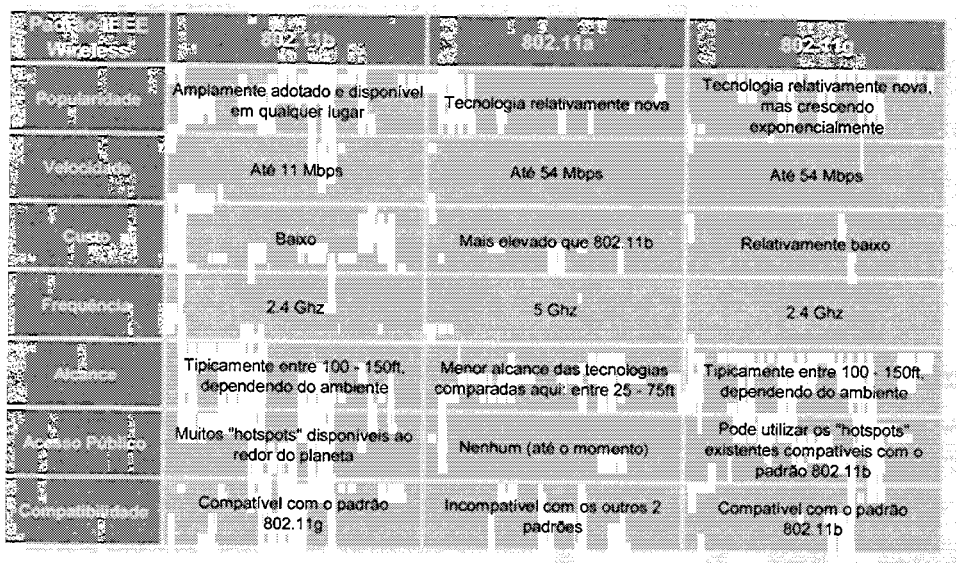


Figura 3.2: Comparação entre as tecnologias WIFI existentes.

- **PCS Banda Estreita**: PCS é o acrônimo usado para *Personal Communication Services*, que inclui uma ampla gama de dispositivos de uso pessoal, como pagers, celulares, entre outros. Os dados, aqui, são transmitidos através de microondas. Um dos dispositivos mais conhecidos a usar essa tecnologia wireless é o Blackberry, um pager full-duplex (envia e recebe mensagens). Vantagem: alcance. Desvantagem: velocidade de transmissão;
- **PCS Banda Larga**: Tecnologia adotada para transmissão de dados e voz em redes celulares, por exemplo;
- **Satélite**: A tecnologia de transmissão de dados via satélite atinge velocidades respeitáveis, atualmente (1 Mbps de downstream e 2 Mbps de upstream), porém, devido à distância envolvida, os grandes atrasos na transmissão são inevitáveis. Portanto, essa tecnologia não é recomendada para transmissão de dados em rajada (*bursty*). A grande vantagem dessa tecnologia é a sua alta disponibilidade e abrangência;
- **WIMAX**: A sigla é o acrônimo para *Worldwide Interoperability for Microwave Access*, ou Interoperabilidade Global via Acesso Microondas, se fôssemos traduzir. Essa é uma tecnologia extremamente nova, que ainda está em fase de testes pelo mundo afora. A novidade deve durar pouco e, em breve, essa tecnologia será tão comum quanto o WIFI é hoje. A promessa do WIMAX é o alcance oferecido pela

rede celular (praticamente global, hoje) à velocidade de uma LAN Ethernet (100 Mbps). Imagine as possibilidades: você em seu carro, com seu laptop, poderia assistir a um video *stream* (video on-line) de um *pay-per-view* enquanto está preso no trânsito, ou poderia sintonizar uma rádio on-line através de seu cd-player automotivo (obviamente já preparado para isso, num futuro não muito distante).

3.5 Modos de Operação WLAN

Existem basicamente 2 modos de operação de uma rede WLAN: Ad-Hoc e infra-estrutura. No modo Ad-Hoc, um dispositivo WIFI pode comunicar-se com outro sem o intermédio de um ponto de acesso (*access point*). A figura 3.3 ilustra este modo de operação.

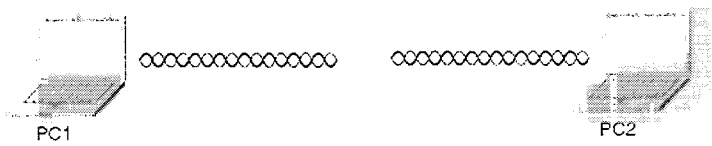


Figura 3.3: Modo de operação wireless Ad-Hoc.

O modo infra-estrutura, por sua vez, implica na implementação de um ponto de acesso wireless (*access point*) conectado à rede Ethernet por meio de um cabo metálico UTP tradicional. Dispositivos configurados para este modo de operação não podem enviar frames diretamente um ao outro. Ao invés disso, eles enviam seus frames para um ponto de acesso, e este o encaminha para o destinatário. A figura 3.4 ilustra este modo de operação.

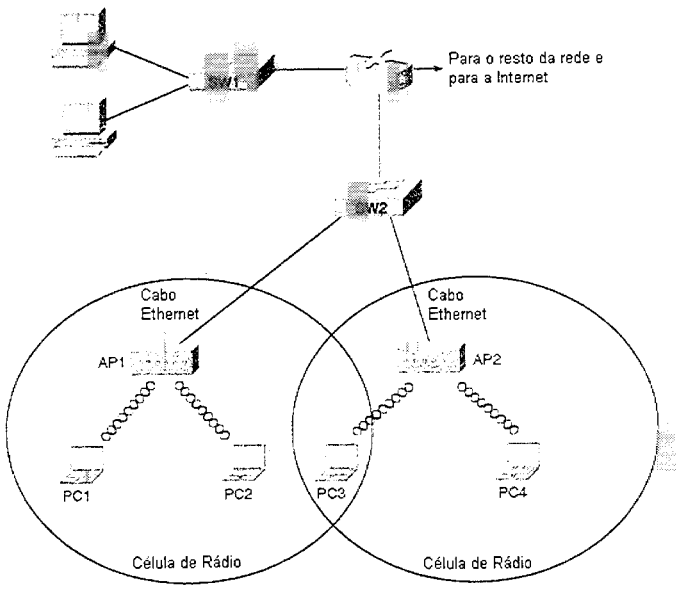


Figura 3.4: Modo de operação wireless infra-estrutura.

O modo de operação infra-estrutura suporta 2 tipos de serviços (*service sets*) chamados de BSS (*Basic Service Set*) e ESS (*Extended Service Set*). A diferença entre ambos é bastante simples. Enquanto o BSS usa apenas 1 ponto de acesso (AP) para criar uma rede WLAN, o ESS utiliza 2 ou mais APs, normalmente criando uma zona de intersecção para permitir a mobilidade (*roaming*) dos usuários de uma célula para outra. A figura 3.4 ilustra o modo infra-estrutura ESS, onde temos o AP1 e o AP2 conectados a mesma rede física e uma interposição das 2 células geradas por cada um dos APs.

O recurso de mobilidade (*roaming*) oferecido pelo ESS garante que o usuário, ao se movimentar de uma célula para outra, não terá de obter um novo endereço IP. Basicamente, o dispositivo do usuário (um laptop, por exemplo) detecta que o sinal de uma determinada célula está ficando fraco e automaticamente procura por um sinal mais forte em uma célula vizinha. Uma vez que este sinal seja identificado, o dispositivo faz a troca de modo transparente ao usuário. O princípio é o mesmo utilizado em redes celulares.

Diferentes modos de operação WLAN e seus nomes

Modo	Tipo de serviço (Service Set)	Descrição
Ad-Hoc	Independent Basic Service Set (IBSS)	Não existe a figura do AP. Os dispositivos WIFI comunicam-se diretamente.
Infra-estrutura (1 AP)	Basic Service Set	Um único AP forma a rede WLAN
Infra-estrutura (2+ APs)	Extended Service Set	Múltiplos APs formam a rede WLAN, possibilitando a mobilidade do usuário entre células

3.6 Transmissão Sem-fio

Transmitir via ondas de rádio demanda a obtenção de uma licença específica, dependendo da freqüência em que se deseja transmitir. A razão disso é reduzir as chances de interferências em serviços públicos como rádios (AM e FM), TV ou serviços vitais/estratégicos, como a comunicação entre aeronaves, por exemplo. Agora, imagine se precisássemos obter uma licença para poder operar um telefone sem-fio, um aparelho celular ou um laptop com WIFI? Seria inviável a comercialização deste tipo de tecnologia. Tendo isso em mente, os órgãos reguladores (por exemplo, o FCC nos EUA e a ANATEL no Brasil) determinaram faixas específicas de freqüências que não necessitam de licença para serem utilizadas. Fabricantes devem seguir as normas definidas por cada país para obter a autorização de comercializar seus produtos. Se você tem algum dispositivo sem-fio com você, procure pelo selo da ANATEL. Se for um produto de uma empresa idônea, certamente você encontrará o selo certificando que o aparelho em questão segue as normas estabelecidas pelo órgão para transmissão sem-fio no Brasil.

Faixas de frequência liberadas de licença pelos orgãos reguladores

Faixa de Frequencia	Nome	Exemplos de Dispositivos
900 KHz	Industrial, Scientific, Mechanical (ISM)	Telefones sem fio mais antigos
2.4 GHz	ISM	Telefones sem fio mais modernos e dispositivos WIFI 802.11, 802.11b, 802.11g
5 GHz	Unlicensed National Information Infrastructure (U-NII)	Telefones sem fio mais modernos e dispositivos WIFI 802.11a, 802.11n

3.7 Classes de Codificação Sem-fio

Quando um dispositivo WIFI ou um AP envia seus dados, ele consegue alterar (modular) a freqüência, amplitude e a fase do sinal de rádio para representação de "0"s e "1"s. Os detalhes destas técnicas de codificação estão bastante além do escopo do exame CCNA, entretanto, é importante conhecer as 3 classes de codificação mais comuns.

- **Frequency Hopping Spread Spectrum (FHSS)** - Utiliza todas as freqüências disponíveis, alternando de uma para outra (*hopping*). Ao utilizar diferentes freqüências para outra (*hopping*). Ao utilizar diferentes freqüências para um dispositivo tem maior chance transmissões consecutivas, um dispositivo tem maior chance de evitar interferência de um outro dispositivo que utilize a mesma faixa de freqüência liberada. O padrão 802.11 original adota esta técnica, porém, os padrões mais recentes (802.11a, 802.11b e 802.11g), não;
- **Direct Sequence Spread Spectrum (DSSS)** - Esta classe de codificação foi projetada para uso na faixa liberada de 2.4 GHz. DSSS utiliza um ou vários canais (ou freqüências) distintos. Esta faixa tem uma largura de banda de 82 MHz, variando de 2.402 GHz à 2.483 GHz. Conforme definido pelo FCC, esta faixa pode ter 11 diferentes canais parcialmente sobrepostos, conforme ilustra a figura 3.5.

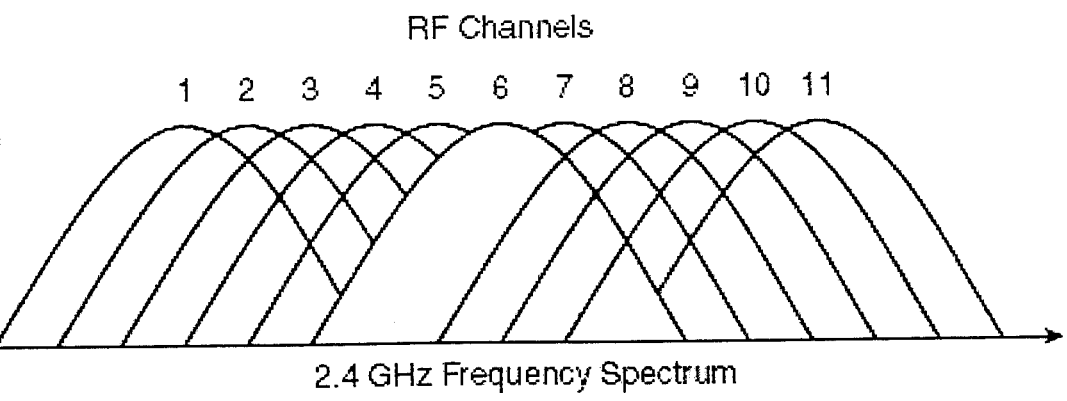


Figura 3.5: Canais DSSS.

Embora grande parte dos canais ilustrados na figura encontrem-se sobrepostos, 3 canais (1, 6 e 11) não se interseccionam a ponto de interferir um no outro. Estes 3 canais podem ser utilizados em uma mesma WLAN, já que praticamente não interferem um no outro.

A importância dos canais não sobrepostos é grande quando você está desenhando uma rede WLAN ESS, ou seja, uma rede WLAN na qual mais de um AP será empregado. Desta forma, APs que se encontram em áreas de sobreposição de sinais podem ser configurados para trabalhar em um dos 3 diferentes canais. A figura 3.6 ilustra este conceito.

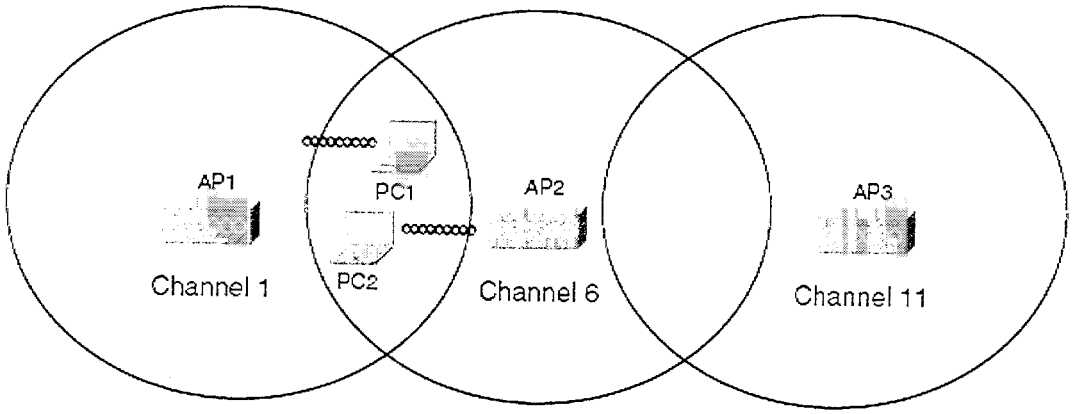


Figura 3.6: Modo ESS com 3 APs utilizando canais DSSS diferentes.

- **Orthogonal Frequency Division Multiplexing (OFDM)** - De modo análogo ao DSSS, WLANs que utilizam OFDM também podem usar múltiplos canais não sobrepostos.

A tabela a seguir sumariza as principais características de cada uma das 3 classes vistas.

Nome da Classe de Codificação	Utilizada em
Frequency Hopping Spread Spectrum (FHSS)	802.11
Direct Sequence Spread Spectrum (DSSS)	802.11b
Orthogonal Frequency Division Multiplexing (OFDM)	802.11a, 802.11g

NOTA: O padrão emergente conhecido por 802.11n utiliza OFDM, assim como múltiplas antenas, uma tecnologia também conhecida como Multiple Input Multiple Output (MIMO).

3.8 Interferência

Assim como um rádio convencional ou um telefone sem-fio, uma rede WLAN pode sofrer com interferências originadas nas mais diversas fontes.

Interferências podem ser causadas por outras ondas de rádio transmitidas na mesma freqüência utilizada pela WLAN (exemplos: telefone sem-fio ou mesmo um forno de microondas) ou por barreiras físicas existentes no trajeto da onda de rádio, como paredes, piso e teto. Interferências físicas (barreiras) podem causar a atenuação (enfraquecimento) do sinal de rádio emitido, limitando o seu alcance. Isso ocorre, pois o sinal é parcialmente absorvido pelo material presente na barreira. Outros tipos de barreiras físicas podem refletir o sinal, especialmente verdadeiro se a barreira conter uma grande quantidade de metal. Esta reflexão do sinal de rádio pode gerar pontos cegos, onde a WLAN simplesmente deixa de funcionar, ou mesmo a redução do raio de abrangência da rede.

O SNR (*Signal-to-Noise Ratio*) é a medida utilizada para determinar o nível de interferência ativa (causada por outras ondas de rádio na mesma freqüência).

3.9 Área de Cobertura, Velocidade e Capacidade

A área de cobertura de uma rede WLAN é definida pelo espaço no qual dispositivos WIFI são capazes de enviar e receber dados com sucesso. A área de cobertura gerada por um determinado AP depende de uma série de fatores:

- Potência de transmissão;
- Freqüência utilizada;
- Interferências e obstruções;
- Proximidade do AP à determinados materiais (ex. concentração de metais)

Existe uma série de outros fatores que influenciam o diâmetro da área de cobertura, mas estes estão fora do escopo do exame CCNA.

A força do sinal influencia diretamente na velocidade em que os dados podem ser transmitidos por ele. Sinais fracos não podem transportar dados em alta velocidade, apenas em baixa. Por este motivo, os padrões WLAN suportam múltiplas velocidades. Um dispositivo próximo ao AP pode ter um sinal forte e, desta forma, pode transmitir

a uma velocidade maior que outro dispositivo mais afastado. Uma das formas de aumentar a área de cobertura de uma rede sem-fio é utilizar antenas especiais e aumentar a potência de transmissão. É possível aumentar o ganho da antena, que nada mais é do que a potência adicionada ao sinal de rádio pela antena. Basicamente, para se dobrar a área de cobertura de uma rede sem-fio é preciso quadruplicar o ganho proporcionado pela antena, lembrando de não ultrapassar a potência máxima definida pelos órgãos reguladores.

3.10 Implementação WLAN

A implementação de WLAN deve levar em consideração uma série de fatores, alguns bastante críticos, como segurança. O primeiro passo deve ser colocar a WLAN para funcionar. Assim que for verificada a conectividade entre um dispositivo e um AP, então, podemos começar a implementação das políticas de segurança. Eis uma sugestão de checklist a ser seguido em uma implementação WLAN:

- Verifique a existência e operação da rede cabeada, incluindo o funcionamento de serviços essenciais como DHCP, DNS, VLANs e conexão com a Internet (se aplicável);
- Instale o AP, configure-o e verifique sua conectividade com a rede cabeada;
- Configure os parâmetros wireless, como o *Service Set ID* (SSID), porém, nada de segurança, ainda;
- Configure ao menos um dispositivo WIFI, como um laptop, para testar o funcionamento da rede WLAN;
- Verifique se a rede WLAN está funcionando;
- Configure as políticas de segurança no AP e no cliente WIFI;
- Verifique novamente o funcionamento da rede WLAN.

Vamos examinar com um pouco mais de detalhe cada um dos passos descritos anteriormente, incluindo a parte de segurança.

3.10.1 Verificação da Operação da Rede Cabeada

Alguns pontos importantes devem ser observados. Um deles é que, normalmente, o AP é conectado a uma porta de acesso no switch, ou seja, pode ser que esta porta esteja associada a uma determinada VLAN. É importante ter em mente que, se o modo escolhido de operação WLAN for o ESS, todos os APs devem estar associados às mesmas VLANs, como a figura 3.7 ilustra.

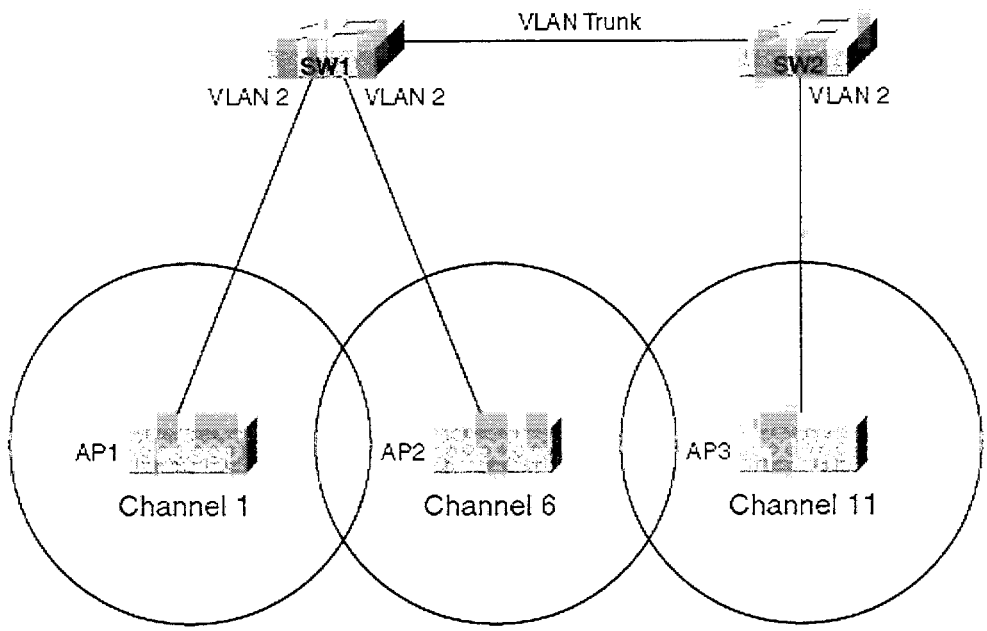


Figura 3.7: WLAN em modo ESS com os APs associados à mesma VLAN (2).

3.10.2 Instalação e Configuração do AP

Assim como switches Ethernet convencionais, APs encontram-se definidos na camada 2 e, portanto, não necessitam de um endereço IP para operar. Entretanto, também assim como switches, é interessante configurarmos um endereço IP nos APs para fins de gerenciamento e configuração. O AP utiliza um cabo *Ethernet straight-trhough* para conexão com a rede cabeada. O ideal é conectá-lo à uma porta de 100 Mbps, especialmente se o AP for trabalhar com taxas de transferências elevadas.

3.10.3 Configuração dos Detalhes WLAN no AP

Grande parte dos APs existentes hoje não necessitam de configurações adicionais para que funcionem. Basta conectá-los a uma rede cabeada utilizando suas configurações de fábrica e pronto! Entretanto, muitos destes APs podem ser configurados com uma série de parâmetros que podem adicionar segurança e elevar a performance da rede que está sendo concebida. A seguinte lista elenca alguns dos parâmetros que podem (em alguns APs, devem) ser configurados:

- Padrão IEEE a ser utilizado (a, b, g ou múltiplo);
- Canal (freqüência) a ser utilizado no AP;
- Service Set Identifier (SSID);
- Potência de transmissão.

Cada WLAN necessita de um identificador único. O SSID é nada mais que o identificador de uma rede WLAN. Em modo BSS, cada AP deve ter um SSID distinto. Já em modo ESS, os APs pertencentes ao mesmo Service Set devem possuir o mesmo SSID. O SSID é formado por até 32 caracteres ASCII.

onfiguração do Cliente WIFI

nte, um cliente WIFI é qualquer dispositivo que tenha uma ue trabalhe dentro de um dos padrões já mencionados (IEEE ou g). Pode ser um Palm, um iPhone da Apple, um laptop o um desktop. Como vimos, o AP pode precisar de algumas ções para poder funcionar. Já o cliente WIFI , muitas vezes, sa de nenhuma configuração. Basta habilitar a antena e os s que rodam no dispositivo fazem o restante. Existem hoje no uma série de aplicativos que atuam junto com as interfaces dispositivos, ajudando no processo de auto-configuração. É o *Microsoft Zero Configuration Utility* (ZCF), que já é parte e dos Windows mais recentes. Mesmo assim, se algum o precisar ser manualmente especificado, basta acessar as ções WIFI de seu dispositivo e configurá-lo.

erificação do Funcionamento da WLAN

o passo para verificação de que a WLAN está operacional é a interface WIFI do dispositivo cliente encontra-se ativa e endereço IP (o endereço IP pode ser obtido automaticamente, e um servidor DHCP na rede, ou configurado manualmente, de como a rede se encontra configurada). Uma vez verificada , deve-se tentar o acesso a outros elementos de rede, como dor ou a Internet, se aplicável. Se o teste falhar, é preciso o problema em potencial:

- O AP encontra-se convenientemente instalado e configurado? Ex: verifique se o canal configurado no AP não se sobrepõe com o canal configurado em um AP vizinho.
- O AP encontra-se próximo a uma grande concentração de metais (um armário metálico, por exemplo)?
- O ambiente onde o AP foi instalado está sujeito às interferências externas (telefones sem-fio, forno de microondas ou qualquer outro elemento que possa interferir nas ondas de rádio do AP)?

3.10.4 C

Basicame
antena qu
802.11a, b
ou mesm
configura
não preci
aplicativo
mercado
WIFI dos
caso do
integrant
parâmetr
configura

3.10.5 V

O primeir
checar se
possui um
no caso d
depende
esta parte
um servic
identifica

- A área de cobertura do AP é ampla o suficiente para alcançar o dispositivo WIFI? Caso negativo, mais um AP pode ser necessário (habilitação do modo ESS de serviço).

Um modo de identificar problemas em redes WLAN é pegar um dispositivo móvel - como um laptop - e mover-se de um ponto próximo ao AP para um ponto mais distante. Desta forma, pode ser possível identificar pontos-cegos e outras anomalias. Isso pode ser chamado de um *site-survey* bem básico.

3.10.6 Segurança de Redes Wireless

Para encerrar o tópico de redes sem-fio, vamos analisar os aspectos de segurança inerentes a uma rede deste tipo. É importante entender que redes sem-fio introduzem uma série de vulnerabilidades que não existem em redes convencionais. Algumas destas vulnerabilidades permitem o acesso e o furto de informações críticas, ou mesmo que um invasor interrompa algum servidor crítico, causando prejuízos astronômicos para uma grande corporação. Por estas razões, é importante compreender quais os riscos e quais as medidas preventivas disponíveis para implementação.

Dentre as ameaças existentes, eis as que fazem parte do escopo do exame CCNA:

- **War drivers** - Normalmente, este tipo de ataque é impetrado por indivíduos que querem ter livre acesso à Internet. Eles atuam movendo-se com um laptop e uma antena WIFI em busca de um AP que não tenha esquemas de segurança habilitados para então ter acesso à rede;
- **Hackers** - A motivação por trás destes invasores é a obtenção de informações com algum valor, ou simplesmente, o terrorismo cibernético (derrubar servidores, etc). Redes sem-fio desprotegidas são a porta de entrada para a rede toda;
- **Funcionários** - Funcionários também podem consistir em uma ameaça, na medida em que podem inadvertidamente auxiliar os hackers a ganhar acesso à rede. Um exemplo seria um funcionário que adquire um AP de R$ 200,00 e o instala na rede da empresa sem informar ninguém;
- **Rogue AP** - Trata-se de um AP "clonado". O invasor captura frames emitidos pela rede WLAN e, analisando estes frames, consegue obter informações como SSID da rede e

as chaves de segurança criptografas (se em uso). Usando um método qualquer (como o de força bruta), eventualmente pode conseguir descriptografar as chaves e usar estas informações para configurar um AP "clone", externo, fazendo com que os usuários da rede WLAN o vejam como parte legítima da rede. Se um dispositivo de um funcionário se registrar neste AP "pirata", o funcionário pode digitar informações críticas que podem ser facilmente capturadas pelo invasor e utilizadas posteriormente para atacar a rede corporativa.

Para mitigar estes riscos, 3 tipos principais de ferramentas podem ser utilizadas em uma rede WLAN:

- **Autenticação mútua (*Mutual Authentication*)** - Este tipo de ferramenta deve ser utilizada entre o cliente e o AP. O processo de autenticação utiliza uma senha secreta, chamada de *key* (chave), que deve ser configurada tanto no cliente WIFI quanto no AP. Por meio do uso de sofisticados algoritmos, o AP é capaz de determinar se o cliente possui, de fato, conhecimento da chave em uso. Da mesma forma, o cliente faz essa checagem do seu lado, para certificar-se que o AP em uso é idôneo. O interessante deste processo é que a chave nunca é enviada de um lado ao outro, reduzindo as probabilidades de interceptação e ataque;
- **Criptografia (*Encryption*)** - Este método utiliza uma chave secreta e um algoritmo matemático para criptografar o conteúdo dos frames da rede WLAN. O cliente então utiliza um outro algoritmo para descriptografar o frame e processá-lo;
- **Ferramentas antiintrusão** - Esta categoria engloba uma série de ferramentas, as mais comuns sendo *Intrusion Detection Systems* (IDS) e *Intrusion Prevention Systems* (IPS), além de ferramentas específicas para redes WLAN. A Cisco define a arquitetura SWAN (*Structured Wireless-Aware Network*), que compreende uma série de ferramentas, algumas focando em riscos específicos, como a identificação "rogue APs".

A tabela apresentada na seqüência, resume as principais vulnerabilidades discutidas e as ações sugeridas para mitigar os riscos associados.

Vulnerabilidade	Solução
War drivers	Mecanismos eficientes de autenticação
Furto de informações via WLAN	Mecanismos eficientes de criptografia
Acesso externo a rede via WLAN	Mecanismos eficientes de autenticação
Instalação não-autorizada de APs	Aplicação de IDS / SWAN
AP Clonado (rogue AP)	Mecanismos eficientes de autenticação, IDS / SWAN

3.11 Padrões de Segurança WLAN

Os padrões de segurança WLAN vêm evoluindo conforme o tempo passa e a demanda por políticas de segurança mais rígidas aumenta. O padrão inicialmente proposto para implementação de segurança em WLANs, conhecido por *Wired Equivalent Privacy* (WEP) possuía uma série de problemas. Os outros 3 padrões discutidos neste tópico representam uma evolução dos padrões posteriormente criados para corrigir as falhas encontradas no WEP. A tabela apresentada a seguir ilustra a evolução destes padrões no tempo.

Padrão	Ano	Definido por
Wired Equivalent Privacy (WEP)	1997	IEEE
The interim Cisco solution while awaiting 802.11i	2001	Cisco, IEEE 802.1x Extensible Authentication Protocol (EAP)
Wi-Fi Protected Access (WPA)	2003	Wi-Fi Alliance
802.11i (WPA2)	2005+	IEEE

3.11.1 Wired Equivalent Privacy (WEP)

O WEP era o padrão de segurança adotado pelo 802.11 original, provendo serviços de criptografia e autenticação. O problema é que o WEP oferecia apenas métodos fracos de autenticação e criptografia, facilmente quebrados por invasores. Os principais problemas com o WEP são:

- **Static Preshared Keys (PSK)** - O valor da chave precisava ser configurado em cada cliente WIFI e cada AP, sem que existisse um método dinâmico de troca de chaves sem intervenção humana. Como resultado, a maioria das pessoas não se incomodava em trocar as chaves em intervalos regulares, principalmente nas empresas com número de elementos wireless elevado;

- **Chaves facilmente crackeadas** - O comprimento das chaves era pequeno (64 bits, sendo que destes, apenas 40 compunham a chave única). Isso facilitava a predição da chave, uma vez que uma cópia de um frame da rede fosse capturado. Somando-se isso ao fato de que as chaves raramente eram trocadas, os invasores tinham todo o tempo do mundo para tentar descobrir a chave e, finalmente, invadir a rede.

Algumas táticas foram criadas na tentativa de reduzir as vulnerabilidades identificadas no padrão WEP. Uma delas foi bloquear o *broadcast* do SSID pelo AP. Clientes WIFI necessitam de algumas informações do AP para poderem se conectar a ele. Uma destas informações é o SSID. Impedindo o AP de enviar esta informação livremente pelas ondas de rádio pode dificultar a vida de eventuais invasores. Este processo é conhecido como *SSID Cloaking*. Outra tática utilizada é o filtro de endereço MAC. Essencialmente, esta técnica consiste em definir, no AP, quais os endereços físicos (MAC) autorizados a comunicar-se com ele. Ambas as técnicas são válidas, mas não são suficientes para impedir um ataque real.

3.11.2 Cisco Interim Solution

Devido aos sérios problemas apresentados pelo WEP, a Cisco e outros fabricantes decidiram arregaçar as mangas e partir para o trabalho, criando soluções proprietárias. A solução da Cisco incluía algumas melhorias proprietárias no método de criptografia, além de incorporar o padrão IEEE 802.1x de autenticação. Eis as melhorias propostas pela Cisco em seu "padrão":

- *Dynamic Key Exchange* (ao invés de chaves estáticas);
- Autenticação (802.1x);
- Cada pacote era criptografado de forma diferente.

3.11.3 Wi-Fi Protected Access (WPA)

Logo após a Cisco criar seu método proprietário de segurança para redes sem-fio, uma organização chamada *Wi-Fi Alliance* estava para finalizar um novo padrão de segurança ao passo que o IEEE estava trabalhando no padrão 802.11i. O mercado, entretanto, demandava uma solução rápida, não havia tempo para esperar a publicação do padrão IEEE, um processo normalmente burocrático e moroso. Assim sendo, o grupo de trabalho *Wi-Fi Alliance* pegou o que já havia sido

feito pelo IEEE para o padrão 802.11i, fez algumas suposições, e criou um padrão "de fato", que foi batizado de WPA.

O padrão WPA, essencialmente, faz o mesmo que a solução proprietária criada pela Cisco, mas com algumas nuances. WPA inclui a opção de utilizar a troca dinâmica de chaves utilizando um protocolo chamado TKIP (*Temporal Key Integrity Protocol*). O WPA também incorpora a autenticação via 802.1x, porém, permite também a autenticação utilizando PSK (*preshared keys*). Não é muita diferença, se formos analisar friamente. A diferença REAL entre o WPA e a solução Cisco é que o WPA é um padrão de mercado, podendo ser aplicado em diversos dispositivos, de diversos fabricantes, enquanto que a solução Cisco é proprietária. A solução Cisco e o WPA não são compatíveis.

3.11.4 IEEE 802.11i e WPA-2

Em 2005 o IEEE finalmente publicou o padrão 802.11i. Seguindo as mesmas linhas do WPA e da solução proposta pela Cisco, o padrão 802.11i também implementava esquemas mais rígidos de criptografia, troca dinâmica de chaves e autenticação. Entretanto, estes padrões não são compatíveis entre si. Um dos avanços alcançados pelo 802.11i em relação a solução proposta pela Cisco e ao WPA foi a inclusão do padrão AES (*Advanced Encryption Standard*). O padrão AES provê um método ainda mais seguro de criptografia, com chaves mais extensas e algoritmos de criptografia mais robustos.

A tabela apresentada a seguir apresenta um comparativo entre as diversas soluções comentadas.

Standard	Key Distribution	Device Authentication	User Authentication	Encryption
WEP	Static	Yes (weak)	None	Yes (weak)
Cisco	Dynamic	Yes	Yes (802.1x)	Yes (TKIP)
WPA	Both	Yes	Yes (802.1x)	Yes (TKIP)
802.11i (WPA2)	Both	Yes	Yes (802.1x)	Yes (AES)

Questões de Revisão – Redes Sem-fio

1. Qual é a taxa máxima de transmissão estipulada para o padrão WIFI IEEE 802.11b?

a) 2Mbps b) 10Mbps
c) 11Mbps d) 54Mbps

2. Qual das seguintes alternativas lista os canais de freqüência não sobrepostos existentes quando se utiliza 802.1b DSSS?

a) 1,2,3 b) 1,5,9 c) 1,6,11
d) a,b,g e) 22,33,44

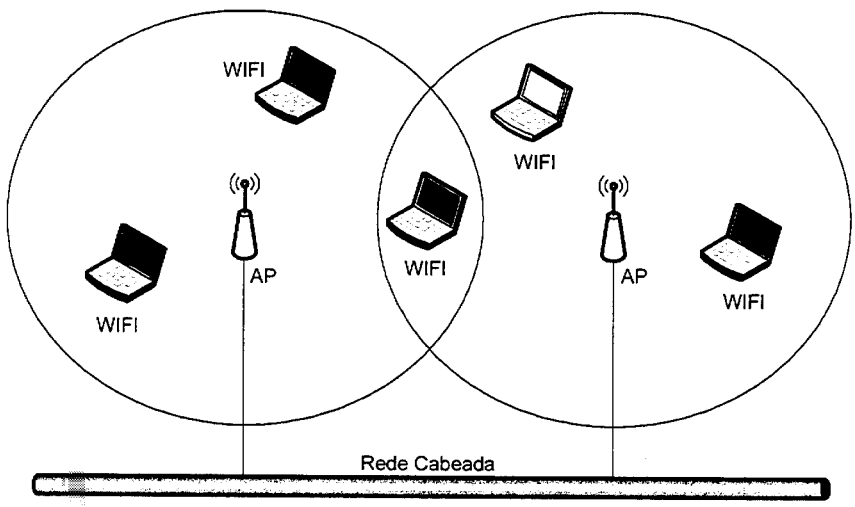
3. Qual dos seguintes serviços permite que um usuário com laptop mova-se entre diferentes APs sem perder a conectividade ou ter seu IP alterado?

a) ESS b) DSSS c) BSS
d) IBSS e) Roaming

4. Um único AP 802.11g foi configurado e instalado no centro de uma sala quadrada. Alguns usuários estão reclamando de performance baixa enquanto outros operam em máxima velocidade. Quais as possíveis causas deste problema (selecione 3)?

a) Criptografia TKIP incompatível.
b) Valor do SSID nulo.
c) Telefones sem-fio nas imediações.
d) Valores de SSID diferentes.
e) Armários de metal.
f) Tipo de antena e direção.

5. Observe o diagrama. O que pode ser concluído?



a) A área de intersecção é chamada de BSS.
b) O diagrama representa uma rede em modo ESS.
c) Os APs em cada célula devem ser configurados para utilizar o canal 1.
d) A área de intersecção deve ser menos de 10% da área para evitar interferências.
e) Os 2 APs devem ser configurados para operar em canais distintos.

6. Qual a tecnologia *spread spectrum* definida pelo padrão IEEE 802.11b?

a) DSSS b) IR c) ESS
d) FHSS e) OFDM

7. Qual o padrão de segurança WLAN criado pelo *Wi-Fi Alliance*?

a) WEP b) WAP c) WPE
d) WPA e) Cisco

8. E qual camada do modelo OSI um *Access Point* (AP) pode ser definido?

a) Física b) Enlace c) Rede
d) Transporte e) Aplicação

Respostas das Questões de Revisão – Redes Sem-fio

1. C

2. C

3. A - A rede formada por 2 ou mais APs interligados à uma mesma rede física (e lógica, no caso de haver VLANs) é chamada *Extended Service Set,* e permite a mobilidade (*roaming)* de usuários de uma célula para outra, sem interrupção do serviço. Para que isso ocorra, os APs devem trabalhar em canais não-sobrepostos.

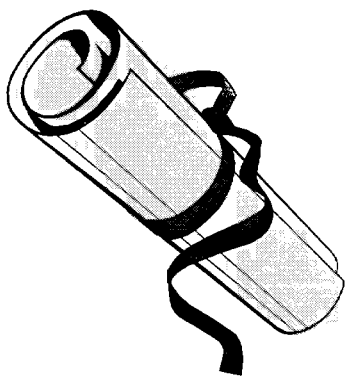
4. C, E, F - Telefones sem-fio e superfícies metálicas são causas freqüentes de interferência em uma rede WLAN. Estes fatores, aliados ao tipo de antena utilizada, influenciam diretamente no tamanho da área de cobertura e qualidade do sinal.

5. B, E

6. A

7. D

8. B



4 Switching e VLANs

4.1 Tópicos Abordados

- Comutação na Camada de Enlace (*Layer-2 Switching*);
- O Processo de Aprendizagem de Endereços (*Address Learning Process*);
- Decisões de Encaminhamento/Filtragem;
- Esquemas de Inibição de Loops (*Loop Avoidance Schemes*);
- Protocolo *Spanning Tree* (STP);
- Tipos de Comutação LAN.

4.2 Comutação na Camada de Enlace

A comutação (*switching*) na camada de Enlace é baseada no endereço de hardware, o que significa que o endereço MAC da placa de rede do dispositivo é utilizado para filtragem da rede. Switches utilizam chips especiais, chamados "ASICs", para formar e manter as tabelas de filtragem (*filter tables*).

Switches são rápidos porque não analisam informações pertinentes à camada de Rede, analisando, em seu lugar, os endereços de hardware dos frames (também chamados de endereços MAC) antes de decidir pelo encaminhamento ou abandono deles. O que torna a comutação na camada de Enlace tão eficiente é a não-modificação no pacote de dados, apenas no frame que o encapsula. Como nenhuma modificação

no pacote é realizada, o processo de comutação é muito mais rápido e menos suscetível a erros do que o processo de roteamento.

A comutação na camada de Enlace pode ser utilizada para conectividade entre grupos de trabalho e para a segmentação da rede (quebra dos domínios de colisão). Ela aumenta a largura de banda disponível para cada usuário, uma vez que cada conexão (interface) disponibilizada pelo switch representa seu próprio domínio de colisão. Devido a esse fator, podem-se conectar múltiplos dispositivos em cada interface.

A comutação na camada de Enlace, entretanto, possui algumas limitações. O modo correto de se criar redes comutadas eficientes é certificando-se que os usuários permanecerão ao menos 80% do seu tempo no segmento local. Redes comutadas quebram domínios de colisão, entretanto, a rede ainda é um grande domínio de *broadcast*, o que pode limitar o tamanho da rede, assim como causar problemas de performance. *Broadcasts* e *multicasts*, juntamente com a vagarosa convergência do protocolo *Spanning Tree* (falaremos dele mais adiante) podem vir a ser problemas sérios à medida que a rede cresce. Devido a esses (e outros) fatores, switches de camada 2 não podem substituir completamente os routers (dispositivos de camada 3) em uma internetwork.

Bridges e switches são definidos na mesma camada (Enlace). Existem, porém, algumas importantes diferenças entre esses dois dispositivos que devem ser lembradas:

- O processamento das bridges é baseado em software, enquanto os switches têm seu processamento baseado em hardware (ASICs);
- Bridges podem ter apenas uma ocorrência de *Spanning Tree* por bridge, enquanto switches podem ter várias;
- Bridges podem ter até 16 portas, enquanto switches, pelo fato de possuírem hardware dedicado, podem ter centenas.

As três principais funções de um switch na camada de Enlace são:

1. **Aprendizagem de endereços**: Switches e bridges registram o endereço do hardware transmissor de cada frame recebido em determinada porta (interface) e adiciona essa informação à tabela MAC;
2. **Decisões de filtragem/encaminhamento**: Assim que um frame é recebido em uma porta do switch, este verifica o endereço do hardware de destino e identifica a interface de saída através de checagem na tabela MAC;

3. **Esquema de inibição de loops**: Se múltiplas conexões forem criadas entre switches visando redundância, loops de rede podem ocorrer. O protocolo *Spanning Tree* (STP) é usado para evitar que loops de rede ocorram, permitindo assim a criação de links redundantes (o protocolo STP age bloqueando as portas redundantes, evitando a ocorrência de loops de camada 2).

Os principais pontos a saber sobre switches são:

- Processo de comutação baseado em hardware;
- Velocidade de transmissão limitada ao meio (*wire speed transmission*);
- Baixa latência/espera (*low latency*);
- Baixo custo;
- Alta eficiência.

4.2.1 Processo de Aprendizagem de Endereços

Todo switch forma uma tabela - chamada "tabela MAC" - que mapeia os endereços de hardware (*MAC addresses*) dos dispositivos às portas (interfaces) às quais eles se encontram conectados. Assim que um switch é ligado, essa tabela encontra-se vazia. Quando um dispositivo inicia uma transmissão e uma porta (interface) do switch recebe um frame, o switch armazena o endereço de hardware do dispositivo transmissor em sua tabela MAC, registrando a interface à qual esse dispositivo está conectado. Num primeiro momento, o switch não tem outra opção a não ser "inundar" a rede com esse frame, uma vez que ele ainda não possui em sua tabela MAC o registro da localização do dispositivo destinatário. Esse tipo de transmissão é conhecido como *broadcast*. Se um determinado dispositivo responder a essa mensagem de *broadcast* enviando um frame de volta, o switch irá, então, capturar o endereço de hardware (MAC) desse dispositivo e registrá-lo em sua tabela MAC, associando o endereço MAC desse dispositivo à interface (porta) que recebeu o frame.

O switch tem agora dois endereços em sua tabela MAC, podendo assim estabelecer uma conexão ponto a ponto entre os dois dispositivos. Isso significa que os frames pertencentes a essa transmissão serão encaminhados apenas aos dois dispositivos participantes. Nenhuma outra porta do switch irá receber os frames, a não ser as duas portas mapeadas. É essa a grande diferença entre switches e hubs. Em uma rede composta por hubs, frames são encaminhados a todas as portas, o tempo todo, criando um grande domínio de colisão.

Se os dois dispositivos não se comunicarem com o switch novamente por um determinado período de tempo, este irá deletar os endereços de sua tabela MAC, mantendo-a assim o mais atualizada possível.

Para ilustrar o processo, vamos supor que, em uma rede composta por seis estações de trabalho interligadas por um switch, a estação 1 queira se comunicar com a estação 6. A figura 4.1 ilustra como ocorre essa comunicação uma vez que a tabela MAC já se encontre formada. O valor imediatamente abaixo de cada estação seria o correspondente ao respectivo endereço MAC gravado na sua placa de rede (NIC). Cada estação encontra-se conectada a uma porta do switch (e0, e1, e2, e3, e4, e5). A figura também ilustra o formato de uma tabela MAC formada para a rede em questão.

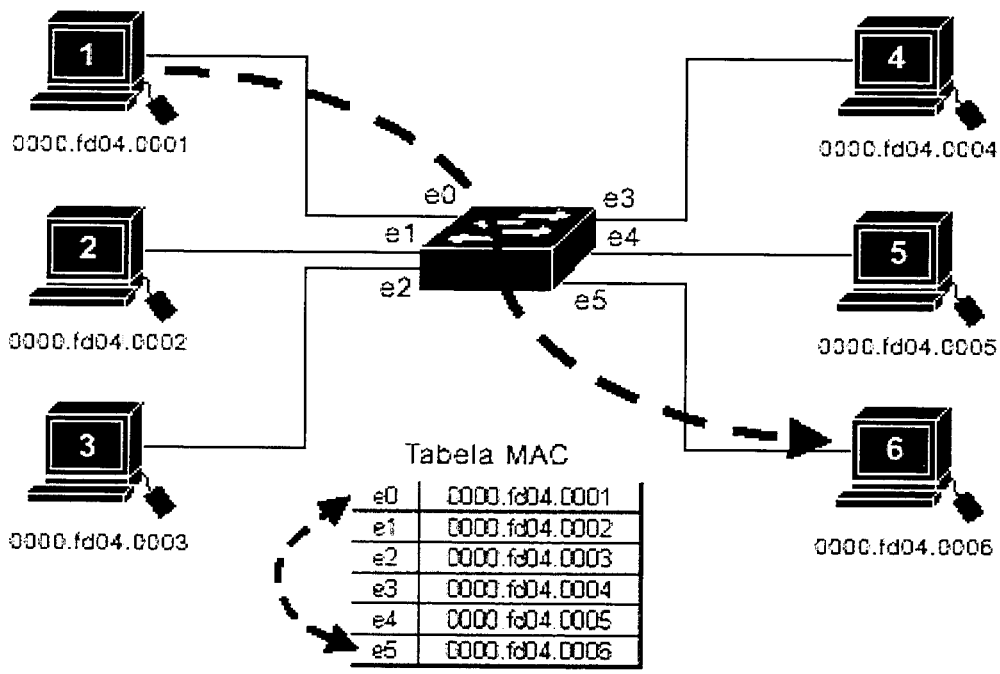


Figura 4.1: A comunicação em uma rede comutada.

4.2.2 Processos de Encaminhamento e Filtragem

Assim que um frame chega à interface de um switch, o endereço do hardware de destino é comparado com a tabela MAC. Se o endereço de destino for conhecido e estiver presente na tabela, o frame será encaminhado apenas para a porta de saída associada àquele endereço.

O switch não transmite o frame para todas as interfaces, apenas para a interface de destino. Esse processo, conhecido como filtragem de frames (*frame filtering*), preserva a largura de banda de outros segmentos da rede.

Se o endereço do hardware de destino, entretanto, não estiver listado na tabela MAC do switch, o frame é, então, propagado para todas as

interfaces ativas (*broadcasting*), com exceção da interface na qual ele foi recebido. Se um dispositivo responder a essa transmissão, a tabela MAC é atualizada com a localização desse dispositivo (interface).

4.2.3 Esquemas de Inibição de Loops

O estabelecimento de conexões (links) redundantes é sempre uma boa idéia entre switches. Redundância, nesse caso, é usada para evitar a completa queda da rede no caso da falha de um link.

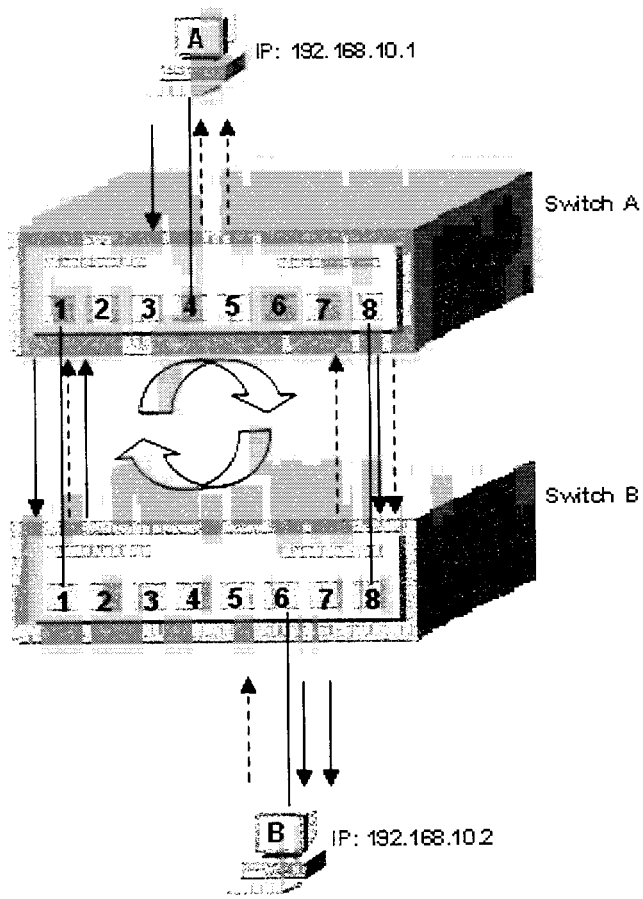


Figura 4.2: Loops na rede ocasionados por links redundantes.

Embora a redundância em links possa ser extremamente útil, ela pode trazer mais problemas do que resolvê-los. Uma vez que frames podem ser propagados através de todos os links redundantes simultaneamente, um fenômeno chamado *loop* pode ocorrer, além de outros problemas, como:

- Caso nenhum esquema de inibição de loops de rede seja implantado, os switches poderão propagar frames continuamente na rede. Esse fenômeno é conhecido como "tempestade de broadcast" (*broadcast storm*). A figura 4.2 ilustra como uma mensagem de *broadcast* pode ser continuamente propagada pela rede;

- Aumento das chances de um dispositivo receber múltiplas cópias de um mesmo frame, uma vez que esse frame pode chegar de diferentes segmentos simultaneamente;
- A tabela MAC ficará confusa sobre a localização (interface) de um determinado dispositivo, uma vez que o switch pode receber determinado frame de mais de um link. Pode ocorrer de o switch não encaminhar o frame, uma vez que estará constantemente atualizando sua tabela MAC com a localização do hardware transmissor. Esse fenômeno é conhecido como *trashing* da tabela MAC;
- Um dos maiores problemas é a geração de múltiplos loops, ou seja, um loop dentro de outro. Se uma tempestade de *broadcast* então ocorrer, o switch ficará sem condições de desempenhar a comutação de pacotes, literalmente "travando" a rede.

4.2.3.1 A Solução: O Protocolo Spanning Tree (STP)

A extinta DEC (*Digital Equipment Corporation*) foi a criadora original do protocolo *Spanning Tree*. O IEEE homologou posteriormente sua própria versão do protocolo, denominada IEEE 802.1d. Os switches Cisco utilizam a versão IEEE do protocolo *Spanning Tree*, que não é compatível com a versão original da DEC.

O papel principal do STP é evitar que loops de rede ocorram em redes de camada de Enlace. O STP monitora constantemente a rede identificando todos os links em atividade e certificando-se que loops de rede não ocorram, através da desativação de links redundantes. O modo como o protocolo STP faz isso é "elegendo" um switch-raiz (*root bridge*) responsável pela definição de toda a topologia da rede.

Em uma rede, apenas um switch-raiz pode existir. Todas as interfaces ou portas do switch-raiz são denominadas "portas designadas" (*designated ports*) e encontram-se sempre no modo de operação denominado "modo de encaminhamento" (*forwarding-state*). Interfaces operando em modo de encaminhamento podem tanto enviar quanto receber dados.

Os outros switches presentes na rede são denominados não-raiz (*non-root bridges*). No caso desses switches, a porta com "menor custo" (determinada pela largura de banda do link em questão) ao switch-raiz é chamada de "porta-raiz" (*root-port*) e também se encontrará em modo de encaminhamento, podendo enviar e receber dados. As portas restantes com menor custo ao switch-raiz serão denominadas "portas

designadas". Se em uma rede com diversos switches o custo de duas (ou mais) portas for o mesmo, o ID do switch deverá ser usado e será considerada designada a porta referente ao switch com o menor ID. As portas restantes serão consideradas portas não-designadas. Estas se encontrarão em modo bloqueio (*blocking mode*), não podendo enviar ou receber dados.

4.2.3.1.1 Como Determinar o Switch-Raiz

Switches e bridges rodando STP trocam informações através do que chamamos de *Bridge Protocol Data Units* (BPDUs). BPDUs enviam mensagens de configuração via *frames multicast*. O ID (identificador) de cada switch é enviado aos outros dispositivos através das BPDUs. O ID do switch é utilizado na determinação do switch-raiz da rede e também da porta-raiz. Esse ID tem um comprimento de 8 bytes, e inclui o valor de prioridade (*priority value*) e o endereço de hardware (MAC address) do dispositivo. O valor de prioridade default para todos os dispositivos rodando a versão IEEE do STP é 32.768 (lembre-se disso!).

Para determinar o switch-raiz, os valores de prioridade e os endereços de hardware são combinados. Se dois switches têm o mesmo valor de prioridade (o que é muito comum), então o endereço de hardware será utilizado para a definição do switch-raiz, que será aquele com o ID mais baixo.

ID mais baixo.

r exemplo, vamos supor dois switches: A e B. O switch A tem o de prioridade default (32.768) e o endereço de hardware f11.aab2.1111. O switch B, por sua vez, também tem o valor de dade default (32.768), porém, seu endereço de hardware é f11.aab2.1112. Pelas regras anteriormente descritas, o switch A nesse caso, definido como switch-raiz, pois seu ID (que é o ado da combinação: prioridade + MAC) é menor que o do switch ab2.1111 < ... aab2.1112).

.2 Determinação da Porta Designada

e determinar a(s) porta(s) que será(ão) usada(s) para comunicação switch-raiz, você precisa definir, antes, o "custo" do link tado à porta em questão. O protocolo STP faz isso se baseando gura de banda disponível para cada link.

.3 Modos de Operação das Portas de um Switch

rtas de um switch ou bridge rodando STP podem variar entre modos:

com o

Po
valor
0000.0
priori
0000.0
seria,
resulta
B (...a

4.2.3.1

Para s
com o
conect
na lar

4.2.3.1

As po
quatro

- **Blocking**: Não encaminhará frames. Pode receber e analisar BPDUs. Todas as portas de um switch encontram-se em modo *blocking* quando ele é ligado;
- **Listening**: Recebe e analisa BPDUs para certificar-se de que não ocorrerão loops na rede antes de começar o encaminhamento de frames;
- **Learning**: Registra os endereços dos hardwares conectados às interfaces e forma a tabela MAC. Não encaminha frames, ainda;
- **Forwarding**: Envia e recebe frames.

Tipicamente, switches se encontram ou no modo *blocking* ou no modo *forwarding*. Uma porta em modo *forwarding* é tida como tendo o menor custo ao switch-raiz. Entretanto, se a topologia da rede se alterar (devido a uma falha em um link, à adição de outro switch pelo administrador de rede etc.) todas as portas conectadas em redundância de um switch retornarão aos modos *listening* e *learning*.

O modo *blocking* é usado para impedir o acontecimento de loops de rede. Uma vez que o switch determina o melhor caminho (porta) ao switch-raiz, todas as outras portas entrarão em modo *blocking*. Portas em modo *blocking* podem receber BPDUs. Se um switch por algum motivo determinar que uma porta em modo *blocking* deve tornar-se uma porta designada, ela entrará em modo *listening*, analisando todas as BPDUs recebidas para certificar-se de que não criará um loop uma vez que entre em modo *forwarding*.

4.2.3.2 Definição de Convergência

Convergência ocorre quando switches encerram a alternância desde o modo *blocking* até o modo *forwarding*. Não há transmissão de dados durante o processo de convergência. O processo é muito importante, pois assegura que as tabelas MAC de todos os switches da rede sejam consistentes. Antes de dados serem encaminhados, as tabelas MAC de todos os switches devem ser atualizadas. O grande problema inerente ao processo de convergência é o tempo consumido - em média, 50 segundos para ir do modo *blocking* ao modo *forwarding*. Esse timer pode ser alterado, se necessário, embora não seja recomendado.

4.2.3.3 Exemplo de Funcionamento do Protocolo Spanning Tree

É importante entender claramente como o protocolo STP funciona em uma rede. A figura 4.3 ilustra uma situação onde os dois switches

encontram-se conectados a dois segmentos de rede, formando links redundantes. Note que os valores de prioridade para ambos são os mesmos (32.768). Porém, observe os endereços de hardware. Analisando-os determinaremos o switch-raiz.

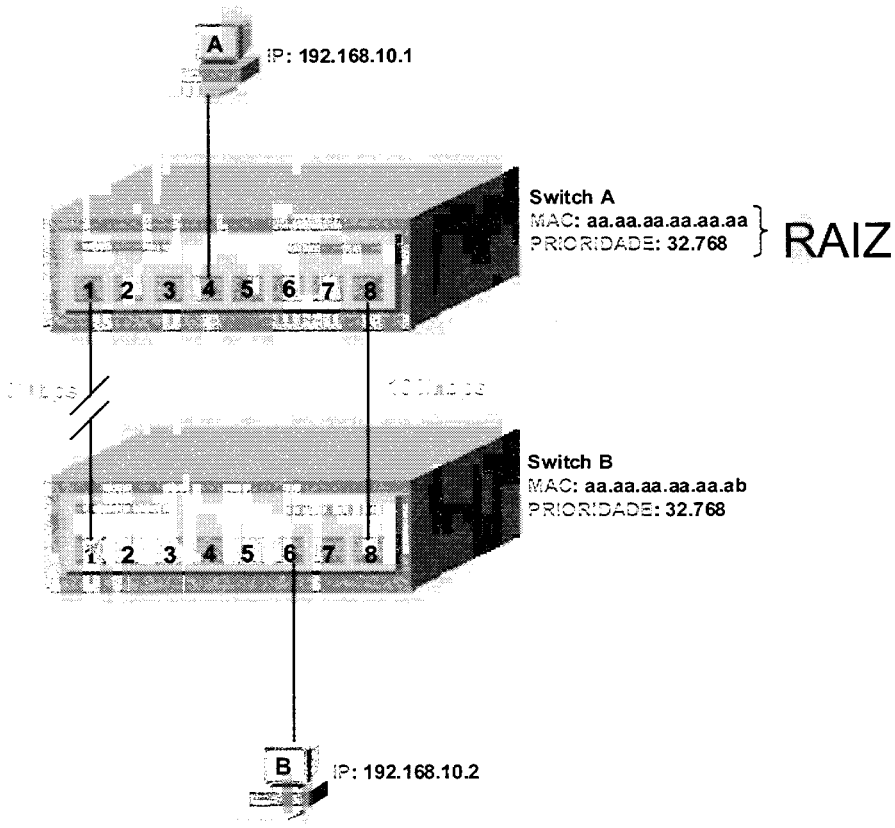


Figura 4.3: Exemplo do protocolo Spanning Tree em ação.

Como o switch A possui o endereço de hardware mais baixo (...aa), ele será o switch-raiz. Para a determinação da porta-raiz, precisaremos analisar o custo dos links que chegam a cada porta do switch B. Uma vez que o custo da porta 8 é menor (100BaseT < 10BaseT), esta será a porta-raiz.

Passemos à determinação das portas designadas. Lembre-se: o switch-raiz sempre tem todas as suas portas designadas, portanto, ambas as portas do switch-raiz serão denominadas "portas designadas". Como as duas portas do switch A já foram devidamente classificadas, a porta 1 do switch B será considerada não-designada e, como tal, o switch B a colocará em modo *blocking*, evitando assim que qualquer loop de rede venha a ocorrer.

E se as duas portas do exemplo anterior tivessem o mesmo custo (por exemplo, ambas operassem a 100 Mbps)? Qual delas seria bloqueada? Nesse caso, o *spanning tree* adota o bloqueio da porta de maior número (a porta 8 seria bloqueada já que 8 > 1). Observe o exemplo da figura 4.4, para compreender ainda melhor este mecanismo.

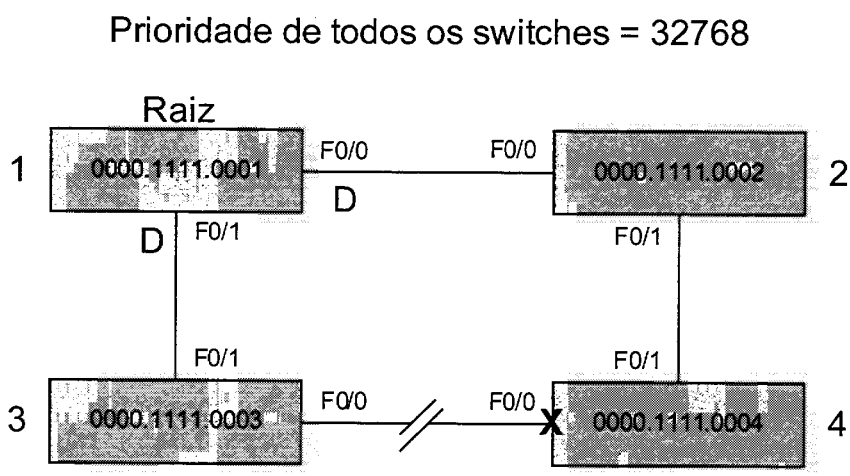


Figura 4.4: Mais um exemplo do protocolo Spanning Tree em ação.

Neste exemplo, o switch "1" foi eleito a raiz da rede, já que ele possui o menor *Bridge ID* (como a prioridade de todos os switches é igual, o desempate é feito pelo MAC, e no caso, o MAC do switch "1" é o menor da rede). Resta saber qual porta será bloqueada para interromper o loop, e em qual switch. Observando o diagrama, o switch "4" é o que apresenta o maior endereço de hardware (MAC). Por este motivo, uma de suas duas portas ativas será colocada em modo *blocking*. Como ambas possuem a mesma largura de banda, outros elementos devem ser considerados na decisão. No caso, o custo para o switch raiz (Switch 1) seria o mesmo, tanto pela porta F0/0 quanto pela porta F0/1. Assim sendo, o STP opta pelo caminho que passa pelo switch com o menor MAC (o switch 2, no caso). Ou seja, a porta F0/0 seria a porta bloqueada. Seguindo o diagrama, a porta F0/0 do switch "4" é a porta-raiz deste switch, já que é o caminho mais curto para o switch raiz (na verdade, o único caminho). No switch "3", a porta F0/0 é uma porta designada, enquanto a porta F0/1 é a porta raiz e, finalmente, no switch "2", a porta F0/0 é a porta raiz, enquanto a porta F0/1 é uma porta designada.

4.2.4 Tipos de Comutação

A latência envolvida na comutação de um frame em um switch depende do modo de comutação (*switching mode*) configurado nele. Existem, basicamente, três tipos de comutação:

- **Store and forward**: Este é o único método suportado nos modelos mais novos da linha Catalyst (como o 2960, 3560, 3750, por exemplo). Como o nome sugere - armazene e encaminhe -, esse modo de comutação faz com que o frame seja, em um primeiro momento, completamente recebido e armazenado no buffer do switch. Em seguida, uma

checagem de erros (CRC - *Cyclic Redundant Check*) é efetuada e, finalmente, o endereço de destino é localizado na tabela MAC. Como o frame é primeiramente copiado para o buffer do switch, para apenas depois ser encaminhado, a latência desse modo é a maior dos três. O frame é descartado caso um erro seja detectado na checagem, caso seja muito curto (menos de 64 bytes, incluindo o campo CRC) ou muito longo (mais de 1518 bytes, incluindo o campo CRC). Caso não sejam identificados erros, o endereço do hardware destino é localizado na tabela MAC e a porta de saída é identificada (supondo que o endereço exista na tabela). Somente então o frame é encaminhado ao seu destino;

- **Cut-through (tempo real)**: Esse é o modo predominante quando se fala em comutação LAN. Nesse modo, o switch copia apenas o endereço de destino (os primeiros 7 bytes seguindo o campo *Preamble*) para seu buffer. Logo após, o endereço do hardware de destino é localizado na tabela MAC, a interface de saída é determinada e o frame é encaminhado ao seu destino. Esse modo provê baixa latência, pois o encaminhamento do frame começa assim que o endereço de destino é identificado e a interface de saída determinada;
- **FragmentFree (cut-through modificado)**: Esse modo é uma modificação do *cut-through*, pois aguarda a passagem da janela de colisão (*collision window* - 64 bytes) antes de encaminhar o pacote. Seu funcionamento é assim, pois se considera a alta probabilidade de que, se um frame possui algum erro, este será identificado nos 64 bytes iniciais. Portanto, o modo *FragmentFree* promove uma checagem de erros mais confiável, acrescentando muito pouco à latência do processo.

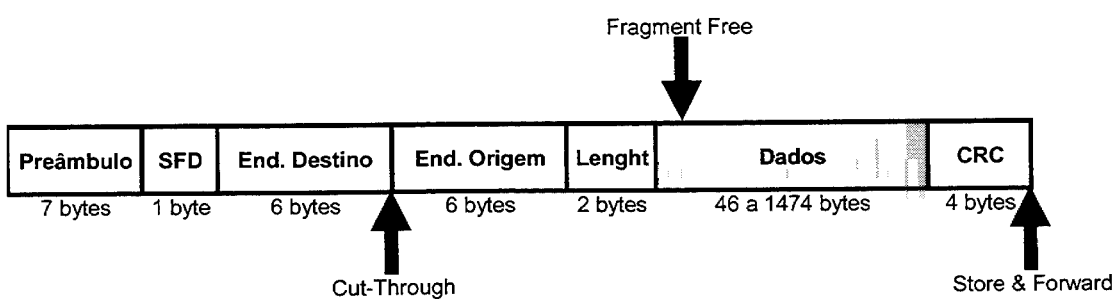


Figura 4.5: Ponto de resposta (em um frame) para cada um dos modos de comutação.

4.2.5 Spanning Tree PortFast

Imagine que você tenha um servidor ou qualquer outro dispositivo que você tenha 100% de certeza que não criará um loop de camada 2 em sua rede se conectado a um switch. Neste caso, é vantajoso informar ao switch que esta porta específica (onde o dispositivo se conecta) não precisa participar do processo de convergência. *PortFast* faz exatamente isso em um switch Cisco.

Trata-se de um comando que pode ser usado APENAS em portas de acesso (a definição de portas de acesso encontra-se no próximo tópico: VLANs) e que, quando habilitado, exclui as portas configuradas do processo de convergência do *spanning tree*, ou seja, estas portas ficam ativas imediatamente.

Esta funcionalidade, entretanto, deve ser usada com cuidado, já que ela desabilita o STP nas portas configuradas e pode, eventualmente, causar um loop de camada 2 caso não seja implementada com o devido conhecimento.

4.2.6 Spanning Tree UplinkFast

Este é outro recurso, em linha com o que foi apresentado anteriormente. O comando *UplinkFast*, entretanto, é direcionado a uplinks, ou seja, conexões entre switches. O *UplinkFast*, assim como o *PortFast*, deve ser usado com extrema cautela, e apenas quando se tem um caminho redundante para o switch raiz, ou seja, o comando deve apenas ser configurado em portas no modo *blocked*.

Basicamente, este recurso permite ao switch encontrar um caminho alternativo para o switch raiz ANTES que o link ativo venha a falhar. Isso significa que, caso o link primário falhe, o link secundário (que encontrava-se bloqueado pelo STP) será ativado bem mais rapidamente. O recurso *UplinkFast* normalmente é utilizado em switches de acesso.

4.2.7 Spanning Tree BackboneFast

Temos ainda mais um recurso para agilizar o processo de convergência de uma rede comutada que rode STP: *BackboneFast*. Diferentemente do *UplinkFast*, que é voltado para uplinks em switches de acesso, o *BackboneFast* deve ser aplicado em todos os switches da rede. Sua função é determinar inconsistências na topologia.

Apesar de não se encontrar habilitado por default nos switches Cisco, este recurso é benéfico já que pode economizar até 20 segundos no processo de convergência de uma rede STP, quando ativado.

4.2.8 Rapid Spanning Tree Protocol (802.1w)

O protocolo *Rapid Spanning Tree* (RSTP) é uma versão melhorada do protocolo STP que vimos (802.1d), mas que incorpora todas as melhorias anteriormente mencionadas (*PortFast, UplinkFast, BackboneFast*). Na verdade, a Cisco criou estas 3 funcionalidades para amenizar as limitações impostas pelo protocolo STP tradicional. O problema é que estas funcionalidades apenas funcionam em switches Cisco. O *Rapid Spanning Tree* é uma resposta do IEEE, ou seja, funciona em switches de qualquer fabricante. Resumindo, basta ativar o RSTP e você terá todos os recursos anteriormente mencionados funcionando de forma coesa, reduzindo de forma gritante o tempo de convergência em uma rede comutada.

4.2.9 EtherChannel

Etherchannel é uma forma de agrupar links redundantes de forma a criar um canal virtual cuja banda equivaleria a soma da banda dos links que o compõem. Por exemplo, ao se agrupar (*bundle*) 2 links de 100Mbps, temos um canal virtual de 200Mbps. A vantagem de utilizar esta tecnologia é que podemos ter links redundantes sem que um ou mais deles fiquem ociosos (em modo *blocked*), melhorando a performance da rede e, por tabela, o tempo de convergência. Existe a versão Cisco do *EtherChannel*, chamada de *Port Agregation Protocol* (PAgP), e a versão do IEEE (802.3d), chamada de *Link Agregation Control Protocol* (LACP). Ambas operam de forma semelhante, mas suas configurações nos switches é diferente. Trataremos da configuração dos switches mais adiante.

4.3 Virtual LANs (VLANs)

Em uma rede comutada, a rede é plana (*flat*), ou seja, todos os pacotes *broadcast* transmitidos são "enxergados" por todos os dispositivos conectados à rede, mesmo que um dispositivo não seja o destinatário de tais pacotes.

Uma vez que o processo de comutação na camada 2 segrega domínios de colisão, criando segmentos individuais para cada dispositivo conectado ao switch, as restrições relacionadas à distância impostas pelo padrão Ethernet são reduzidas, significando que redes geograficamente maiores podem ser construídas. Quanto maior o número de usuários e dispositivos, maior o volume de *broadcasts* e pacotes que cada dispositivo tem de processar transitando na rede.

Outro problema inerente às redes comutadas é a segurança, uma vez que todos os usuários "enxergam" todos os dispositivos.

Com a criação de VLANs, você pode resolver uma boa parte dos problemas associados à comutação na camada 2. Eis algumas das razões para se criar LANs Virtuais (VLANs):

- Redução do tamanho e aumento do número de domínios de *broadcast*;

Nota: *Perceba que, apesar de o tamanho dos domínios de broadcast ser reduzido, seu número aumenta. Isso é lógico se você lembrar que antes do uso VLANs tínhamos apenas um grande domínio de broadcast. Conforme VLANs vão sendo criadas, o número de domínios broadcast aumenta, porém o tamanho de cada novo domínio é menor que o domínio original (redução no tamanho).*

- Agrupamento lógico de usuários e de recursos conectados em portas administrativamente definidas no switch;
- VLANs podem ser organizadas por localidade, função, departamento etc., independentemente da localização física dos recursos;
- Melhor gerenciabilidade e aumento de segurança da rede local (LAN);
- Flexibilidade e escalabilidade.

4.3.1 Redução do Tamanho dos Domínios de Broadcast

Os routers, por definição, mantêm as mensagens de broadcast dentro da rede que os originou. Switches, por outro lado, propagam mensagens de broadcast para todos os seus segmentos. Por esse motivo, chamamos uma rede comutada de "plana", porque se trata de um grande domínio de broadcast.

Um bom administrador de redes deve certificar-se de que a rede esteja devidamente segmentada para evitar que problemas em um determinado segmento se propaguem para toda a rede. A maneira mais eficaz de se conseguir isso é através da combinação entre comutação e roteamento (*switching* e *routing*). Uma vez que o custo dos switches vem caindo, é uma tendência real que empresas substituam redes baseadas em hubs por redes baseadas em switches. Em uma VLAN, todos os dispositivos são membros do mesmo domínio de *broadcast*. As mensagens de *broadcast*, por default, são barradas de todas as portas em um switch que não sejam membros da mesma VLAN.

Routers devem ser usados em conjunto com switches para que se estabeleça a comunicação entre VLANs, o que impede que mensagens de broadcast sejam propagadas por toda a rede.

4.3.2 Melhor Gerenciabilidade e Aumento de Segurança da Rede Local (LAN)

Um dos grandes problemas com redes planas é que o nível mais alto de segurança é implementado através dos routers. A segurança é gerenciada e mantida pelo router, porém qualquer um que se conecte localmente à rede tem acesso aos recursos disponíveis naquela VLAN específica. Outro problema é que qualquer um pode conectar um analisador de rede em um hub e, assim, ter acesso a todo tráfego daquele segmento de rede. Ainda outro problema é que usuários podem se associar a um determinado grupo de trabalho simplesmente conectando suas estações ou laptops a um hub existente, ocasionando um certo "caos" na rede.

Por meio da criação de VLANs, os administradores adquirem o controle sobre cada porta e cada usuário. O administrador controla cada porta e quais recursos serão alocados a ela. Os switches podem ser configurados para informar uma estação gerenciadora da rede sobre qualquer tentativa de acesso a recursos não-autorizados. Se a comunicação inter-VLANs é necessária, restrições em um router podem ser implementadas. Restrições também podem ser impostas a endereços de hardware (MAC), protocolos e a aplicações.

Switches convencionais apenas analisam frames para filtragem, não chegam a analisar qualquer informação de camada de Rede. Isso pode ocasionar a propagação de *broadcasts* pelo switch. Ao se criar VLANs, entretanto, você está criando domínios de *broadcast*, ou seja, está segmentando sua rede local. Uma mensagem de *broadcast* enviada por um dispositivo membro de uma VLAN "x" não será propagada para portas do switch associadas a uma VLAN "y". Ao associar portas em um switch ou grupo de switches conectados entre si (*switch fabric*) a determinadas VLANs, você tem a flexibilidade de adicionar apenas os usuários desejados ao domínio de *broadcast* criado, independentemente de sua localização física. Isso pode evitar fenômenos onerosos para a rede, como as "tempestades de broadcast".

Quando uma VLAN torna-se muito volumosa, mais VLANs podem ser criadas para evitar que mensagens de *broadcast* consumam uma largura de banda excessiva. Quanto menor o número de usuários em uma VLAN, menor o domínio de *broadcast* criado.

4.3.2.1 Comunicação Inter-VLANS

Para que a comunicação na camada 3 entre os dispositivos aconteça, todos os dispositivos conectado à uma mesma VLAN devem estar inseridos em uma mesma rede IP. É importante ressaltar que é parte integrante de um bom projeto de redes colocar cada VLAN em uma rede IP diferente, pois desta forma, a comunicação inter-VLANs torna-se possível. Se duas VLANs distintas forem colocadas em uma mesma rede IP, a comunicação entre elas jamais será possível. Agindo da forma correta, cada VLAN fará parte de uma rede IP diferente e, desta forma, um router poderá permitir a comunicação inter-VLANs roteando os pacotes entre as diferentes redes IP. Observe a figura 4.6.

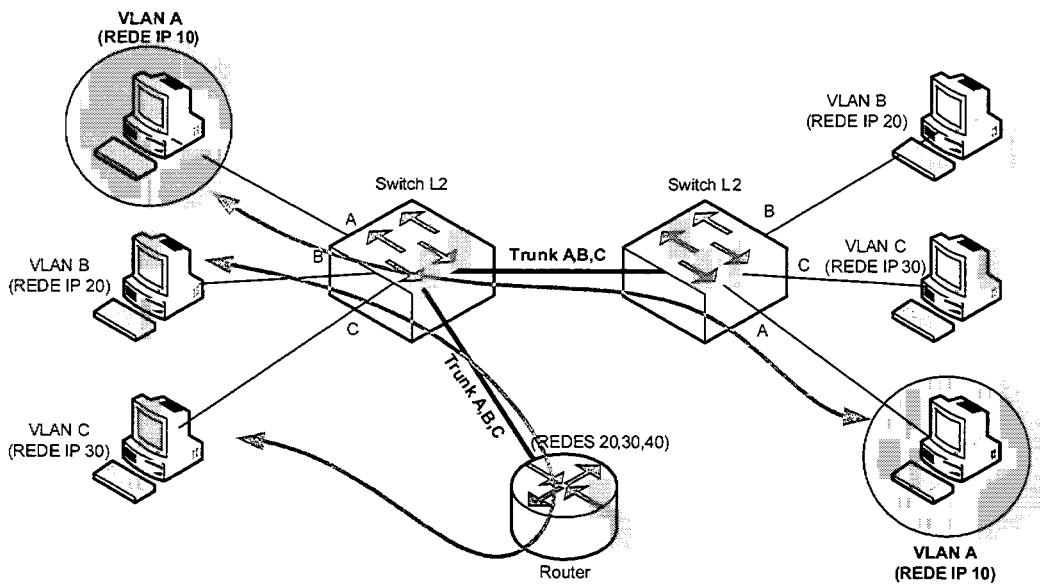


Figura 4.6: Comunicação inter-VLANs por intermédio de um router.

Neste exemplo, as 3 VLANs apresentadas são conectadas a um router por meio de uma conexão especial chamada *trunk* (trunks, como veremos mais adiante, são responsáveis pelo transporte de frames contendo a identificação sobre qual VLAN pertencem), possibilitando a comunicação inter-VLAN.

Switches possibilitam uma flexibilidade e escalabilidade maior que routers. Por meio da utilização de switches você pode agrupar usuários por grupos de interesse, que são conhecidos como VLANs organizacionais. Ainda assim, switches não podem substituir routers. Na figura 4.7, temos 3 VLANs. Os dispositivos membros de determinada VLAN podem se comunicar com outros da mesma VLAN sem problemas. Para se comunicarem com dispositivos de outra VLAN, porém, é necessária a implementação de um router. Quando associados a uma determinada VLAN, os dispositivos entendem que, de fato, fazem parte de um "backbone colapsado". Resumindo, a comunicação inter-

VLANs deve ser feita por intermédio de um router ou outro dispositivo que atue na camada 3. A figura 4.7 apresenta uma outra alternativa para a comunicação inter-VLANs, que é a utilização de switches layer-3, ou seja, switches que também possuem a habilidade de rotear pacotes IP. No exemplo, apenas o switch da esquerda possui esta capacidade.

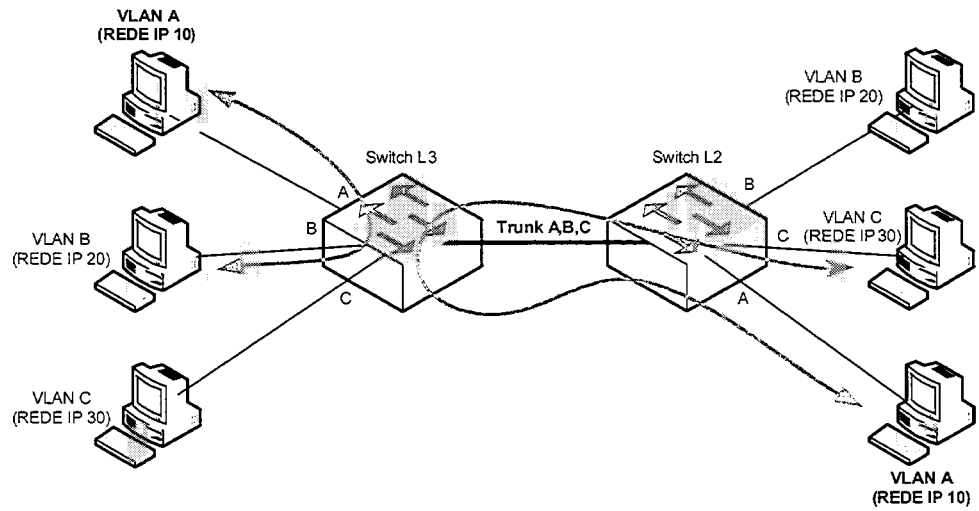


Figura 4.7: Comunicação inter-VLANs por intermédio de um switch L3.

4.3.3 Tipos de Associações VLAN

VLANs são, tipicamente, criadas por um administrador de redes, que designa determinadas portas de um switch para uma determinada VLAN. Essas são chamadas VLANs estáticas. Caso o administrador inclua todos os endereços de hardware dos dispositivos da rede em um banco de dados específico, os switches podem ser configurados para designar VLANs dinamicamente.

4.3.3.1 Associação Estática

O modo mais comum e seguro de se criar uma VLAN é estaticamente. A porta do switch designada para manter a associação com uma determinada VLAN fará isso até que um administrador mude a sua designação. Esse método de criação de VLANs é fácil de implementar e monitorar, funcionando muito bem em ambientes onde o movimento de usuários dentro de uma determinada rede é controlado.

4.3.3.2 Associação Dinâmica

VLANs dinâmicas determinam a designação de uma VLAN para um dispositivo automaticamente. Através do uso de softwares específicos de gerenciamento, é possível o mapeamento de endereços de hardware (MAC), protocolos e até mesmo aplicações ou logins de usuários para

VLANs específicas. Por exemplo, suponha que os endereços de hardware dos laptops de uma rede tenham sido incluídos em uma aplicação que centraliza o gerenciamento de VLANs. Se um host é então conectado à porta de um switch que não tenha uma VLAN associada, o software gerenciador procurará pelos endereços de hardware armazenados e, então, associará e configurará a porta do switch para a VLAN correta (mapeamento MAC x VLAN). Se um usuário muda de lugar, o switch poderá associar automaticamente a VLAN correta para ele, onde quer que esteja. Embora este método simplifique muito a vida do administrador uma vez que o banco de dados MAC x VLAN esteja formado, um esforço considerável é exigido inicialmente, na criação do mesmo.

4.3.4 Identificação de VLANs

VLANs podem se espalhar por uma "malha" de switches interconectados. Os switches desse emaranhado devem ser capazes de identificar os frames e as respectivas VLANs às quais estes pertencem. Para isso foi criado o recurso *frame tagging* (ao pé da letra, "etiquetamento de frames" - utilizaremos o termo "identificação de frames", no entanto). Utilizando o recurso de identificação de frames, os switches podem direcionar os frames para as portas apropriadas.

Existem dois diferentes tipos de link em um ambiente comutado:

- **Links de acesso (*access links*):** Links que são apenas parte de uma VLAN e são tidos como a VLAN nativa da porta. Qualquer dispositivo conectado a uma porta ou link de acesso não sabe a qual VLAN pertence. Ele apenas assumirá que é parte de um domínio de *broadcast*, sem entender a real topologia da rede. Os switches removem qualquer informação referente às VLANs dos frames antes de enviá-los a um link de acesso. Dispositivos conectados a links de acesso não podem se comunicar com dispositivos fora de sua própria VLAN, a não ser que um router faça o roteamento dos pacotes;
- **Links de Transporte (*trunk links*):** Também denominados *uplinks*, podem carregar informações sobre múltiplas VLANs, sendo usados para conectar switches a outros switches, routers ou mesmo a servidores[1]. Links de Transporte são suportados em Fast ou Gigabit Ethernet

[1] Desde que sua interface suporte o protocolo ISL ou 802.1q.

somente (é importante lembrar-se desta característica: links de transporte não são suportados em 10BaseT Ethernet). Para identificar a VLAN à qual um determinado frame Ethernet pertence, os switches Cisco suportam duas diferentes técnicas: ISL (*Inter-Switch Link Protocol*) e 802.1q. Links de Transporte são utilizados para transportar VLANs entre dispositivos e podem ser configurados para transportar todas as VLANs ou somente algumas. Links de Transporte ainda possuem uma VLAN nativa (*default* - VLAN1), que é utilizada para gerenciamento e em caso de falhas.

O processo de "entroncamento" de links permite que você torne uma única interface (ou porta) de um switch ou servidor parte de múltiplas VLANs simultaneamente. O benefício disso é que um servidor, por exemplo, pode ser membro de duas ou mais VLANs de forma concomitante, o que evita que usuários de VLANs diferentes tenham de atravessar um router para poder ter acesso aos recursos desse servidor. O "entroncamento" de portas é bastante comum na conexão entre switches (uplinks), já que os links de transporte podem transportar informações sobre algumas ou todas as VLANs existentes através de apenas um link físico. Caso os links entre switches (uplinks) não sejam entroncados, apenas informações sobre a VLAN 1 (chamada VLAN *default*) serão transportadas através do link. Ao se criar uma porta transporte (*trunk port*), informações sobre todas as VLANs são transportadas através dela, por default. VLANs indesejadas devem ser manualmente excluídas do link para que suas informações não sejam propagadas através dele.

4.3.5 Frame Tagging

Um switch conectado a uma rede de grande porte necessita fazer um acompanhamento dos usuários e frames que atravessam o aglomerado de switches e VLANs. Uma "malha" de switches (também conhecida como *switch fabric*) é um grupo de switches que compartilham as mesmas informações de VLAN. O processo de identificação de frames (*frame tagging*) associa, de forma única, uma identificação a cada frame. Essa identificação é conhecida como *VLAN ID* ou *VLAN color*.

A tecnologia de *frame tagging* foi criada pela Cisco para ser utilizada quando um frame Ethernet atravessasse um link de transporte (*trunked link*). A identificação (*tag*) da VLAN é removida do frame antes que ele deixe o link de transporte, tornando o processo totalmente transparente. Cada switch que o frame atravessa deve identificar o ID (tag) da VLAN

a que ele pertence e, então, determinar o que fazer com ele baseado na tabela de filtragem (*filter table*). Caso o frame alcance um switch que possua outro link de transporte, ele será encaminhado através da porta onde esse link se encontra. Uma vez que o frame alcance uma porta para um link de acesso, o switch remove a identificação da VLAN. O dispositivo final receberá os frames sem ter de entender à qual VLAN eles pertencem, garantindo a transparência do processo.

4.3.6 Métodos de Identificação de VLANs

Para o exame CCNA, o conhecimento de dois métodos de identificação de VLANs é importante. São eles: Cisco ISL (*Inter-Switch Link*) e IEEE 802.1q. Cada um desses métodos de identificação deve ser entendido como um tipo de encapsulamento diferente.

- **ISL (*Inter-Switch Link*)**: Exclusivo aos switches Cisco, o encapsulamento ISL pode ser utilizado em links *Fast* e *Gigabit Ethernet*, somente. Pode ser aplicado às interfaces de switches, de routers e de servidores, para seu "entroncamento". O "entroncamento" de interfaces de servidores é muito útil se você estiver criando VLANs funcionais e não quiser quebrar a regra 80/20 (80% do tráfego a ser mantido localmente). O servidor que é truncado é membro de todas as VLANs (domínios de broadcast) simultaneamente, o que significa que os usuários não precisam atravessar um dispositivo de camada 3 (ex.: um router) para ter acesso a ele, reduzindo a complexidade e aumentando a performance da rede.

O método ISL literalmente encapsula frames Ethernet com informações sobre VLANs. Essa informação, adicionada ao encapsulamento do frame, permite a multiplexação de VLANs (transmissão de múltiplas VLANs) por meio de apenas um link de transporte. Através do uso do ISL, é possível a interconexão de múltiplos switches, mantendo a segregação das informações sobre cada VLAN conforme dados trafegam pela "malha" de switches, pelos Links de Transporte.

Entre as vantagens do ISL estão a baixa latência e a velocidade limitada ao meio físico (*wire speed*) em uso. Lembre-se que o ISL é um método externo de identificação, ou seja, o frame original não é alterado, sendo apenas encapsulado por um cabeçalho ISL cujo comprimento é de 26 bytes. Uma vez que o frame é encapsulado, apenas dispositivos (ou interfaces) compatíveis com ISL estarão habilitados a decodificá-

lo. Outro detalhe importante: o frame encapsulado pode ter um comprimento de até 1548 bytes. Dispositivos não compatíveis que venham a receber um frame ISL podem entender este como um frame de comprimento anormal, uma vez que ele ultrapassa o tamanho máximo definido pelo padrão Ethernet, que seria de 1518 bytes.

Ao ser encaminhado a uma porta de transporte (*trunk link*), cada frame é encapsulado com a informação da respectiva VLAN. Interfaces de rede compatíveis com ISL permitem aos servidores enviar e receber frames gerados por diferentes VLANs. Desse modo, dispositivos de múltiplas VLANs podem acessar um mesmo servidor sem a necessidade de atravessar um dispositivo de camada 3, como um router.

É importante entender que o encapsulamento ISL apenas ocorre se o frame for encaminhado a uma porta de transporte (*trunk link*). O encapsulamento ISL é removido do frame caso este seja encaminhado a uma porta de acesso.

- **IEEE 802.1q**: Criado pelo IEEE (Instituto de Engenheiros Elétricos e Eletrônicos) para ser um método padrão para a identificação de frames, esse método insere um campo específico dentro do frame, responsável pela identificação da VLAN. Para estabelecimento de Links de Transporte entre switches Cisco e switches de outro fabricante, esse é o método a ser utilizado (é de extrema importância lembrar-se dessa definição). É interessante ressaltar que os switches mais novos da Cisco não suportam mais o encapsulamento ISL, suportando apenas o IEEE 802.1q. Isso mostra uma tendência da Cisco em abandonar o ISL em um futuro bastante próximo.

4.3.7 Roteamento entre VLANs

Já falamos um pouco sobre isso. Dispositivos dentro de uma mesma VLAN encontram-se dentro do mesmo domínio de *broadcast* e podem se comunicar sem problemas. VLANs segmentam a rede, criando diferentes domínios de *broadcast*. Para que dispositivos em diferentes VLANs se comuniquem, é necessário, o uso de um dispositivo de camada 3, como um router ou um switch L3.

Um router com uma interface para cada VLAN pode ser usado ou, simplesmente, um router que suporte ISL ou 802.1q. No caso de apenas algumas VLANs (duas ou três), um router com duas ou três interfaces Ethernet já seria o suficiente. Entretanto, no caso de termos mais VLANs

do que interfaces disponíveis, o roteamento ISL ou 802.1q em uma única interface *FastEthernet* pode ser adotado. Uma interface FastEthernet com encapsulamento ISL ou 802.1q habilitado é conhecida pelo termo *router-on-a-stick*. Como vimos, outro meio de implementar o roteamento inter-VLANs é o uso de um switch Layer-3, como os das linha 3560 e 3750, da Cisco. Switches L3 implementam a pilha de protocolos TCP/IP, não ficando restritos à camada 2 do modelo OSI. Em resumo, switches L3 são capazes de rotear pacotes IP.

4.3.8 O Protocolo VTP (Virtual Trunk Protocol)

A Cisco criou o *Virtual Trunk Protocol* para gerenciar e manter a consistência de todas as VLANs configuradas em uma rede.

Para permitir que o protocolo VTP gerencie as VLANs existentes na rede, é necessário, antes, a criação de um servidor VTP. Todos os servidores que necessitem compartilhar informações sobre VLANs devem utilizar a mesma identificação de domínio, e um switch pode se encontrar em apenas um domínio a cada vez. Isso significa que um switch pode compartilhar informações do domínio VTP apenas com switches configurados dentro do mesmo domínio VTP. Informações VTP são enviadas entre switches através das portas de transporte (*trunk ports*).

Switches propagam diversas informações gerenciais do domínio VTP a que pertencem, como o número de revisão da configuração (*configuration revision number*) e todas as VLANs conhecidas, acompanhadas de parâmetros específicos. Switches podem ser configurados para encaminharem informações VTP, mas para não permitirem que seus bancos de dados VTP sofram atualizações ou mesmo para ignorarem informações sobre atualizações. Isso é chamado de Modo VTP Transparente (*VTP Transparent Mode*).

Senhas podem ser criadas objetivando um maior controle do domínio VTP criado. Todos os switches pertencentes a um mesmo domínio, no entanto, devem ser configurados com a mesma senha, o que pode tornar o processo um tanto quanto complexo.

Switches detectam VLANs adicionais durante uma atualização VTP e se preparam para receber em suas portas de transporte informações sobre as novas VLANs detectadas. As atualizações propagadas possuem números de revisão (*revision numbers*). Quando um switch identifica um número de revisão mais alto, ele sabe que a atualização a ser recebida encontra-se mais atualizada, sobrescrevendo seu banco de dados com as informações contidas nela.

Entre as principais vantagens de se utilizar o sistema VTP, citamos as seguintes:

- Permite que administradores adicionem, deletem e renomeiem VLANs, sendo essas alterações automaticamente propagadas para todos os switches pertencentes ao domínio VTP;
- Provê configuração de VLAN consistente entre todos os switches pertencentes a um mesmo domínio;
- Permite que VLANs sejam truncadas através de redes mistas, como Ethernet para ATM LANE ou FDDI;
- Mantém um controle e monitoramento acurados sobre VLANs;
- Dinamicamente reporta VLANs adicionadas para todos os switches pertencentes ao domínio;
- Permite a adição *plug-and-play* de VLANs.

4.3.8.1 Modos de Operação VTP

Uma vez inseridos em um domínio VTP, switches podem ser configurados para interagir com as atualizações VTP propagadas de três formas distintas (figura 4.8):

1. **Server (servidor)**: Modo default para todos os switches da linha Catalyst. É necessário ao menos um servidor em um domínio VTP para propagação de informações sobre VLANs através dele. O switch deve se encontrar em modo servidor (*server mode*) para ser capaz de criar, adicionar ou deletar VLANs em um domínio VTP. A mudança de informações VTP também deve ser efetuada em modo servidor. Qualquer alteração sofrida por um switch em modo servidor é propagada para todo o domínio VTP;
2. **Client (cliente)**: No modo cliente, switches recebem informações de servidores VTP e enviam e recebem atualizações, mas não podem efetuar mudanças. Nenhuma porta em um switch no modo cliente pode ser associada a uma nova VLAN antes de o servidor VTP notificar o switch cliente da existência dessa nova VLAN. Dica: antes de habilitar um switch como servidor, configure-o como cliente. Dessa forma, ele receberá todas as informações corretas sobre VLANs. Uma vez atualizado, habilite-o como servidor;

3. **Transparent (transparente)**: Um switch configurado no modo transparente não participa do domínio VTP, mas ainda assim encaminha atualizações VTP através dos links configurados. Switches VTP transparentes podem adicionar ou deletar VLANs, uma vez que o switch mantém sua própria base de dados e não a compartilha com outros. Esse modo é considerado significante apenas localmente, já que alterações realizadas não são propagadas para nenhum domínio VTP.

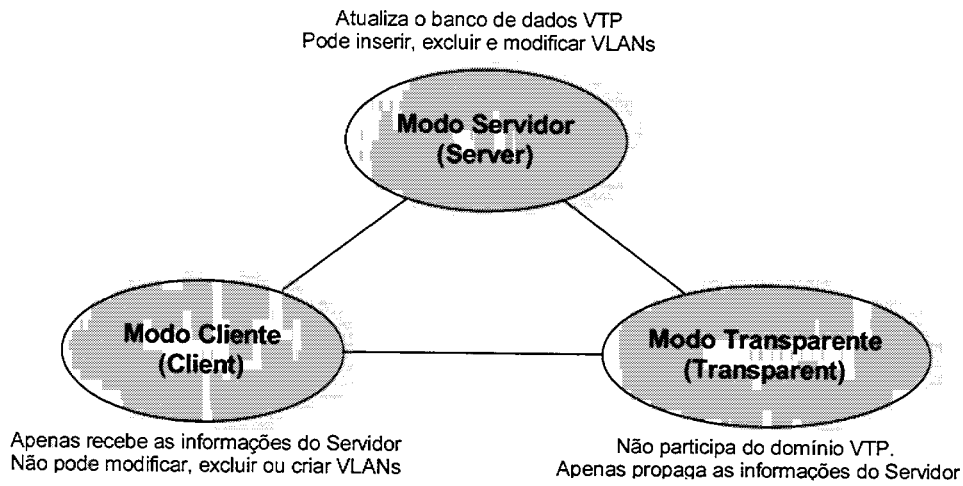


Figura 4.8: Modos de operação VTP.

4.3.8.2 VTP Pruning

Você pode conservar a largura de banda configurando o VTP para reduzir o volume de *broadcasts* (propagações de atualizações). Esse procedimento é conhecido como *pruning* (poda). O processo de *VTP pruning* realiza a propagação de atualizações apenas para links de transporte que de fato necessitem de tal informação. Qualquer link de transporte que não necessite da informação sendo propagada não a receberá. Por exemplo, se um switch não tiver nenhuma porta associada à VLAN 12 e uma mensagem de *broadcast* for enviada através dessa VLAN, ela não atravessará o link de transporte até esse switch. Por default, *VTP pruning* encontra-se desabilitado em todos os switches Cisco.

***Importante**: Quando o VTP pruning é habilitado em um servidor VTP, todo o domínio torna-se habilitado para o processo. Por default, as VLANs de número 2 até 1005 são elegíveis para implementação do processo de pruning. Pruning nunca pode ser implementado na VLAN 1, por ser considerada a VLAN administrativa.*

Questões de Revisão – Switching

1. Qual método de comutação executa um CRC em cada frame antes de encaminhá-lo à porta de saída?

a) Cut-through
b) Store and forward
c) FragmentCheck
d) FragmentFree

2. Qual método de comutação verifica somente o endereço de hardware destino no cabeçalho do frame, antes de encaminhá-lo à porta de saída?

a) Cut-through
b) Store and forward
c) FragmentCheck
d) FragmentFree

3. Quais das afirmações a seguir são verdadeiras a respeito do modo blocking de uma porta em um switch rodando o protocolo STP?

a) Nenhum frame é transmitido ou recebido nessa porta.
b) BPDUs são enviados e recebidos na porta bloqueada.
c) BPDUs continuam sendo recebidos na porta bloqueada.
d) Frames são enviados e recebidos na porta bloqueada.

4. O uso de switches de camada 2 provê qual das seguintes vantagens?

a) Comutação baseada em hardware (ASICs)
b) Alta performance
c) Alta latência
d) Alto custo

5. Quais informações são usadas para determinação do switch-raiz em uma rede comutada?

a) Prioridade
b) Custo dos links conectados ao switch
c) Endereço MAC
d) Endereço IP

6. Quais informações são usadas para determinação da porta designada em um switch rodando o protocolo STP?

a) Prioridade
b) Custo dos links ligados ao switch
c) Número da porta
d) Endereço IP

7. Quais são os quatro estados possíveis de uma porta em um switch rodando o protocolo STP?

a) Learning
b) Learned
c) Listened
d) Heard
e) Listening
f) Forwarding
g) Forwarded
h) Blocking
i) Gathering

8. Quais são as três funções básicas de um switch de camada 2?
   a) Aprendizagem dos endereços
   b) Roteamento
   c) Encaminhamento e filtragem
   d) Criação de loops de rede
   e) Inibição de loops
   f) Endereçamento IP

9. Qual afirmação a seguir é verdadeira a respeito dos BPDUs?
   a) São usados para o envio de mensagens de configuração usando broadcasts IP.
   b) São usados para o envio de mensagens de configuração usando multicast.
   c) São usados para definir o custo dos links STP.
   d) São usados para definir o Bridge ID de um switch.

10. Suponha que um switch determinasse que uma porta que se encontrava no modo blocking deve agora ser a porta designada. Qual seria o estado dessa porta, na seqüência?
   a) Unblocked
   b) Forwarding
   c) Listening
   d) Listened
   e) Learning
   f) Learned

11. Quais as diferenças básicas entre uma bridge e um switch de camada 2?
   a) Bridges podem ter somente uma ocorrência de spanning tree por unidade.
   b) Switches podem ter várias ocorrências de spanning tree por unidade.
   c) Bridges podem ter várias ocorrências de spanning tree por unidade.
   d) Switches podem ter somente uma ocorrência de spanning tree por unidade.

12. Quais das afirmações a seguir são verdadeiras?
   a) Switches realizam a comutação de frames via software.
   b) Bridges realizam a comutação de frames via hardware.
   c) Switches realizam a comutação de frames via hardware.
   d) Bridges realizam a comutação de frames via software.

13. O que um switch faz quando um frame é recebido por uma de suas interfaces e o endereço do hardware de destino é desconhecido ou não se encontra em sua tabela de filtragem?

a) Encaminha o frame para o primeiro link disponível.
b) Descarta o frame.
c) Envia um frame broadcast para a rede à procura do dispositivo destino.
d) Envia uma mensagem para o dispositivo origem pedindo a resolução para o nome.

14. Qual tipo de comutação espera por uma janela de colisão antes de examinar o endereço do hardware destinatário na tabela de filtragem MAC e encaminhar o frame para a porta de saída?

a) Cut-through
b) Store and forward
c) FragmentCheck
d) FragmentFree

15. Qual o único tipo de comutação disponível nos novos switches Catalyst, como o 2960

a) Cut-through
b) Store and forward
c) FragmentCheck
d) FragmentFree

16. Como o bridge ID de um switch é transmitido aos switches vizinhos?

a) Via roteamento IP.
b) Através do protocolo STP.
c) Durante os quatro estados de convergência STP, um multicast IP é enviado à rede.
d) Através dos Bridge Protocol Data Units (BPDUs).
e) Via broadcasts durante o processo de convergência.

17. Como a porta-raiz de um switch é determinada?

a) O link com custo mais alto ao switch-raiz torna-se a porta-raiz.
b) O link com custo mais baixo ao switch-raiz torna-se a porta-raiz.
c) A interface que atingir a transferência de BPDUs à taxa mais alta é eleita a porta raiz.
d) O switch-raiz propaga o bridge ID e o switch receptor determinará em qual porta esse broadcast foi recebido, tornando-a a porta-raiz.

18. Quantos switches-raiz são permitidos em uma mesma rede comutada?

a) 10
b) 1
c) Um para cada switch
d) 20

19. O que pode acontecer em uma rede se nenhum esquema de inibição de loops for adotado?

a) Menor tempo de convergência
b) Tempestades de Broadcast
c) Múltiplas cópias de frames
d) Nada ocorrerá

20. Qual o valor da prioridade STP default em um switch Cisco?

a) 32768 c) 100 e) 1
b) 3276 d) 10

Respostas das Questões de Revisão – Switching

1. **B**. O método *store-and-forward* verifica cada frame contra erros de CRC. Possui a mais alta latência dos tipos de comutação disponíveis.

2. **A**. O método *Cut-through* não faz checagem de erros e tem a mais baixa latência dentre os tipos de comutação disponíveis. Esse método apenas verifica o endereço do hardware destinatário e encaminha o frame.

3. **A, C**. BPDUs são recebidos em portas bloqueadas, mas o encaminhamento de frames e BPDUs nelas não é permitido.

4. **A, B**. Switches de camada 2 usam ASICs na filtragem de frames e realizam o processo de comutação via hardware. Switches de camada 2 também provêem velocidade de transferência limitada unicamente ao meio, resultando em baixa latência.

5. **A, C**. Dispositivos de camada 2 rodando STP usam prioridade e o endereço MAC para determinar o switch-raiz da rede.

6. **B, C**. Para switches determinarem portas designadas, o custo de cada link ligado ao switch é usado. Se houver empate nos custos, a porta com menor número é a eleita.

7. **A, E, F, H**. Os quatro estados são *blocking, learning, listening* e *forwarding*.

8. **A, C, E**. São características de switches na camada 2.

9. B. BPDUs são usados para enviar mensagens de configuração para switches vizinhos, incluindo nelas os bridge IDs.

10. **C**. Uma porta quando sai do modo *blocking* sempre passará pelo modo *listening* para certificar-se de que, assim que a porta mudar seu estado para *forwarding*, loops não ocorrerão.

11. **A, B**. Diferentemente de uma bridge, um switch pode ter várias ocorrências diferentes de *spanning tree* por switch. Bridges podem ter apenas uma.

12. **C, D**. Bridges realizam o processo de comutação baseado em software, enquanto switches o fazem via hardware (devido aos ASICs).

13. **C**. Switches encaminham todos os frames com endereço destinatário desconhecido via broadcast para a rede. Se um dispositivo responder ao frame, o switch atualiza sua tabela de endereços MAC para armazenar a localização do dispositivo, evitando assim um broadcast na próxima comunicação com ele.

14. **D**. O método *FragmentFree* analisa os primeiros 64 bytes do frame (também chamado de "janela de colisão") para certificar-se da inexistência de uma colisão. Esse método também é conhecido como *modified cut-through*.

15. **B**. Por default, switches catalyst mais recentes suportam apenas o método Store-and-Forward de comutação.

16. **D**. O bridge ID é enviado através de um frame multicast, dentro de uma atualização BPDU.

17. **B**. Portas-raiz são determinadas usando-se o custo do link ao switch-raiz.

18. **B**. Somente um switch-raiz pode existir em uma mesma rede comutada.

19. **B, C**. Tempestades de broadcast e múltiplas cópias de frames são tipicamente encontradas em redes com múltiplos links para sites remotos, que não adotem nenhum esquema para inibição de loops (como o STP).

20. **A**. A prioridade default em todos switches que rodem STP é 32768.

Questões de Revisão – VLANs

1. Qual das afirmações a seguir é correta com relação às VLANs?

   a) Você deve ter ao menos duas VLANs definidas em qualquer rede comutada Cisco.

   b) Todas as VLANs são configuradas no switch mais rápido que, por default, propaga essas informações a todos os outros switches da rede.

   c) Você não pode ter mais de 10 switches num mesmo domínio VTP.

   d) O protocolo VTP é usado para enviar informações sobre VLANs para switches que pertençam ao mesmo domínio VTP.

2. Quais são os dois modos em que um administrador pode configurar associações VLAN?

a) Através de um servidor DHCP
b) Estaticamente
c) Dinamicamente
d) Através de um banco de dados VTP

3. Qual o tamanho máximo de um frame Ethernet encapsulado pelo frame ISL?

a) 1518
b) 1548
c) 4202
d) 8190

4. Como VLANs dinâmicas podem ser configuradas?

a) Estaticamente
b) Por um administrador
c) Através de um servidor DHCP
d) Através de um Servidor Gerenciador de Políticas VLAN (VMPS)

5. Quais dos seguintes protocolos são usados em links de transporte?

a) Virtual Trunk Protocol
b) VLAN
c) Trunk
d) ISL
e) IEEE 802.1q

6. Quais das seguintes afirmações são verdadeiras com relação ao VTP pruning?

a) VTP pruning encontra-se ativado por default em todos switches Cisco.
b) VTP pruning encontra-se desativado por default em todos switches Cisco.
c) Você apenas pode ativar VTP pruning em switches da linha 4000 ou superior.
d) VTP pruning é habilitado em todos switches, desde que seja ativado em um switch configurado como servidor VTP.

7. Qual o padrão Cisco que encapsula um frame Ethernet, adicionando campo FCS?

a) ISL
b) 802.1q
c) 802.3z
d) 802.3u

8. Qual o efeito de se configurar VTP para modo transparente?

a) O modo transparente apenas encaminha mensagens e atualizações, não as adicionando à sua base de dados.

b) O modo transparente tanto encaminha mensagens e atualizações como também os adiciona à sua base de dados.
c) O modo transparente não encaminha mensagens e atualizações.
d) O modo transparente torna um switch dinamicamente seguro.

9. VTP oferece quais dos seguintes benefícios para uma rede comutada?

a) Cria múltiplos domínios de broadcast na VLAN 1.
b) Permite o gerenciamento centralizado de VLANs.
c) Ajuda a manter a consistência na configuração de VLANs através de todos os switches pertencentes à rede.
d) Permite o entroncamento de VLANs através de redes mistas, como Ethernet para ATM LANE ou FDDI.
e) Oferece o rastreamento e monitoramento preciso das VLANs.
f) Permite a propagação dinâmica das VLANs criadas em um switch configurado em modo servidor para todos switches.
g) Permite a adição *Plug and Play* de VLANs.

10. Qual das seguintes afirmações é verdadeira sobre VTP?

a) Todos switches Cisco operam como servidores VTP, por default.
b) Todos switches Cisco operam no modo VTP transparente, por default.
c) VTP encontra-se ativado por default, com um nome de domínio "Cisco", em todos switches Cisco.
d) Todos switches Cisco operam no modo VTP cliente por default.

11. Qual das seguintes afirmações é verdadeira com relação aos links de transporte?

a) Todas as portas de um switch são links de transporte, por default.
b) Funcionam apenas em redes Ethernet.
c) Você pode configurar links de transporte em portas de qualquer velocidade, seja 10, 100 ou 1000Mbps.
d) Por default, o link de transporte carrega informações de todas as VLANs. As VLANs não desejadas neste link deve ser excluídas manualmente.

12. Quando um switch faz a atualização de sua base de dados VTP?
    a) A cada 60 segundos.
    b) Quando um switch recebe uma atualização que possui um número de revisão mais alto, ele sobrescreve a base de dados contida na NVRAM com a nova base de dados recém-recebida.
    c) Quando um switch recebe uma atualização que possui um número de revisão mais baixo, ele sobrescreve a base de dados contida na NVRAM com a nova base de dados recém-recebida.
    d) Quando um switch recebe uma atualização que possui um número de revisão igual ao de sua base de dados, ele a sobrescreve com a nova base de dados recém-recebida.

13. Qual dos seguintes é um padrão IEEE para frame tagging?
    a) ISL c) 802.1q e) q931a
    b) 802.3z d) 802.3u

14. Qual das seguintes afirmações descreve corretamente um link de transporte?
    a) Eles podem participar de múltiplas VLANs simultaneamente.
    b) Os switches removem qualquer informação de tagging do frame antes de encaminhá-lo a um link ou porta de acesso.
    c) Dispositivos conectados às portas de acesso não podem se comunicar com dispositivos fora de sua VLAN, a menos que a comunicação ocorra por intermédio de um router.
    d) Links de transporte são usados para transportar informações de VLANs entre dispositivos e podem ser configurados para transportar informações sobre todas as VLANs ou apenas algumas.

15. Qual das seguintes afirmações é verdadeira com relação aos links de acesso?
    a) Eles podem participar de múltiplas VLANs simultaneamente.
    b) Os switches removem qualquer informação de tagging do frame antes de encaminhá-lo a um link ou porta de acesso.
    c) Dispositivos conectados às portas de acesso não podem se comunicar com dispositivos fora de sua VLAN, a menos que a comunicação ocorra por intermédio de um router.

d) Links de transporte são usados para transportar informações de VLANs entre dispositivos e podem ser configurados para transportar informações sobre todas as VLANs ou apenas algumas.

16. Qual das seguintes afirmações descreve corretamente os links de acesso?

a) Eles podem transportar informações de múltiplas VLANs.
b) Links de acesso são usados para transportar informações de VLANs entre dispositivos e podem ser configurados para transportar informações sobre todas as VLANs ou apenas algumas.
c) Eles podem apenas ser usados com FastEthernet ou GigabitEthernet.
d) Eles participam de não mais que uma VLAN.

17. Um novo switch acaba de ser incorporado à rede e um link de transporte é configurado entre o novo switch e o switch existente. VTP é usado para gerenciamento das VLANs. Quais VLANs serão permitidas nesse link de transporte?

a) Todas as VLANs existentes são permitidas no link de transporte, por default.
b) Serão permitidas as VLANs (ou intervalo de VLANs) definidas no mesmo domínio VTP.
c) Nenhuma VLAN é permitida, por default.
d) Apenas a VLAN1 é permitida.

18. Qual o modo de operação VTP que não participa do domínio VTP criado, mas encaminha as atualizações VTP através dos links de transporte configurados?

a) ISL
b) Cliente
c) Transparente
d) Servidor

19. Qual é o tamanho do cabeçalho ISL?

a) 2 bytes
b) 6 bytes
c) 26 bytes
d) 1522 bytes

20. Quando o processo de frame tagging é necessário?

a) Quando VLANs atravessam um link de acesso.
b) Quando VLANs atravessam links de transporte.
c) Quando o protocolo ISL é usado em um link de acesso.
d) Quando o protocolo IEEE 802.1q é usado em um link de acesso.

Respostas das Questões de Revisão – VLANs

1. **D**. Switches não propagam informações de VLANs por default. Para tal, você deve configurar um domínio VTP. VTP é usado para propagar informações sobre VLANs através de um link de transporte.

2. **B, C**. Você pode configurar associações VLAN em uma porta tanto estática como dinamicamente.

3. **B**. Um frame ISL pode ser até 1548 bytes.

4. **D**. Um servidor VMPS deve ser configurado com o endereço do hardware de todos os hosts na internetwork.

5. **D, E**. IEEE 802.1q e ISL são os protocolos usados para configurar *trunking* numa porta.

6. **B, D**. Pruning encontra-se desabilitado por default em todos os switches. No entanto, se você ativar pruning em um switch servidor VTP, o domínio VTP inteiro terá esse recurso ativado.

7. **A**. O protocolo ISL encapsula o frame Ethernet com um novo cabeçalho e informação CRC (checagem de erros).

8. **A**. O switch que opera em modo VTP transparente é um switch independente, que pode ser conectado em uma rede para efeito de gerência. Ele não adiciona informação sobre VLANs em sua própria base de dados, nem compartilha a informação sobre as VLANs que possui.

9. **B, C, D, E, F, G**. VTP é usado no caso de você possuir múltiplos switches e múltiplas VLANs configuradas em uma mesma rede. Esse recurso ajuda você a manter uma base de dados VLAN estável e consistente.

10. **A**. Todos os switches Cisco são servidores VTP por default. Nenhuma outra informação VTP encontra-se configurada em um switch por default.

11. **D**. Por default, se você criar um link de transporte, todas as VLANs são propagadas através dele. VLANs indesejadas devem ser excluídas manualmente.

12. **B**. Switches procuram pelo número de revisão mais alto. Caso seja encontrado, a base de dados VLAN atual será sobrescrita pela recém-recebida.

13. **C**. O protocolo IEEE 802.1q foi criado para permitir o estabelecimento de links de transporte entre switches de diferentes fabricantes.

14. **A, D.** Links de transporte - ou *trunks* - são usados para transportar informações sobre VLANs entre switches.

15. **B, C.** Quando um frame atravessa um link de transporte, ele é encapsulado com a informação sobre a VLAN à qual pertence por intermédio do protocolo ISL (frame tagging). Essa informação é removida antes de o frame ser enviado para uma porta ou link de acesso.

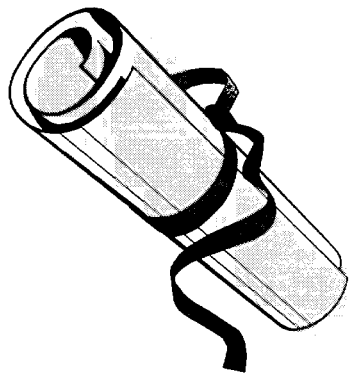
16. **D.** Links de acesso transportam dados apenas para a VLAN à qual pertencem.

17. **B.** Quando o VTP encontra-se gerenciando uma rede comutada, apenas VLANs definidas num mesmo domínio VTP são propagadas através de um link de transporte.

18. **C.** O modo de operação VTP transparente encaminha informação VTP através de links de transporte, porém não atualiza sua base de dados VTP com as informações VTP propagadas.

19. **C.** O cabeçalho ISL possui 26 bytes de extensão.

20. **B.** A Cisco criou o frame tagging para ser usado quando um frame Ethernet necessita atravessar um link de transporte. Frame tagging é um método desenvolvido pela Cisco para identificar individualmente frames provenientes de diferentes VLANs através de um link de transporte.



5 TCP/IP

5.1 Tópicos Abordados

- O Modelo DoD (*Department of Defense Model*);
- Definição de Portas Lógicas;
- Classes de Endereços IPs;
- Técnicas de Subnetting (Máscaras de Rede);
- Sub-redes de Tamanho Variável (VLSM);
- Classless Interdomain Routing (CIDR);
- Sumarização de Endereços;
- IPv6.

5.2 Introdução

O padrão TCP/IP foi criado pelo Departamento de Defesa Americano (DoD) para garantir a preservação da integridade dos dados, assim como manter a comunicação de dados no advento de uma guerra.

Se bem planejada e corretamente implementada, uma rede baseada na combinação de protocolos (*suite*) TCP/IP pode ser independente, confiável e muito eficiente.

O processo de endereçamento IP não é uma tarefa complexa, mas trabalhosa - especialmente para indivíduos destreinados. Existem uma série de fatores que devem ser entendidos e que serão discutidos a seguir. O entendimento e domínio das técnicas para criação e identificação de máscaras de rede (*subnetting masks*) só é atingido com muita prática.

O domínio deste capítulo é de extrema importância para se conseguir um bom resultado tanto no exame CCNA como em um ambiente de trabalho. Prática é fundamental para uma boa assimilação dos itens apresentados neste capítulo. Pratique até que o processo de designação e determinação de endereços IPs seja completamente dominado.

5.3 O Modelo DoD – TCP/IP

Uma vasta gama de protocolos atua na camada de Processo/Aplicação do modelo DoD (TCP/IP), com funções idênticas às das três camadas OSI equivalentes (Aplicação, Apresentação e Sessão - figura 5.1).

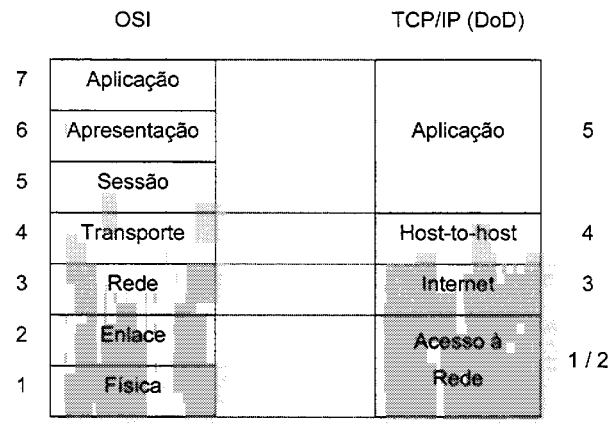


Figura 5.1: Mapeamento do modelo OSI x TCP/IP.

- **Camada de Processo/Aplicação (*Process/Application Layer*)**: É responsável pela definição dos protocolos necessários para a comunicação ponto a ponto pelas aplicações, bem como pelo controle e especificações da interface com o usuário.
- **Camada de Transporte (*Host-to-Host Layer*)**: Espelha as funções da camada de transporte no modelo OSI, definindo protocolos que estabelecem o nível do serviço de transmissão para as aplicações. Essa camada se encarrega de tarefas como a criação de uma conexão ponto a ponto confiável e a entrega de dados, zelando pela sua integridade. Essa camada é também responsável pelo seqüenciamento de pacotes de dados.
- **Camada de Rede (*Internet Layer*)**: Corresponde à camada de rede no modelo OSI, designando protocolos responsáveis pela transmissão lógica de pacotes através da rede. Essa camada é responsável pelo endereçamento lógico dos dispositivos, designando-lhes endereços IPs. A camada de Rede também é responsável pelo roteamento de pacotes através da rede e pelo controle do fluxo de dados durante o processo de comunicação entre dois dispositivos.
- **Camada de Host à Rede (*Network Access Layer*)**: Equivalente às camadas de enlace e física no modelo OSI, é responsável pelo monitoramento do tráfego de dados entre os dispositivos e a rede. Nessa camada também são definidos os protocolos

para a transmissão dos dados através dos meios físicos, assim como a aplicação e análise dos endereços de hardware.

5.4 Estudo das Camadas do Modelo DoD (TCP/IP)

5.4.1 A Camada de Aplicação

São listados, a seguir, alguns dos protocolos e aplicações tipicamente utilizados em redes IP.

- **Telnet**: É conhecido como o "camaleão" dos protocolos. Sua principal função é a emulação de terminais. Ele permite que um usuário em uma máquina remota (cliente) conecte-se aos recursos de outra máquina (servidor Telnet). O nome Telnet vem de *Telephone Network*.
- **FTP/TFTP (*File Transfer Protocol/TrivialFTP*)**: Protocolo utilizado para transferência de arquivos entre duas máquinas. O FTP não apenas é um protocolo, mas também um programa. Operando como um protocolo, FTP é utilizado por outras aplicações. Como um programa, é utilizado para executar transferência de arquivos. TFTP ("T" de *Trivial*) é uma versão mais simplificada do protocolo FTP, usado quando se sabe exatamente o que se procura e sua devida localização. O TFTP não possui as facilidades do FTP, como a pesquisa em diretórios. Ele não faz nada além de enviar e receber arquivos. TFTP é o protocolo utilizado para instalar uma atualização do sistema Cisco em um router Cisco.
- **NFS (*Network File System*)**: Protocolo especializado em compartilhamento de arquivos, permitindo a interoperação entre dois tipos de sistemas de arquivos heterogêneos.
- **SMTP (*Simple Mail Transfer Protocol*)**: Utilizado no gerenciamento e distribuição de e-mails.
- **LPD (*Line Printer Daemon*)**: Protocolo utilizado para o compartilhamento de impressoras.
- **X Window**: Define um padrão para o desenvolvimento de interfaces gráficas em sistemas cliente-servidor.
- **SNMP (*Simple Network Management Protocol*)**: Coleta e manipula informações de rede. Esse protocolo pode também agir como um "cão de guarda" de toda a rede, transmitindo avisos para os administradores sempre que algum evento inesperado ocorrer.
- **DNS (*Domain Name Service*)**: Responsável pelo mapeamento de "nomes" para os endereços IPs.

5.4.2 A Camada de Transporte

A principal função da camada de Transporte é mascarar das aplicações de camada superior as complexidades da rede. Dois protocolos são definidos nessa camada: o TCP e o UDP.

- **TCP (*Transmission Control Protocol*)**: O TCP recebe um fluxo de dados de uma aplicação e os "quebra" em segmentos. Esses segmentos são numerados e seqüenciados, permitindo a remontagem do fluxo assim que os segmentos atingem seu destino. Após o envio desses segmentos, o protocolo TCP aguarda uma confirmação da máquina receptora, retransmitindo os segmentos que não forem devidamente confirmados. Antes que a transmissão se inicie, o protocolo TCP da máquina origem contata o protocolo TCP da máquina destino para que uma conexão seja estabelecida. Essa conexão é chamada de circuito virtual (*virtual circuit*). Esse tipo de comunicação é chamado de "orientada à conexão" (*connection-oriented*). Durante esse "aperto de mão" (*hand-shake*) inicial, o protocolo TCP das pontas envolvidas também determina o volume de dados a ser transmitido antes de ocorrer a confirmação por parte do destinatário. Com tudo acertado com antecedência, o caminho para uma comunicação confiável está pavimentado.

O TCP é um protocolo *full-duplex*, orientado à conexão e altamente confiável. A arquitetura TCP é bastante complexa, o que acarreta em um grande custo em termos de cabeçalho (*overhead*). Como as redes de hoje são muito mais confiáveis do que as redes existentes quando o protocolo TCP foi criado, grande parte das características que garantem essa confiabilidade na transmissão poderia ser dispensada atualmente.

- **UDP (*User Datagram Protocol*)**: Desenvolvedores podem se utilizar do protocolo UDP em lugar ao TCP. UDP é considerado um modelo de escala econômico e um protocolo "magro". Por esse fato, o protocolo UDP utiliza muito menos largura de banda do que o TCP. O protocolo UDP não oferece todo o requinte do TCP, mas realiza eficientemente o trabalho de transporte de dados que não requeiram confiabilidade na entrega. Existe uma gama de situações nas quais o protocolo UDP poderia ser sabiamente empregado em lugar ao TCP. Como exemplo, os sinais de rede constantemente transmitidos pelo protocolo SNMP (os "cães de guarda") congestionariam a rede caso fossem enviados via TCP. O UDP, nesse caso, realiza o transporte desses sinais, uma vez que confiabilidade de entrega não é um fator crítico. Outra utilização para UDP em lugar ao TCP seria quando a confiabilidade de transmissão é plenamente alcançada na camada de processos e aplicações. O protocolo NFS, por exemplo, lida com questões

de segurança à sua própria maneira, tornando desnecessária a utilização do TCP para transporte nesse caso.

UDP recebe blocos de dados das camadas superiores - em vez de fluxos de dados, como ocorre com o TCP - e os quebra em segmentos. Como o protocolo TCP, o UDP numera cada segmento transmitido pelo dispositivo origem, permitindo a reconstrução do bloco de dados no dispositivo destino. O UDP, no entanto, não seqüencia os segmentos como o TCP, não se importando com a ordem em que esses segmentos chegam ao destino. Após a numeração dos segmentos, o UDP os transmite e simplesmente os "esquece". Não existe a confirmação de recebimento pelo dispositivo origem, como ocorre com o TCP. O que ocorre, de fato, é o completo abandono do segmento na rede. Por esse motivo, o UDP é considerado um protocolo não-confiável. Além disso, ele não estabelece um circuito virtual antes do início da transmissão, como ocorre com TCP. Por esse motivo, o UDP também é considerado um protocolo não-orientado à conexão.

Existem, portanto, duas alternativas distintas para o protocolo de transporte de dados:

- **TCP** para um transporte de dados confiável;
- **UDP** para um transporte rápido.

Em resumo, as camadas superiores enviam um fluxo de dados para os protocolos da camada de Transporte, que o "quebra" em segmentos. A camada de Rede encarrega-se de encapsular esses segmentos em pacotes e roteá-los através da rede. Esses pacotes são, então, entregues ao respectivo protocolo de camada de Transporte no dispositivo destino, que se encarrega da reconstrução do fluxo de dados e do seu envio às aplicações ou protocolos das camadas superiores.

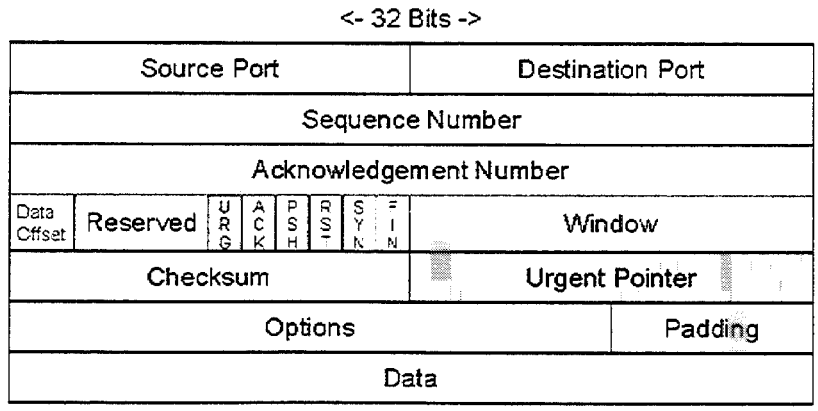


Figura 5.2: Estrutura do cabeçalho TCP.

A figura 5.2 ilustra o formato do cabeçalho (*header*) de um segmento TCP, com os diferentes campos que o compõem. Esta ilustração facilita

o entendimento do processo de como o protocolo TCP segmenta o fluxo de dados recebido e prepara esses segmentos para a camada de Rede (Internet).

Nota: Essa representação do cabeçalho TCP funciona apenas para fins didáticos. Na verdade, o cabeçalho seria algo como cada um dos blocos ilustrados (Source Port, Destination Port, Sequence Number etc.) colocados lado a lado, totalizando uma "linha" de 20 bytes de comprimento (32 bits x 5 camadas). O campo Options possui tamanho variável, podendo aumentar o tamanho total do cabeçalho TCP.

O cabeçalho TCP possui 20 bytes e contém os seguintes campos:

- **Source Port (Porta Origem)**: Número da porta lógica onde a aplicação transmissora está localizada;
- **Destination Port (Porta Destino)**: Número da porta lógica onde a aplicação ou protocolo requisitado está localizado na máquina destinatária;
- **Sequence Number (Número Seqüencial)**: Número utilizado na recolocação dos segmentos na ordem correta;
- **Acknowledgement Number (Número da Confirmação)**: Define qual octeto TCP deve ser aguardado na seqüência;
- **HLEN - Header Lenght (Comprimento do Cabeçalho)**: Define o comprimento do cabeçalho TCP;
- **Reserved**: Esse valor é sempre 0;
- **Code Bits**: Funções de controle utilizadas para iniciar e encerrar uma sessão;
- **Window (Janela)**: Tamanho da janela dados que o remetente tem capacidade de receber, medido em octetos;
- **CheckSum**: Checagem de redundância cíclica (CRC). Lembre-se que o TCP não "confia" nos controles de erro realizados pelas camadas mais baixas, dispondo de um controle próprio para identificação de segmentos corrompidos;
- **Urgent Pointer (Marcação de Urgência)**: Marcação de dados críticos (urgentes);
- **Option (Opção)**: Define o tamanho máximo do segmento TCP;
- **Data (Dados)**: Dados passados para a camada de Transporte, que incluem os cabeçalhos das camadas superiores (encapsulamento).

Já o cabeçalho UDP[1] possui uma complexidade notadamente reduzida, contendo apenas os seguintes campos (figura 5.3):

- **Source Port (Porta Origem)**: Número da porta lógica onde a aplicação transmissora está localizada;
- **Destination Port (Porta Destino)**: Número da porta lógica onde a aplicação ou protocolo requisitado está localizado na máquina destinatária;
- **Lenght (Comprimento)**: Define o tamanho do segmento UDP, incluindo o cabeçalho e dados;
- **CheckSum**: Checagem de redundância (CRC) de campos do cabeçalho e dados;
- **Data (Dados)**: Dados passados para a camada de Transporte, que incluem os cabeçalhos das camadas superiores (encapsulamento).

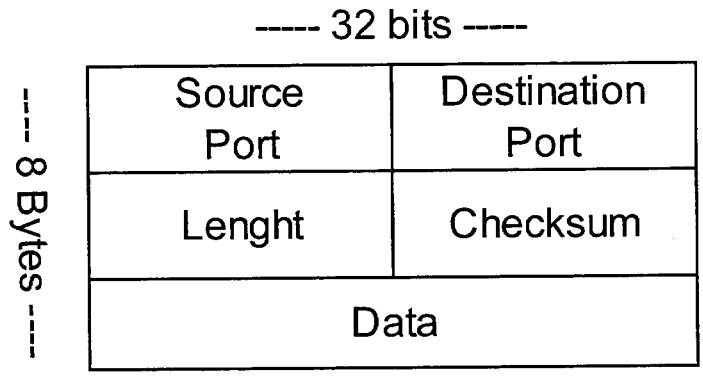


Figura 5.3: Estrutura do cabeçalho UDP.

Eis os pontos mais importantes a serem lembrados com relação aos dois protocolos:

TCP	UDP
Comunicação seqüencial	Comunicação não-seqüencial
Comunicação confiável	Comunicação não-confiável
Comunicação orientada à conexão	Comunicação não-orientada à conexão
Latência elevada (cabeçalho complexo)	Baixa Latência (cabeçalho menor)
Estabelece um circuito virtual	Não estabelece um circuito virtual

[1] Note a diferença de tamanho e complexidade do cabeçalho UDP em relação ao TCP.

5.4.2.1 Portas Lógicas

Os protocolos TCP e UDP utilizam portas lógicas para a comunicação com as camadas superiores. A adoção de portas lógicas permite o registro lógico das diferentes sessões que são estabelecidas através da rede simultaneamente.

O número de portas lógicas de aplicações origem (*source*) é dinamicamente designado pela máquina transmissora e deve ser um número maior ou igual a 1024.

Os números compreendidos entre o intervalo de 0 a 1023 são reservados para identificação das "portas bem-conhecidas" (*well-known port*).

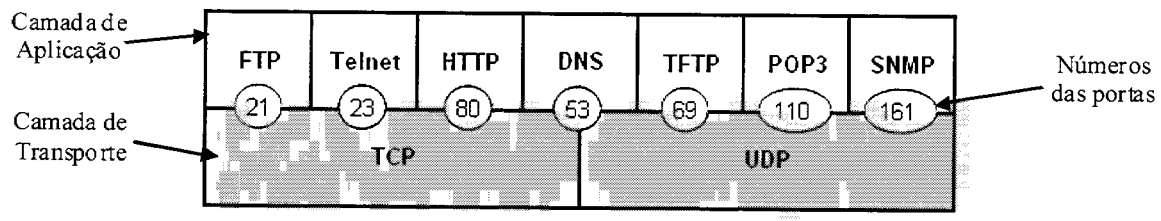


Figura 5.4: Portas lógicas de comunicação TCP/UDP.

Nota: *Um arquivo, que está disponível para download no site da editora <www.visualbooks.com.br>, possui uma lista das portas bem-conhecidas utilizadas pelos protocolos UDP e TCP.*

Sessões que não utilizem uma aplicação que tenha um número de porta reservado (porta bem-conhecida) geram randomicamente esse número, dentro de um intervalo específico (>=1024). Esse esquema de identificação lógica (números de porta) é responsável pela identificação do protocolo (ou aplicação) origem e destino, em um segmento TCP ou UDP.

Os diferentes números de porta que podem ser utilizados são:

- **Números abaixo de 1024**: Conhecidos como *well-known port numbers*, definidos pelo RFC 1700 (*Request For Comment*);
- **Maiores ou iguais a 1024**: Usados pelas camadas superiores para estabelecer sessões com outros dispositivos e pelo protocolo TCP para utilização como endereços de transmissão e destino em um segmento TCP.

Observe bem a primeira parte de segmento TCP ilustrada na figura 5.5. Note que a máquina origem gera aleatoriamente um número de porta lógica de origem (*source port* - 1144). O objetivo é a identificação

lógica das diferentes sessões, estabelecidas simultaneamente com diferentes dispositivos. De que outro modo, por exemplo, um servidor saberia de onde estão chegando determinados segmentos se não houvesse um esquema que identificasse de forma única cada sessão TCP ativa? O TCP e as camadas superiores não "compreendem" o esquema de endereçamento físico (MAC) ou lógico (ex. IP, IPX) para a identificação dos diferentes dispositivos espalhados pela rede, como o fazem as camadas inferiores. Na camada de Transporte, essa identificação é feita através de números associados às portas lógicas.

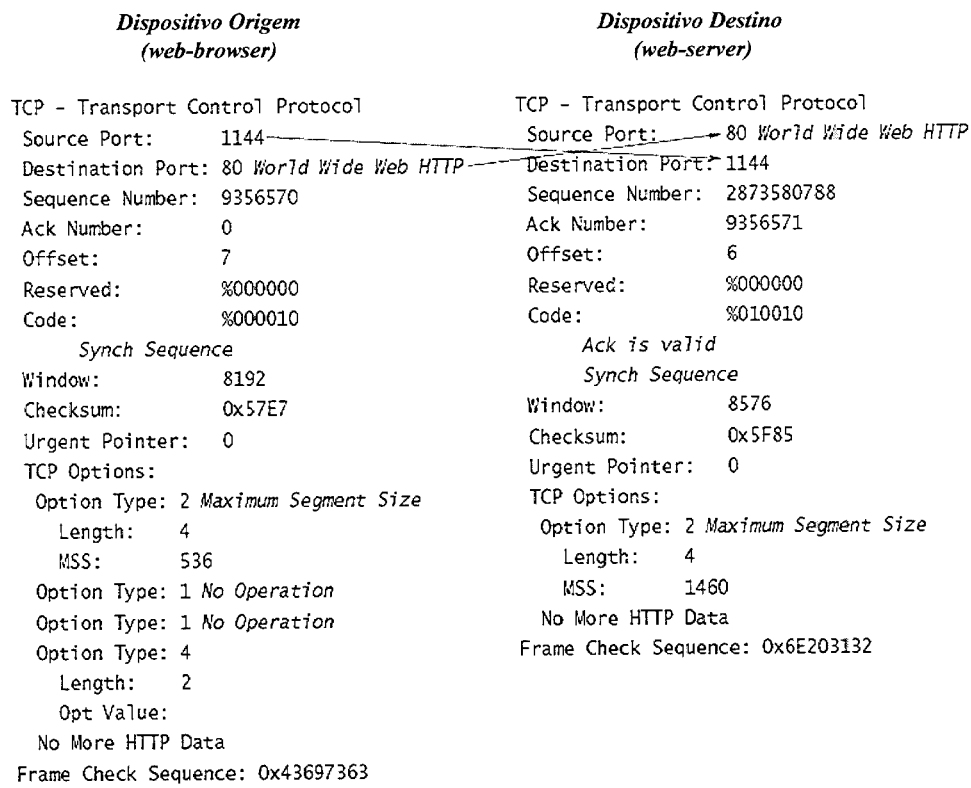


Figura 5.5: Exemplo do esquema de portas lógicas em fragmentos de segmentos capturados.

Repare ainda na primeira seção de segmento TCP. Note que o número da porta destino (*destination port*) é menor que 1024, ou seja, é um número de porta bem-conhecido (HTTP, no caso).

Observe agora o segundo segmento TCP, logo ao lado do primeiro. Podemos afirmar que ambos pertencem à mesma sessão TCP, pois o número da porta destino em um equivale ao número da porta origem no outro e vice-versa.

5.4.3 A Camada Internet

Existem duas razões principais para a existência da camada Internet: roteamento e disponibilização de uma interface de rede unificada para as camadas superiores. Nenhuma das camadas superiores ou inferiores

tem funções relativas ao roteamento de pacotes. Essa complexa e importante tarefa é responsabilidade exclusiva da camada Internet. A segunda tarefa, a de prover uma interface de rede unificada às camadas superiores, garante a compatibilidade entre os diferentes tipos de protocolos de acesso à rede. Se essa função não fosse desempenhada pela camada Internet, programadores teriam de desenvolver diferentes versões de aplicações para cada tipo de acesso existente: uma versão para Ethernet, outra para *Token-Ring* e assim por diante. Para prevenir isso, o protocolo IP promove uma interface de rede unificada para os protocolos das camadas superiores. Ou seja, todos os caminhos não levam a Roma. Levam ao IP! E todos os outros protocolos presentes nessa camada o utilizam. Não se esqueça disso: todos os caminhos através do modelo DoD passam pelo protocolo IP.

Basicamente, quatro protocolos coexistem na camada Internet:

- *Internet Protocol* (IP);
- *Internet Control Message Protocol* (ICMP);
- *Address Resolution Protocol* (ARP);
- *Reverse Address Resolution Protocol* (RARP).

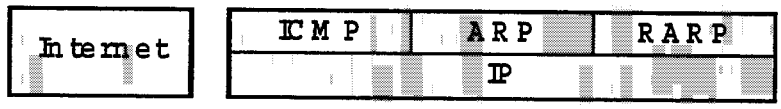


Figura 5.6: Modelo ilustrativo da camada Internet e seus protocolos.

O protocolo IP essencialmente define a camada Internet no modelo DoD. Os outros protocolos nessa camada existem apenas para suportá-lo. O IP poderia ser visto como um protocolo onipresente, no sentido de que está a par de todas as redes interconectadas. Isso é possível por que todos os dispositivos de rede possuem um endereço lógico chamado "endereço IP". O protocolo IP efetua uma análise desse endereço para cada pacote de dados que recebe. Em seguida, utilizando uma tabela de roteamento (*routing table*), ele decide para onde o pacote deve ser enviado, selecionando a melhor rota (que nem sempre é a mais curta! Veremos isso mais adiante). A identificação de dispositivos na rede requer que duas perguntas sejam respondidas: Em qual rede esse dispositivo se encontra? E qual seu endereço nessa rede? A primeira resposta é o endereço lógico (análogo ao nome de uma rua em um endereço de correspondência). A segunda, o endereço físico (a analogia agora seria o número da casa na rua). O IP recebe os segmentos da camada de Transporte e os encapsula em pacotes ou datagramas. No lado destinatário, o IP então remonta esses datagramas de volta em segmentos. Cada datagrama recebe o endereço IP do transmissor e do destinatário. Os routers, dispositivos definidos na camada 3 e que

processam os datagramas, decidem sobre as rotas a serem tomadas com base nos seus endereços IP de destino.

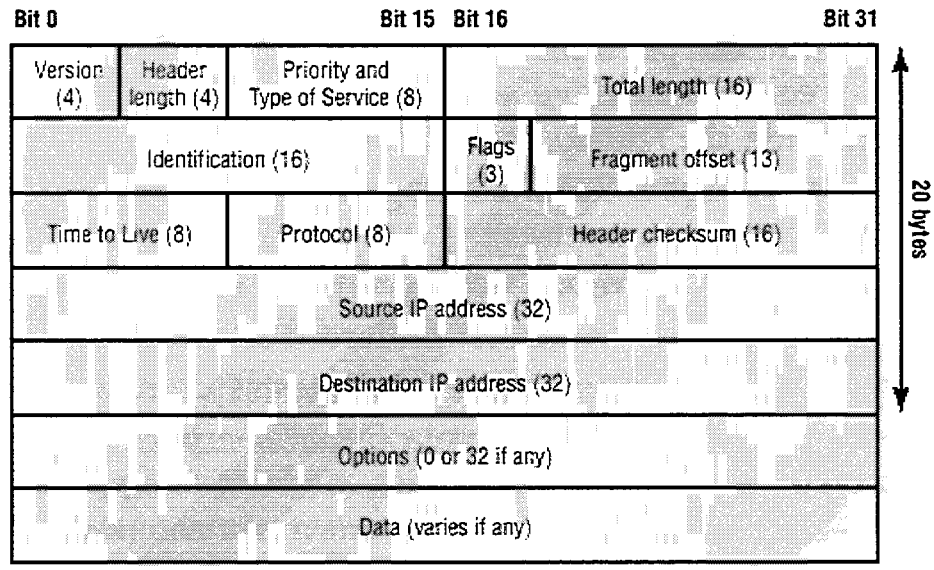


Figura 5.7: Modelo ilustrativo do cabeçalho do protocolo IP.

A figura 5.7 ilustra o formato do cabeçalho IP. Com base nessa figura, podemos analisar pelo que o protocolo IP tem de passar cada vez que dados são enviados das camadas superiores tendo como destino uma rede remota.

Eis os campos que compõem o cabeçalho IP:

- **Version**: Número da versão do protocolo (atualmente 4);
- **HLEN**: Comprimento do cabeçalho;
- **Priority ou ToS *(Type of Service)***: Indica como o datagrama deve ser manipulado. Os primeiros 3 bits definem a prioridade;
- **Total Lenght:** Comprimento total do pacote, incluindo o cabeçalho;
- **Identification:** Valor único para identificação do pacote;
- **Flags:** Especifica se a fragmentação deve ou não ocorrer;
- **Frag offset:** Provê fragmentação e remontagem se um pacote de dados for muito extenso para ser colocado em um frame. Também permite diferentes unidades máximas de transmissão (*Maximum Transmission Units* - MTUs) na Internet;
- **TTL (*Time To Live*/Tempo de Vida):** O valor TTL é estabelecido quando um pacote é originalmente gerado. Ele estabelece o tempo de vida do pacote através de diferentes métricas (número de saltos, tempo etc.). Se o pacote não atingir seu destino antes de o timer TTL expirar, ele é descartado. Isso impede pacotes IPs de circularem continuamente pela Internet, gerando *loopings*;

- **Protocol:** Número da porta lógica do protocolo de camada superior (Transporte). A porta TCP é 6 e a UDP é 17, em hexadecimal (note que aqui falamos de portas lógicas utilizadas pelo protocolo IP. Apesar de o conceito ser parecido, não deve ser confundido com o que vimos na camada de Transporte (TCP e UDP));
- **Header CheckSum:** Checagem de redundância (aplicada ao cabeçalho, apenas);
- **Source IP address:** Endereço IP de origem (32-bits);
- **Destination IP address:** Endereço IP de destino (32-bits);
- **IP option:** Campo utilizado em testes de rede (*debugging*);
- **Data:** Dados enviados pela camada superior (Transporte).

5.4.3.1 Portas Lógicas IP

A comunicação da camada Internet com a camada *Host-to-host* (Transporte) é realizada através de portas lógicas, de modo análogo à comunicação da camada de Transporte com a camada de Aplicação. A figura 5.8 ilustra parte de um pacote capturado por um analisador de rede (como o *Sniffer*). Note que todos os campos discutidos anteriormente estão presentes. Repare ainda que o campo *Protocol* identifica o protocolo de camada superior como sendo o TCP (porta 0x06, em hexadecimal).

Se o cabeçalho IP não carregasse a informação do protocolo da camada de Transporte, o protocolo IP não saberia o que fazer com os dados contidos no pacote. Em destaque, na figura, os endereços lógicos – no caso, endereços IPs – de origem e de destino.

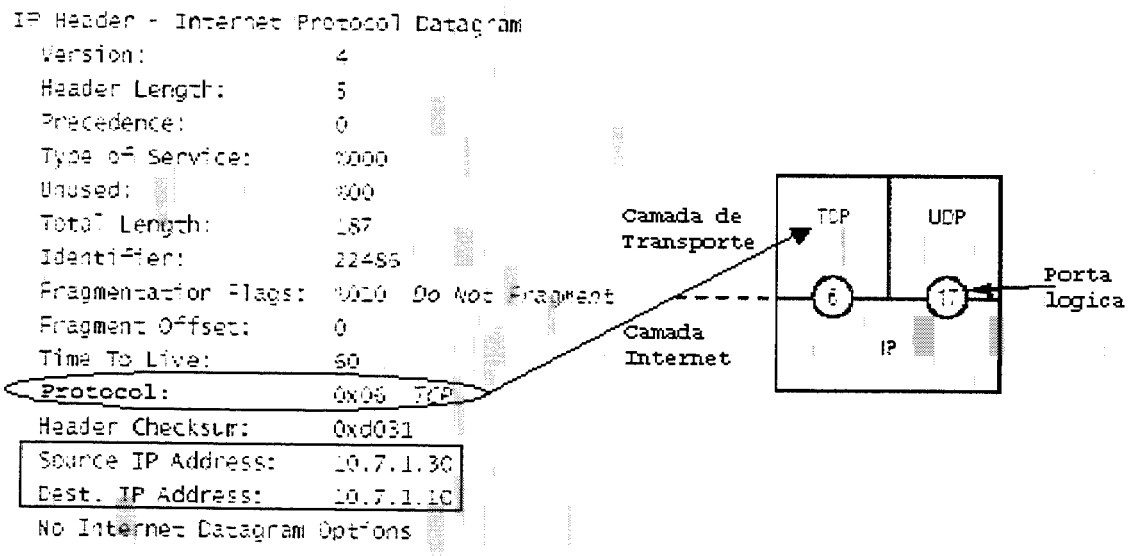


Figura 5.8: Portas lógicas fazem a comunicação da camada Internet com a camada de Transporte.

A figura 5.8 mostra como a camada Internet interpreta os protocolos definidos na camada de Transporte (TCP e UDP) quando os dados precisam ser passados aos protocolos dessa camada.

O campo *Protocol* orienta o protocolo IP para enviar os dados pela porta TCP (6). Outras opções que poderiam aparecer aqui seriam UDP (17), ICMP (1), IPv6 (41), IGRP (9), entre outras. Vale ressaltar que os números das portas são sempre representados em notação hexadecimal (0x).

5.4.3.2 ICMP

O protocolo ICMP (*Internet Control Message Protocol*) é definido na camada Internet e é usado pelo protocolo IP. O ICMP é um protocolo gerenciador, agindo também como um "mensageiro" para o protocolo IP. Suas mensagens são transportadas como datagramas IPs.

O ICMP também é usado na descoberta de rotas para *gateways*. Periodicamente, anúncios (*advertisements*) de routers são transmitidos pela rede, contendo os endereços IPs de suas interfaces ativas. Os dispositivos de rede analisam esses pacotes e atualizam as informações sobre rotas.

O processo de solicitação realizado por um router é uma requisição de anúncios imediatos. Esses anúncios podem ser enviados por dispositivos conectados na rede assim que eles inicializam. Entre os eventos e mensagens mais comuns relacionados ao protocolo ICMP, podemos destacar os seguintes:

- *Destination unreachable* (destino inalcançável);
- *Buffer full* (buffer cheio);
- *Hops* (contagem de "saltos");
- *Ping*;
- *Traceroute*.

Note que, embora o protocolo ICMP seja definido na camada Internet, ele se utiliza do protocolo IP para uma requisição de serviço (ex.: *Ping*). Por isso foi dito que os outros protocolos definidos nessa camada existem apenas para suportar o IP.

5.4.3.3 O Protocolo de Resolução de Endereço ARP (Address Resolution Protocol)

O protocolo ARP (Protocolo de Resolução de Endereço) é responsável por localizar o endereço de hardware de um dispositivo a partir de seu endereço IP conhecido. Seu funcionamento é simples: quando o

protocolo IP tem um datagrama a ser transmitido, ele precisa informar ao protocolo de acesso à rede (*network access protocol*) - como Ethernet ou *Token Ring* - o endereço de hardware (*MAC address*) do dispositivo destinatário na rede local. Se o protocolo IP não encontrar o endereço do hardware destinatário no *ARP cache*, ele utilizará o protocolo ARP para obter essa informação. A figura 5.9 ilustra o processo.

O ARP funciona como um detetive para o protocolo IP. Ele irá interrogar todas as máquinas presentes na rede local (através de uma mensagem de *broadcast*), enviando o endereço IP da máquina que deve responder a esse chamado. Resumindo, o protocolo ARP faz o mapeamento do endereço lógico (IP) para o endereço físico (MAC).

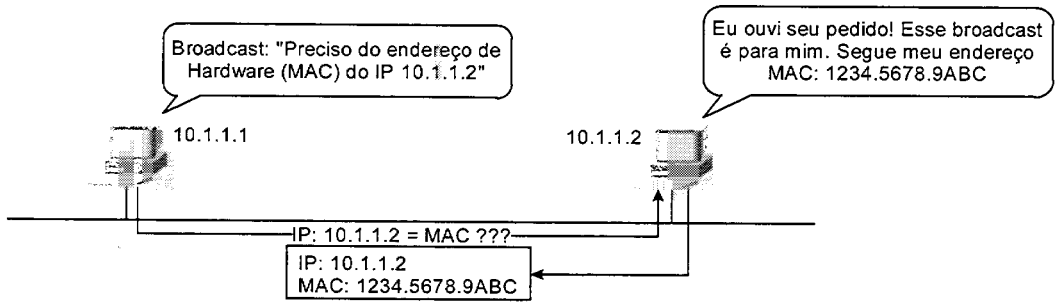


Figura 5.9: O protocolo ARP "em ação".

5.4.3.4 O Protocolo de Resolução de Endereço Reverso RARP (Reverse Address Resolution Protocol)

Uma máquina IP pode ser uma máquina sem disco (*diskless station*), como um "terminal burro" ou um *network computer*. Nesse caso, a máquina não tem como saber, assim que inicializada, seu endereço IP. Mas ela sabe seu endereço de hardware (MAC), uma vez que ele se encontra gravado na placa de rede da máquina.

O protocolo RARP (Protocolo de Resolução de Endereço Reverso) se encarrega de descobrir o endereço IP de uma máquina sem disco enviando mensagens de *broadcast* que contêm seu endereço MAC e uma requisição de endereço IP designado para aquele endereço MAC específico.

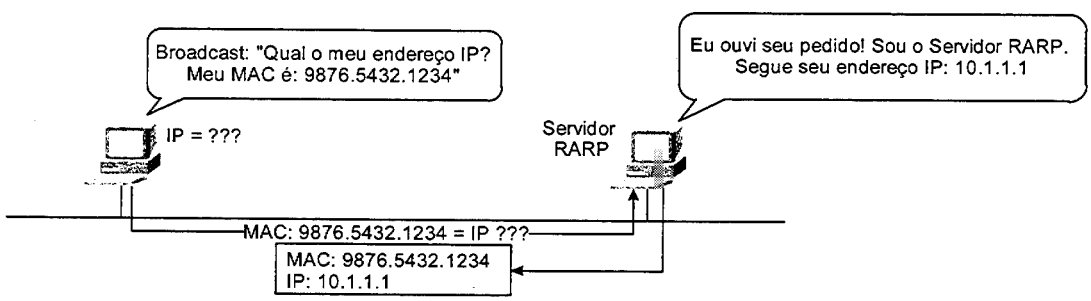


Figura 5.10: Funcionamento do protocolo RARP.

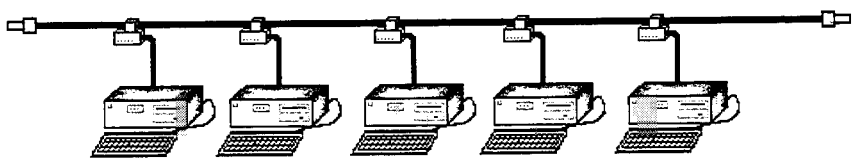
Uma máquina especial na rede, chamada RARP Server, responde a esse chamado enviando uma mensagem-resposta com o endereço IP da máquina solicitante (figura 5.10).

Resumindo, o protocolo RARP resolve endereços físicos (MAC) para endereços lógicos (IP), funcionando de modo exatamente contrário ao protocolo ARP. Daí o nome Protocolo de Resolução de Endereço Reverso (RARP).

5.4.4 A Camada de Acesso à Rede (Network Access Layer)

Na camada de Acesso à Rede são definidos os protocolos de acesso ao meio (como Ethernet, *Token Ring*, *LocalTalk* e FDDI), os padrões de conectores físicos (como RJ-45, V.35, AUI etc.), os padrões de sinalização elétrica (como IEEE 802.2, IEEE 802.3, IEEE 802.5 etc.) e as topologias possíveis (barramento, estrela, anel, mista e árvore), que serão detalhadas a seguir.

5.4.4.1 Barramento



Vantagens:

- Fácil conexão de periféricos ou outras máquinas nesse tipo de topologia;
- Demanda menos cabo do que a topologia estrela.

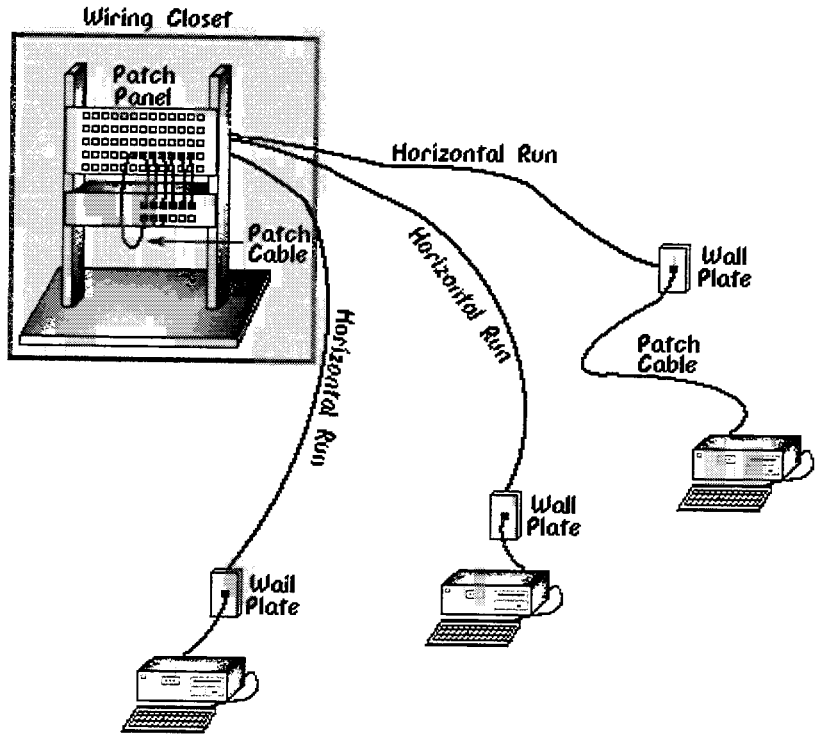
Desvantagens:

- A rede inteira colapsa caso o cabo principal venha a ter problemas;
- Terminadores requeridos em ambos os lados do cabo principal;
- Difícil identificação do problema caso a rede venha a apresentar falhas.

5.4.4.2 Estrela (Topologia Utilizada por Ethernet, Fast Ethernet e LocalTalk)

Vantagens:

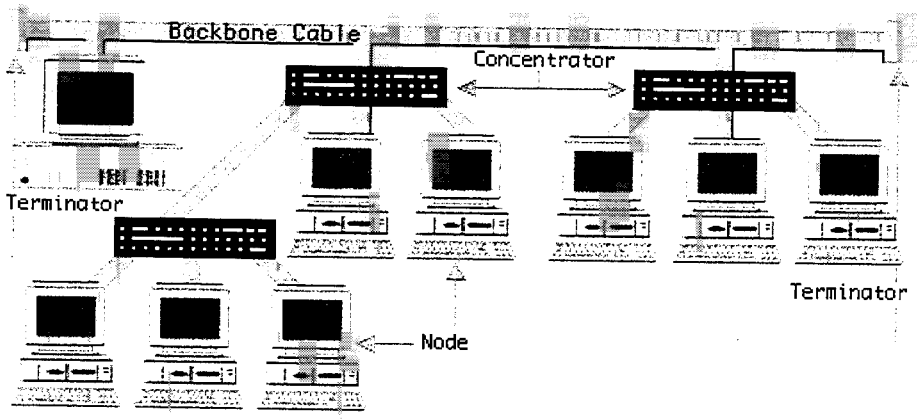
- Fácil de instalar e cabear;
- Não há alteração na rede quando se instala ou se retira algum dispositivo;
- Fácil detecção de falhas e remoção de dispositivos falhos.



Desvantagens:

- Demanda mais cabo do que a topologia de barramento;
- Se o concentrador (hub ou switch) falhar, todos os dispositivos conectados a ele são afetados;
- Custo mais elevado se comparado a topologia barramento devido ao custo dos concentradores.

5.4.4.3 Árvore (Topologia Mista)



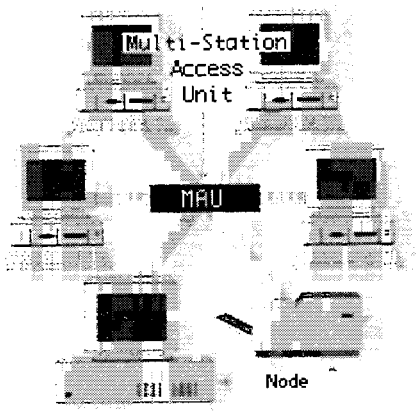
Vantagens:

- Cabeamento ponto a ponto para segmentos individuais;
- Suportado por uma grande gama de revendedores de hardware e software;
- Topologia flexível e de fácil escalabilidade.

Desvantagens:

- O comprimento total de cada segmento é limitado pelo tipo de cabo utilizado;
- Se o segmento principal tiver problemas, a rede inteira irá colapsar;
- Mais difícil de cabear e configurar que outras topologias.

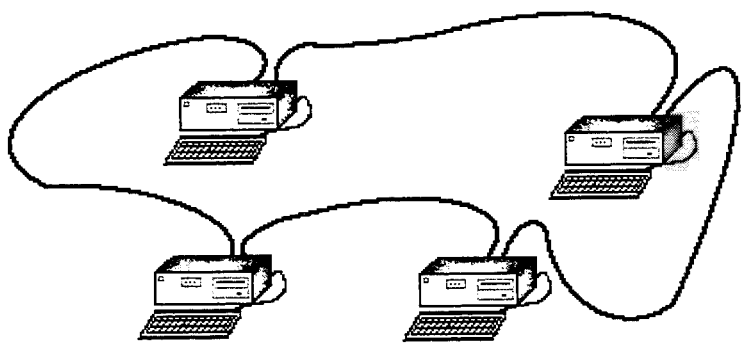
5.4.4.4 Anel Cabeado em Estrela (Topologia Utilizada por Token Ring)



Vantagens / Desvantagens:

- Ver topologia estrela (apesar de ser conhecido como anel, a topologia *Token Ring* é semelhante a uma estrela, uma vez que o anel se encontra, de fato, dentro do concentrador, chamado MAU (*Multistation Access Unit*).

5.4.4.5 Anel (Topologia Utilizada por FDDI)



Vantagens:

- Redundância e eficiência da rede (normalmente essa topologia é constituída por um par de anéis de fibra-óptica, cada um transmitindo dados em uma direção diferente. Se

um dos anéis se rompe ou é interrompido, o fluxo de dados continua devido aos processos de cicatrização (*healing*) e aprendizagem inerentes a essa topologia).

Desvantagens:

- Custo de implementação;
- Complexidade do gerenciamento e manutenção;
- Compatibilidade.

5.5 Endereçamento IP

Um dos mais importantes tópicos na discussão TCP/IP trata dos esquemas de endereçamento IP. O endereço IP é um identificador numérico designado a cada dispositivo conectado a uma rede IP, determinando um local para o dispositivo na rede.

O endereço IP é um endereço lógico (software) e não físico (hardware). O esquema de endereçamento IP foi criado para permitir que um dispositivo em uma rede possa se comunicar com um dispositivo em outra, independentemente dos tipos de LANs envolvidos (Ethernet, *Token-Ring* etc.).

Para entender e dominar os esquemas de endereçamento IP e de suas sub-redes (*subnetting*), é muito importante que se dominem técnicas de conversão binária para decimal assim como potências de base 2. Neste capítulo praticaremos essas técnicas.

Terminologia IP:

- **Bit**: Um dígito - 1 ou 0;
- **Byte**: Uma seqüência de 7 ou 8 bits, dependendo da paridade utilizada. O normal é uma seqüência de 8 bits;
- **Octeto (*octet*)**: Sempre 8 bits;
- **Endereço de Broadcast (*broadcast address*)**: Endereço usado por aplicações e dispositivos para o envio de mensagens a todos os dispositivos de uma rede, simultaneamente (*1-to-all*). Pode-se fazer aqui uma analogia ao sistema aberto de televisão. Todos com um aparelho de TV conseguem captar o sinal de uma TV aberta (ex. TV Cultura), pois o sinal é enviado de um ponto (antena transmissora) para todas as TVs em uma região;
- **Endereço de Multicast (*multicast address*)**: Endereço usado por apenas uma máquina para alcançar um grupo definido de máquinas (*1-to-many*). A analogia que cabe aqui é o sistema

fechado de televisão (TV por assinatura). Apenas um grupo específico de usuários recebe o seu sinal (os assinantes);

- **Unicast (*unicast address*):** Comunicação de uma máquina para apenas outra máquina (*1-to-1*). A analogia aqui seria o *pay-per-view*. Somente o assinante que solicitou o programa (e pagou por ele, no caso) o receberá.

Antes de entrarmos em mais detalhes sobre endereçamento IP, é imprescindível dominar técnicas de conversão binário-decimal. Para se dominar essa técnica, muita prática é necessária. Eis como funciona:

Números binários utilizam 8 bits para definir um número decimal. Esses bits têm seus valores considerados da direita para a esquerda através de um fator que dobra seu valor. Isso ocorre pelo fato de eles serem determinados através de potências de base 2. Eis o porquê do nome do sistema ser binário.

Por exemplo, o número binário 00100110 nada mais é do que a representação de $0x2^7+ 0x2^6+ 1x2^5+ 0x2^4+ 0x2^3+ 1x2^2+ 1x2^1+ 0x2^0 = 0+0+32+0+0+4+2+0=38$ (figura 5.11).

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

0	0	1	0	0	1	1	0

0	x	128	=	0
0	x	64	=	0
1	x	32	=	32
0	x	16	=	0
0	x	8	=	0
1	x	4	=	4
1	x	2	=	2
0	x	1	=	0

00100110 = 32 + 4 + 2 = 38

Figura 5.11: Exemplo de conversão binário-decimal.

Técnicas de memorização e muita prática são muito úteis no domínio do processo de conversão binário-decimal. Dica: memorize a seguinte tabela:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Acredite! A memorização lhe será muito útil para o exame CCNA. A seguir veremos as classes de endereços IP (A, B e C) e suas peculiaridades, assim como técnicas para a segmentação (*subnetting*).

Um endereço IP consiste de 32 bits de informação (32 dígitos binários - "0s" ou "1s"). Esses bits são divididos em quatro quadrantes

chamados de octetos ou bytes, cada um contendo 8 bits. Eis algumas notações aceitas:

- Decimal (dotted-decimal) (ex.: 172.16.30.56);
- Binário (ex.: 10101100.00010000.00011110.00111000);
- Hexadecimal (ex.: AC 10 1E 38).

Todos os exemplos ilustrados anteriormente representam o mesmo endereço IP, notados em diferentes formas (decimal, binário e hexadecimal), sendo a decimal a mais comum.

O endereço de 32 bits é estruturado de forma hierárquica, em oposição a uma forma plana ou não-hierárquica. Embora ambos os esquemas pudessem ser adotados, o esquema hierárquico foi o escolhido por uma razão: melhor performance no roteamento. Embora o esquema "plano" nos disponibilize um intervalo bem maior de endereços possíveis (2^{32} = 4,3 bilhões), se cada endereço fosse único, todos os roteadores na Internet teriam que armazenar o endereço de cada um dos dispositivos conectado a ela. Isso tornaria impossível um processo de roteamento eficaz, mesmo que apenas uma fração dos endereços viesse a ser, efetivamente, utilizada.

A solução para esse problema foi a adoção de um esquema de endereçamento de três níveis (hierarquia), divididos em: **REDE. <SUBNET> . HOST** (veja figura 5.13). Esse esquema de endereçamento pode ser comparado ao esquema de endereçamento telefônico tradicional: a primeira parte (REDE) identifica uma grande área; a segunda (<SUBNET>) já é mais específica e define a área de chamada, e, finalmente, a última parte - o sufixo - (HOST) identifica o número do cliente na rede.

Outro tipo de rede que adota endereçamento hierárquico é a rede de telefonia. Você nunca parou para pensar no real significado dos números de telefone? Veja na figura 5.12, a decomposição do número 55 11 3344-1234. Note que cada parte desse número identifica algo na rede, partindo de algo bastante abrangente (país) e chegando a uma parte bem específica (assinante). O endereçamento IP pega uma "carona" nessa mesma lógica.

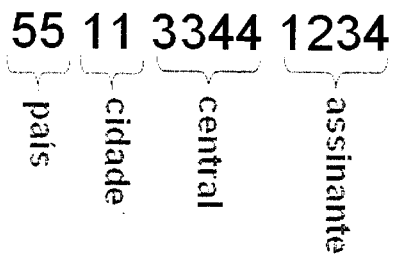


Figura 5.12: Ilustração da hierarquia usada nos números telefônicos.

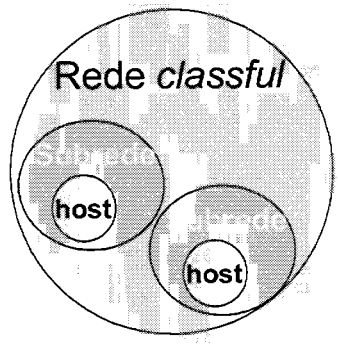


Figura 5.13: Modelo hierárquico aplicado a uma rede.

O endereço de rede (*network address*) identifica cada rede distintamente. Toda e qualquer máquina em uma rede divide o mesmo endereço de rede como parte de seu endereço IP. No endereço IP 172.16.30.56, por exemplo, a parte 172.16 identifica a rede, sendo portanto o seu endereço. O endereço do nó (*node address*) identifica individualmente cada dispositivo conectado na rede, em oposição ao endereço de rede, que identifica em grupo. No exemplo anterior, 30.56 seria o endereço do dispositivo na rede. Os projetistas da Internet decidiram por criar classes de redes baseadas no tamanho delas. Para um pequeno número de redes possuindo um grande número de dispositivos conectados foi criada a classe A de redes (*class A networks*). No outro extremo, temos a classe C, que possui um grande número de redes e um pequeno número de dispositivos conectados a cada uma. A classe B seria um meio termo entre a classe A e a classe C.

	8 bits	8 bits	8 bits	8 bits	Intervalo	Exemplo
Classe A	NET	HOST	HOST	HOST	0-127	1.2.3.4
Classe B	NET	NET	HOST	HOST	128-191	130.10.100.45
Classe C	NET	NET	NET	HOST	192-223	203.232.183.2
Classe D	Classe reservada para endereços multicast					
Classe E	Classe reservada para pesquisa					

Tabela 5.1: Classes de endereços IP.

A subdivisão de um endereço IP nas porções de rede e nó é determinada pela classe em que se encontra tal endereço. A tabela 5.1 sumariza as cinco classes de endereços existentes.

5.5.1 Determinação dos Intervalos

Para assegurar a eficiência no processo de roteamento, os projetistas da "Grande Rede" definiram uma regra para a seção de bits iniciais de cada endereço para cada classe existente. Por exemplo, como um roteador "sabe" que um endereço pertencente à classe A sempre tem

seu primeiro bit 0, ele é capaz de iniciar o encaminhamento do pacote depois de ler apenas esse bit. É aí que está a grande diferença entre as classes de endereços A, B e C (Tabela 5.2).

128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	0*
1	0	0	0	0	0	0	0	128
1	1	0	0	0	0	0	0	192
1	1	1	0	0	0	0	0	224
1	1	1	1	0	0	0	0	240

128	64	32	16	8	4	2	1	
0	1	1	1	1	1	1	1	127**
1	0	1	1	1	1	1	1	191
1	1	0	1	1	1	1	1	223
1	1	1	0	1	1	1	1	239
1	1	1	1	0	1	1	1	247

* resultado de (0*128)+(0*64)+(0*32)+(0*16)+(0*8)+(0*4)+(0*2)+(0*1)
** resultado de (0*128)+(1*64)+(1*32)+(1*16)+(1*8)+(1*4)+(1*2)+(1*1)

Tabela 5.2: Determinação dos intervalos usando o primeiro octeto.

5.5.1.1 Classe A de Endereços

Em um endereço pertencente à classe A, o primeiro byte sempre define o endereço de rede, enquanto os 3 bytes restantes definem o endereço do dispositivo nessa rede (*host*):

rede . host . host . host

Os projetistas do esquema de endereçamento definiram que o primeiro bit do primeiro byte de um endereço pertencente à classe A deve estar desligado, ou seja, tem valor 0. Isso significa que um endereço pertencente à classe A deve estar compreendido entre 0 e 127, pois o endereço máximo seria 01111111 = 127. Eis como esses endereços são definidos:

0xxxxxxx: Se desligarmos e depois ligarmos todos os 7 bits seguintes ao 0, ou seja, se todos assumirem o valor 1, descobriremos o intervalo de endereços IP pertencentes à classe A de endereçamento:

00000000 = 0
01111111 = 127

Portanto, um endereço pertencente à classe A seria definido entre 0 e 127 no primeiro octeto, não podendo ser nem mais, nem menos (discutiremos endereços "ilegais" adiante).

A porção de rede dos endereços de classe A tem o tamanho de 1 byte, com o primeiro bit deste byte reservado e os 7 bits restantes disponíveis para manipulação. Como resultado, o número máximo de redes que pode ser obtido com um endereço de classe A é 128 (126, na verdade, uma vez que os 7 bits restantes não podem ser todos 0 (00000000), assim como o número 127 também está restrito por tratar-se de um endereço reservado). A porção de host dos endereços de classe A possui 24 bits (3 bytes) disponíveis para endereçamento de dispositivos na rede (*host address*). Portanto,

poder-se-ia obter 2^{24} (16.777.216) endereços únicos para cada endereço de rede pertencente à classe A. Entretanto, uma vez que não são permitidos endereços com todos os bits iguais a 1 ou a 0 (por serem reservados), o número real de endereços disponíveis para endereçamento de dispositivos em uma rede classe A seria:

$2^{24} - 2 = 16.777.214$ endereços possíveis.

5.5.1.1.1 Endereços Reservados, Privativos ou Ilegais

Antes de nos aprofundarmos neste capítulo, é importante saber que algumas redes encontram-se reservadas para usos específicos e outras sequer podem ser usadas para endereçamento de dispositivos IP.

A RFC[2] 1918 determina que um intervalo de endereços para cada uma das classes definidas - A, B e C - seja reservado para uso interno, ou seja, esses endereços não são roteáveis na Internet. São eles:

10.0.0.0	a	10.255.255.255	1 rede Classe A
172.16.0.0	a	172.31.255.255	16 redes Classe B
192.168.0.0	a	192.168.255.255	255 redes Classe C

Para que uma rede interna de uma empresa, usando uma das redes anteriormente listadas, consiga acessar um recurso na Internet, um artifício de tradução de endereços (conhecido como NAT - *Network Address Translation*) deve ser empregado. Veremos mais adiante como implementar NAT em routers Cisco.

Além das redes anteriormente ilustradas, ainda temos uma classe "A" inteira considerada ilegal para uso:

127.0.0.0	a	127.255.255.255	loopback interno (localhost)

5.5.1.1.2 Classe A – Endereços Válidos

Eis um exemplo de como se descobrir os endereços de dispositivos válidos de uma rede classe A:

10.0.0.0 - Todos os bits desligados (0) = endereço de rede

10.255.255.255 - Todos os bits ligados (1) = endereço de broadcast

Os endereços válidos para dispositivos estão compreendidos entre o endereço de rede e o endereço de *broadcast* (10.0.0.1 a 10.255.255.254). Note que 0s e 255s são endereços válidos. Tudo o que você deve lembrar ao determinar endereços válidos é que nem todos os bits podem estar ligados ou desligados simultaneamente.

---

[2] *REQUEST FOR COMMENTS* - Tratam-se de "*standards*" definidos que regem, entre outras coisas, os esquemas de endereçamento IP.

5.5.1.2 Classe B de Endereços

Em um endereço de classe B, os primeiros 2 bytes designam a porção de rede, enquanto os 2 bytes restantes designam a porção do host. O formato de um endereço de classe B, então, seria:

rede . rede . host . host

Por exemplo, no endereço IP 172.16.30.56, 172.16 determina o endereço da rede, enquanto 30.56 determina o endereço do dispositivo nessa rede.

Com o endereço de rede sendo formado por 2 bytes (com 8 bits cada), teríamos então 2^{16} possíveis combinações de endereços. No entanto, os projetistas da Internet definiram que os 2 primeiros bits do primeiro byte de um endereço classe B sejam fixados em 1 e 0, respectivamente, o que nos deixa apenas 14 bits para manipulação (2^{14} = 16.384 endereços possíveis).

Endereços de classe B disponibilizam 2 bytes para endereçamento de dispositivos na rede, menos os dois padrões reservados (tudo 0 e tudo 1), o que nos deixa um número de 2^{16} - 2 = 65.534 endereços possíveis para dispositivos para cada endereço de rede classe B.

5.5.1.2.1 Classe B – Endereços Válidos

Eis um exemplo de como descobrir os endereços de dispositivos válidos de uma rede classe B:

172.16.0.0 - Todos os bits desligados (0) = endereço de rede

172.16.255.255 - Todos os bits ligados (1) = endereço de broadcast

Os endereços válidos para dispositivos estão compreendidos entre o endereço de rede e o endereço de *broadcast* (172.16.0.1 a 172.16.255.254). Note que 0s e 255s são endereços válidos. Mais uma vez, ao se determinar o intervalo de endereços válidos para dispositivos, você deve lembrar que nem todos os bits podem estar ligados ou desligados simultaneamente.

5.5.1.3 Classe C de Endereços

Em um endereço de classe C, os primeiros 3 bytes designam a porção de rede, enquanto que o byte restante designa a porção do host. O formato de um endereço de classe C, então, seria:

rede . rede . rede . host

Por exemplo, no endereço IP 192.16.30.56, 192.16.30 determina o endereço da rede, enquanto que 56 determina o endereço do dispositivo nessa rede.

Com o endereço de rede sendo formado por 3 bytes (com 8 bits cada), teríamos então 2^{24} possíveis combinações de endereços. Porém, os projetistas da Internet definiram que os 3 primeiros bits do primeiro byte de um endereço classe C sejam fixados em 1, 1 e 0, respectivamente, o que nos deixa apenas 21 bits para manipulação (2^{21} = 2.097.152 endereços de rede possíveis).

Endereços de classe C disponibilizam apenas 1 byte para endereçamento de dispositivos na rede, menos os dois padrões reservados (tudo 0 e tudo 1), o que nos deixa um número de $2^8 - 2 = 254$ endereços possíveis para dispositivos para cada endereço de rede pertencente à classe C.

5.5.1.3.1 Classe C – Endereços Válidos

Eis um exemplo de como se descobrir os endereços de dispositivos válidos de uma rede classe C:

192.16.10.0 - Todos os bits desligados (0) = endereço de rede

192.16.10.255 - Todos os bits ligados (1) = endereço de broadcast

Os endereços válidos para dispositivos estão compreendidos entre o endereço de rede e o endereço de *broadcast* (192.16.10.1 a 192.16.10.254). Mais uma vez, ao se determinar o intervalo de endereços válidos para dispositivos, você deve se lembrar que nem todos os bits podem estar ligados ou desligados simultaneamente.

5.5.2 Subnetting

Antes de mais nada, é importante sabermos os benefícios alcançados com a criação de sub-redes (*subnet*):

- Redução do tráfego da rede;
- Otimização da performance da rede;
- Simplificação do gerenciamento da rede;
- Distribuição coerente de LANs sobre grandes distâncias.

Discutimos, anteriormente, como definir e identificar intervalos válidos para endereçamento de dispositivos sobre redes pertencentes às classes A, B e C através do "ligamento" e do "desligamento" dos bits reservados para esse endereçamento.

Entretanto, estávamos definindo apenas uma rede. E se desejássemos pegar um endereço de rede e criar seis sub-redes a partir dele? Teríamos de efetuar uma operação conhecida como *subnetting*, que permite que peguemos uma grande rede e a desmembremos em redes menores. Existem muitas razões para a criação de sub-redes:

- **Redução do tráfego na rede:** Tráfego reduzido significa melhor performance e mais segurança. Com o uso de roteadores, a maior parte do tráfego permanece na rede local e apenas pacotes destinados a outras redes os atravessam. Recordemos que roteadores criam domínios de *broadcast*. Quanto menor o domínio de *broadcast* criado, menor o tráfego naquele segmento de rede;
- **Gerenciamento simplificado**: É mais fácil a identificação e isolamento de problemas em grupos de redes menores, interconectadas, do que em apenas uma grande rede;
- **Distribuição coerente de LANs sobre grandes distâncias**: Uma vez que links WAN (*Wide Area Network*) são consideravelmente mais lentos que links LAN, apenas uma e volumosa rede que atinge grandes distâncias está mais sujeita a gerar problemas em cada um dos pontos listados anteriormente. A conexão de múltiplas redes menores faz o sistema funcionar mais eficientemente.

5.5.2.1 Passos para uma Bem-sucedida Implementação de Sub-redes

Para criar sub-redes, separe bits da porção de um endereço IP destinada ao endereçamento de hosts e reserve-os para a definição de uma sub-rede. Isso significa menos bits para o endereçamento de hosts. Portanto, quanto mais sub-redes definidas, menor o número de bits destinados ao endereçamento de dispositivos.

Antes de se definir sub-redes, é importante determinar os requisitos necessários e planejar para condições futuras.

5.5.2.1.1 Máscaras de Rede ou de Sub-rede (Subnet Masks)

Para que o esquema de endereçamento de sub-redes funcione a contento, todos os dispositivos conectados necessitam saber qual a parte do endereço de host que será destinada ao endereço da sub-rede. Isso é conseguido através da designação de uma máscara de rede a cada dispositivo. Essa máscara é um valor de 32-bits que permite ao

recipiente dos pacotes IPs distinguir entre as porções de rede e de host de um endereço IP.

A máscara de rede de 32 bits é composta de 0s e 1s. A ocorrência de 1s representa as posições que se referem ao endereço de rede ou de sub-rede.

Nem todos os endereços de rede necessitam que uma sub-rede seja criada. Nesses casos, uma máscara de rede padrão (*default subnet mask*) é utilizada. Isso é, basicamente, o mesmo que se dizer que essa rede não possui um endereço de sub-rede. As máscaras de rede padrão utilizadas para classes de endereço A, B e C são ilustradas a seguir:

Classe	Formato	Máscara Padrão
A	rede.host.host.host	255.0.0.0
B	rede.rede.host.host	255.255.0.0
C	rede.rede.rede.host	255.255.255.0

Essas máscaras padrão têm suas porções de rede (255) imutáveis. Em outras palavras, não é possível definir uma máscara de sub-rede de classe B como 255.0.0.0. (Reiterando... possível é, mas estaríamos utilizando uma técnica chamada *supernetting*, que não é cobrada no exame CCNA. Para o exame, guarde a informação que as regras para mascaramento **não devem ser infringidas!**).

Para uma máscara de sub-rede de classe A, o primeiro byte não pode ser alterado. Ele deve ter o formato mínimo de 255.0.0.0. Do mesmo modo, não é permitido designar uma máscara no formato 255.255.255.255, uma vez que isso seria o equivalente a ter todos os bits como 1 ou a um endereço de broadcast. Uma máscara de classe B deve começar como 255.255.0.0 e uma de classe C, 255.255.255.0.

5.5.2.1.2 Definição de Sub-redes de Classe C

Existem diversas técnicas para a criação de sub-redes. Fica a seu critério decidir qual funciona melhor para você. Primeiro, discutiremos o método binário de criação e, a seguir, veremos um método mais simples de se fazer a mesma coisa. Você deve estar se perguntando: Por que já não ir para o modo mais simples? Porque é necessário entender como sub-redes são definidas em detalhes, uma vez que isso é uma importante parte do exame CCNA.

Agora, um excelente conselho: Procure entender a tabela a seguir. Mais adiante você irá entender o quão útil essa informação será para você, não apenas no exame, mas em sua vida como administrador de redes.

	1	2	3	4	5	6	7	8
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	64	32	16	8	4	2	1
128	1	0	0	0	0	0	0	0
192	1	1	0	0	0	0	0	0
224	1	1	1	0	0	0	0	0
240	1	1	1	1	0	0	0	0
248	1	1	1	1	1	0	0	0
252	1	1	1	1	1	1	0	0
254	1	1	1	1	1	1	1	0
255	1	1	1	1	1	1	1	1

Em um endereço de classe C, apenas 1 byte (8 bits) encontra-se disponível para endereçamento de dispositivos na rede. Lembre-se que os bits reservados para sub-redes devem começar da esquerda para a direita. Isso significa que as máscaras de rede podem ser as ilustradas na figura anterior (0, 128, 192, 224, 240, 248, 252, 254 e 255).

A RFC 950 determina que não pode haver apenas 1 bit para definição de sub-redes, uma vez que esse bit teria de estar sempre "ligado" ou "desligado", o que seria "ilegal". Portanto, em uma rede classe C, por exemplo, a primeira máscara de rede permitida seria 192 (11000000) e a última, 252 (11111100), uma vez que são necessários pelo menos 2 bits para definição de hosts.

Nota: *O comando ip subnet-zero permite que a regra anterior seja "quebrada" para sub-redes, permitindo que as duas sub-redes consideradas "inválidas" (sub-rede "0" e a sub-rede "all-one") sejam usadas. A partir da versão 12.0 do IOS, o comando ip subnet-zero passou a ser incorporado por default na configuração de routers. Neste livro, iremos nos focar apenas nas regras impostas pela RFC.*

O exame CCNA não vai lhe pedir simplesmente para determinar máscaras de sub-redes de diferentes classes. Ele também poderá lhe passar uma máscara de rede pronta e perguntar:

- Quantas sub-redes tal máscara produz?
- Quantos endereços de host válidos são obtidos por sub-rede?
- Quais são as sub-redes válidas?
- Quais os hosts válidos em cada sub-rede?
- Qual o endereço de broadcast de cada sub-rede?

Para responder a essas perguntas, apresentarei três métodos:

1. O Método Binário

Nesta seção você aprenderá a determinar sub-redes de classe C e a responder as perguntas anteriores utilizando o método binário. Pegaremos como exemplo a primeira máscara de rede disponível à classe C, que utiliza 2 bits para sub-rede. No exemplo mencionado, falamos da máscara 255.255.255.192 (em binário: 11111111.11111111.11111111.11000000).

Como vimos, 192 é o mesmo que 11000000 em binário (lembra-se do conselho de memorizar os esquemas apresentados na página anterior?), ou seja, reservamos 2 bits para a definição de sub-redes e 6 bits para a definição de hosts.

Quais são as sub-redes?

Uma vez que os bits reservados para sub-redes não podem estar todos ligados ou desligados simultaneamente, as duas sub-redes válidas são:

01000000 = 64 e **10**000000 = 128 (00000000 = ilegal e 11000000 = ilegal)

Sub-rede 64		
Sub-rede	**Host**	**Significado**
01	000000 = 64	Endereço de rede
01	000001 = 65	Primeiro host válido
01	111110 = 126	Último host válido
01	111111 = 127	Endereço de broadcast

Sub-rede 128		
Sub-rede	**Host**	**Significado**
10	000000 = 128	Endereço de rede
10	000001 = 129	Primeiro host válido
10	111110 = 190	Último host válido
10	111111 = 191	Endereço de broadcast

Os hosts válidos serão definidos como valores compreendidos entre os intervalos das sub-redes, menos todos os bits ligados e todos os bits desligados. Para identificar os hosts válidos, primeiramente identifique a sub-rede, desligando todos os bits de host (veja quadros anteriores). Em seguida, ligue todos os bits de host para identificar o endereço de *broadcast* da sub-rede identificada. Os endereços válidos para hosts deverão estar compreendidos entre esses dois números (sub-rede e endereço de *broadcast*). Os quadros anteriores ilustram o processo para as duas sub-redes possíveis nesse caso (64 e 128).

O método apresentado até que é bastante simples. No entanto, o que aconteceria se, em vez de apenas 2 bits para sub-redes, tivéssemos 9, 10 ou mesmo 20? Esse método seria praticamente inviável. Ele é muito útil para aprendizagem. Na prática, no entanto, utilizaremos um método mais prático e dinâmico.

2. O Método Alternativo

Quando você se depara com uma máscara de rede e precisa determinar o número de sub-redes, hosts válidos e endereços de *broadcast* que a máscara define, tudo o que você tem a fazer é responder às cinco perguntas listadas anteriormente.

É importante, nesse ponto, que você domine potências de base 2. Veja o subitem *Definição de Sub-redes de Classe C*, neste capítulo. Eis um método prático de determinar a resposta para cada uma das cinco questões:

a) **Quantas sub-redes?** $2^x - 2$ = quantidade de sub-redes, onde "x" representa o número de bits "mascarados" ou o número de 1s. Por exemplo: 11000000 seria $2^2 - 2 = 2$. Nesse caso, haveria duas sub-redes possíveis com tal máscara;

b) **Quantos hosts válidos por sub-rede?** $2^y - 2$ = quantidade de hosts válidos, onde "y" representa o número de bits disponíveis para manipulação dos endereços de host ou o número de 0s. Por exemplo: 11000000 seria $2^6 - 2 = 62$. Nesse caso, existem 62 endereços válidos para hosts por sub-rede;

c) **Quais são as sub-redes válidas?** 256 - máscara de rede = valor da sub-rede base. A esse resultado, soma-se o valor obtido até que se atinja o número da máscara (que seria inválido). Seguindo nosso exemplo: 256 - 192 = 64 (número base e primeira sub-rede válida), 64 + 64 = 128 (segunda sub-rede válida), 128 + 64 = 192 (valor da máscara = sub-rede inválida). Portanto, as sub-redes válidas seriam 64 e 128;

d) **Qual o endereço de *broadcast* para cada sub-rede?** O endereço de *broadcast* seria o valor imediatamente anterior ao da próxima sub-rede (ou da máscara, se estivermos falando da última sub-rede na seqüência). Em nosso exemplo, temos as sub-redes 64 e 128. O endereço de *broadcast* da primeira seria 128 - 1 = 127. Já o da segunda, 192 (valor da máscara) - 1 = 191;

e) **Quais os hosts válidos?** Os valores válidos seriam os compreendidos entre as sub-redes, menos todos os bits ligados e desligados. A melhor maneira de se identificar esses valores é descobrindo as sub-redes válidas e os endereços de *broadcast* de cada uma. Em nosso exemplo, os hosts válidos estariam compreendidos nos intervalos entre 65-126 para a primeira sub-rede e 129-190 para a segunda (pois 64 e 128 são os valores que definem as respectivas sub-redes e não podem ser utilizados no endereçamento de hosts).

3. Definindo Sub-redes "de cabeça"

Exemplo de questão:

Dados o endereço e máscara de rede a seguir, determine a que sub-rede ele pertence, qual o intervalo válido de hosts e qual o endereço de *broadcast*:

192.168.10.33 = Endereço de rede

255.255.255.224 = Máscara de rede

Apesar de tudo o que vimos até agora, é possível definir sub-redes mentalmente, assim como determinar as respostas das cinco perguntas apresentadas anteriormente. Como fazê-lo? Simples. Apenas siga os passos descritos. Vamos utilizar o endereço dado no exemplo anterior:

192.168.10.33 = Endereço de rede

255.255.255.224 = Máscara de rede

Primeiramente, determine a sub-rede e endereço de *broadcast* do endereço de rede anterior (192.168.10.33).

***Atenção**: Essa é uma típica questão da prova CCNA.*

Isso pode ser feito respondendo-se à questão três das cinco questões mencionadas anteriormente:

256 - 224 = 32

32 + 32 = 64

O endereço encontra-se entre as duas sub-redes e, portanto, deve ser parte da sub-rede *32*.

A próxima sub-rede é a *64*, portanto, o endereço de *broadcast* dessa sub-rede seria:

64 - 1 = *63*.

O intervalo válido de hosts, então, seria 192.168.10.*33* a 192.168.10.*62*

Pronto! Mental e rapidamente o problema foi resolvido. Esse método pode ser aplicado não apenas à classe C de endereços, mas também às classes A e B, como veremos a seguir.

Vale ressaltar mais uma vez que esse é o formato de questão comum à prova CCNA quando se trata de sub-redes. Um endereço e uma máscara de rede são dados. O exame pode pedir que se determinem os itens exemplificados anteriormente (o novo formato inclui estudos de caso, mas para a sua resolução basta a aplicação da técnica anterior).

Pratique bastante. Quatro a cinco questões da prova tratam de sub-redes IPs. Acertá-las pode ser a diferença entre passar ou ser reprovado.

Aplicação dos métodos às classes B e C:

A definição de sub-redes em endereços de classe B não foge às regras utilizadas para a classe C. A única diferença é que, agora, teremos menos bits disponíveis para manipulação de sub-redes e, conseqüentemente, mais bits disponíveis para manipulação de hosts.

Endereços de classe B nos disponibilizam 16 bits para endereçamento de hosts. Isso significa que podemos, de fato, utilizar 14 bits para definição de sub-redes, uma vez que devemos deixar ao menos 2 bits para endereçamento de hosts obrigatoriamente.

Lembra-se da tabela que sugeri que fosse memorizada anteriormente? Preste atenção nela. Uma vez que os bits de sub-rede têm seu início da esquerda para a direita, os números obtidos são sempre os mesmos. É importante que esse padrão seja memorizado.

Para a definição de sub-redes de classe B, o processo é o mesmo utilizado para casos de classe C. Utilize os mesmos valores de sub-rede utilizados para classe C, porém, adicione um 0 à porção de rede e um 255 à seção de *broadcast* no quarto octeto.

Exemplo Classe B:

Peguemos o endereço de rede classe B 172.16.0.0 e a máscara de rede 255.255.255.0 (ao contrário do que se possa pensar, nesse caso essa é uma máscara de rede classe B e não uma máscara padrão de classe C).

Endereços de classe B utilizam a máscara padrão 255.255.0.0, o que deixa 14 bits para definição de sub-redes, já que se deve deixar ao menos 2 bits para definição de hosts. A máscara 255.255.255.0 aplicada a um endereço de classe B utiliza 8 bits para definição de sub-redes. Portanto:

1) Número de sub-redes: $2^8 - 2 = 254$;
2) Número de hosts: $2^8 - 2 = 254$;
3) Sub-redes válidas: 256 - 255 = 1, 2, 3, 4 etc. (todas definidas no terceiro octeto!), ou seja, as sub-redes seriam: 172.16.***1***.0, 172.16.***2***.0, 172.16.***3***.0, 172.16.***4***.0, ..., 172.16.***254***.0;
4) Endereço de broadcast para cada sub-rede: 172.16.1.255, 172.16.2.255 etc.;
5) Intervalo válido de hosts para cada sub-rede: 172.16.1.***1*** - 172.16.1.***254*** (lembre-se: trata-se dos valores compreendidos entre o valor da sub-rede [ex.: 172.16.1.*0*] e o do endereço de *broadcast* [172.16 .1.*255*]).

Mais um Exemplo Classe B:

Dados o endereço e máscara de rede a seguir, determine a que sub-rede ele pertence, qual o intervalo válido de hosts e qual o endereço de *broadcast*:

172.16.10.33 = Endereço de rede
255.255.255.224 = Máscara de rede

Primeiramente, determine a sub-rede e endereço de *broadcast* do endereço de rede anterior (172.16.10.33). Isso pode ser feito respondendo-se à questão três das cinco questões mencionadas há pouco:

256 - 224 = *32*.
32 + 32 = *64*.

O endereço encontra-se entre as duas sub-redes e, portanto, deve ser parte da sub-rede 32. Contudo, recorde-se que o terceiro octeto é tido como parte da sub-rede, portanto, a resposta seria a sub-rede *10.32*.

A próxima sub-rede seria a *10.64*, portanto, o endereço de *broadcast* dessa sub-rede é o *10.63*.

O intervalo válido de hosts seria, para esse caso, 172.16.*10.33* a 172.16.*10.62*.

Mais uma vez o problema foi resolvido mental e rapidamente.

Recorde-se de deixar ao menos 2 bits para definição de hosts. Isso é fundamental.

Exemplo Classe A:

Endereço de classe A 10.0.0.0 e máscara de rede 255.255.0.0

Endereços de classe A utilizam a máscara padrão 255.0.0.0, o que deixa 22 bits para definição de sub-redes, uma vez que se deve deixar ao menos 2 bits para definição de hosts. A máscara 255.255.0.0 aplicada a um endereço de classe A utiliza 8 bits para definição de sub-redes. Portanto:

1) Número de sub-redes: $2^8 - 2 = 254$;
2) Número de hosts: $2^{16} - 2 = 65.534$;
3) Sub-redes válidas: 256 - 255 = 1, 2, 3, 4 etc. (todas definidas no segundo octeto!), ou seja, as sub-redes seriam: 10.*1.0.0*, 10.*2.0.0*, 10.*3.0.0*, 10.*4.0.0*, ..., 10.*254.0.0*;
4) Endereço de broadcast para cada sub-rede: 10.*1.255.255*, 10.*2.255.255* etc.;
5) Intervalo válido de hosts para cada sub-rede: 10.*1.0.1* - 10.*1.255.254* (lembre-se: trata-se dos valores compreendidos entre o da sub-rede [ex.: *10.1.0.0*] e o do endereço de broadcast [*10.1.255.255*]).

Finalmente, existe um outro método, ainda mais prático, para ser adotado em questões do tipo "Qual a sub-rede do endereço x.y.w.z, sendo que a máscara utilizada é xxx.yyy.www.zzz?". É realmente muito simples e pode ser adotado para qualquer classe de endereçamento (A, B ou C). Nesse método, utilizaremos as seguintes regras:

a) Sempre que um "255" for identificado na máscara, o valor imediatamente correspondente do endereço IP será mantido;
b) Sempre que um "0" for identificado na máscara, esse mesmo "0" será repetido.

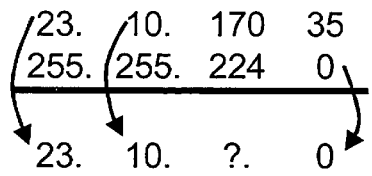
Exemplo:

Dados o endereço e máscara de rede a seguir, determine que sub-rede ele pertence, qual o intervalo válido de hosts e qual o endereço de *broadcast*:

23.10.170.35= Endereço de rede

255.255.224.0 = Máscara de rede

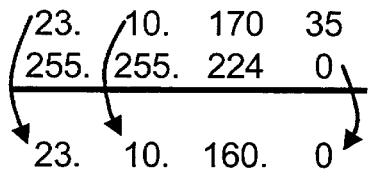
Utilizando a técnica mencionada:



Portanto, fica apenas faltando calcular o "ponto de interrogação". Para fazê-lo, conforme já sabemos:

256 - 224 = *32* (intervalo da sub-rede)

Sendo que *32* é o intervalo identificado e *170* é o valor presente em nosso endereço IP (23.10.*170*.35), basta encontrar qual o valor múltiplo de *32* que seja imediatamente inferior ou igual ao valor em questão (*170*). Se fizermos as contas rapidamente chegaremos em *160* (se somarmos 32 a esse valor, "estouramos", já que 192 é maior que 170). Portanto, nossa "interrogação" é igual a *160*. Nossa sub-rede ficaria (completando-se agora com as informações obtidas):



Portanto, o endereço IP 23.10.170.35, usado com a máscara 255.255.224.0 pertence à sub-rede 23.10.160.0. Simples ou não?

Nota: *Ao contrário do que muitos pensam, um endereço IP terminado em .255 pode, SIM, ser um endereço de um host em uma rede, e não um mero endereço de broadcast! Como? Simples! Imagine a máscara padrão de uma rede classe "A", por exemplo, sendo aplicada ao endereço de rede (classe "A") 10.0.0.0. Teríamos, então, 24 bits reservados para a definição de hosts em cada uma das 126 redes possíveis com essa configuração. Como resultado, teríamos:*

a) 10.0.0.0 = endereço da rede
b) 10.255.255.255 = endereço de broadcast
c) 10.0.0.1 = primeiro host válido
d) 10.255.255.254 = último host válido

Observe que o endereço 10.10.10.255, por exemplo, é um endereço válido para a definição de um host na rede 10, uma vez que se encontra entre o intervalo que define os endereços válidos (todos os valores compreendidos entre o endereço de rede e o endereço de broadcast dela)!

5.5.2.2 Uso da Sub-rede "0" e da Sub-rede "All-One" (Ip Subnet-zero)

Existe ainda alguma polêmica sobre a cobrança desse conhecimento no novo exame CCNA. Existem indícios mostrando que seria de bom tom o candidato ao novo exame conhecer as regras de sub-redes com o recurso *ip subnet-zero* ativado nos routers. Por esse motivo, esse assunto será brevemente discutido. De acordo com alguns sites especializados, *ip subnet-zero* apenas deverá ser usado para cálculos de sub-redes se for explicitamente solicitado na questão do exame. Do contrário, a regra imposta pela RFC 950 de eliminar as sub-redes "0" e "all-one" (o "-2" no cálculo de sub-redes) continua valendo e deve ser aplicada.

A Cisco suporta a criação e o uso de sub-redes "0" e *"all-ones"* já há algum tempo, através do comando *ip subnet-zero*, porém, apenas a partir da versão 12.0 esse comando passou a encontrar-se habilitado por default. Esse comando, basicamente, faz com que o router ignore a regra do "-2" para criação de sub-redes, regra esta imposta pela RFC 950. Apesar de suportado, continua sendo incorreto o uso de tais sub-redes. O motivo pelo qual o uso das sub-redes "0" e *"all-ones"* é desaconselhado pela RFC é simples: evitar confusão. Uma vez que ambas as sub-redes são utilizadas, pode haver confusão sobre o que é endereço da rede *classful* e o endereço de *broadcast* dela, e o que é o endereço da primeira sub-rede (sub-rede "0") e o *broadcast* da última sub-rede (sub-rede *"all-ones"*). Veja um exemplo a seguir:

Vamos pegar o endereço *classful* 192.168.10.0 e aplicar a máscara 255.255.255.192.

Adotando o método *subnet-zero*, vamos identificar as sub-redes que temos. Como o método *subnet-zero* ignora a regra do "-2" para a criação de redes, o cálculo para identificar o número de sub-redes que essa máscara nos disponibiliza seria o seguinte:

2^x = Número de sub-redes, onde "x" é o número de bits sendo usados na porção de host da máscara. Observe que não estamos usando o "-2" no cálculo de sub-redes.

Portanto, no nosso caso, como estamos usando 2 bits para definição de sub-redes no último octeto, o cálculo seria $2^2 = 4$ sub-redes, que seriam:

256 - 192 = 64 (intervalo no qual as sub-redes ocorrem):

Sub-rede 0		
Sub-rede	**Host**	**Significado**
00	000000 = 0	Endereço de rede
00	000001 = 1	Primeiro host válido
00	111110 = 62	Último host válido
00	111111 = 63	Endereço de broadcast

Sub-rede 64		
Sub-rede	**Host**	**Significado**
01	000000 = 64	Endereço de rede
01	000001 = 65	Primeiro host válido
01	111110 = 126	Último host válido
01	111111 = 127	Endereço de broadcast

Sub-rede 128		
Sub-rede	**Host**	**Significado**
10	000000 = 128	Endereço de rede
10	000001 = 129	Primeiro host válido
10	111110 = 190	Último host válido
10	111111 = 191	Endereço de broadcast

Sub-rede 192		
Sub-rede	**Host**	**Significado**
11	000000 = 192	Endereço de rede
11	000001 = 193	Primeiro host válido
11	111110 = 254	Último host válido
11	111111 = 255	Endereço de broadcast

Observe que a primeira sub-rede (sub-rede "0") - que seria eliminada pela regra imposta pela RFC 950 ("-2") - possui seu endereço de rede

igual ao endereço da rede *classful* (192.168.10.0). Observe também que o endereço de *broadcast* da última sub-rede (sub-rede *"all-ones"*, que também seria eliminada pela regra da RFC 950) é exatamente o mesmo endereço de *broadcast* da rede *classful* (192.168.10.255). Esse é o principal motivo para se evitar o uso de sub-redes "0" e "all-ones", mesmo ambas sendo suportadas pelo IOS.

Mais uma vez (nunca é demais frisar isso), apenas adote a regra da sub-rede "0" se isso estiver sendo explicitamente solicitado na questão do exame! Do contrário, efetue os cálculos de sub-redes usando a regra imposta pela RFC 950, como vimos anteriormente (a regra do "-2").

Nota: *A regra da sub-rede "0" permite que se utilizem todas as sub-redes fornecidas pela máscara de sub-rede, porém, o "-2" continua tendo de ser usado para definição dos hosts. Portanto, para descobrir quantos hosts válidos você pode obter por sub-rede no exemplo anterior, use a mesma regra que vimos até agora:* $2^x - 2$*, onde "x" é o número de "0s" que sobraram na máscara. No nosso caso, restaram 6 "0s", portanto:* $2^6 - 2 = 62$ *hosts por sub-rede.*

5.5.3 Sub-redes de Tamanho Variável (VLSM)

VLSM (*Variable Lenght Subnet Mask*), antes parte exclusiva do exame CCNP Routing, passou a ser um assunto cobrado no exame CCNA. Isso faz sentido já que, cada vez mais, VLSM é parte integrante da vida de um engenheiro de redes.

Afinal, o que é VLSM? Para que serve? Como faço para entender e usar essa técnica? Essas são as questões mais comuns quando VLSM é apresentado pela primeira vez. Normalmente, os leitores pensam "Meu Deus... cálculo de sub-redes normais já é complicado! Imagine esse VLSM!!!"

Bom, um certo crédito tem que ser dado a essa pergunta, não há dúvidas! Mas vamos ver um método relativamente simples para entender essa técnica.

Para simplificar, vamos definir VLSM como, simplesmente, "divisão avançada de sub-redes". Como dividir uma rede em sub-redes nós já vimos. VLSM leva esse processo um passo além. Ele permite a divisão das sub-redes geradas (uma, algumas ou todas) em sub-redes ainda menores, permitindo uma melhor utilização dos endereçamentos IPs e - aí vai a principal vantagem - permitindo que o recurso de sumarização seja usado (desde que o protocolo de roteamento suporte ambos: VLSM e

sumarização). Protocolos *classful*, como o RIPv1 e o IGRP, não suportam VLSM, portanto, de nada adianta empregar essa técnica se sua rede está usando esses protocolos. Já RIPv2, EIGRP e OSPF, pelo fato de serem protocolos *classless*, suportam tanto VLSM quanto sumarização de rotas.

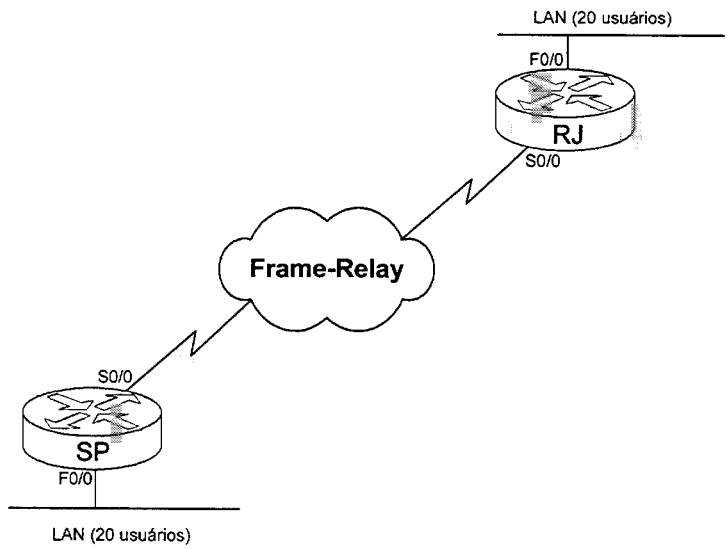
VLSM - Vantagens:

- Flexibiliza o esquema engessado de endereçamento IP, saindo da regra das Classes (A, B e C);
- Permitem sumarização de "n" redes IPs, em apenas um endereço, reduzindo o tamanho das tabelas de roteamento e o processamento pelo roteador.

VLSM - Desvantagens:

- Apenas protocolos de roteamento do tipo *Classless* (ex.: RIPv2, OSPF, EIGRP, BGP) suportam esse tipo de endereçamento;
- A utilização do método VLSM exige mais do administrador de rede, já que torna a definição do plano de endereçamento uma tarefa mais complexa.

O melhor modo de ilustrar VLSM é através de um pequeno cenário. Vamos supor que uma empresa X possua uma rede conforme o diagrama apresentado a seguir.



Analisando o diagrama, identificamos a necessidade da criação de pelo menos três redes (uma para cada LAN e uma para a WAN), sendo que duas delas devem suportar ao menos 20 hosts. O problema é que devemos conseguir isso com apenas um endereço classe C (vamos usar a rede 192.168.10.0). O único modo de conseguir o que é pedido é através da divisão desse endereço em sub-redes. Aproveitando para

retomar o que já vimos: se eu preciso de três sub-redes válidas, qual a máscara a ser adotada?

$$2^x - 2 >= 3 \bullet x = 3 \ (2^3 = 8 - 2 = 6 \ ; 6 >= 3)$$

O valor de "x" encontrado (3) equivale ao número de bits da máscara padrão que devemos "roubar" dos hosts (os "0s", lembra-se?) para conseguir o número desejado de sub-redes. Ou seja, transformaremos 3 "0s" em "1s" na máscara padrão classe C:

11111111.11111111.11111111.00000000 = 255.255.255.0 (máscara padrão)

11111111.11111111.11111111.**111**00000 = 255.255.255.224

Portanto, a máscara a ser adotada para o nosso exercício deve ser 255.255.255.224 (ou /27, se você contar o número de "1s" na máscara). Quais as seis sub-redes válidas que essa máscara nos fornece? Se você está com dúvida aqui, volte ao início da parte de endereçamento IP e reveja os conceitos ali apresentados.

192.168.10.32	192.168.10.64	192.168.10.96
192.168.10.128	192.168.10.160	192.168.10.192

Definido isso, vamos começar o endereçamento pelo router "SP":

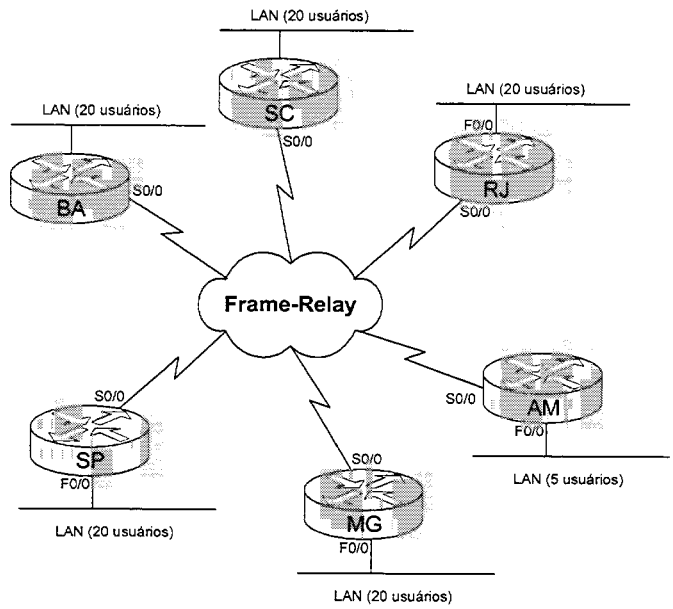
- **Rede da LAN:** 192.168.10.32 /27
- **Endereço da interface do router:** 192.168.10.33
- **Endereço de broadcast:** 192.168.10.63 (lembre-se, o endereço de broadcast é sempre o da próxima rede (64 no caso) menos 1).
- **Rede da WAN:** 192.168.10.64 /27
- **Endereço da interface serial:** 192.168.10.65
- **Endereço de broadcast:** 192.168.10.95

Seguindo agora para o router "RJ":

- **Rede da LAN:** 192.168.10.96 /27
- **Endereço da interface do router:** 192.168.10.97
- **Endereço de broadcast:** 192.168.10.127
- **Rede da WAN:** 192.168.10.64 /27
- **Endereço da interface serial:** 192.168.10.66
- **Endereço de broadcast:** 192.168.10.95

Aí está. Observe que a rede usada por ambas as seriais é a mesma. Isso é lógico, já que ambas devem pertencer à mesma rede para haver comunicação. Cada uma das sub-redes obtidas comporta até 30 hosts,

ou seja, estamos dentro do que nos foi solicitado até o momento. Até agora, apenas o uso de técnicas de sub-redes foi o suficiente para montarmos o plano de endereçamento IP necessário e, ainda, ficamos com três redes de "sobra". Porém, imaginemos que, num futuro não muito distante, nossa pequena empresa cresça e inaugure mais quatro filiais, que serão incorporadas à rede resultando no diagrama apresentado a seguir.



Bom, o que temos aqui, agora, é um autêntico problema de plano de endereçamento. Temos de continuar com apenas uma rede classe C como base (192.168.10.0), mas ao mesmo tempo temos que acomodar as novas localidades e usuários. Com a máscara que havíamos definido anteriormente, conseguíamos obter seis sub-redes válidas, cada uma comportando até 30 hosts. Note que a rede conectada ao router do Amazonas (AM) possui apenas cinco usuários conectados a ela, e não há previsão desse número crescer, já que se trata apenas de um escritório de representação. Em contrapartida, se nossa máscara nos entrega apenas seis sub-redes, temos agora a necessidade de endereçar 7 (6 LANs e 1 WAN). Como resolvemos esse impasse?

Aqui entra VLSM. A idéia é aproveitar melhor os endereços IPs disponíveis, de modo que consigamos endereçar tudo o que precisamos de forma racional.

As seis redes que conseguimos com nossa máscara /27, novamente, são:

192.168.10.32	192.168.10.64	192.168.10.96
192.168.10.128	192.168.10.160	192.168.10.192

Vamos separar uma para cada LAN (pensaremos na WAN posteriormente):

SP 192.168.10.32
RJ 192.168.10.96
MG 192.168.10.128
BA 192.168.10.160
SC 192.168.10.192

Mas espere aí... falta AM! O "esquecimento" foi proposital. Vamos tentar acomodar AM dentro da sub-rede definida anteriormente para a WAN (192.168.10.64). O motivo disso é que a atual necessidade da WAN é de apenas seis hosts (cada uma das seriais dos routers), deixando uma "sobra" de 24 endereços IPs! Podemos dividir novamente essa sub-rede para obter duas novas redes: uma para endereçar as conexões WAN e outra para endereçar a rede LAN de AM. Para isso, usaremos VLSM:

Rede: 192.168.10.64
Máscara:11111111.11111111.11111111.**11**100000 = 255.255.255.224

A técnica aqui é seguir transformando os bits "0" em "1" na máscara, para que alcancemos o que estamos procurando, que basicamente é a criação de duas novas sub-redes dentro da sub-rede 192.168.10.64!

A fórmula a ser usada difere da usada anteriormente no sentido de que, aqui, não precisamos usar o "-2" na fórmula (a regra do "-2" não é aplicável para alocação de bits para sub-redes VLSM):

$2^x >= 2 \square\ x = 1\ (2^1 = 2;\ 2 >= 2)$

Portanto, devemos pegar um "0" e transformá-lo em "1" em nossa máscara:

11111111.11111111.11111111.**1110**0000 = 255.255.255.240

Temos agora duas novas sub-redes, cada uma podendo conter até 14 hosts (para saber o número de hosts por sub-rede, o cálculo a ser feito é $2^x - 2$, onde x é o número de zeros na máscara. Lembre-se sempre que, na máscara, "1s" são para redes, e "0s", para hosts!).

Ótimo, temos então duas novas redes! Quais são elas?

256 - 240 = 16 (intervalo no qual as sub-redes ocorrem)

Rede original = 192.168.10.64

+16 = 192.168.10.80

Visto que já usamos os endereços .65 e .66 nas conexões WAN entre SP e RJ, vamos seguir essa metodologia. Na "nova" rede .64 definiremos todas as conexões WAN de nossa rede, e na "nova" rede .80, a LAN de AM. Nosso novo plano de endereçamento, portanto, ficaria assim:

	SP	RJ	SC	MG	BA	AM
LAN	192.168.10.32 /27	192.168.10.96 /27	192.168.10.128 /27	192.168.10.160 /27	192.168.10.192 /27	192.168.10.80 /28
WAN	192.168.10.64 /28	192.168.10.64 /28	192.168.10.64 /28	192.168.10.64 /28	192.168.10.64 /28	192.168.10.64 /28

Observe como as máscaras se alteram (/27 para a maioria das LANs e /28 para a LAN de AM e para as conexões WAN). Estamos variando as máscaras! Por isso o nome Sub-redes de Tamanho Variável (VLSM).

Nota: *Se estivéssemos usando RIPv1 ou IGRP nessa rede, esse plano de endereçamento não funcionaria a contento, já que RIPv1 e IGRP são protocolos* classfull, *ou seja, não transportam informações das máscaras em seus updates.*

5.5.4 Classless Interdomain Routing (CIDR)

Apesar de este tópico não estar diretamente relacionado ao exame CCNA (nem mesmo ao 640-801), é interessante mencionar algo acerca de CIDR (pronuncia-se "Sáider"). Basicamente, a idéia por trás deste padrão de endereçamento[3] é o contrário da proposta das sub-redes. Enquanto nessa última movemos os bits de host ("0s") para criar um número maior de redes, com CIDR a idéia básica é sumarizar diversas redes em apenas uma, movendo-se a porção de rede ("1s") da máscara original. Esse processo também é conhecido por *Prefix Routing* ou *Supernetting*.

Exemplo: Uma determinada empresa necessita de uma rede IP válida para acesso à Internet. Mediante solicitação, o órgão competente (no Brasil seria a FAPESP) libera o seguinte endereço à empresa solicitante:

200.100.48.0 /**21**

Note que estamos falando de um endereço classe "C" (200.x.x.x), porém, com uma máscara menor que a padrão de classe "C" (a padrão seria /24 = 255.255.255.0). O que isso significa?

/21 = 255.255.248.0 = 11111111.11111111.11111000.00000000

Note que 3 bits da máscara padrão foram "desligados", ampliando o alcance da máscara. Isso significa que a empresa solicitante recebeu não uma classe "C", mas 8! Por que 8? Basta fazer a conta: 2^x, onde "x" é o número de "0s" desligados da máscara original (3). Portanto, $2^3 = 8$. E quais são as classes "C" designadas?

Sabemos que são 8 e que a primeira é a 200.100.48.0.

Para certificar-se de qual seria a primeira rede, basta fazer o velho cálculo:

[3] CIDR é definido pelas RFCs 1517, 1518, 1519 e 1520.

256 – 248 = 8 (intervalo no qual as *supernets* ocorrem). Portanto, se tivesse dito que um dos endereços recebidos pela empresa solicitante era 200.100.51.0 e pedisse para que você localizasse o primeiro e o último, basta saber que o número que você procura é um múltiplo de 8. O múltiplo de 8 imediatamente inferior ao IP fornecido (200.100.51.0) seria 200.100.48.0! (51 não é múltiplo; 48, sim).

Portanto, as redes classe "C" seriam:

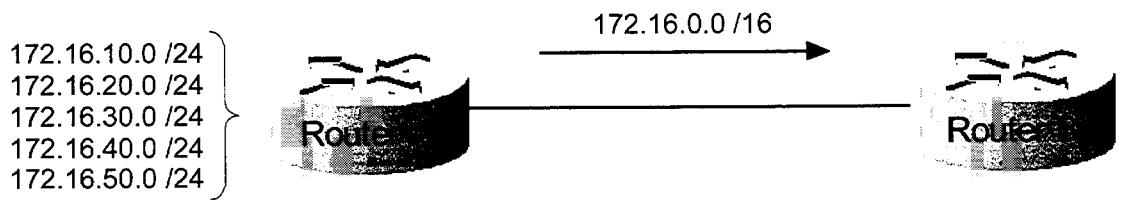
200.100.48.0	200.100.49.0	200.100.50.0	200.100.51.0
200.100.52.0	200.100.53.0	200.100.54.0	200.100.55.0

Qual a vantagem disso tudo? A vantagem é principalmente dos provedores de Internet, que com CIDR conseguem uma redução substancial da tabela de roteamento, através da sumarização das oito classes de endereços alocados para a empresa em questão em apenas um endereço, com prefixo */21*. Ou seja, nas tabelas de roteamento dos provedores, em vez de serem propagados oito endereços classe "C" (*/24*), apenas um endereço */21* será propagado (200.100.48.0 */21*). Bastante prático, não acha?

Nota: *Assim como VLSM, CIDR não funciona se usado com protocolos* classful, *como RIPv1 e IGRP.*

5.5.5 Sumarização

A sumarização de rotas - também conhecida como "agregação de rotas" - permite que protocolos propaguem a informação de várias redes usando apenas uma - a rota sumarizada. A seguir temos um exemplo simples que ilustra o processo:



Note que apenas a rede 172.16.0.0 está sendo propagada. Isso é exatamente o que protocolos do tipo *classful* fazem. Como eles não propagam informações de máscaras (no caso, /24), apenas a rede *classful* é divulgada em seus updates - o que pode ser bastante inconveniente se você possui redes descontíguas. Esse é um exemplo simples de sumarização. Vamos a um mais complexo.

Lembrando que uma das vantagens em se adotar VLSM é exatamente a de poder sumarizar rotas, como poderíamos sumarizar as redes contidas

no intervalo 192.168.16.0 a 192.168.31.0? O primeiro passo aqui é descobrir o tamanho do bloco válido. Os blocos válidos iniciam em 4 e continuam com a multiplicação desse valor por 2 (4, 8, 16, 32, 64 etc.). No intervalo desejado (192.168.16.0 - 192.168.31.0), temos exatamente 16 sub-redes, portanto, podemos adotar o bloco 16. Para finalmente chegar à máscara que sumarizará essas 16 redes, basta fazer o cálculo [256 - tamanho do bloco]. No nosso caso, 256 - 16 = 240. Nossa máscara seria, portanto, 255.255.240.0. Note que o valor "240" foi colocado no 3o. octeto, pois esse é o octeto a ser sumarizado. Portanto, nosso endereço sumarizado seria o primeiro endereço do intervalo de IPs fornecido, seguido da máscara que acabamos de encontrar: 192.168.16.0 255.255.240.0. Com isso estaremos divulgando 16 endereços de classe "C" através de apenas um update de roteamento.

Vamos agora complicar um pouco mais. Suponha que a seguinte rede lhe é passada:

192.1.144.0 */20*

E deseja-se saber, dos endereços IPs a seguir, quais fariam parte desse endereço sumarizado (isso pode ser uma questão de exame, portanto, procure entender a lógica do processo):

192.1.*159*.2	192.1.*160*.11	192.1.*138*.41
192.1.*151*.254	192.1.*143*.145	192.1.*1*.144

Aqui, a dica é descobrir, antes de mais nada, em qual octeto a sumarização ocorre. Isso deve ser fácil de perceber, mas na dúvida, observe a máscara (/20): ela indica que a sumarização ocorre no 3o. octeto (255.255.240.0).

O "bloco" a ser usado, então, é 16 (256 - 240 = 16).

Para fazer o cálculo do intervalo, partindo-se da rede sumarizada dada (192.1.144.0), devemos fazer o seguinte:

1) Subtrai-se "1" do bloco encontrado (*16 - 1 = 15*);

Nota: *Temos sempre que subtrair 1 do número do bloco, pois a contagem começa em "0" e não em "1". Se não subtrairmos "1", nossa contagem resultará em uma rede a mais do que deveríamos obter.*

2) Soma-se o valor encontrado (15) ao valor da rede sumarizada (192.1.*144*.0 + 15 = 192.1.*159*.0).

Ou seja, os endereços compreendidos entre 192.1.*144*.0 a 192.1.*159*.0 pertencem a esse endereço sumarizado. De nossa lista, apenas os endereços a seguir satisfazem essa condição:

192.1.*159*.2 e 192.1.*151*.254

Outro método para se chegar à mesma conclusão é através de cálculos binários. Basicamente, você deve converter para binário o terceiro octeto da rede sumarizada fornecida, e comparar os padrões com o terceiro octeto dos outros endereços. Esse método é um pouco mais trabalhoso, mas menos sujeito a erros:

192.1.144.0 */20*

144 em binário seria *1001*0000 (observe que apenas destacamos os bits até onde os "1s" aparecem. Os "0s" que seguem são irrelevantes para a comparação de padrão com as outras redes). Sabemos que 144 é a rede "mãe", pois apenas "0s" seguem o padrão de 4 bits (1001).

Dos outros endereços, teríamos:

159 **1001**xxxx
160 1010xxxx
138 1000xxxx
151 **1001**xxxx
143 1000xxxx
1 0000xxxx

Portanto, observando-se com atenção, percebemos que apenas as redes 192.1.*159*.2 e 192.1.*151*.254 possuem o mesmo padrão binário no terceiro octeto (*1001*) adotado pelo endereço de rede sumarizado, sendo essas as duas únicas redes que fazem parte da rede sumarizada 192.1.144.0 */20*. Observe também que é possível dizer qual é a máscara, observando-se o número de bits que formam o padrão (4 bits no caso: 1001). Assim, como temos 4 bits formando o padrão no terceiro octeto, nossa máscara sumarizada seria /20 (16 bits dos 2 primeiros octetos + 4 bits do terceiro).

Finalmente, um último exercício apenas para deixar este assunto muito bem sedimentado. Qual endereço sumarizaria as redes a seguir?

172.16.10.0 /24	172.16.11.0 /24	172.16.12.0 /24	172.16.15.0 /24

Novamente, o primeiro passo é descobrir quantas redes pertencem ao intervalo de que estamos falando. O modo mais simples é fazer esta conta: [maior rede - menor rede + 1]: 15 - 10 + 1 = 6. Portanto, devemos escolher um bloco que seja **maior ou igual** ao valor encontrado. No nosso caso, o bloco seria 8.

O próximo passo é descobrir a máscara da rede sumarizada. Isso pode ser atingido através de outro cálculo simples: [256 - valor do bloco], ou seja, 256 - 8 = 248.

Finalmente, precisamos descobrir qual o endereço resultante da rede sumarizada. Lembre-se de que, para que seja um endereço sumarizado, o valor do octeto onde a sumarização ocorre (no nosso caso, o terceiro octeto) deve ser igual ao valor do bloco encontrado (no nosso caso, 8). Logo, nossa rede seria 172.16.8.0.

Problema resolvido. O endereço de rede que sumariza as quatro redes apresentadas seria:

172.16.8.0 /21 (lembre-se que /21 é equivalente a 255.255.248.0). Note que esse endereço sumariza não apenas as quatro redes apresentadas, mas um total de oito redes (172.16.8.0 a 172.16.15.0). Não é possível sumarizar apenas os quatro endereços apresentados.

Pelo método binário:

10 = *00001*010
11 = *00001*011
12 = 00001100
15 = 00001111

Os quatro endereços dividem o mesmo padrão de 5 bits à esquerda (00001). Para descobrir a rede "mãe" basta pegar os 5 bits do padrão e completá-los com "0s": 00001*000* = 8. Assim, nossa rede "mãe" seria 172.16.8.0. Quanto à máscara, como temos somente 3 bits livres após o padrão, basta "puxar" a máscara até "descobri-los". Se fizermos isso no terceiro octeto, teremos a máscara /21 (16 bits dos dois primeiros octetos + 5 bits usados pelo padrão no terceiro octeto = 21). Outra forma é usar o bloco no cálculo, como já vimos: O bloco é 8, como já descobrimos anteriormente. 256 - 8 = 248. 255.255.248.0 = /21. Como você pode notar, existem inúmeras maneiras de se alcançar o mesmo resultado.

5.6 IP version 6 (IPv6)

Este é um dos novos tópicos abordados pelo exame 640-802. IPv6 é mais do que uma nova versão do protocolo IP atual (IPv4), que é atualmente a base da Internet. Trata-se de um protocolo totalmente novo, já que apresenta uma arquitetura de cabeçalho completamente diferente, introduzindo novos serviços e aprimorando os já existentes. Em termos de escalabilidade, o IPv6 quadruplica o número de bits disponíveis para endereçamento, ou seja, temos 128 bits - contra apenas 32 do IPv4. Para se ter uma idéia da magnitude do novo esquema de endereçamento provido pelo IPv6, se todas as redes IPv4 fossem migradas para IPv6, seria possível alocar um endereço de rede único

para cada dispositivo de rede em operação no planeta (3,4 * 10^{34} endereços). A previsão atual para a exaustão de todos os endereços IPv4 livres para atribuição à operadores é em abril de 2010, o que significa que a transição da versão do IPv4 para o IPv6 é inevitável num futuro próximo. O governo dos Estados Unidos da América, por exemplo, já determinou que todas as suas agências federais devem suportar o protocolo IPv6 até 2008.

5.6.1 Principais Motivações para a Migração do IPv4 para IPv6

- **Espaço de endereçamento:** A maior parte dos endereços disponíveis hoje no IPv4, encontram-se alocados na classe C, que é insuficiente para muitas organizações. Os endereços de classe B estão praticamente esgotados;
- **Qualidade de serviço:** O IPv6 prevê a acomodação dos serviços convergentes (por exemplo: VoIP, streaming de vídeo em tempo real, etc), suportando intrinsecamente classes de serviço diferenciadas;
- **Mobilidade:** A mobilidade vem se tornando um fator muito importante na sociedade. O IPv6 permite a mobilidade dos usuários, onde estes podem ser contatados em qualquer rede, por meio de seu endereço IPv6 de origem, ou seja, cada pessoa no planeta poderia ter um endereço IPv6 como se fosse um número de identidade.

5.6.2 Novidades nas Especificações do IPv6

- **Espaço de endereçamento:** Os endereços IPv6 têm um tamanho de 128 bits;
- **Autoconfiguração de endereço:** Suporte para atribuição automática de endereços numa rede IPv6, podendo ser omitido o servidor de DHCP a que estamos habituados no IPv4;
- **Endereçamento hierárquico:** Simplifica as tabelas de encaminhamento dos routers da rede, diminuindo assim a carga de processamento dos mesmos;
- **Formato do cabeçalho:** Totalmente remodelados em relação ao IPv4;

- **Cabeçalhos de extensão:** Opção para incorporar requerimentos adicionais, ad-hoc;
- **Suporte à qualidade de serviço diferenciada:** Aplicações de áudio e vídeo passam a estabelecer conexões apropriadas tendo em conta às suas exigências em termos de qualidade de serviço (QoS);
- **Capacidade de extensão:** Permite adicionar novas especificações de forma simples;
- **Encriptação:** Diversas extensões no IPv6 permitem, à partida, o suporte para opções de segurança como autenticação, integridade e confidencialidade dos dados.

5.6.3 Formato do Datagrama IPv6

Um datagrama IPv6 é constituído por um cabeçalho base, ilustrado na figura 5.14, seguido de zero ou mais cabeçalhos de extensão, seguidos depois pelo bloco de dados.

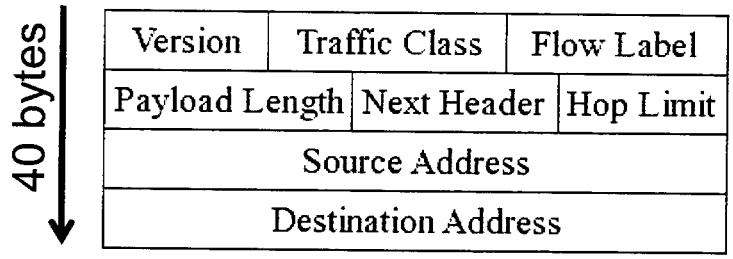


Figura 5.14 – Formato do cabeçalho IPv6

Características do Cabeçalho Base do Datagrama IPv6:

- Tem menos informação que o cabeçalho do IPv4. Por exemplo, o *checksum* será removido do cabeçalho, que nesta versão considera que o controle de erros das camadas inferiores é confiável;
- O campo *Traffic Class* é usado para assinalar a classe de serviço a que o pacote pertence, permitindo assim dar diferentes tratamentos a pacotes provenientes de aplicações com exigências distintas. Este campo serve de base para o funcionamento do mecanismo de Qualidade de Serviço (QoS) na Rede;
- O campo *Flow Label* é usado com novas aplicações que necessitem de bom desempenho. Permite associar datagramas que fazem parte da comunicação entre duas aplicações. Usados para enviar datagramas ao longo de um caminho predefinido;

- O campo *Payload Length* representa, como o nome indica, o volume de dados em bytes que o pacote transporta;
- O campo *Next Header* aponta para o primeiro *header* de extensão. Usado para especificar o tipo de informação que está depois do cabeçalho corrente;
- O campo *Hop Limit* tem o número de *hops* transmitidos antes de descartar o datagrama, ou seja, este campo indica o número máximo de saltos (passagem por encaminhadores) que o datagrama pode dar, antes de ser descartado, semelhante ao TTL do IPv4.

5.6.4 Fragmentação e Determinação do Percurso

Em redes IPv6, o responsável pela fragmentação é o *host* que envia o datagrama, e não os routers intermediários, como ocorre em redes IPv4. No IPv6, os routers intermediários descartam os datagramas maiores que o MTU (*Maximum Transmit Unit*) máximo da rede. O MTU será o MTU máximo suportado pelas diferentes redes entre a origem e o destino. Para isso o *host* envia pacotes ICMP de vários tamanhos. Quando um pacote chega ao *host destino*, todos os dados a serem transmitidos são fragmentados no tamanho deste pacote que alcançou o destino. O processo de descoberta do MTU é dinâmico, porque o percurso pode ser alterado durante a transmissão dos datagramas.

5.6.5 Múltiplos Cabeçalhos

Uma das novidades do IPv6, é a possibilidade de utilização de múltiplos cabeçalhos encadeados. Estes cabeçalhos adicionais permitem uma maior eficiência, já que o tamanho do cabeçalho pode ser dimensionado de acordo com as necessidades de transmissão. Também permite uma maior flexibilidade, já que possibilita a adição de novos cabeçalhos para atender às novas especificações, conforme estas surjam.

As especificações atuais recomendam a seguinte ordem:

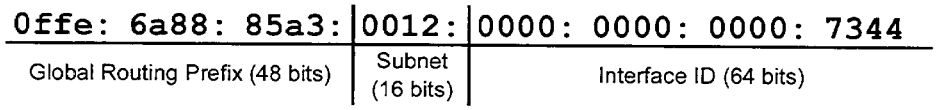
1. *IPv6;*
2. *Hop-By-Hop Options Header;*
3. *Destination Option Header;*
4. *Routing Header;*
5. *Fragment Header;*
6. *Authentication Security Payload Header;*
7. *Destination Options Header;*
8. *Upper-Layer Header.*

5.6.6 Endereçamento

O endereçamento no IPv6 é de 128 bits e, assim como seu antecessor (o IPv4), inclui prefixo de rede e sufixo de host. No entanto, não existem classes de endereços, como ocorre no IPv4. Dessa forma, a fronteira do prefixo e do sufixo pode ser em qualquer posição do endereço.

Um endereço padrão IPv6 deve ser formado por um campo *provider ID, subscriber ID, subnet ID e node ID*. Recomenda-se que o último campo tenha pelo menos 48 bits para comportar o endereço MAC.

Os endereços IPv6 são normalmente escritos como oito grupos de 4 dígitos hexadecimais, sendo estes divididos em 3 grupos. Por exemplo:



O interessante é que, "0"s à esquerda e uma seqüência contígua de "0"s podem ser omitidos, como no exemplo ilustrado a seguir, utilizando o endereço anterior como base:

ffe:6a88:85a3:12:0:0:0:7344 ou

ffe:6a88:85a3:12::7344

Vale ressaltar que o uso de "::" apenas é permitido **uma única vez no endereço.** Portanto, se tivéssemos o endereço:

0ffe:6a88:0000:0000:85a3:0000:0000:7344

Ele poderia ser escrito nos formatos:

ffe:6a88:0:0:85a3:: 7344

ffe:6a88::85a3:0:0:7344

Nota: *O entendimento do formato dos endereços IPv6 e sua correta grafia é um dos pontos mais importantes sobre este tópico para o exame CCNA.*

Assim como no IPv4, o IPv6 possui alguns tipos de endereços especiais:

- **Unicast:** Cada endereço corresponde a uma interface (dispositivo);
- **Global Unicast:** Endereço unicast público e roteável na Internet;
- **Link-Local:** Equivalentes aos endereços privados do IPv4, ou seja, não são roteados publicamente;

- **Unique Local:** Também não-roteáveis publicamente, entretanto, são únicos globalmente;
- **Multicast:** O mesmo conceito utilizado no IPv4. Um datagrama enviado para um endereço *multicast* é recebido por todos os dispositivos parte deste grupo *multicast*;
- **Anycast:** Trata-se de uma versão modificada do *multicast*. Ao invés do datagrama ser enviado a todos os participantes do grupo, como no *multicast*, ele é enviado apenas para um dos dispositivos, por exemplo, o mais próximo. Este tipo de endereço é uma novidade existente apenas no IPv6.

5.6.7 Estruturas de Endereços de Transição

Os endereços IPv6 podem ser, até certo ponto, compatíveis com IPv4, podendo o primeiro conter endereços IPv4. Para tal, os 128 bits do IPv6 ficam assim divididos:

- campo de 80 bits colocado a '0' (zero);
- campo de 16 bits colocado a '0' (zero);
- endereço IPv4 de 32 bits.

Ou seja, um endereço IPv6 compatível com um endereço IPv4 teria este formato:

::<endereço IPv4>

Endereços IPv6 nativos podem ser mapeados para endereços IPv4 em routers que suportem ambos os protocolos, permitindo que elementos IPv4 estabeleçam um "túnel" através de uma estrutura IPv6. Neste caso, diferentemente do exemplo anterior, no qual endereços IPv6 compatíveis com endereços IPv4 são manualmente gerados, este mapeamento de endereços ocorre automaticamente nos routers que suportam ambos os protocolos. Para tal, os 128 bits do IPv6 teriam o seguinte formato:

- campo de 80 bits colocado a '0' (zero);
- campo de 16 bits colocado a 'F';
- endereço IPv4 de 32 bits.

Como resultado, endereços IPv6 nativos mapeados para IPv4 teriam a seguinte sintaxe:

::FFFF:<endereço IPv4>

5.6.8 Endereços IPv6 Especiais

- **0:0:0:0:0:0:0:1** - Equivalente ao endereço IPv4 127.0.0.1;
- **0:0:0:0:0:0:192.168.0.1** - Exemplo de sintaxe de um endereço IPv4 grafado no formato IPv6;
- **2000::/3** - Intervalo dos endereços *Global Unicast;*
- **FC00::/7** - Intervalo de endereços *Unique Local;*
- **FE80::/10** - Intervalo de endereços *Link-Local;*
- **FF00::/8** - Intervalo de endereços *Multicast;*
- **2002::/16** - Usado no modo "6to4", um modo de transição que permite aos endereços IPv6 trafegarem em uma rede IPv4 sem a necessidade de se configurar túneis.

5.6.9 Autoconfiguração

IPv6 traz de volta uma funcionalidade que já existia em protocolos mais antigos, como o velho IPX da Novell: a possibilidade de um host se autoconfigurar com um endereço de rede. O modo como o IPv6 faz isso, inclusive, é muito parecido com o método utilizado pela Novell. O host determina a informação de prefixo por meio de um router na rede e, uma vez de posse desta informação, ele adiciona como Interface ID o endereço MAC de sua placa de rede. Este tipo de configuração chama-se *stateless*, pois o host é configurado obtendo apenas a informação do prefixo do router. Nenhum outro dispositivo é envolvido. No caso de um servidor DHCP existir (sim, IPv6 também pode usar um servidor DHCP, chamado DHCPv6), a configuração do IP no host é denominada *stateful*.

5.6.10 Protocolos de Apoio ao IPv6

Para operar em conjunto com a nova versão do protocolo IP, algumas aplicações e protocolos tiveram de ser revistos. Eis alguns deles:

- ICMP - ICMPv6;
- DHCP - DHCPv6;
- EIGRP - EIGRPv6;
- OSPF - OSPFv3 (note que aqui é v3 e não v6!).

5.6.11 Migração para IPv6

Certamente você deve ter imaginado que o processo de migração do protocolo IPv4 (atual) para o IPv6 não deve ser fácil. Basta imaginar a

quantidade de elementos envolvidos. Isso dá para assustar até o mais bravo dos engenheiros de rede! Entretanto, esta migração já teve início faz algum tempo. Se não percebemos, é porque o que quer que seja que estão fazendo, estão fazendo certo. Parte dos *backbones* Internet existentes hoje já operam na versão 6 do protocolo IP. Como isso é possível se nossos PCs, roteadores e outros elementos de rede ainda rodam a versão 4 do protocolo? Existem algumas técnicas de migração que podem ser utilizadas para que o protocolo IPv6 coexista, sem maiores problemas, o tempo que for necessário com o IPv4. Irei apresentá-las a seguir:

5.6.11.1 Dual Stacking

Dual stacking é a técnica de migração mais popular, e basicamente, consiste em rodar simultaneamente, em um mesmo roteador, os protocolos IPv4 e IPv6. Neste modo, uma mesma interface de um roteador será configurada com endereços IPv4 e IPv6, ou seja, uma mesma interface pode receber e encaminhar pacotes IPv4 e IPv6, sem problemas. A vantagem deste método é que novos elementos de rede já podem ser endereçados em IPv6, e os elementos já existentes podem ser migrados em fases sem grandes impactos. A configuração em roteadores também é bastante simples.

5.6.11.2 Tunelamento 6to4 (6to4 Tunneling)

Esta técnica consiste em encapsular um datagrama IPv6 com um cabeçalho IPv4 para que pacotes IPv6 possam atravessar redes que ainda rodam a versão 4 do protocolo. A desvantagem deste método é que, como o datagrama IPv6 é encapsulado com um cabeçalho IPv4, estamos adicionando *overhead* ao pacote de dados.

Questões de Revisão – TCP/IP

1. Qual o protocolo que atua na camada de Transporte e permite comunicação não orientada à conexão entre hosts?

a) IP
b) ARP
c) TCP
d) UDP

2. Qual o protocolo que atua na camada de Transporte e estabelece circuitos virtuais entre hosts antes do início da transmissão de dados?

a) IP
b) ARP
c) TCP
d) UDP

3. Qual protocolo presente na Camada de Rede (Internet) não é orientado à conexão, mas é responsável pela comunicação lógica entre dois hosts?

a) IP
b) ARP
c) TCP
d) UDP

4. Um host envia um pedido via frame broadcast para a rede e seu propósito é que alguma máquina na rede responda a esse pedido com um endereço IP para ser usado por esse host. Qual protocolo de Camada de Rede está sendo usado nesse processo?

a) RARP
b) ARPA
c) ICMP
d) TCP
e) IPX

5. Se uma determinada interface de um router está com o buffer em via de se esgotar, qual protocolo do conjunto de protocolos IPs pode ser usado para informar esse fato aos dispositivos vizinhos?

a) RARP
b) ARP
c) ICMP
d) IP
e) TCP

6. É dado o endereço IP 172.16.10.22 /28. Qual o intervalo válido de hosts?

a) 172.16.10.20 a 172.16.10.22
b) 172.16.10.1 a 172.16.10.255
c) 172.16.10.16 a 172.16.10.23
d) 172.16.10.17 a 172.16.10.31
e) 172.16.10.17 a 172.16.10.30

7. Qual intervalo numérico define, no primeiro octeto, um endereço de rede de classe B?

a) 1-126
b) 1-127
c) 128-190
d) 128-191
e) 129-192
f) 192-220

8. Qual intervalo numérico define, no primeiro octeto, um endereço de rede de classe C?

a) 1-127
b) 129-192
c) 203-234
d) 192-223

9. Quantos bytes possui um endereço Ethernet?

a) 3
b) 4
c) 5
d) 6
e) 7
f) 8
g) 16

10. Qual o protocolo usado para descobrir o endereço de hardware de um dispositivo local?

a) RARP
b) ARP
c) IP
d) ICMP
e) BootP

11. Qual dos seguintes é o endereço de broadcast enviado para uma rede de classe B, usando-se a máscara de rede padrão definida para essa classe?

a) 172.16.10.255
b) 172.16.255.255
c) 172.255.255.255
d) 255.255.255.255

12. Qual classe de endereços IPs permite um máximo de apenas 254 endereços de host por endereço de rede?

a) A
b) B
c) C
d) D
e) E

13. Qual é o endereço de broadcast da sub-rede que o endereço 10.254.255.19 255.255.255.248 pertence?

a) 10.254.255.23
b) 10.254.255.24
c) 10.254.255.255
d) 10.255.255.255

14. Qual é o endereço de broadcast da sub-rede que o endereço 172.16.99.99 255.255.192.0 pertence?

a) 172.16.99.255
b) 172.16.127.255
c) 172.16.255.255
d) 172.16.64.127

15. Qual máscara de sub-rede você usaria para obter 12 sub-redes em uma rede classful /24?

a) 255.255.255.252
b) 255.255.255.248
c) 255.255.255.240
d) 255.255.255.255

16. Qual o intervalo de portas válido que um host pode usar para estabelecer uma sessão com um outro host?

a) 1-1023
b) 1024 e acima
c) 1-256
d) 1-65534

17. Qual dos seguintes intervalos define os números de portas bem-conhecidas?

a) 1-1023
b) 1024 e acima
c) 1-256
d) 1-65534

18. Qual é o endereço de broadcast da sub-rede que o endereço 10.10.10.10 255.255.254.0 pertence?

a) 10.10.10.255
b) 10.10.11.255
c) 10.10.255.255
d) 10.255.255.255

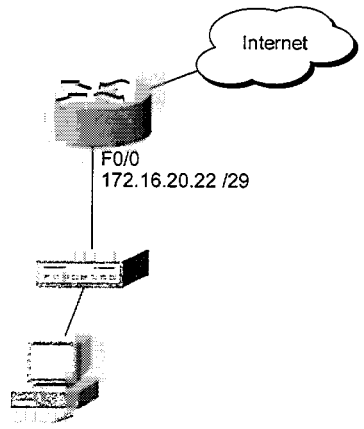
19. Qual é o endereço de broadcast da sub-rede a que o endereço 192.168.210.5 255.255.255.252 pertence?

a) 192.168.210.255
b) 192.168.210.254
c) 192.168.210.7
d) 192.168.210.15

20. Se você precisasse dividir um endereço de classe B em exatamente 510 sub-redes, qual máscara de sub-rede você deveria utilizar?

a) 255.255.255.252
b) 255.255.255.128
c) 255.255.0.0
d) 255.255.255.192

21. Observe o diagrama a seguir e responda: qual poderia ser o endereço IP do host ilustrado?



a) 172.16.20.23
b) 172.16.20.16
c) 172.16.20.17
d) 172.16.20.24

22. Você possui uma sub-net 192.168.10.224 /28, porém, precisa usar VLSM para que ela passe a acomodar duas novas sub-redes, cada uma comportando até 6 hosts. Qual seriam as novas sub-redes e suas respectivas máscaras?

a) 192.168.10.228 /29 e 192.168.10.232 /30
b) 192.168.10.224 /29 e 192.168.10.232 /29
c) 192.168.10.224 /30 e 192.168.10.232 /30
d) 192.168.10.228 /29 e 192.168.10.236 /29

23. Quais dos endereços de rede a seguir não são sumarizados pelo endereço 172.16.8.0 /21?

a) 172.16.7.0
b) 172.16.8.0
c) 172.16.10.0
d) 172.16.12.0
e) 172.16.15.0
f) 172.16.16.0

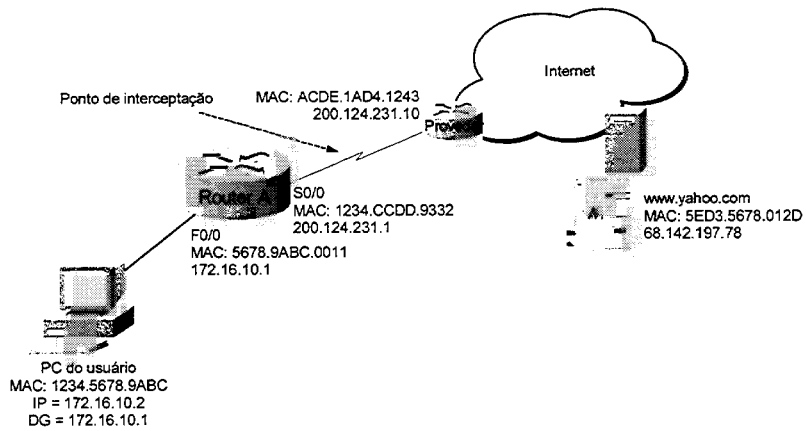
24. Qual o principal benefício atingido com o uso de CIDR?

a) A sumarização de diversas redes em apenas uma, aumentando o tamanho da tabela de roteamento.
b) A divisão de uma grande rede em redes menores, mais fáceis de serem gerenciadas.
c) A sumarização de diversas redes em apenas uma, reduzindo o volume da tabela de roteamento.
d) A divisão de uma rede pequena em porções ainda menores, aumentando a segurança da rede como um todo.

25. Como poderia ser feita a sumarização dos endereços 192.168.10.0, 192.168.11.0, 192.168.15.0?

a) Não há como sumarizar esses endereços
b) 192.168.8.0 /21
c) 192.168.0.0 /24
d) 192.168.10.0 /21

26. Analisando o diagrama a seguir, se o usuário ilustrado tentar um acesso ao site do Yahoo e os dados gerados por essa solicitação forem interceptados no ponto assinalado, o que encontraremos como origem e destino do pacote IP, supondo que NAT não esteja sendo utilizado?



a) A. O: 200.124.231.1 D: 200.124.231.10
b) B. O: 200.124.231.1 D: 68.142.197.78
c) C. O: 172.16.10.2 D: 200.124.231.10
d) D. O: 172.16.10.2 D: 68.142.197.78
e) E. O: 1234.5678.9ABC D: 5ED3.5678.012D
f) F. O: 1234.CCDD.9332 D: ACDE.1AD4.1243

27. Quais as duas afirmações sobre endereços IPv6 são verdadeiras?

a) Zeros à esquerda são sempre requeridos.
b) A notação "::" é utilizada para informar uma seqüência de campos hexadecimais compostos de "0"s.

c) A notação "::" é utilizada para separar os campos-chave do endereço.
d) Uma única interface tem múltiplos endereços IPv6 de diferentes tipos associados à ela.

28. Qual a notação do endereço de loopback de um host configurado com IPv6?

a) 127.0.0.1
b) 0.0.0.0
c) 0.0.0.0.0.0.0.0
d) ::1
e) 0.0::1

29. Qual alternativa melhor descreve endereços Global Unicast?

a) Datagramas endereçados a um endereço *Unicast* são entregues a um único host.
b) Estes são, normalmente, endereços roteáveis na internet pública.
c) Estes são endereços privados não-roteáveis na internet pública.
d) Estes são endereços não-roteáveis na internet pública, porém, globalmente únicos para cada host.

30. Qual alternativa melhor descreve endereços Unicast?

a) Datagramas endereçados a um endereço Unicast são entregues a um único host.
b) Estes são, normalmente, endereços roteáveis na internet pública.
c) Estes são endereços privados não-roteáveis na internet pública.
d) Estes são endereços não-roteáveis na internet pública, porém, globalmente únicos para cada host.

31. Qual alternativa melhor descreve endereços Link-Local?

a) Datagramas endereçados a um endereço Link-Local são entregues a um grupo de hosts.
b) Estes são, normalmente, endereços roteáveis na internet pública.
c) Estes são endereços privados não-roteáveis na internet pública.
d) Estes são endereços não-roteáveis na internet pública, porém, globalmente únicos para cada host.

32. Qual alternativa melhor descreve endereços Unique-Local?

a) Datagramas endereçados a um endereço Unique-Local são entregues ao primeiro host disponível.
b) Estes são, normalmente, endereços roteáveis na internet pública.
c) Estes são endereços privados não-roteáveis na internet pública.
d) Estes são endereços não-roteáveis na internet pública, porém, globalmente únicos para cada host.

33. Qual o método existente para migração do IPv4 para IPv6 que demanda um roteador ter endereços das 2 versões configuradas em uma mesma interface?

a) Dual Stacking
b) 6to4 tunneling
c) 6to4 stacking
d) IPv6 stacking
e) NATv6

Respostas das Questões de Revisão – TCP/IP

1. **D**. UDP é o protocolo usado na camada de transporte para permitir uma comunicação não-orientada à conexão.

2. **C**. TCP estabelece um circuito virtual antes da transmissão de dados. Esse processo estabelece uma sessão de transporte confiável, conhecida como comunicação orientada à conexão.

3. **A**. IP é usado no endereçamento de hosts e no roteamento de pacotes através da rede, não sendo orientado à conexão. O protocolo IP, por si só, é um protocolo que realiza seu trabalho baseado na premissa do "melhor esforço". Os protocolos de camada superior conferem ao IP características de confiabilidade (TCP) ou não (UDP).

4. **A**. RARP é usado para encontrar um endereço IP através de um endereço de hardware conhecido.

5. **C**. ICMP é usado para enviar mensagens de redirecionamento para o dispositivo de origem.

6. **E**. 256–240=16. A primeira sub-rede é a 16; a segunda é a 32. Esse host deve estar na sub-rede 16; o endereço de broadcast é 31 e o intervalo válido de hosts é 17 à 30.

7. **D**. Uma rede classe B é definida no primeiro octeto entre o intervalo 128-191.

8. **D**. A rede de classe C é definida no primeiro octeto entre o intervalo 192-223.

9. **D**. Um endereço Ethernet (MAC) tem um comprimento de 6 bytes (48 bits).

10. **B**. ARP é usado para encontrar o endereço de hardware através de um endereço IP conhecido.

11. **B**. A porção de rede de um endereço de classe B tem a extensão de 2 bytes, o que significa que sobram 2 bytes para o endereçamento de hosts. O endereço de rede deve ser 172.16.0.0, ou seja, todos os bits reservados para endereçamento de hosts encontram-se desligados. O endereço de *broadcast* possui todos os bits reservados para endereçamento de hosts ligados, ou seja, 172.16.255.255.

12. **C**. Um endereço de rede de classe C possui apenas 8 bits para a definição dos hosts, portanto $2^8-2=254$.

13. **A**. 256-248=8. A primeira sub-rede é a 8, a segunda é a 16, a terceira é a 24. Esse host deve estar na sub-rede 16; o endereço de *broadcast* é 23 e o intervalo válido de hosts é 17 a 22.

14. **B**. No terceiro octeto: 256-192=64. A primeira sub-rede é a 64.0; a segunda sub-rede é a 128.0. Esse host deve estar na sub-rede 64.0; o endereço de broadcast é 127.255 e o intervalo válido de hosts é 64.1 a 127.254.

15. **C**. Dê uma olhada nas alternativas e verifique qual máscara de rede dará a você o que você precisa. 252 lhe dá 62 sub-redes ($2^6-2=62$), 248 lhe dá 30 sub-redes ($2^5-2=30$), 240 lhe dá 14 sub-redes ($2^4-2=14$) e 255 é inválido.

16. **B**. Hosts em processo de estabelecer uma sessão podem usar qualquer número de porta igual ou superior a 1024.

17. **A**. Os números de portas de 1 a 1023 são considerados números de portas bem conhecidos e são reservados para aplicações específicas (ex.: http = porta 80).

18. **B**. No terceiro octeto: 256-254=2. A primeira sub-rede é a 10.1.2.0; a segunda é a 10.1.4.0, depois 10.1.6.0, 10.1.8.0 etc. Perceba que 2 bits do terceiro octeto e os 8 bits do quarto octeto são destinados ao endereçamento de hosts. Nessa questão o host é parte da sub-rede 10.10.10.0, o endereço de broadcast é 10.10.11.255 (1 - o endereço da próxima sub-rede [10.10.12.0]) e o intervalo de hosts válidos vai de 10.10.10.1 a 10.10.11.254.

19. **C**. 256-252=4. A primeira sub-rede é a 4; a segunda é a 8. Esse host deve estar na sub-rede 4; o endereço de *broadcast* é 7 e o intervalo válido de hosts é 5 a 6 (2 hosts apenas).

20. **B**. Aqui, a pergunta que você deve se fazer é: $2^x - 2 = 510$, ou seja, 2 elevado a qual potência menos 2 me resulta em exatamente 510 sub-redes? $2^9 - 2 = 510$! Assim, estamos usando 9 bits da porção de hosts para montar nossa máscara, então: 255.255.255.128.

21. **C**. A máscara usada aqui é 255.255.255.248 (/29). 256-248=8, portanto, o endereço que procuramos deve estar contido no intervalo de 16 a 23. A alternativa A refere-se ao *broadcast* dessa rede, portanto, trata-se de um endereço inválido para endereçamento de hosts.

22. **B**. Seguindo as regras de sumarização já vistas, bastaria você identificar que a máscara /28 equivale à 255.255.255.240, portanto, as sub-redes ocorrem de 16 em 16. Se temos uma sub-rede específica e desejamos reparti-la em duas, basta mover a máscara 1 bit para a direita. Dessa forma, criaríamos duas novas sub-redes: 192.168.10.224 e 192.168.10.232, ambas sob a máscara 255.255.255.248 (/29).

23. **A, F**. A máscara usada para sumarização é 255.255.248.0 (/21). 256-248=8, portanto, as redes sumarizadas encontram-se no intervalo de 172.16.8.0 a 172.16.15.0 (8 sub-redes).

24. **C**. CIDR possibilita que blocos de redes IPs sejam propagados como apenas uma rede, reduzindo assim o tamanho da tabela de roteamento.

25. **B**. 15-10=5, logo, o bloco que devemos adotar é o de tamanho 8, o que também indica que as redes ocorrem em intervalos de 8. 192.168.10.0 não é múltiplo de 8 (10 não é múltiplo), portanto, sabemos que essa não é a rede "mãe" que sumarizará esses endereços. O primeiro múltiplo de 8 imediatamente inferior à menor rede apresentada (10, no caso) seria o próprio 8. Dessa forma, nossa rede "mãe" seria 192.168.8.0. Resta descobrir a sua máscara agora. Sabemos que o bloco usado é 8. $2^x = 8$; $x = 3$. Portanto, precisamos "apagar" 3 bits de nossa máscara padrão (/24) para sumarizar esses endereços. O resultado é /21 (255.255.248.0). As redes sumarizadas por esse endereço seriam as contidas no intervalo de 192.168.8.0 a 192.168.15.0 (8 redes no total). Para fazer o mesmo usando o método binário:

*00001*010 = 10

*00001*001 = 11

*00001*111 = 15

Observe que as três redes dividem um mesmo padrão de bits mais significativos (à esquerda) no terceiro octeto. Como temos 3 bits após o padrão: $2^3 = 8$ (o mesmo bloco que encontramos pelo outro método). A rede mãe, portanto, seria a que se inicia com o padrão de bits seguido

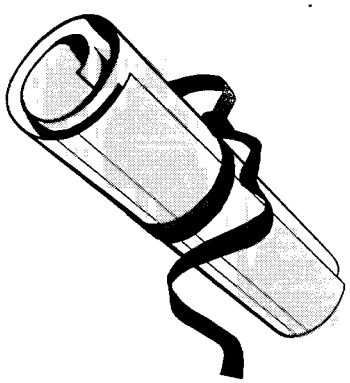
de "0s": 00001000 = 8, ou seja, a rede mãe seria 192.168.8.0. Como se pode notar, chegamos ao mesmo resultado.

26. D. Essa é uma questão importante e muita atenção deve ser dada a ela.

Cabeçalho Frame		Cabeçalho Pacote		
d:ACDE.1AD4.1243	o:1234.CCDD.9332	d:68.142.197.78	o:172.16.10.2	**DADOS**

No exemplo anterior, temos um "retrato" do pacote capturado no ponto de interceptação. Note que o pacote (encapsulado dentro do frame) **não se altera** (os endereços IPs de origem e destino sempre serão os mesmos, até que o pacote atinja seu destino final). O frame, por sua vez, sempre sofre alterações conforme ele atravessa a rede. Por esse motivo, os endereços de origem e destino serão modificados. É o que vemos aqui: endereço de origem do pacote: IP do host; endereço de destino do pacote: IP do Yahoo; endereço de origem do frame: MAC da interface serial do Router A (interface que gerou o frame ou "reencapsulou o pacote"). Endereço de destino do frame: MAC da interface do router do provedor. Note que, assim que entrar na próxima rede, o cabeçalho do frame mudará outra vez e, assim, sucessivamente.

27. B, D
28. D
29. B
30. A
31. C
32. D
33. A



6 Configuração Básica de Roteadores Cisco

6.1 Tópicos Abordados

- O Sistema Cisco IOS (*Internetwork Operating System*);
- O Modo *Setup* em um Router Cisco;
- Conectando-se a um Router nos Modos Usuário e Privilegiado;
- Encontrando Comandos através dos Recursos de Ajuda (*help*);
- Utilizando Comandos através do Modo de Edição;
- Configurando Senhas, Identificação e Mensagens;
- Configurando uma Interface com Endereços IPs e Máscaras de Sub-rede;
- Copiando a Configuração para a NVRAM;
- Utilizando o Cisco Secure Device Manager (SDM).

6.2 O Sistema Cisco IOS (Internetwork Operating System)

O Cisco IOS é o núcleo dos roteadores e de grande parte dos switches da Cisco. Quase todos os equipamentos Cisco rodam o sistema Cisco IOS, entretanto, nem todos os switches Cisco o suportam (isso porque algumas linhas de switches eram originalmente de outras empresas, como a *Stratacom*, que foram adquiridas pela Cisco).

O IOS foi criado para transportar serviços de rede e disponibilizar aplicações voltadas à rede. O sistema IOS é utilizado para implementar as seguintes funções em um hardware Cisco:

- Transportar funções e protocolos de rede;
- Estabelecer tráfego de alta velocidade entre dispositivos;
- Disponibilizar ferramentas de segurança para controle de acesso e bloqueio de usuários não-autorizados;
- Prover escalabilidade para facilitar o crescimento da rede e redundância;
- Prover confiabilidade para conexão aos recursos da rede.

O sistema IOS pode ser acessado através da porta console de um roteador (uma porta serial de baixa velocidade, normalmente disponibilizada nos formatos RJ-45 ou DB-15), de um modem ou mesmo via Telnet. O acesso ao sistema IOS via linhas de comando é conhecido como uma sessão EXEC (*EXEC session*).A figura 6.1 ilustra as portas e slots do modelo 2801, um dos roteadores da nova linha Cisco de equipamentos.

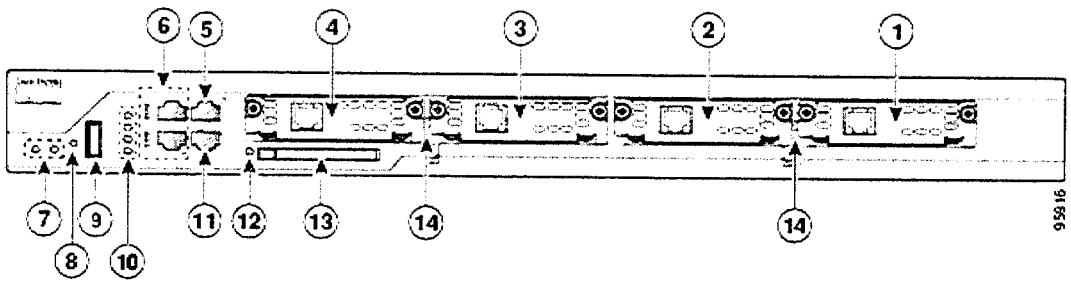


Figura 6.1: Ilustração da parte traseira do roteador Cisco 2801.

1	Slot 0 (VIC or VWIC, for voice only)	8	Auxiliary Power (AUX/PWR) LED
2	Slot 1 (WIC, VIC, VWIC, or HWIC)	9	Universal serial bus (USB) port
3	Slot 2 (WIC, VIC, or VWIC)	10	AIM/PVDM LEDs
4	Slot 3 (WIC, VIC, VWIC, or HWIC)	11	Auxiliary port
5	Console port	12	Compact flash (CF) LED
6	Fast Ethernet ports and LEDs	13	External CompactFlash memory card slot
7	System LEDs	14	Removable center card guides to allow double-wide HWIC-D installation

Tabela 6.1: Portas e slots do modelo 2801.

Você pode se conectar a um router Cisco para configurá-lo, verificar sua configuração, solucionar problemas ou checar estatísticas. Existem diferentes maneiras de se conectar a um router Cisco, sendo a mais comum através da porta Console (número 5 na tabela).

A porta Console usualmente é uma porta RJ-45 (figura 6.1). Não há senha pré-configurada para essa porta, como default.

Nota: *Para conexão com a porta Console, eis como o seu emulador de terminal (Windows HyperTerminal, por exemplo) deve ser configurado:*

- *9600bps;*
- *8 Data Bits;*
- *Parity None;*
- *Stop Bits 1;*
- *Flow Control None.*

Outro modo de se conectar a um router Cisco é através de uma porta Auxiliar (*Auxiliary port*) (11), que funciona como uma porta Console e que pode ser utilizada como tal. Entretanto, essa porta permite que sejam configurados comandos de modem para que um acesso discado (via modem) seja realizado. Isso significa que você pode discar para o modem conectado à porta Auxiliar do router e configurá-lo remotamente, procedimento este muito útil em casos nos quais as portas locais do router encontram-se *down*. Para exemplificar, imagine que você acaba de configurar um router que se encontra remotamente distante. Você retorna à sua cidade e, em seguida, o telefone toca. É o seu cliente dizendo que o router que você acaba de configurar está agindo de forma estranha. Nesse caso, você tem duas opções: voltar ao local onde se encontra o router e fisicamente checá-lo (opção não muito boa, não é verdade?) ou - se você conectou um modem à porta Auxiliar do router em questão - discar via *HyperTerminal*, por exemplo, para o número do modem e acessar o router remotamente. Essa última opção é bastante prática, visto que você poderia fazer isso de sua própria casa, prestando assim um serviço rápido e eficiente.

O terceiro modo de se conectar a um router é através de um programa cliente Telnet, que é um programa emulador que funciona como um "terminal-burro". Você pode utilizar Telnet para se conectar a qualquer porta ativa de um router, seja ela serial, Ethernet ou qualquer outra porta de comunicação - que possua um endereço IP configurado - ativa.

Na figura 6.1, ilustramos as portas e slots do modelo 2801, um dos routers da linha 28xx da Cisco. Note que, este modelo de roteador possui apenas suas portas FastEthernet fixas. Ele possui 4 slots para a inserção das mais diversas interfaces que vão desde módulos com até 4 portas seriais, até módulos com portas de voz (FXS, FXO, E1, E&M), para interconexão com a rede pública de telefonia ou aparelhos PABX.

É importante saber como a numeração das interfaces ocorre em um roteador Cisco, de acordo com as novas regras criadas pela empresa recentemente. No caso do 2801, por exemplo, as interfaces têm sua numeração da seguinte forma:

Slot Number	Slot Type	Interface Numbering Range
Onboard ports	Fast Ethernet	0/0 and 0/1
0	VIC / VWIC (voice only)[2]	0/0/0 to 0/0/3
1	HWIC / WIC / VIC / VWIC[1]	0/1/0 to 0/1/3 (single-wide HWIC) 0/1/0 to 0/1/7 (double-wide HWIC)
2	WIC / VIC / VWIC[1]	0/2/0 to 0/2/3
3	HWIC / WIC / VIC / VWIC[1]	0/3/0 to 0/3/3 (single-wide HWIC) 0/3/0 to 0/3/7 (double-wide HWIC)

[1] A VWIC in slots 1, 2, and 3 can operate in both data and voice mode; in slot 0, a VWIC can only operate in voice mode.

[2] **Slot 0** in 2801 can be configured for voice only; thus **PRI** configurations with VWIC is not possible. **Slot 0** can be configured for **CAS** signaling.

Observe que não temos apenas módulos WIC, mas VWIC (*Voice*) e HWIC (alta densidade de portas, um módulo deste suporta até 4 portas seriais, por exemplo). Além disso, a Cisco lançou a arquitetura *double-wide*, onde é possível utilizar módulos de tamanho duplo, removendo a divisão entre dois slots consecutivos (figura 6.2).

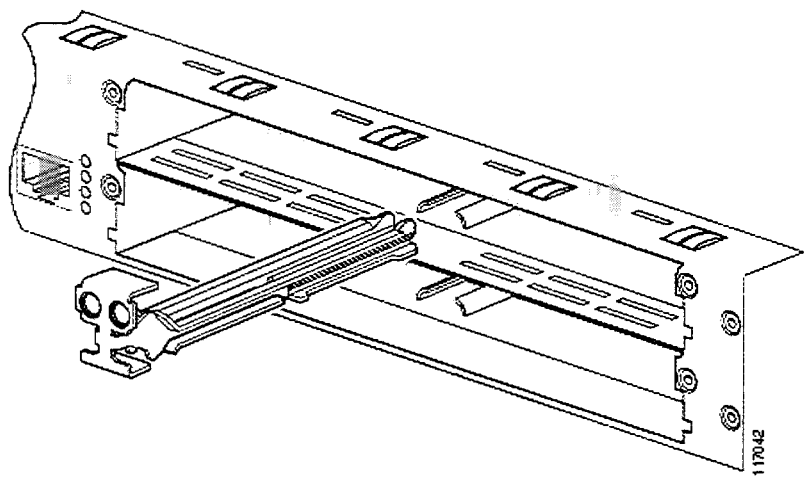


Figura 6.2: Arquitetura double-wide.

Portanto, se quiséssemos configurar a segunda porta serial presente em um módulo WIC-2T instalado no slot 2 de um roteador Cisco 2801, teríamos que acessar a interface **Serial 0/2/1**. Maiores detalhes podem ser obtidos no site da Cisco <http://www.cisco.com/en/US/products/hw/routers/ps282/products_tech_note09186a008035b051.shtml>.

6.2.1 A Rotina de Inicialização de um Router Cisco

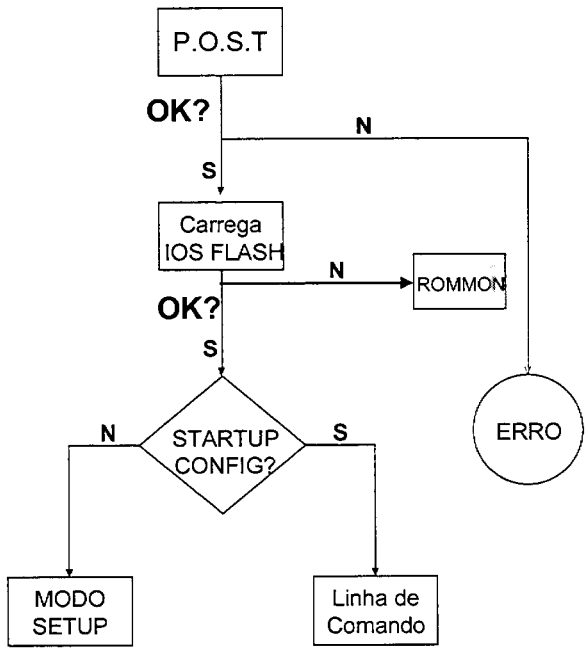


Figura 6.3: Diagrama do esquema de inicialização de um roteador Cisco.

Quando um roteador Cisco é ligado, ele executa uma checagem geral do hardware chamada POST (*Power On Self Test*) e, se passar, ele irá procurar e carregar o sistema IOS da memória FLASH, se o arquivo estiver presente. A memória FLASH é um tipo de memória eletronicamente deletável, programável e acessível apenas para leitura (*Erasable Programmable Read-Only Memory* = EEPROM). O IOS será carregado na memória RAM do roteador, e então tentará localizar um arquivo de configuração chamado *startup-config*, que fica armazenado por default na memória RAM não-volátil (NVRAM), ou seja, um tipo de memória análoga à RAM tradicional, cujo conteúdo é mantido por baterias (ou seja, seu conteúdo não é perdido quando o dispositivo é desligado).

Caso não exista nenhum arquivo de configuração na NVRAM (ex.: há um router novo ou o arquivo foi deletado), o router irá trazer o que chamamos de *setup mode* (veja diagrama). Esse é um modo básico de configuração, que permite o ajuste do router passo a passo por intermédio de menus. Você pode optar pela configuração via menus (*setup*) a qualquer momento digitando o comando *setup* no modo privilegiado do IOS. O modo *setup*, apesar de descomplicado, cobre apenas comandos genéricos. É bastante útil quando você não sabe como configurar determinados protocolos, como *bridging* ou *DECnet*, por exemplo.

Você tem à sua disposição duas escolhas quando utiliza o modo *setup*: Gerenciamento *Básico*, bastante limitado, e *Estendido*. O modo

básico permite apenas configurações para conectividade básica do router; já o modo estendido permite que se configurem parâmetros globais, assim como parâmetros de interface, oferecendo um maior controle sobre o hardware (router).

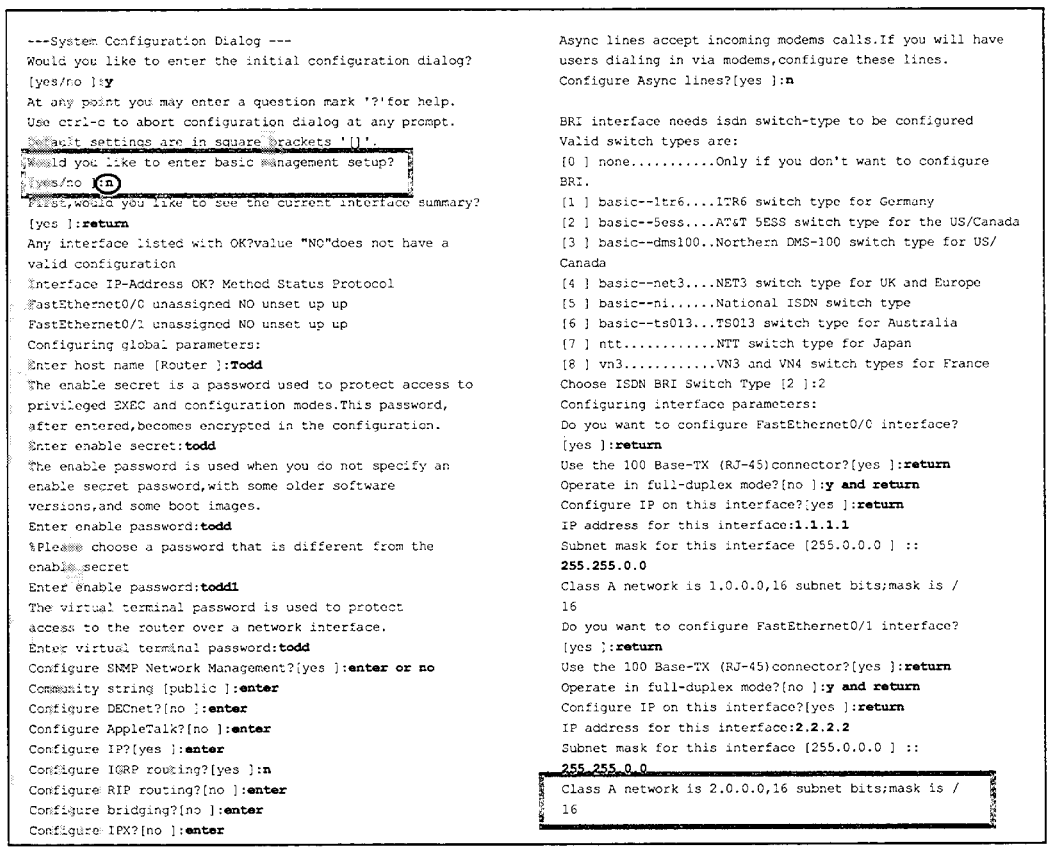


Figura 6.4: Tela de configuração via setup estendido.

Repare na configuração anterior em que o modo *setup* pede duas senhas (*passwords*). Falaremos de senhas mais adiante, porém, é necessário que se entenda que, na verdade, apenas uma delas é importante: *enable secret password*. A outra senha (*enable password*) era utilizada em routers com sistema IOS com versões anteriores à 10.3 e foi mantida para efeitos de compatibilidade. Entretanto, o modo *setup* exige que ambas sejam configuradas. Além disso, elas precisam ser distintas. A *enable password* **nunca** será usada se a *enable secret password* estiver configurada no router.

A próxima senha é utilizada para sessões Telnet com o router. A razão pela qual o modo *setup* configura uma senha Telnet (VTY) é porque, **se uma senha para as linhas VTY (Telnet) não for configurada, você não pode, por default, conectar-se a um router via Telnet.** Falaremos em detalhes sobre senhas mais adiante.

A configuração ilustrada anteriormente é deveras simplista, mas já é o suficiente para inicializar e configurar um router de modo muito rápido.

Note que a máscara de rede é apresentada no formato */16*, o que significa que 16 de 32 bits estão sendo usados para definição de sub-redes. Um ponto interessante do gerenciamento estendido é a opção que o usuário recebe no final:

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:0
```

Você pode ir para o modo CLI (configuração via linha de comando) e descartar o *running-config [0]*, pode voltar ao *setup* e repetir o processo *[1]* ou pode salvar a configuração criada, que após gravada na NVRAM recebe o nome de *startup-config*. Esse arquivo será então carregado toda vez que o router for inicializado. No nosso caso, a opção *[0]* (descartar configuração e entrar no modo CLI) foi escolhida.

6.2.2 A Interface de Comando (CLI)

A interface de linha de comando (CLI - *Command Line Interface*) é sem dúvida o modo mais completo de se configurar um router, uma vez que lhe oferece uma gama de opções muito mais variada e um maior poder de customização. Para entrar na interface de comando, simplesmente escolha *NO* no diálogo inicial de configuração (veja a figura anterior). Após esse passo, o router irá lhe mostrar mensagens com informações sobre todas as interfaces disponíveis nele.

6.2.2.1 Conectando-se (Logging in) a um Router

Após a apresentação do status das interfaces e você ter pressionado <Enter>, um prompt aparecerá (similar a um prompt do DOS [>] - veja a ilustração seguinte). Você se encontra no que chamamos de modo usuário (*user mode*). Você apenas pode alterar ou criar configurações em um router se estiver logado em modo privilegiado (*privileged mode*). Para entrar em modo privilegiado, digite o comando *enable* no prompt do modo usuário (*router>enable*). Ao digitar esse comando e teclar <Enter>, o prompt se altera para um sinal # (*router#*).

Prompt	Modo
>	Usuário
#	Privilegiado

É importante saber diferenciar em que modo você está entrando os comandos em um router. O exame CCNA sabe disso e irá testar seus conhecimentos neste ponto: uma vez em modo privilegiado, você pode

digitar o comando *disable* para retornar ao modo usuário; uma vez no modo usuário, digitando-se o comando *logout* ou *exit* você encerra a sessão.

Para tornar a vida dos administradores de rede mais fácil, o IOS aceita abreviações para alguns comandos. Por exemplo, o comando *enable* pode ser digitado apenas *en*.

```
Would you like to enter the initial configuration dialog?
[yes]:n
Would you like to terminate autoinstall? [yes]:[Enter]

Press RETURN to get started!

00:00:42: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
00:00:42: %LINK-3-UPDOWN: Interface Serial0/0, changed
state to down
00:00:42: %LINK-3-UPDOWN: Interface Serial0/1, changed
state to down
00:00:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
00:00:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to down
00:00:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/1, changed state to down
00:01:30: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
00:01:31: %LINK-5-CHANGED: Interface Serial0/0, changed
state to administratively down
00:01:31: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
00:01:31: %LINK-5-CHANGED: Interface Serial0/1, changed
state to administratively down
00:01:32: %IP-5-WEBINST_KILL: Terminating DNS process
00:01:38: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 2600 Software (2600-BIN-M), Version 12.2(13),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 04-Jan-03 19:23 by dschwart

Router>
Router>enable
Router#
```

No modo de configuração CLI, você pode efetuar configurações globais no router digitando o comando *config terminal* (#config t), o que o colocará em modo de configuração global (*global configuration mode*) e possibilitará mudanças ao que chamamos de *running-config* (configuração armazenada na DRAM, que se encontra em atividade no router). A partir desse ponto, todas as configurações afetarão o router integralmente. Digitando apenas *#config* lhe serão apresentadas algumas opções (*terminal, memory* ou *network*), sendo *terminal* a default.

Para alterar configurações armazenadas na DRAM (*running-config*), utilizamos a opção terminal. Para efetuar alterações nas configurações armazenadas na NVRAM (*startup-config*), utilizamos a opção *memory* (ou *mem*). Finalmente, se você desejasse alterar um arquivo de configuração armazenado em um servidor TFTP, você optaria pela opção *network* (ou *net*). Portanto, se você digitar *#config-mem* ou *#config-net* você estará, de fato, substituindo sua *running-config* atual por uma armazenada na NVRAM (*mem*) ou em um servidor TFTP (*net*). É importantíssimo lembrar-se disso!

6.2.2.2 Estudo dos Diferentes Prompts do CLI

Como foi anteriormente mencionado, é de extrema importância que se entendam os diferentes tipos de prompts que existem no sistema IOS, pois assim você pode saber exatamente onde está quando estiver configurando um router. **Sempre cheque os prompts antes de efetuar uma configuração** (ou de responder a uma questão no exame!).

Descreveremos brevemente todos os prompts com os quais você irá se deparar no decorrer dos próximos tópicos.

Prompt	Significado
>	Acesso em modo usuário.
#	Acesso em modo privilegiado.
(config)#	Modo de configuração global.
(config-if)#	Modo de configuração de interface.
(config-subif)#	Modo de configuração de subinterface.
(config-line)#	Modo de configuração de linha (ex. AUX, CON ou VTY).
(config-router)#	Modo de configuração de protocolos de roteamento.

Tabela 6.2: Resumo dos prompts a serem estudados.

Prompt de interfaces:

```
Router(config)#interface ?
  Async              Async interface
  BVI                Bridge-Group Virtual Interface
  CTunnel            CTunnel interface
  Dialer             Dialer interface
  FastEthernet       FastEthernet IEEE 802.3
  Group-Async        Async Group interface
  Lex                Lex interface
  Loopback           Loopback interface
  MFR Multilink      Frame Relay bundle interface
  Multilink          Multilink-group interface
  Null               Null interface
  Serial             Serial
  Tunnel             Tunnel interface
  Vif PGM            Multicast Host interface
  Virtual-Template   Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing
  range              Interface range command
Router(config)#interface fastethernet 0/0
Router(config-if)#
```

Note na figura anterior que, logo após digitarmos o comando *#interface,* digitamos um ponto de interrogação (*?*). Isso é parte do **sistema de ajuda** do IOS. Observe que o IOS traz todas as interfaces disponíveis no router em questão, facilitando o próximo passo do comando. Basta identificar a interface desejada e adicioná-la ao comando (ex. *#interface FastEthernet0/0* ou, simplesmente, *#int f0/0*). Note que o prompt mudará para *(config-if)#*, indicando que você se encontra agora no **modo de configuração de interface.**

O sistema IOS não indica em qual interface você está trabalhando, o que pode tornar sua vida mais complicada se você não souber onde exatamente está. Um modo simples de contornar essa situação é tomar nota de cada ação tomada. Isso pode evitar um "retrabalho" posterior ou mesmo a configuração errônea de uma interface.

Prompt de subinterfaces:

```
Router(config)#int fastethernet0/0.?
<0-4294967295> FastEthernet interface number
Router(config)#int fastethernet0/0.1
Router(config-subif)#
```

O recurso de subinterfaces permite que você crie uma enorme gama de interfaces virtuais em um router. O prompt mudaria então para *(config-subif)#* nesse modo. Falaremos mais a fundo sobre subinterfaces mais adiante. Por hora, concentre-se no prompt, apenas.

Prompt de comandos de linha (*line commands*):

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line ?
  <0-70> First Line number
  aux     Auxiliary line
  console Primary terminal line
  tty     Terminal controller
  vty     Virtual terminal
  x/y     Slot/Port for Modems

Router(config)#line console 0
Router(config-line)#
```

Para configuração de senhas de modo usuário, utilize o comando *line* no modo de configuração global. No exemplo anterior, o comando *(config)#line console 0* é tido como um comando global, e qualquer comando digitado a partir do prompt *(config-line)#* é tido como um sub-comando.

Prompt de configuração de protocolos de roteamento:

Finalmente, para configuração de protocolos de roteamento como RIP ou IGRP, o prompt seria *(config-router)#*.

Nota: *Nas versões mais recentes do IOS (12.3 em diante) é possível executar comandos exec (como show, copy, ping, etc) diretamente de qualquer prompt em que você se encontrar, por meio do comando auxiliar do.*

Exemplo: Router(config)# do show run

Observe no exemplo acima que, mesmo estando no prompt de configuração, podemos executar o comando show, por meio do comando do.

6.2.2.3 Recursos de Ajuda

Você pode se utilizar dos recursos de ajuda para auxiliá-lo na configuração de um router. Utilizando um ponto de interrogação (?)

em qualquer prompt (e em qualquer modo) você obtém uma lista dos comandos disponíveis para aquele prompt.

Para localizar comandos que começam com uma determinada letra, basta digitar a letra em questão seguida de um ponto de interrogação (?), como no exemplo que segue:

```
Router#c?
clear clock configure connect copy
```

Para determinar o próximo comando em uma string, digite primeiro o comando e, em seguida, um espaço e um ponto de interrogação (?), como no exemplo a seguir:

```
Router#clock ?
   set  Set the time and date
 Router#clock set ?
   hh:mm:ss  Current Time
```

Se acontecer de você receber um erro *% Incomplete command,* você saberá que a linha de comando digitada não está completa. Algo está faltando. Utilize o recurso anterior para determinação do comando faltante. Outras mensagens de erro comuns são:

```
Router(config)#access-list 110 permit host 1.1.1.1
                                         ^
% Invalid input detected at '^' marker.
```

```
Router#sh te
% Ambiguous command: 'sh te'

Router#sh te?
tech-support template terminal
```

O primeiro dos erros acima aponta que após a marca "^" um comando inválido ou inexistente foi digitado. A partir desse ponto, utilize o recurso de ajuda para auxiliá-lo na identificação do comando apropriado. No segundo caso, utilize o ponto de interrogação imediatamente após o comando digitado para que lhe seja apresentada uma lista com as opções de comando válidas.

6.2.2.4 Comandos de Edição Avançados

A tabela a seguir ilustra os comandos de edição avançada que o IOS utiliza. O IOS lembra vagamente um *shell* do UN*X. Na verdade, há um motivo para isso: o IOS é um sistema baseado neste S.O. Aqueles que estão familiarizados com o editor de textos *Vi* do UN*X não terão dificuldade em utilizar os comandos anteriormente listados, uma vez

que são exatamente os mesmos. Para os que nunca viram esses comandos antes, recomenda-se praticá-los. Pelo menos uma questão sobre eles estará no exame.

Comando	Função
Ctrl+A	Move o cursor para o início da linha.
Ctrl+E	Move o cursor para o final da linha.
Esc+B	Move o cursor uma palavra para trás.
Ctrl+F	Move o cursor um caractere para frente.
Esc+F	Move o cursor uma palavra para frente.
Ctrl+D	Deleta apenas um caractere à direita.
Backspace	Deleta apenas um caractere à esquerda.
Ctrl+R	Reapresenta uma linha.
Ctrl+U	Deleta uma linha.
Ctrl+W	Deleta uma palavra.
Ctrl+Z	Finaliza o modo de configuração e retorna ao modo EXEC (raiz).
Tab	Completa a digitação de um comando.
Ctrl+P	Apresenta o último comando digitado.
Ctrl+N ou seta p/ baixo	Reapresenta o comando previamente digitado.

Tabela 6.3: Resumo dos comandos de edição a serem estudados.

Outro recurso de edição que deve ser mencionado é o rolamento automático de linhas longas. No exemplo a seguir, o comando digitado atingiu a margem direita e foi, automaticamente, movido 10 espaços para a esquerda. O sinal *$* indica que a linha foi rolada para a esquerda.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#$110 permit host 171.10.10.10 0.0.0.0 host
```

Você pode rever o histórico de comandos digitados no router através do comando *show history*, e pode alterar o tamanho do buffer usando o comando *terminal history size xxx*, onde *xxx* pode ser um número de 0 a 255. O tamanho default do buffer é 10, ou seja, os 10 últimos comandos são armazenados e podem ser vistos usando-se o comando *sh history*. Através do comando *sh terminal* é possível verificar o tamanho do buffer ativo.

É de extrema importância o entendimento, prática e memorização da tabela anterior. Por mais desnecessária que ela possa parecer, o exame CCNA irá testar seus conhecimentos nos comandos apresentados.

6.2.2.5 Reunindo Informações Básicas sobre o Router

O comando *sh version* é de extrema utilidade, sendo utilizado para a obtenção de uma série de informações.

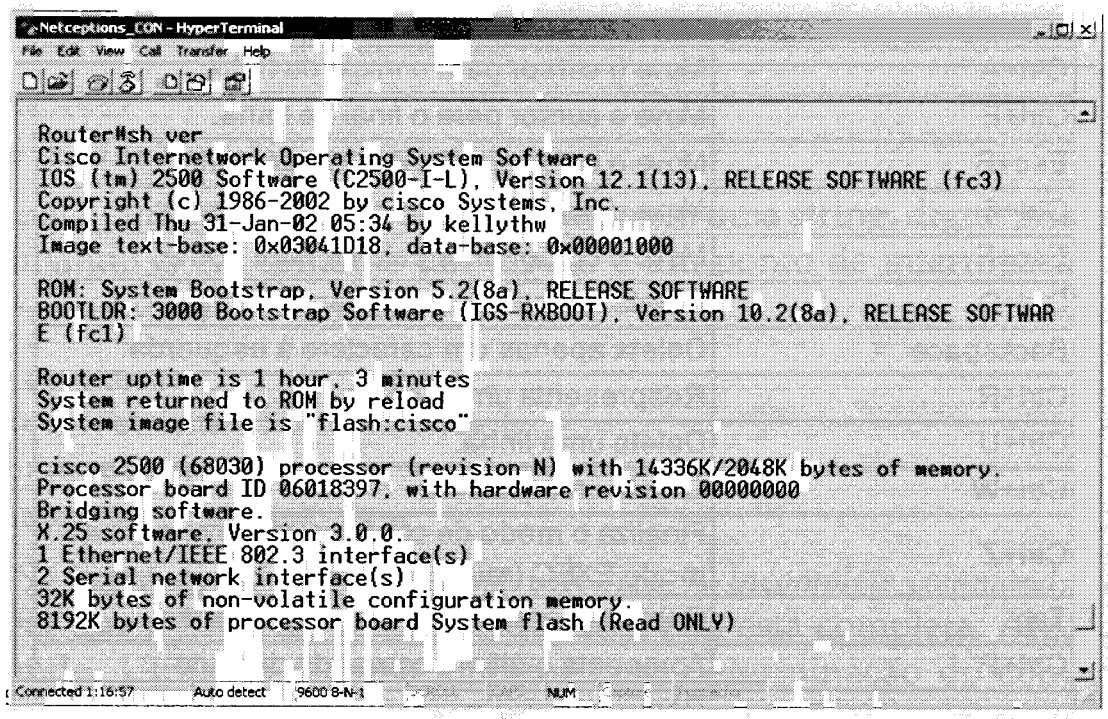


Figura 6.5: Exemplo do comando sh version em ação.

Entre as informações obtidas através desse comando, eis as mais importantes:

- Versão do sistema IOS em uso;
- Tempo em que o router está ligado;
- Nome da imagem *flash* em uso;
- Modelo e configuração física do router em uso;
- Listagem das interfaces disponíveis;
- Tamanho da NVRAM;
- Tamanho da FLASH;
- Configuração do registro (*register*). Default = 0x2102.

6.2.2.6 Configuração de Senhas

Existem cinco tipos de senhas que podem ser criadas e aplicadas para segurança de routers Cisco. As duas primeiras são utilizadas para restringir o acesso ao modo privilegiado (*enable*). Assim sendo, uma vez aplicadas, uma senha será pedida toda vez que o comando *enable* for digitado no modo usuário. As outras três são utilizadas para restringir o acesso ao router através das portas de Console, Auxiliar ou Telnet.

```
a) Router(config)#enable ?
   last-resort     Define enable action if no TACACS servers respond
   password        Assign the privileged level password
   secret          Assign the privileged level secret
   use-tacacs      Use TACACS to check enable passwords

   Router(config)#enable secret ccna
   Router(config)#enable password ccna
```

```
b) Router(config)#line ?
    <0-70>  First Line number
    aux     Auxiliary line
    console Primary terminal line
    vty     Virtual terminal
```

```
c) Router#config t
   Enter configuration commands, one per line. End with CNTL/Z.
   Router(config)#line aux ?
    <0-0> First Line number
   Router(config)#line aux 0
   Router(config-line)#login
   Router(config-line)#password ccna
```

```
d) Router(config)#line console ?
     <0-0> First Line number
   Router(config)#line console 0
   Router(config-line)#password ccna1
   Router(config-line)#login
```

```
e) Router(config-line)#line vty 0 ?
    <1-4> Last Line Number
   Router(config-line)#line vty 0 4
   Router(config-line)#password ccna2
   Router(config-line)#login
```

a) Senhas em Modo Privilegiado (*enable passwords*):

Devem ser configuradas em modo privilegiado. As seguintes opções são disponibilizadas:

- **Last-resort:** Deve ser utilizada se a autenticação é feita através de um servidor TACACS. Apenas é utilizada se o servidor TACACS estiver com problemas. Caso esteja OK, não é utilizada;
- **Password:** Utilizada para configuração de senhas de modo privilegiado em routers rodando o sistema IOS em versão anterior à 10.3. Não é utilizada caso a senha *enable secret* esteja configurada no router;
- **Secret:** Senha criptografada, definida em modo privilegiado para restrição de acesso ao router;

- **Use-tacacs:** Direciona o router a efetuar o processo de autenticação através de um servidor TACACS. Muito conveniente se você dispõe de dezenas ou mesmo centenas de routers. Imagine-se alterando a senha de 200 routers... Os servidores TACACS permitem que você altere a senha de vários routers de uma só vez.

Se você tentar configurar a senha *enable* e a senha *enable secret* como sendo a mesma, o router lhe apresentará uma mensagem. Caso você tente novamente inserir a mesma senha, o router aceitará, porém, nenhuma das senhas estará funcionando. Portanto, não se preocupe em configurar a senha *enable*, a não ser que você esteja utilizando um router antigo.

b) Senhas de Modo Usuário (*line passwords*):

Devem ser configuradas em modo privilegiado. Pode-se configurar senhas nas linhas console, auxiliar e Telnet (VTY).

c) Senha Auxiliar (*auxiliary password*):

Para configurar a senha auxiliar, você deve estar no modo de configuração global (*global configuration mode*) e, então, digitar o comando *line aux ?*. Note que você recebe apenas a alternativa 0-0, uma vez que há apenas uma porta auxiliar.

d) Senhas de Console (*console passwords*):

Para configurar a senha de console, você também deve estar no modo de configuração global. Digite o comando *line console ?*. Note que você recebe apenas a alternativa 0-0, uma vez que há apenas uma porta auxiliar.

e) Senhas de Telnet (*Telnet passwords*):

Para configurar senhas para usuários terem acesso ao seu router via Telnet, utilize o comando *line vty*. Routers que não estejam rodando a versão Enterprise do Cisco IOS estão limitados a cinco portas Telnet (0-4).

Em nosso exemplo, o router dispõe de 198 portas Telnet (0-197). A melhor maneira de se determinar a quantidade de portas Telnet disponíveis é utilizando o recurso de ajuda (*?*).

```
Router(config-line)#line vty 0 ?
 <1-197> Last Line Number
Router(config-line)#line vty 0 197
Router(config-line)#login
Router(config-line)#password ccna4
```

Se você tentar se conectar a um router que não esteja com uma senha Telnet (VTY) configurada, você receberá uma mensagem de erro dizendo que a conexão foi recusada, pois a senha não foi definida (*connection refused because VTY password is not set*). Você pode configurar um router para que ele aceite conexões Telnet mesmo que uma senha não se encontre definida através do comando *no login* (veja a seguir). Após os routers terem sido devidamente configurados com endereços IPs, você pode se conectar remotamente a um router através do aplicativo Telnet (basta ir ao prompt do DOS e digitar Telnet e o IP do router-alvo, por exemplo).

```
Router(config-line)#line vty 0 4
Router(config-line)#no login
```

6.2.2.7 Outros Comandos de Console

```
Router(config)#line con 0
Router(config-line)#exec-timeout ?
 <0-35791> Timeout in minutes
Router(config-line)#exec-timeout 0 ?
 <0-2147483> Timeout in seconds
 <cr>
Router(config-line)#exec-timeout 0 0
Router(config-line)#logging synchronous
```

Existem outros comandos importantes de se saber com relação às portas de console. O comando *exec-timeout [m s]* define o *timeout* para o modo EXEC do console em minutos (*m*) e segundos (*s*). Para não ocorrer o timeout, configure o timer para *0 0*. Se você quiser definir um timeout de 1 segundo, por exemplo, utilize o comando *exec-timeout 0 1*.

Outro comando interessante é o *logging synchronous*. Esses comando deveria ser definido por default, mas não o é. O que ele faz é impedir que mensagens de console fiquem constantemente aparecendo em sua tela, interrompendo a entrada que você está tentando digitar. Isso faz com que a leitura de suas entradas seja muito mais clara.

6.2.2.8 O Processo de Criptografia de Senhas

Por default, apenas o comando *enable secret* cria uma senha criptografada. A criptografia de senhas de modo usuário deve ser efetuada manualmente. Note que você pode identificar todas as senhas menos a *enable secret* quando você digita o comando *show running-config* em um router:

```
Router#sh run
[...]
!
enable secret 5 $1$fTrsK.gTysbG56I/PsfrtE3N@.
enable password netceptions
!
[...]
line con 0
password netceptions
```

Para manualmente criptografar senhas não-criptografadas por default (*user-passwords*), utilize o comando *service password-encryption*. Em seguida, ilustramos um exemplo de como proceder:

```
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#service password-encryption
Router(config)#enable password netceptions
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password netLAB
Router(config-line)#line con 0
Router(config-line)#login
Router(config-line)#password SENHACONSOLE1
Router(config-line)#line aux 0
Router(config-line)#login
Router(config-line)#password SENHAAUX1
Router(config-line)#exit
Router(config)#no service password-encryption
(O comando acima desativa o recurso de encriptação de senhas)
Router(config)#^Z
```

Agora, ao digitar o comando *show running-config* você notará que as senhas *enable* e as senhas de linha (*enable/ line passwords*) aparecem criptografadas.

6.2.2.9 Utilização do Recurso Pipe

Ao utilizar o comando *show* em roteadores e switches Cisco, algumas vezes, você pode desejar aplicar um filtro para obter um resultado mais rapidamente. O *pipe* (representado pelo caracter " | ") possibilita a utilização de uma série de filtros juntamente com o comando *show*. Eis alguns exemplos:

```
CCNA41#sh run | ?
  append    Append redirected output to URL (URLs supporting
             append operation
            only)
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output to URL
  section   Filter a section of output
  tee       Copy output to URL

CCNA41#sh run | begin interface
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip http server
no ip http secure-server
!
control-plane
!
--More--

CCNA41#sh ip route | include 192.168.10
C    192.168.10.0/24 is directly connected, Loopback1
```

6.2.2.10 Configuração de Banners (Mensagens)

Você pode configurar banners em um router para que, assim que um usuário se conecte nesse determinado router ou um administrador estabeleça uma sessão Telnet a ele, por exemplo, uma mensagem (banner) apresente a informação que você deseja. Uma razão para a configuração de banners em um router é a apresentação de avisos de segurança a usuários que se conectam à sua rede através desse router. Existem quatro diferentes tipos de banners disponíveis: *exec, incoming, login* e *motd.*

O banner *motd* (*message of the day* - mensagem do dia) é o mais utilizado e apresenta uma mensagem a todos que se conectem ao router, não importando o caminho. O modo para configurá-lo é exemplificado a seguir:

```
Router(config)#banner motd ?
LINE c banner-text c, where 'c' is a delimiting
character
Router(config)#banner motd @
Enter TEXT message. End with the character '@'.
Bem-vindo(a) ao CiscoLAB. Se você não possui autorização
Para estar aqui, deve desconectar imediatamente!
@
Router(config)#^Z
Router#
00:25:12: %SYS-5-CONFIG_I: Configured from console by console
Router#exit
```

Note, em destaque, o caractere delimitador utilizado (@). Você pode utilizar qualquer caractere que deseje, **desde que ele não apareça na mensagem.**

Os outros banners existentes (*exec, incoming* e *login*) possuem as seguintes funções:

- **Exec:** Permite a configuração de uma mensagem para ser apresentada quando uma sessão EXEC (como um acesso via Console ou via Telnet) é iniciada;
- **Incoming:** Permite a configuração de mensagens que são apresentadas aos usuários que se conectem via linha Console, linha Auxiliar ou Telnet reverso (*reverse Telnet*);
- **Login:** Permite a configuração de mensagens que serão apresentadas a todos os terminais conectados. Esse banner é apresentado logo após o banner *motd*, mas antes dos prompts de login. Para desabilitar globalmente o banner login, você deve deletá-lo através do comando *no banner login* (normalmente, para desabilitar um comando que se encontra ativado no IOS, basta redigitá-lo com o comando *no* precedendo-o).

6.2.2.11 Configuração de Interfaces em um Router

A configuração de interfaces é uma das mais importantes configurações realizadas em um router. Sem interfaces devidamente ajustadas, um router é inútil. Algumas das configurações utilizadas em uma interface

tratam de endereços de rede, largura de banda, tipo de meio de acesso, entre outros.

Diferentes routers utilizam diferentes métodos para escolha das interfaces utilizadas, uma vez que suas configurações físicas variam de modelo para modelo e de acordo com as placas de expansão que eles possuem instaladas. Para determinar quais as interfaces disponíveis em seu router, utilize o ponto de interrogação (*?*): *(config)#int ?*

Uma vez descobertas quais as interfaces disponíveis, descubra quantas portas podem ser configuradas através do comando: *(config)#**int serial ?** (exemplo para interface serial).

Dependendo do router que você irá configurar, você irá se deparar com diferentes configurações de hardware. Por exemplo, o router modelo 2522 possui uma interface 10BaseT (RJ-45). A linha 2500 é fixa, ou seja, não permite que módulos sejam acoplados, expandindo sua funcionalidade. Já linhas modulares, como a série 2600, oferecem uma maior flexibilidade através da possibilidade de expansão pela adição de módulos. Séries modulares utilizam um slot físico no router e um número de porta no módulo plugado a esse slot. Por exemplo, em um router da linha 2600, a configuração de uma porta *Fast Ethernet* seria *interface slot/porta*:

```
Router(config)#int fastethernet ?
 <0-1> FastEthernet interface number
Router(config)#int fastethernet 0
% Incomplete command.
Router(config)#int fastethernet 0?
/
Router(config)#int fastethernet 0/?
 <0-1> FastEthernet interface number
```

Nota: *As interfaces presentes nos chassis dos routers modulares, assim como nos slots "WIC" preexistentes (dois, no caso da linha 2600), sempre iniciam a contagem como "0" (ex.: int s0/0 – primeiro slot "WIC" e int s0/1 – segundo slot "WIC"). Interfaces presentes no módulo "NM" iniciam sua contagem em "1" (ex.: int s1/0).*

Note que você **não pode** digitar *int fastethernet 0*. Você deve digitar o comando completo, incluindo os respectivos slot e porta. Você poderia digitar *int fa 0/0*, para abreviar.

Para definir o tipo de conector utilizado, você pode utilizar o comando *media-type*:

```
Router(config)#int fa 0/0
Router(config-if)#media-type ?
100BaseX     Use RJ45 for -TX; SC FO for -FX
MII          Use MII connector
```

Esse comando é necessário dependendo da placa que estiver em seu router. Se em uma mesma placa dois tipos de conectores co-existirem (ex.: AUI e RJ45), o comando *media-type* deve ser aplicado para definir qual conector será usado. Normalmente, esse comando não é necessário.

6.2.2.12 Ativando (No Shut) e Desativando (Shut) uma Interface

Por default, todas as interfaces em um router encontram-se desativadas (*shutdown*). Para ativar uma interface, utilize o comando *no shutdown* e para desativá-la, digite *shutdown*.

Se uma interface estiver desativada, quando você digitar o comando *show interface* a mensagem *administratively down* será apresentada, indicando que a interface está desativada por opção do administrador e não por problemas de hardware (1).

Utilizando o comando *no shutdown* (2), ativamos a interface em questão.

Finalmente, digitando o comando *show interface*, novamente, a mensagem apresentada será de que a interface e o protocolo de linha (*line protocol*) estão *up* (ativos) (3), indicando que a interface em questão está funcional (no caso de não haver problemas de comunicação com a outra ponta, ou mesmo físicos, com a interface ou o meio em questão):

```
1) Router#sh int ethernet0
   Ethernet0 is administratively down, line protocol is down
```

```
2) Router#config t
   Enter configuration commands, one per line. End with
   CNTL/Z.
   Router(config)#int ethernet0
   Router(config-if)#no shutdown
   Router(config-if)#^Z
   00:57:08: %LINK-3-UPDOWN: Interface Ethernet0, changed
   state to up
   00:57:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface
   Ethernet0, changed state to up
```

```
3) Router#sh int ethernet0
   Ethernet0 is up, line protocol is up
```

6.2.2.13 Configuração de Endereçamento IP em Interfaces

Você não é obrigado a utilizar endereços IPs em seus routers, entretanto, o IP é tipicamente utilizado em todos os routers (e dispositivos de rede em geral). Para configurar endereços IPs nas interfaces de um router, utilize o comando *ip address* no modo de configuração de interface. Não se esqueça de digitar o comando *no shut* para ativar a interface configurada (a). Para verificar o status da interface (que inclui o endereçamento associado a ela), utilize os comandos *show int* ou *show running-config*. Outros comandos úteis para checagem de interfaces são *sh int summary* e *sh ip int brief*, exemplificados a seguir.

```
Router#sh int summ

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0          0     0    0     0     0    1     0    0    0
  FastEthernet0/1          0     0    0     0     0    0     0    0    0
* Serial0/0/0              0     0    0    41  4000    6  6000    7    0
* Loopback0                0     0    0     0     0    0     0    0    0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown


Router#sh ip int brief
Interface          IP-Address      OK? Method Status                Protocol
FastEthernet0/0    10.135.128.3    YES manual up                    up
FastEthernet0/1    unassigned      YES NVRAM  administratively down down
Serial0/0/0        192.168.101.1   YES NVRAM  up                    up
Loopback0          172.16.100.12   YES NVRAM  up                    up
```

Se quiser adicionar um segundo endereço IP a uma mesma interface, você deve utilizar o comando *secondary*. Se você simplesmente digitar outro endereço IP e teclar <Enter>, este irá substituir o endereço IP existente e sua máscara de rede. Para adicionar um (ou mais) endereço IP secundário, utilize o comando *secondary* (b). A checagem pode ser feita, entre outras maneiras, através do comando *sh run* (c):

```
a) Router#config t
   Enter configuration commands, one per line. End with CNTL/Z.
   Router(config)#int e0
   Router(config-if)#ip address 192.168.10.1 255.255.255.0
   Router(config-if)#no shut

b) Router(config-if)#ip address 192.168.20.1 255.255.255.0 secondary
   Router(config-if)#ip address 192.168.30.1 255.255.255.0 secondary
   Router(config-if)#^Z
```

```
c) Router#sh run
   Building configuration...
   Current configuration:
   [output cut]
   !
   interface Ethernet0
   ip address 192.168.20.1 255.255.255.0 secondary
   ip address 192.168.30.1 255.255.255.0 secondary
   ip address 192.168.10.1 255.255.255.0
   !
```

Para configurar uma interface serial, existem algumas especificações que devem ser discutidas. Tipicamente, a interface estará conectada a um dispositivo CSU/DSU (*Channel Service Unit/Data Service Unit*), que proverá o clocking (sincronização) para a linha. Entretanto, se você dispuser de uma topologia *back-to-back*, como as utilizadas em laboratório (ou por algum outro motivo), uma das pontas precisa prover o clocking.

O dispositivo que se encontra na ponta DCE (*Data Communication Equipment*) do cabo deve realizar essa função. Por default, todos os routers Cisco são dispositivos DTE (*Data Terminal Equipment*), portanto, você deve configurar determinada interface para prover o clocking se ela vai agir como um dispositivo DCE. Você deve configurar uma interface serial DCE através do comando *clock rate*:

```
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#int s0
Router(config-if)#clock rate 64000
 %Error: This command applies only to DCE interfaces
Router(config)#int s1
Router(config-if)#clock rate 64000
Router(config-if)#
```

Não há mal algum em tentar configurar o clocking em uma interface serial. No entanto, se a interface em questão não se tratar de uma DCE (como no exemplo anterior, onde tentamos aplicar o comando à interface DTE S0), a configuração será rejeitada. Note que o comando *clock rate* é dado em **bits por segundo**.

Um comando que pode ser utilizado para saber se a interface em questão encontra-se conectada a um cabo DTE ou DCE é o *show controllers*. Esse comando apresenta informações sobre a interface física *per se*. Ele também nos informará sobre o tipo de cabo serial conectado a uma porta serial. Tipicamente este será um cabo DTE, que então se

conectará a um tipo de DSU. A sintaxe desse comando é: *sh controllers s [x]*, onde *[x]* é o número da interface serial. **Note o espaço entre a letra *s* e o número da interface. Isso é importante!**

O próximo comando que deve ser compreendido com relação às interfaces seriais é o *bandwidth*. Todo router Cisco vêm de fábrica com a largura de banda (*bandwidth*) default para links seriais de uma T1 (1.544Kbps). É importante compreender que isso nada tem a ver com a velocidade com que os dados são transmitidos através do link serial. A largura de banda (*bandwidth*) de um link serial é utilizada por protocolos roteadores, como IGRP, EIGRP e OSPF para o cálculo do melhor custo para uma rede remota (métricas). Se você está utilizando roteamento RIP, a configuração de *bandwidth* será totalmente irrelevante (uma vez que esse protocolo utiliza o número de *hops* (saltos) até o destino como medida):

```
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#int s0
Router (config-if)#bandwidth ?
 <1-10000000> Bandwidth in kilobits
Router(config-if)#bandwidth 256
```

6.2.2.14 Configurando Hostnames, Descrições e Salvando Configurações

Para configurar um nome para determinado router, utilize o comando *hostname*. Esse comando é relevante apenas localmente, o que significa que não há interferência em como o router executa a procura de nomes pela rede:

```
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname netcep
netcep(config)#hostname Netceptions
Netceptions(config)#
```

Configurar descrições em interfaces de um router pode ser muito útil para o administrador. Como o *hostname*, o comando *description* é apenas localmente relevante. Esse é um comando útil, pois pode ser usado para se manter números de circuitos organizados, como no exemplo:

```
Netceptions(config)#int e0
Netceptions(config-if)#description DEPTO RH001
Netceptions(config-if)#int s0
Netceptions(config-if)#desc LINK_E1 MATRIZ ALEMANHA|CIRCUITO:11020DEU
```

Você pode verificar a descrição das interfaces tanto com o comando *show run* quanto com o *show int*.

Quando você executa configurações em um router, você está alterando a configuração chamada *running-config*, ou seja, a configuração que está armazenada na memória volátil do router (DRAM). Se você não a salvar, quando o router for desligado ela será perdida (como no conteúdo da memória RAM de um computador). Uma vez finalizada a configuração, portanto, esta deve ser salva na memória não-volátil (NVRAM), e passará a se chamar *startup-config*; assim, na próxima vez em que o router for ligado, essa configuração será carregada. Você pode efetuar esse processo manualmente através do comando *copy running-config startup-config* ou, simplesmente, *copy run start*.

Para verificar o conteúdo das configurações, utilize os comandos *sh run* (*running-config*) ou *sh start* (*startup-config*). Você ainda pode deletar a *startup-config* através do comando *erase start*.

6.2.2.15 Verificação da Configuração

Obviamente, o comando *show running-config* seria a melhor maneira de se verificar a configuração de um router, assim como o comando *show startup-config* seria a melhor maneira de se verificar a configuração a ser carregada na próxima vez que o router for ligado.

Entretanto, uma vez que você verifica a *running-config* e constata que tudo parece em ordem, você pode verificar essa configuração com utilidades, como o comando *ping* e o comando *telnet*.

Você pode "pingar" utilizando-se de diferentes protocolos e verificar isso digitando *ping ?* no modo usuário ou privilegiado.

Você pode utilizar o comando *trace* para determinar o caminho que um pacote utiliza quando atravessa a rede. O comando *trace* também pode ser utilizado com diferentes protocolos.

Ambos os comandos apresentados são muito úteis para diagnóstico e teste de redes. O comando *telnet*, no entanto, é a melhor utilidade, uma vez que utiliza o protocolo IP na camada de rede e o TCP na camada de transporte para estabelecer uma sessão com um dispositivo remoto. Resumindo, se você consegue estabelecer uma sessão telnet com outro host, sua conectividade IP tem de estar boa.

Outro modo de se verificar a configuração é através do comando *show interface* (*sh int*). O primeiro comando, por instinto, seria *sh int ?*. Este apresenta uma lista das interfaces disponíveis, como já mencionado. Escolha a interface desejada e verifique-a digitando, por exemplo, *show int f0/0*.

Nesse caso, obteríamos a seguinte saída:

```
Router>sh int f0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 0014.a9e9.2c08 (bia
0014.a9e9.2c08)
  Description: LAN interface to customer LAN
  Internet address is 10.135.128.3/20
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 6w2d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 130000 bits/sec, 32 packets/sec
  5 minute output rate 169000 bits/sec, 28 packets/sec
     46299298 packets input, 448640565 bytes
     Received 1782217 broadcasts, 8882 runts, 0 giants, 0 throttles
     50060 input errors, 41178 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     40494160 packets output, 1297159397 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

A interpretação da saída do comando *sh int* é de extrema importância. A mais importante informação obtida é o estado dos links e dos protocolos. Se, no caso anterior, a saída informar *Ethernet 0 is up, line protocol is up*, então o link está ativo e sem problemas.

O **primeiro parâmetro refere-se à camada física** (meio) e encontra-se ativado quando recebe entrada de dados. O **segundo parâmetro refere-se à camada de enlace** e monitora *keepalives* da outra ponta conectada.

- `Interface is up, line protocol is up`
- `Interface is up, line protocol is down`
- `Interface is down, line protocol is down`
- `Interface is administratively down, line protocol is down`

No primeiro caso (*Int up, line up*), o link está ativo e funcional. Já no segundo caso (*Int up, line down*), pode existir um problema de *clocking* (sincronização) ou de *framing*. Cheque os *keepalives* de ambas as pontas e certifique-se de que são equivalentes, verifique se o clocking está configurado e se o tipo de encapsulamento é o mesmo para ambas as pontas.

No terceiro caso (*Int down, line down*) o problema deve ser no meio (ex. cabo) ou na interface. Verifique se o cabo está devidamente conectado e se as interfaces envolvidas encontram-se operacionais.

No último caso (*Int administratively down, line down*), a interface encontra-se desativada por opção do administrador (através do comando *shut*). Para ativá-la, digite o comando *no shut*.

Uma outra saída de configuração que é importante ser notada refere-se ao *keepalive*, que é o intervalo usado pelos routers para checagem da comunicação. **O tempo default é de 10 segundos**. Se ambos os routers não tiverem seu keepalive configurados com o mesmo parâmetro, a comunicação será falha (caso 2, acima). Você pode resetar os contadores em uma interface através do comando *clear counters [interface]*.

6.2.2.16 Cisco Secure Device Manager (SDM)

Uma alternativa ao uso do CLI (*Command Line Interface*) para a configuração de roteadores é o *Secure Device Manager* da Cisco. Esta ferramenta permite que se configure praticamente qualquer coisa em um roteador Cisco por meio de uma interface gráfica bastante intuitiva. É possível configurar desde o nome do roteador e o endereço IP em uma interface, até configurações complexas como VPNs, *Firewalls*, NAT, roteamento, etc. Mas o SDM é mais do que um mero configurador. Adicionalmente, ele permite realizar auditorias de segurança no roteador e verificar a utilização de recursos (memória, CPU). Uma vantagem de utilizar o SDM é que, as configurações geradas por ele são 100% compatíveis com o que o suporte da Cisco (o TAC) recomenda. Em caso de dúvidas, se o suporte da Cisco for acionado, seu problema

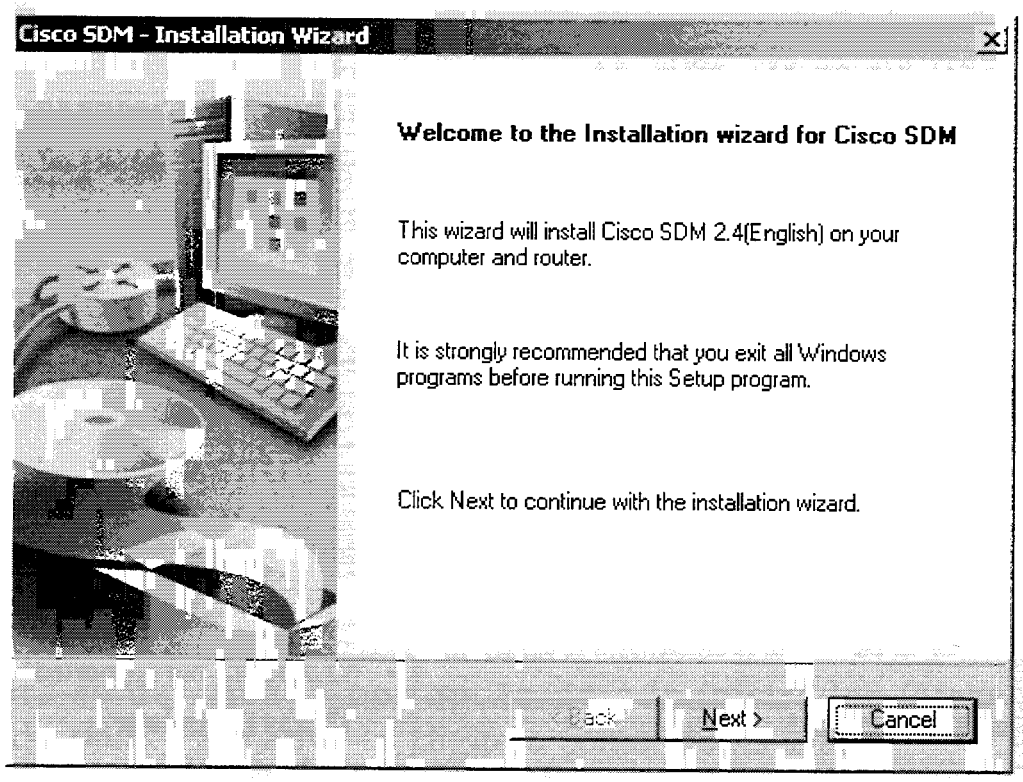
poderá ser identificado com mais rapidez. A seguir, uma tabela com as versões de IOS e linhas de roteadores suportadas pelo SDM:

SDM-Supported Routers	SDM-Supported Cisco IOS Versions
Cisco 831, 836, and 837	12.2(13)ZH or later.
Cisco 1701, 1710, 1721, 1751, 1751-v ,1760, and 1760-v	• 12.2(13)ZH, or later • 12.2(13)T3 or later • 12.3(1)M or later • 12.2(11)T6 not supported
Cisco 1711 and 1712	• 12.2(15)ZL
Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and 2691	• 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 not supported[1] • 12.2(13)ZJ
Cisco 3620, 3640, 3640A, 3661, and 3662	• 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 not supported[1]
Cisco 3725 and 3745	• 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 not supported[1]

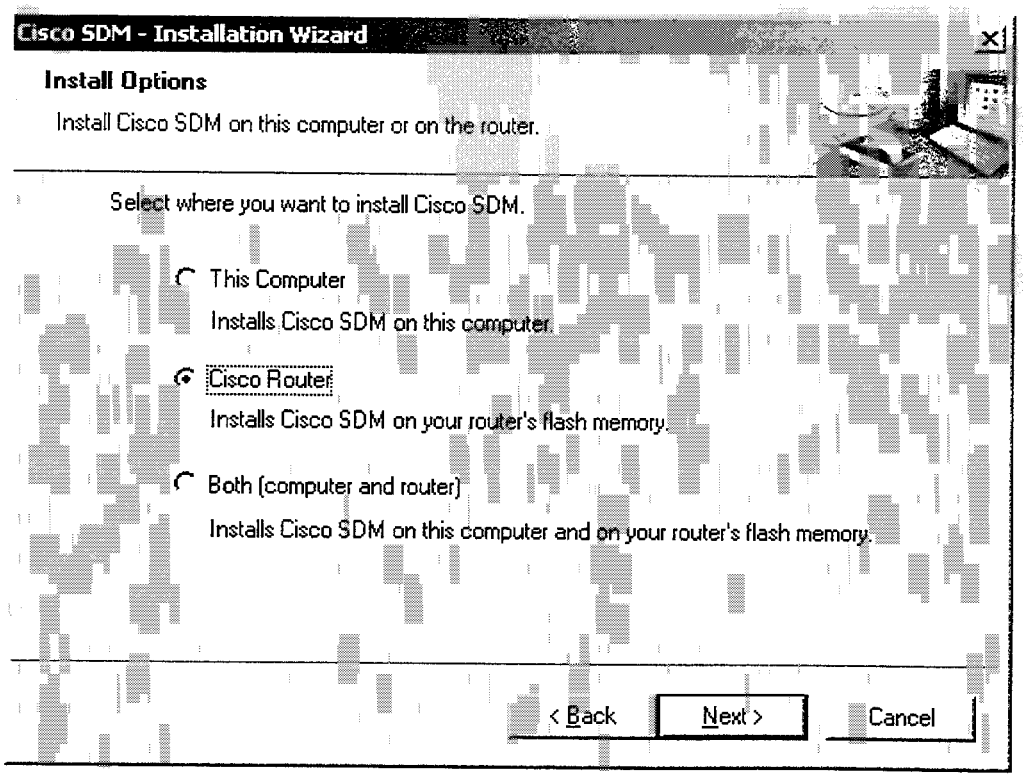
Os modelos mais recentes de roteadores (como as linhas 18xx, 28xx ou 38xx) já saem de fábrica com esta ferramenta instalada. Modelos mais antigos (como as linhas 17xx ou 26xx) também podem ser configuradas utilizando o SDM, mas é preciso instalar a ferramenta. O SDM é gratuito. Basta logar-se no site da Cisco e baixá-lo. O endereço direto para a ferramenta no site da Cisco é <http://www.cisco.com/go/sdm>. A instalação é bastante simples. Basta que o router tenha conectividade com o PC a partir do qual o SDM será instalado. Além disso, o router precisa ser pré-configurado com as linhas abaixo:

```
ip http server
ip http authentication local
username cisco privilege 15 password 0 cisco
!(pode ser outro username e senha)
line vty 0 4
privilege level 15
login local
transport input telnet
exit
```

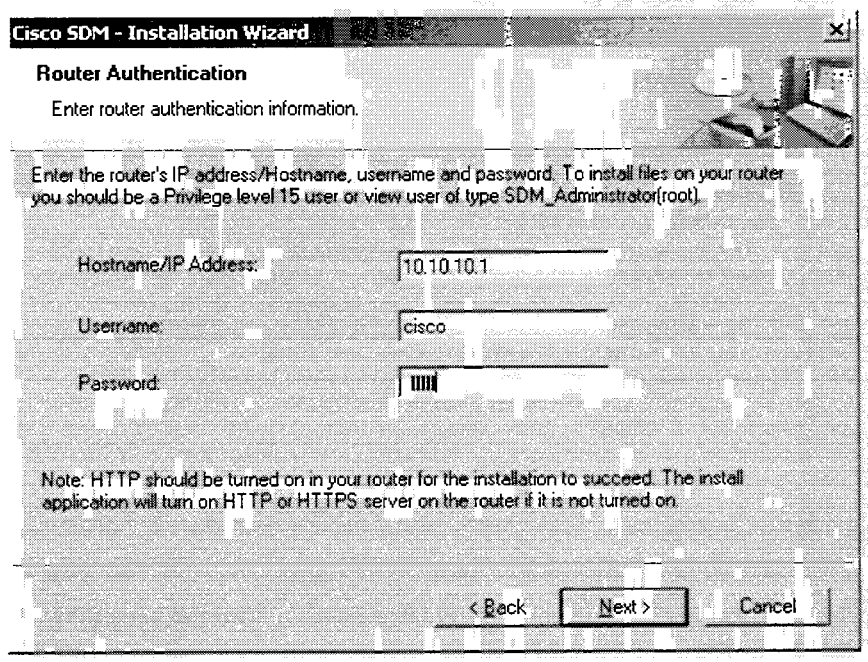
Uma vez que o router esteja pré-configurado e com conectividade ao PC, rode o instalador do SDM (um executável). A tela seguinte será apresentada.



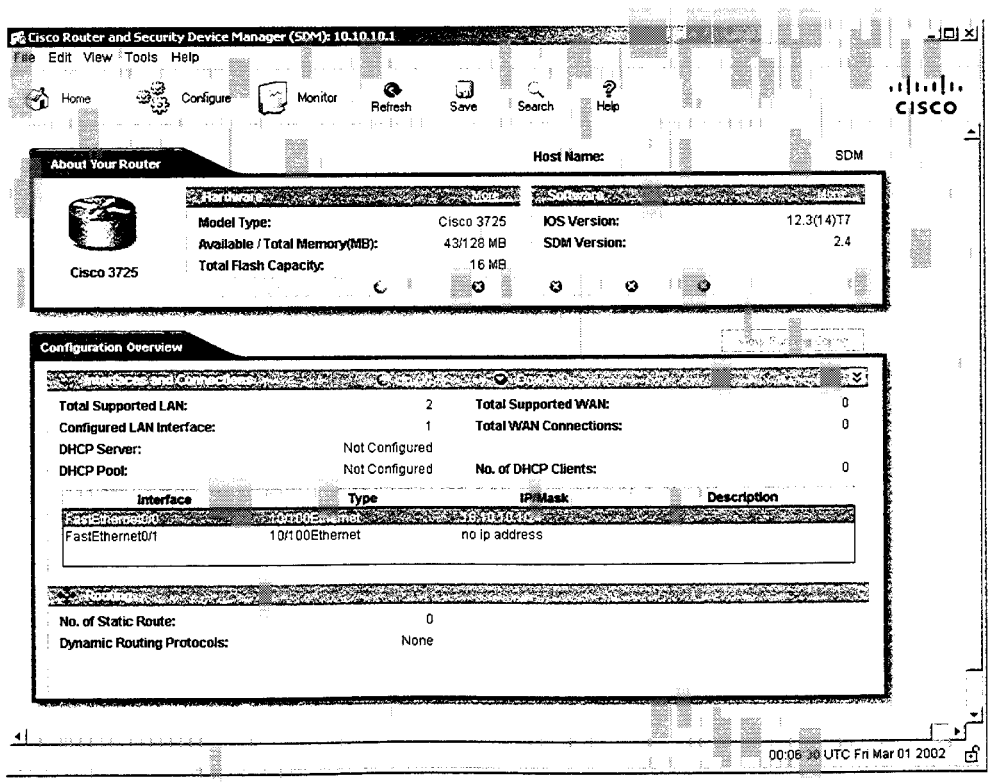
Selecione a instalação em um router



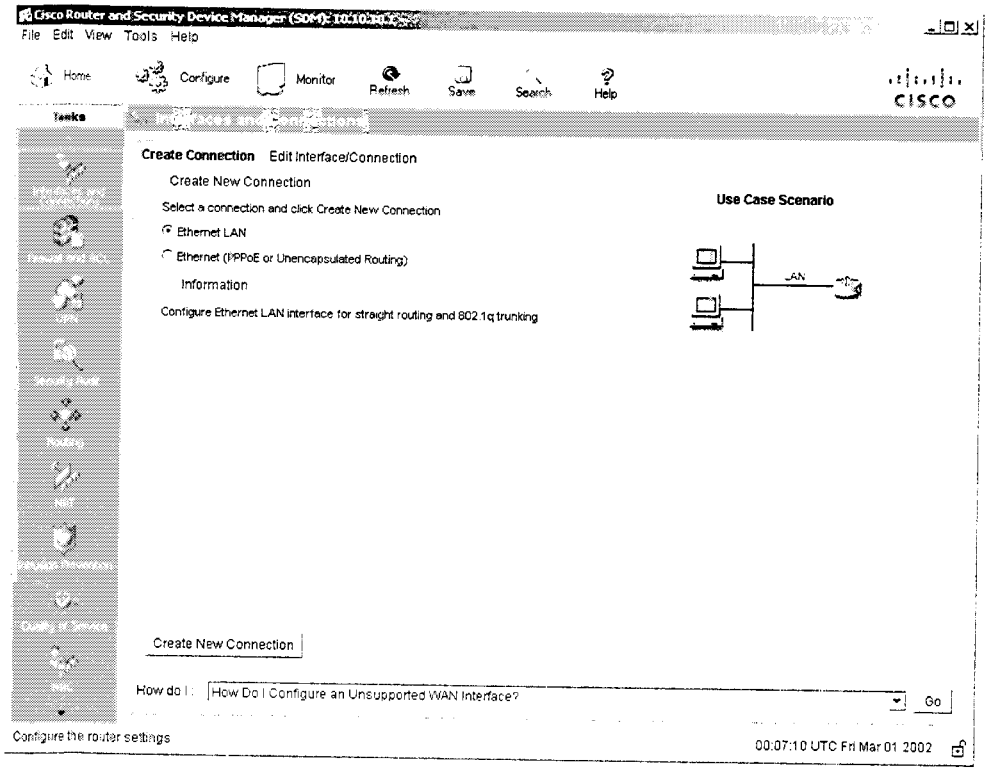
Coloque as informações anteriormente configuradas (IP do router, *username* e senha)



E depois é só seguir o passo-a-passo e aguardar a instalação. Os arquivos do SDM serão copiados na memória *flash* do router – por isso, é importante ter pelo menos 14MB disponíveis. Uma vez que a instalação seja finalizada, basta abrir um navegador Web (preferência para o MS Explorer, já que algumas funções parecem não funcionar no *Firefox*) e digitar o endereço IP do roteador. Após a tela de autenticação, será apresentada a tela inicial do SDM no seu navegador Web. Observe que a tela inicial traz uma série de informações sobre o router como: modelo, memória disponível, versão do IOS e versão do SDM. Também traz informações sobre interfaces e serviços disponíveis.

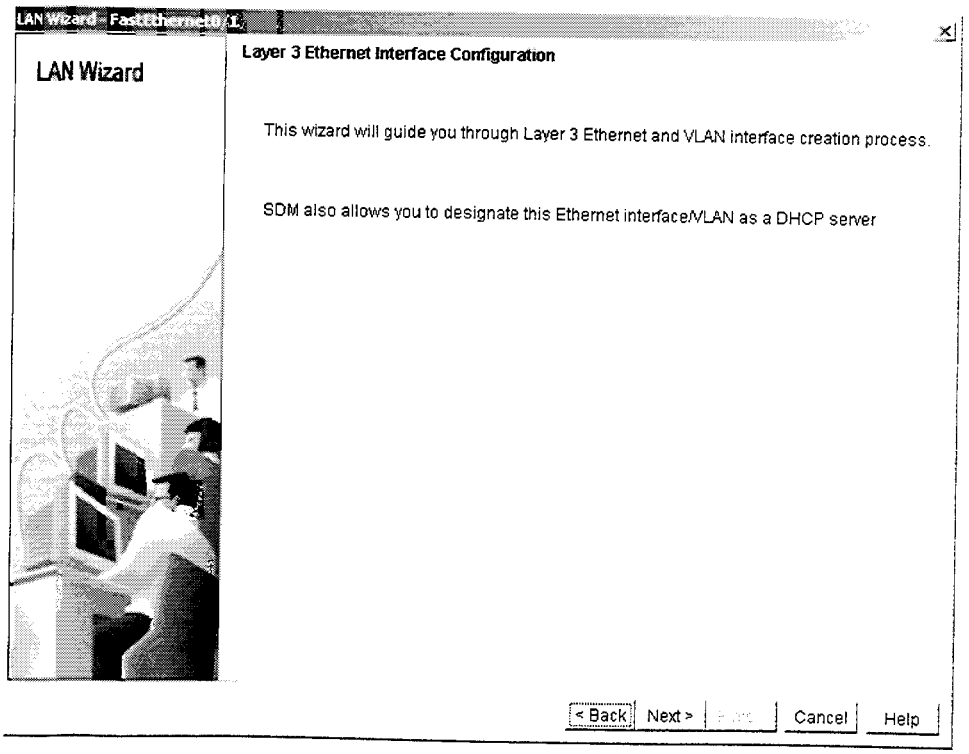


Clicando no botão *Configure*, somos levados à próxima tela:

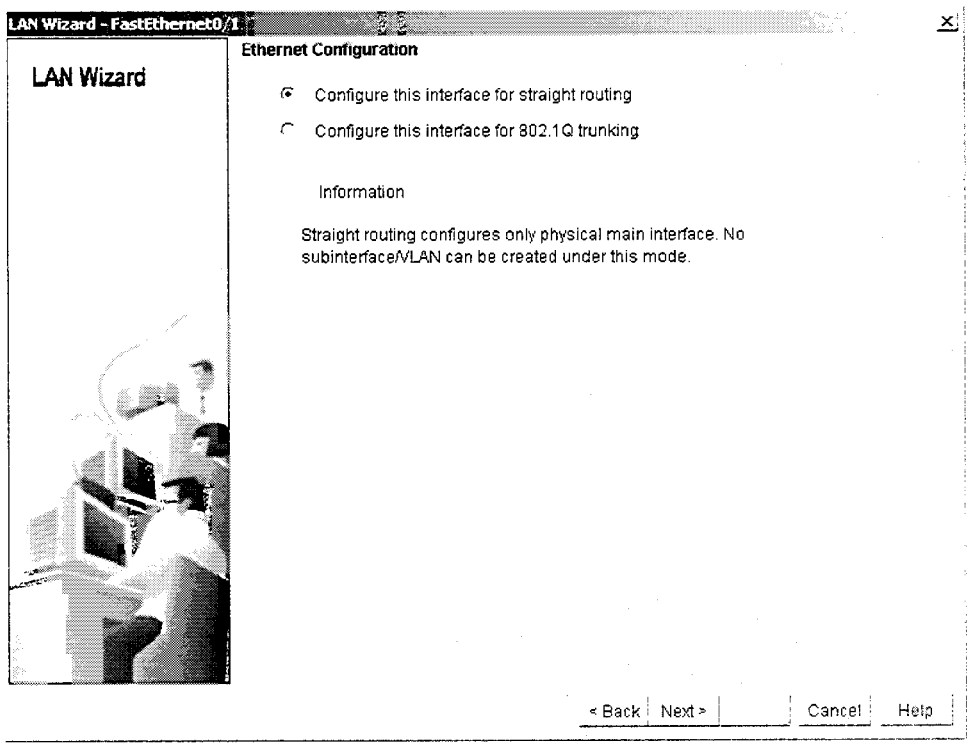


Note que, à esquerda, são apresentadas todas as opções de configurações possíveis, via SDM. Não são poucas. Neste exemplo, vou demonstrar como configurar uma das interfaces LAN (F0/1), e vou configurar o router para agir como um servidor DHCP. Você notará como é simples. É tudo muito auto-explicativo!

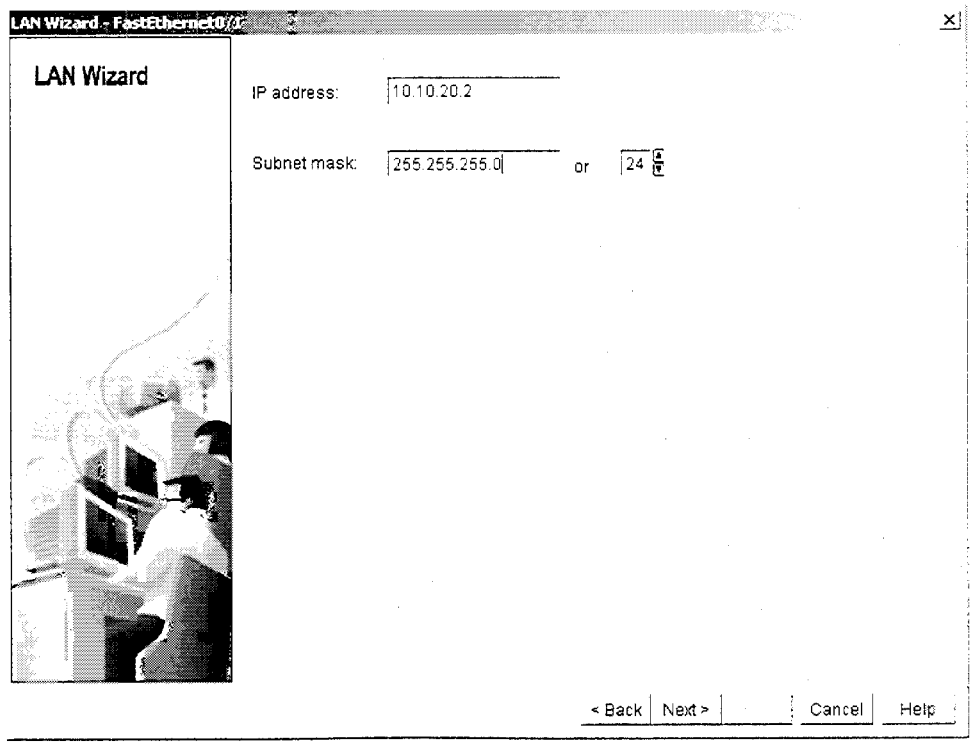
Apenas clique *Next* nesta tela.



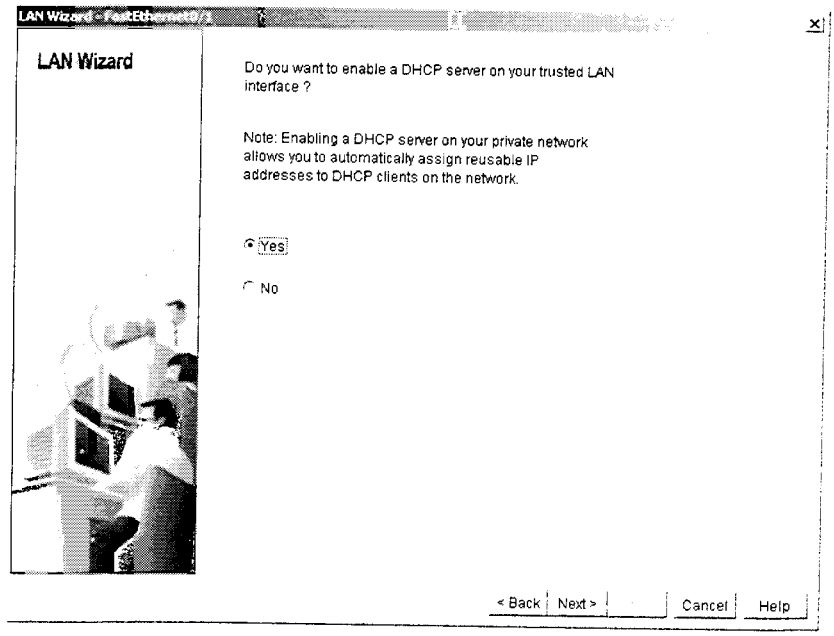
Selecione a primeira opção nesta tela (observe que poderíamos configurar roteamento dot1q nesta interface, se desejássemos).



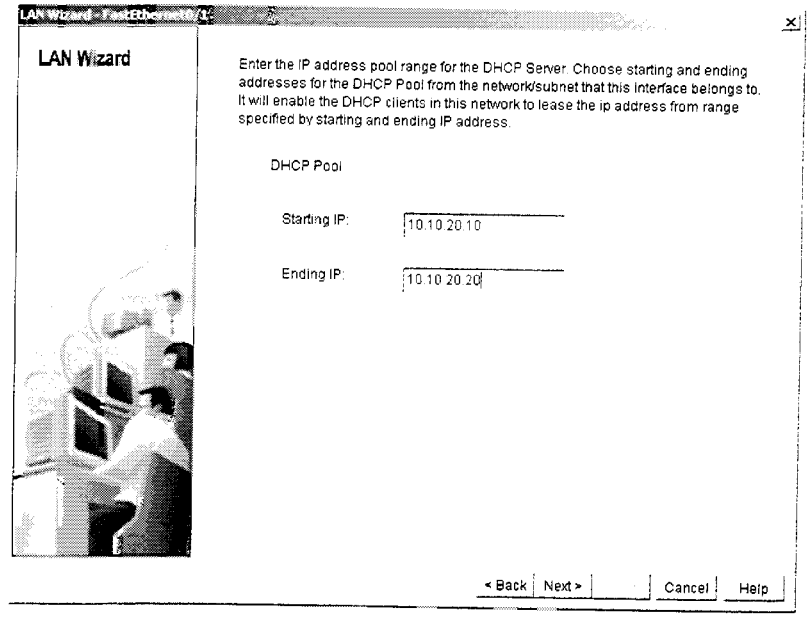
Entre com o endereço IP e máscara de rede desejados.

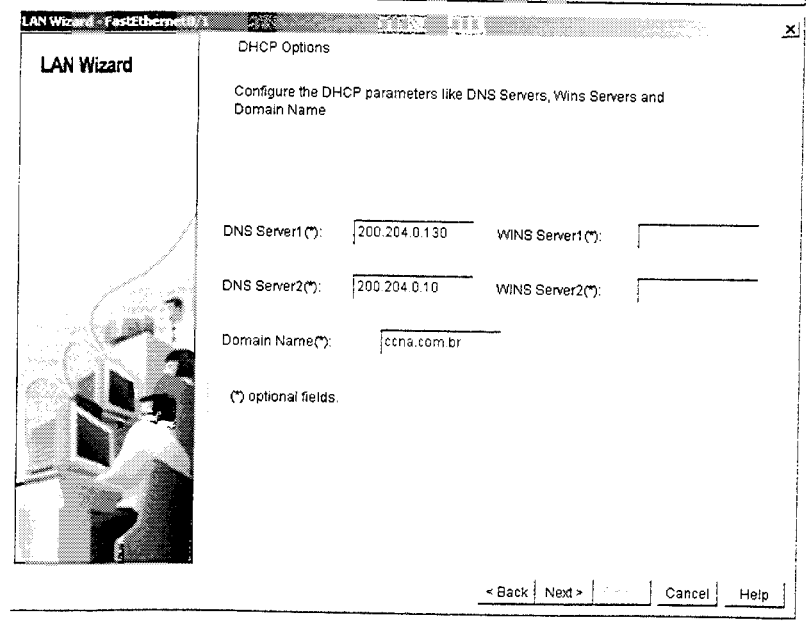


Na seqüência, nos é perguntado se desejamos configurar o router como DHCP para a rede LAN. Vamos optar por *Sim*.

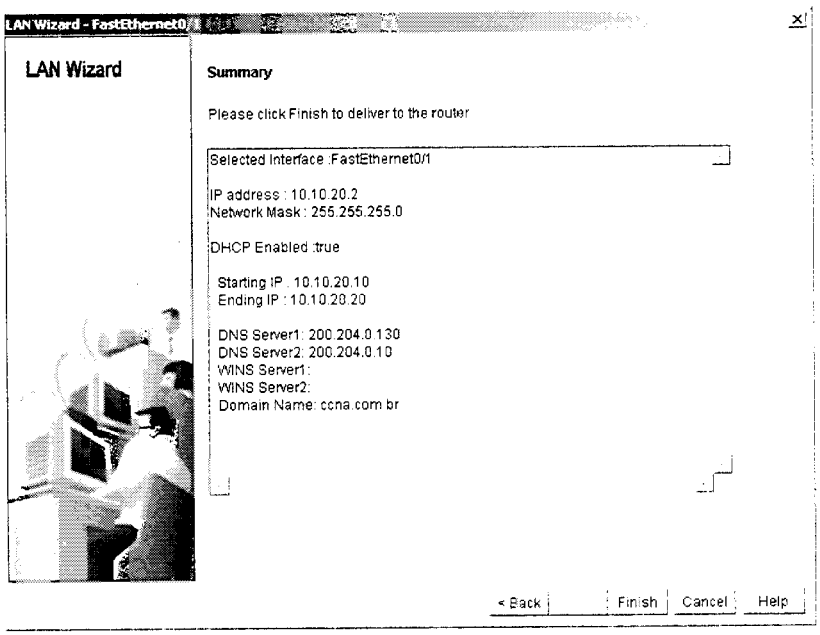


Entramos com os parâmetros para o DHCP.

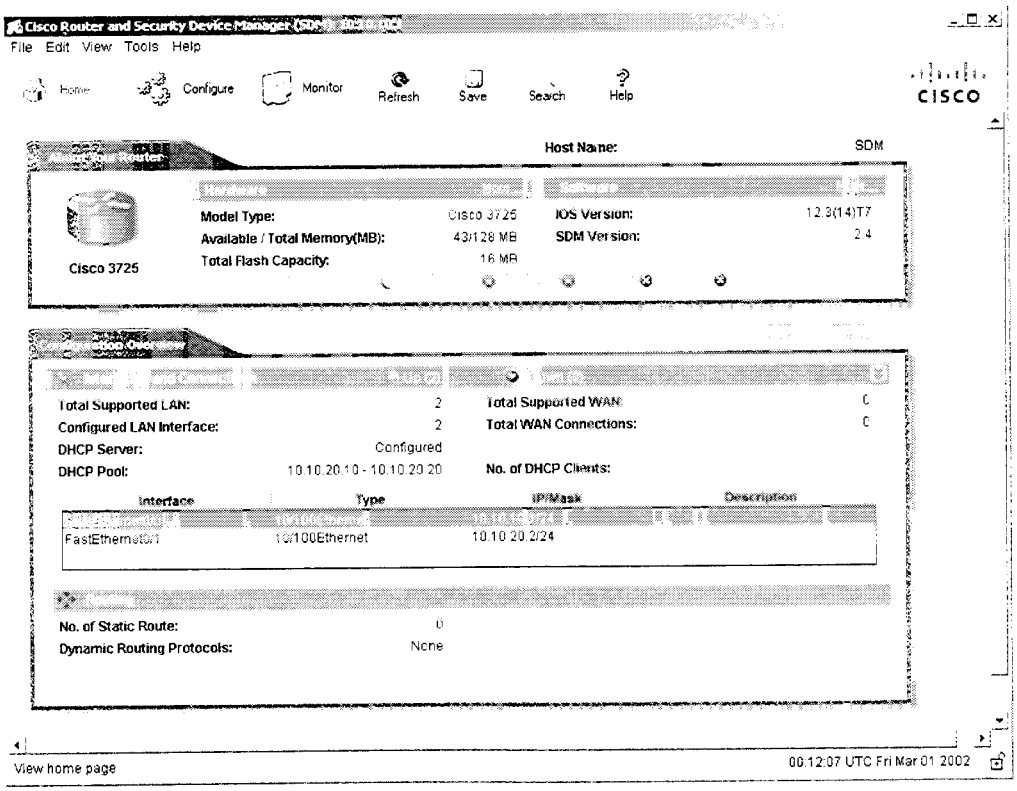




E encerramos a configuração.



Ao clicar em *Finish*, na tela anterior, as configurações são enviadas ao router. Se voltarmos à tela inicial, veremos que, agora, mais informações são apresentadas.



Devemos agora clicar no ícone *Save* e o SDM fará a cópia das configurações para a NVRAM. Pronto! Configuramos o router usando o SDM! Este é apenas um breve exemplo para apresentar a ferramenta. Caso você tenha curiosidade em testá-la, é possível utilizar o *Dynamips* para emular um roteador compatível com o SDM (por exemplo, um 3620),

proceder com a instalação do SDM e utilizá-lo, como se fosse um router verdadeiro.

Questões de Revisão – Configuração Básica de Roteadores Cisco

1. Quando um router é inicializado pela primeira vez, de onde o IOS é carregado, por default?

a) Boot ROM
b) NVRAM
c) Flash
d) ROM

2. Quais são os dois modos de se entrar no modo *setup* em um router?

a) Digitando o comando clear flash.
b) Digitando o comando erase start e reinicializando o router.
c) Digitando o comando setup.
d) Digitando o comando setup mode.

3. Se você se encontra no modo privilegiado e quer retornar ao modo usuário, qual comando deve ser digitado?

a) Exit
b) Quit
c) Disable
d) Control+Z

4. Qual comando de edição avançado move o cursor para o começo da linha?

a) Ctrl+E
b) Ctrl+F
c) Ctrl+B
d) Ctrl+A

5. Qual comando de edição avançado move o cursor para o final da linha?

a) Ctrl+E
b) Ctrl+F
c) Esc+B
d) Ctrl+A

6. Qual comando de edição avançado move o cursor para frente de um caractere?

a) Ctrl+E
b) Ctrl+F
c) Ctrl+B
d) Ctrl+A

7. Qual comando de edição avançado move o cursor para trás uma palavra?

a) Ctrl+E
b) Ctrl+F
c) Esc+B
d) Ctrl+A

8. Qual comando apresenta a versão do IOS que está sendo usado no router?

a) show flash
b) show flash file
c) show ip flash
d) sh ver

9. Qual comando mostra a você o conteúdo de EEPROM no seu router?

a) show flash
b) show flash file
c) show ip flash
d) sh ver

10. Qual comando mostra se um cabo DTE ou DCE encontra-se conectado à porta serial 0?

a) sh int s0
b) sh int serial 0
c) sho controll s 0
d) sho controllers s0

11. Qual comando evita que mensagens vindas do console sobrescrevam comandos que você está tentando digitar?

a) no logging
b) logging
c) logging asynchronous
d) logging synchronous

12. Qual comando permite aos usuários estabelecer uma conexão Telnet a um router sem que uma senha de modo usuário lhes seja pedida?

a) login
b) no login
c) O Telnet pode ser efetuado sem que nenhuma senha seja necessária, por default
d) no password

13. Qual comando informa ao router para encerrar a sessão console apenas um segundo após o último caractere ter sido digitado?

a) Timeout 1 0
b) Timeout 0 1
c) Exec-timeout 1 0
d) Exec-timeout 0 1

14. Como se configura todas as suas linhas Telnet com uma senha "ccna"?

a)
```
line vty
login
password ccna
```

b)
```
line vty 0 4
login
password ccna
```

c)
```
line vty 1
no login
password ccna
```

d)
```
line vty 0 4
password ccna
no login
```

15. Como se configura uma senha para a porta auxiliar?

a) line aux 1 | passw [senha] | no login
b) line aux 0 | passw [senha] | no login
c) line aux 0 4 | passw [senha] | login
d) line aux 0 | passw [senha] | login

16. Qual dos seguintes comandos criptografa suas senhas de modo usuário em um roteador Cisco?

a) Router#encryption on
b) Router(config)#password encryption
c) Router(config)#service password encryption
d) Router#service password encryption

17. Que comando você digita para salvar sua configuração atual e fazer com que ela seja carregada assim que o roteador for reiniciado?

a) (config)#copy current to starting
b) Router#copy starting to running
c) Router(config)#copy running-config star
d) Router#copy run start

18. Quando em modo *setup*, quais os dois tipos de configuração possíveis?

a) Basic
b) Advanced
c) Extended
d) Expanded

19. Qual comando apaga o conteúdo da NVRAM em um router?

a) delete nvram
b) delete startup
c) erase nvram
d) erase start

20. Qual seria um possível problema com uma interface, se após digitar o comando show interface serial 0 aparecesse a seguinte mensagem: Serial0 is administratively down, line protocol is down?

a) Os timers de keepalive não estão consistentes.
b) O administrador desativou intencionalmente a interface.
c) O administrador está emitindo pacotes "PING" da interface em questão.
d) Os cabos encontram-se desconectados.

Respostas das Questões de Revisão – Configuração Básica de Roteadores Cisco

1. **C.** O Sistema Cisco IOS é carregado da memória *Flash* por default.

2. **B, C**. Não que você deva usar o modo setup, mas, ca desejasse, você poderia apagar o conteúdo da NVRAM usando comando erase startup-config e, então, reinicializar o router. Vo também poderia digitar setup no modo privilegiado a qualqu momento.

3. **C**. O comando disable encerra a sessão privilegiada e retor você ao modo usuário.

4. **D**. O comando de edição Ctrl+A levará seu cursor para o come da linha.

5. **A**. O comando de edição Ctrl+E levará seu cursor para o final linha.

6. **B**. O comando de edição Ctrl+F moverá seu cursor um caracte para frente.

7. **C**. O comando de edição Esc+B moverá seu cursor uma palav para trás.

8. **D**. O comando show version lhe apresentará a versão do I(rodando no router. O comando sh flash não apresenta a informaç de versão, mas o nome da imagem do sistema armazenado nela.

9. **A**. A EEPROM é a FLASH e a FLASH é onde o IOS é armazena e de onde é carregado, por default. O comando show flash apresenta conteúdo da memória FLASH.

10. **C**. O comando show controllers serial 0 mostrará que tipo cabo (DTE ou DCE) encontra-se conectado à interface, além de outr informações úteis.

11. **D**. Esse é um comando útil. O uso desse comando evita q mensagens geradas pelo console venham a sobrescrever os comand na medida em que são digitados.

12. **B**. O comando no login aplicado às linhas VTY (Telnet) configu portas VTY (Telnet) para não executarem o procedimento autenticação.

13. **D**. O comando exec-timeout configura o timeout do console e minutos e segundos.

14. **B**. O comando line vty 0 4 configura as cinco portas VTY. comando login informa ao router que a checagem de senhas de ser habilitada para essas portas (por segurança, esse comandc ativado por default em todas as portas VTY em routers Cisco). último comando, password ccna, define a senha para a porta cor sendo "ccna".

15. **D**. Você pode obter acesso à porta auxiliar usando o comando line auxiliary 0 (como há apenas uma porta auxiliar, ela sempre será aux 0). Desse ponto em diante, o processo é o descrito. Lembre-se de que o comando login é necessário para habilitar a checagem de senhas nesta porta.

16. **C**. Para criptografar as senhas de modo usuário e privilegiado, use o comando de configuração global service password-encryption antes de configurar suas senhas.

17. **D**. Para salvar a configuração atual na NVRAM use o comando copy run start ou simplesmente wr.

18. **A, C**. O modo de configuração básico permite configurar somente o necessário para administração do sistema. Já o modo de configuração estendido permite que você se aprofunde na configuração, permitindo a configuração individual de cada interface presente no sistema, entre outras coisas.

19. **D**. O comando erase startup-config apaga o conteúdo da NVRAM, colocando o router em modo setup caso ele seja reinicializado após o processo.

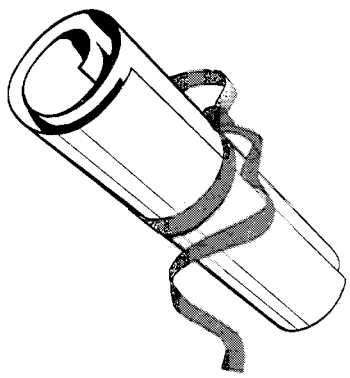
20. **B**. Se uma interface encontra-se administrativamente desativada, a princípio não existe um problema concreto. O administrador simplesmente não ativou a interface em questão. Qualquer problema - se existir - apenas será percebido após a ativação (no shut) da interface em questão.

Relação dos Comandos Analisados

Comando	Descrição
?	Apresenta ajuda sobre determinado comando.
bandwidth	Define a largura de banda em uma determinada interface.
banner	Cria um banner que é apresentado sempre que alguém se conecta ao router.
clear counters	Limpa as estatísticas de uma interface.
clock rate	Prove sincronização (*clocking*) em uma interface serial DCE.
config memory	Copia a configuração NVRAM (*startup*) para FLASH (*running*).
config network	Copia a configuração armazenada em um servidor TFTP para a FLASH.
config terminal	Coloca no modo de configuração global.

Comando	Descrição
copy run start	Copia a configuração da FLASH para a NVRAM.
description	Define uma descrição para uma interface.
disable	Encerra a sessão em modo privilegiado e leva para o modo usuário.
enable	Inicia sessão em modo privilegiado.
enable password	Define a senha não-criptografada *enable*.
enable secret	Define a senha criptografada *enable secret*. Esta substitui a senha *enable*.
erase startup	Deleta a configuração armazenada na NVRAM.
exec-timeout	Define o timeout para uma sessão de console em minutos e segundos.
hostname	Define o nome de um router.
interface	Leva para o modo de configuração de interface.
interface fastethernet 0/0	Modo de configuração de interface para uma interface *FastEthernet*.
interface fastethernet 0/0.1	Cria uma subinterface.
interface serial 5	Modo de configuração de interface para a interface serial 5.
ip address	Configura endereçamento IP em uma interface.
line	Permite a configuração de senhas de modo usuário.
line aux	Modo de configuração de interface auxiliar.
line console 0	Modo de configuração de console.
line vty	Modo de configuração de terminal VTY (Telnet).
logging synchronous	Barra mensagens de console.
logout	Encerra uma sessão de console.
media-type	Define o tipo de mídia em uma interface.
no shutdown	Ativa uma interface.
ping	Testa conectividade IP.
service password-encryption	Usado para criptografar senhas de modo usuário e a senha *enable*.
show controllers s 0	Apresenta o status de uma interface DTE ou DCE.
show history	Apresenta os dez últimos comandos digitados, por default.
show interface s0	Apresenta as estatísticas da interface Serial 0.
show run	Apresenta a configuração ativa no router.

Comando	Descrição
show start	Apresenta a configuração backup (NVRAM) do router.
show terminal	Apresenta o tamanho do histórico definido.
show version	Apresenta estatísticas do router.
shutdown	Desativa uma interface, levando-a ao modo administrativamente desativada.
Tab	Acaba de digitar um comando para você.
telnet	Usado para testar conectividade e configurar um router.
terminal history size	Altera o tamanho do histórico (10-255).
trace	Testa conectividade IP.



7 Roteamento IP

7.1 Tópicos Abordados

- Roteamento Estático *(Static Routing);*
- Roteamento Dinâmico *(Dynamic Routing);*
- Roteamento Default *(Default Routing);*
- NAT *(Network Address Translation);*
- Sumarização de Rotas Usando EIGRP e OSPF.

Neste capítulo discutiremos o processo de roteamento IP. Esse é um tópico muito importante a ser entendido, uma vez que é pertinente a todos os routers e configurações que utilizam o protocolo IP. Os três tipos básicos de roteamento já foram listados anteriormente, e será sobre esses tipos que discutiremos a partir de agora.

Antes de mais nada, é importante compreender o que é o processo de roteamento. Se a definição de roteamento pudesse de fato ser sintetizada em apenas uma frase, creio que a seguinte frase seria a mais apropriada: Um conjunto de regras que definem como dados originados em uma determinada sub-rede devem alcançar uma outra.

Como já vimos, para partir de uma rede e alcançar outra, um roteador precisa fazer o direcionamento do pacote, analisando o seu cabeçalho e consultando sua tabela de roteamento. Sempre que sairmos de uma rede e entrarmos em outra, um roteador estará por trás desse processo. Um exemplo: no prompt do DOS de um PC qualquer com conexão à Internet, digite o comando *tracert www.yahoo.com.br* e observe o resultado:

```
C:\Documents and Settings\PC_Marco>tracert www.yahoo.com.br

Rastreando a rota para hp.latam.vip.bro.yahoo.com
[200.152.161.127] com no máximo 30 saltos:

  1    <1 ms    <1 ms    <1 ms  PC_Marco [10.0.0.1]
  2    16 ms    16 ms    16 ms  200-100-100-
100.dsl.telesp.net.br [200.100.100.100]
  3    17 ms    16 ms    16 ms  200-204-30-
1.dsl.telesp.net.br [200.204.30.1]
  4    17 ms    16 ms    16 ms  200-148-160-
177.bbone.tdatabrasil.net.br [200.148.160.177]
  5    20 ms    18 ms    20 ms  A-3-0-2-br-spo-og-
ptt1.bbone.tdatabrasil.net.br [200.153.4.186]
  6    19 ms    16 ms    16 ms  200.185.4.2
  7    18 ms    16 ms    18 ms  200.185.6.41
  8    19 ms    18 ms    20 ms  200.185.6.100
  9    19 ms    20 ms    19 ms  200.185.60.34
 10    17 ms    19 ms    19 ms  slb1.bro.yahoo.com
[200.152.160.30]
 11    20 ms    19 ms    17 ms  hp.latam.vip.bro.yahoo.com
[200.152.161.127]

Rastreamento concluído.
```

Note que o que fizemos, basicamente, foi descobrir quantos saltos (nós) existem entre a máquina origem (*PC_Marco*) e destino (*www.yahoo.com.br*), e as respectivas estatísticas até cada um desses pontos. Percebemos que, nesse teste, existem 11 "saltos" desde meu PC até o servidor onde o domínio *www.yahoo.com.br* encontra-se hospedado. Mas, afinal, o que são esses "saltos" ou "nós"? Se você prestar atenção aos endereços IPs sendo atravessados, perceberá que as redes mudam conforme um novo ponto é adicionado à lista. Ou seja, iniciamos na rede 10.0.0.0 (minha rede interna), passamos para a rede 200.100.100.0 (rede da Telefônica - estou usando uma conexão ADSL *Speedy*), depois vamos para a rede 200.204.30.0 e assim por diante. Se estamos mudando de redes, os endereços listados na saída do comando *tracert* são roteadores! Isso mesmo, esses são os endereços dos dispositivos que estão encaminhando os pacotes de uma rede à outra, portanto, routers.

Nota: *Lembre-se de que a função de um router é encaminhar pacotes de uma rede IP para outra. Um router não encaminha pacotes para uma mesma rede, por default. Por exemplo: Se você tem um router com duas interfaces e tentar configurar ambas com IPs de uma mesma rede, o router irá acusar um erro.*

A título de curiosidade, a figura 7.1 mostra o mesmo resultado do *trace* anteriormente ilustrado, porém, de forma gráfica. O software que realiza essa proeza chama-se *NeoTrace* e é bastante interessante - e o

melhor, pode ser obtido de graça procurando-se pelo seu nome no Google ou no Yahoo.

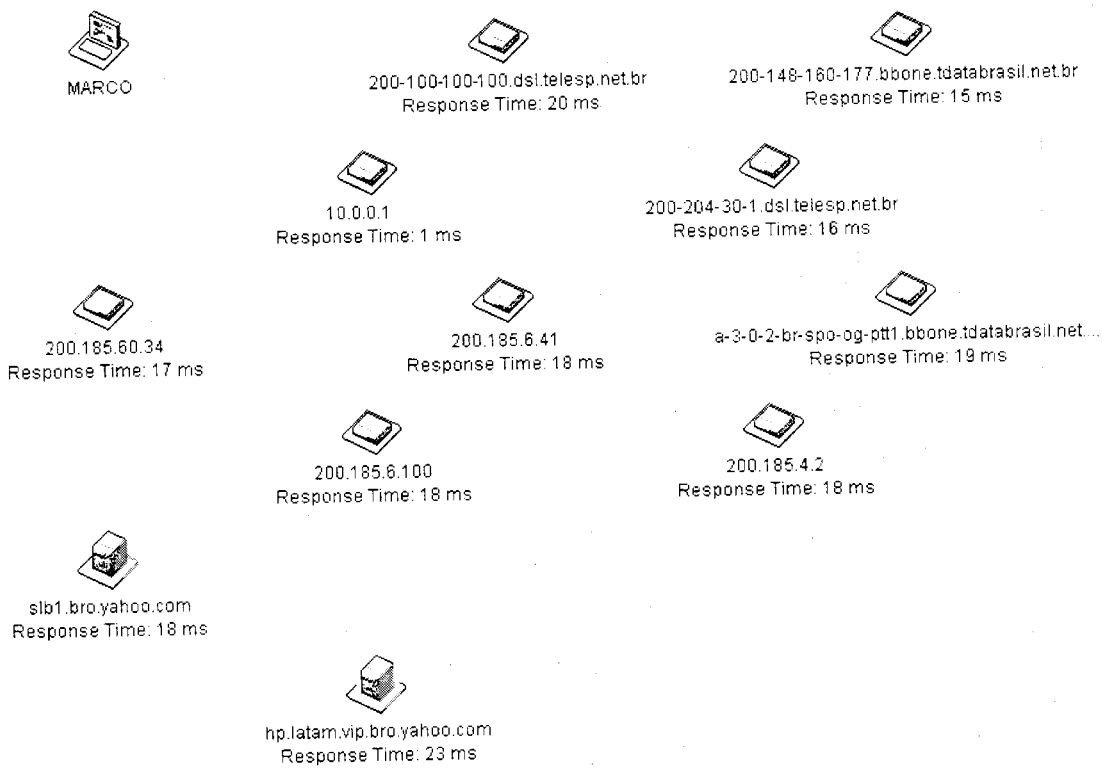


Figura 7.1: Saída proporcionada pelo software NeoTrace (que pode ser obtido no endereço: <http://downloads-zdnet.com.com/NeoTrace-Pro/3000-2648-7139158.html>).

7.2 O Processo de Roteamento

O processo de roteamento é efetuado para se transmitir um pacote de dados de um dispositivo em uma rede para um dispositivo em outra. Se sua rede não possui routers, então você não está, de fato, roteando. O papel dos routers é direcionar o tráfego para todas as redes em uma *internetwork*. Para ser capaz de efetuar o roteamento de pacotes, o router deve ter conhecimento de, no mínimo, o seguinte:

- Endereço de destino;
- Routers vizinhos;
- Rotas possíveis às redes remotas;
- Melhor rota para cada rede remota;
- Como manter e verificar informações relativas ao roteamento.

O router "aprende" sobre redes remotas através da comunicação com routers vizinhos (roteamento dinâmico) ou através do administrador (roteamento estático). O router, então, cria uma tabela de roteamento que descreve como encontrar tais redes remotas. Por

default, o router já possui conhecimento sobre todas as redes que se encontram diretamente conectadas. Caso a rede não se encontre diretamente conectada, ele deve descobrir o caminho para alcançá-la, seja via roteamento dinâmico, estático ou default.

Roteamento estático é o processo de criação de tabelas de rotas (*routing tables*) pelo administrador, manualmente. Já o roteamento dinâmico utiliza protocolos de roteamento (*routing protocols*) para se comunicar com routers vizinhos e, automaticamente, gerar tal tabela. Nesse processo, todos os routers pertencentes à rede atualizam suas tabelas entre si após um intervalo constante de tempo. Se uma mudança ocorrer na rede, os protocolos de roteamento informam automaticamente todos os routers conectados sobre a mudança. Caso o processo de roteamento estático esteja sendo utilizado, o administrador deve, a cada mudança na rede, atualizar as tabelas de rotas de todos os routers da rede manualmente.

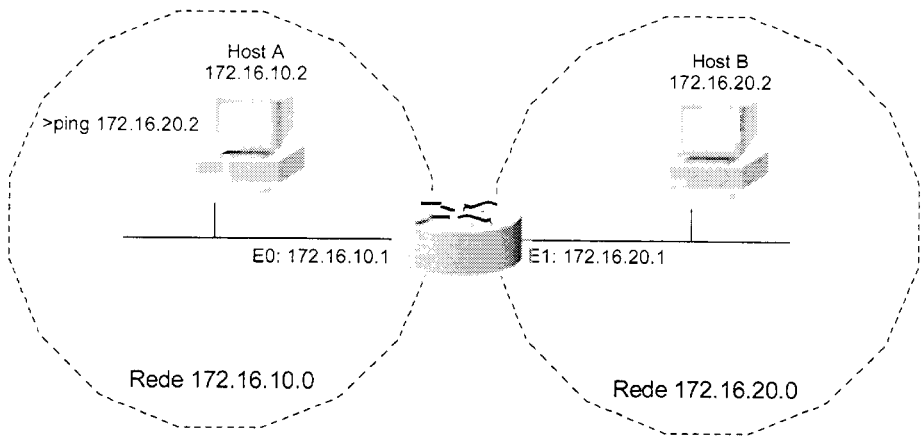


Figura 7.2: Funcionamento do processo de roteamento IP.

O processo de roteamento IP é relativamente simples e não muda, independentemente do tamanho ou complexidade da rede. Utilizemos a ilustração 7.2 para explicar passo a passo o que acontece quando o *Host A* tenta se comunicar com o *Host B* (executando um comando *ping*) em uma rede diferente:

1. Da interface de comando (CLI), um usuário na *rede 10* digita o comando *ping 172.16.20.2*. Um pacote ICMP é então gerado no *Host A*;
2. O protocolo IP trabalha em conjunto com o protocolo ARP (*Address Resolution Protocol*) para determinar para qual rede o pacote é destinado. Uma vez determinado que o pacote em questão é destinado a uma rede remota e não à local, ele é enviado para o router para que, então, seja roteado para a rede destino;

***Dica**: Entre no DOS de um PC, digite arp -a e observe sua saída. Se nada lhe for apresentado, dê um ping em uma máquina vizinha e execute o comando arp -a novamente.*

3. Para o *Host A* enviar um pacote para o router, ele deve saber o endereço de hardware (MAC) da interface conectada à rede local (*E0*). Para obter esse endereço, o host realiza uma pesquisa no ARP cachê;
4. Caso o endereço IP da interface E0 não se encontre no ARP cache, o *Host A* emite uma mensagem de *broadcast* ARP, procurando identificar o endereço de hardware que corresponde ao endereço IP 172.16.10.1. É por esse motivo que, normalmente, o primeiro *ping* expira (*time out*) e os outros quatro são bem-sucedidos. Uma vez que o endereço seja armazenado no ARP cache do host, não ocorrem mais *time outs*;
5. A interface E0 do router responde com seu endereço de hardware. O *Host A*, agora, tem tudo o que é necessário para transmitir o pacote para o router. A camada de rede passa o pacote gerado através da requisição ICMP (*ICMP echo request* = *PING*) para a camada de enlace, juntamente com o endereço de hardware para onde o *Host A* deseja enviar o pacote (interface E0 do roteador). O pacote inclui o endereço IP da origem (*source address*) e do destino (*destination address*), assim como o protocolo ICMP especificado no campo *protocolo* da camada de rede;
6. A camada de enlace gera um *frame* (quadro) que encapsula o pacote com informações de controle necessárias à sua transmissão pela rede local. Essas informações incluem os endereços de hardware da origem (*Host A*) e do destino (*Router*) e o campo *type*, que especifica qual o protocolo de camada de rede em atividade (no caso, IP);
7. A camada de enlace do *Host A* passa o *frame* gerado para a camada física, que codifica os dados em 0s e 1s e os transmite através da interface local;
8. O sinal é captado pela interface *Ethernet 0* do router, que realiza um processo de sincronização com o preâmbulo (*preamble* - seqüência alternada de 0s e 1s para sincronização) e efetua a extração do frame. A interface, após a extração do frame, efetua uma checagem (CRC) e compara o resultado obtido com o campo FCS, localizado no final do frame, assegurando-se de que a integridade do frame foi mantida;

9. O endereço de hardware do destino é checado. O campo *type* do *frame*, então, se encarrega de informar para qual protocolo de rede o pacote de dados deve ser entregue. Em nosso exemplo, o protocolo IP encontra-se especificado no campo *type*, logo, o pacote de dados é passado a esse protocolo. O *frame* é então descartado e o pacote original, gerado pelo *Host A*, é armazenado no buffer do router;
10. O protocolo IP verifica o endereço IP de destino do pacote recebido para certificar-se que o pacote é, de fato, destinado ao router. Como o endereço de destino é 172.16.20.2, o router determina - através de uma rápida checagem em sua tabela de roteamento (*routing table*) - que esse endereço é uma rede diretamente conectada à interface *Ethernet 1* (rede 172.16.20.x);
11. O router armazena o pacote no buffer da interface *Ethernet 1*. Ele precisa agora gerar um *frame* para transmitir o pacote ao seu destino final, o *Host B*. Primeiramente, o router checa sua tabela ARP (*ARP cache*) para determinar se o endereço de hardware de destino já foi resolvido para o endereço IP em uma comunicação anterior (do mesmo modo que o *Host A* fez no passo 4!). Caso negativo, o router emite uma mensagem de *broadcast* ARP pela interface *E1* para que o endereço 172.16.20.2 seja localizado;
12. O *Host B* responde a essa mensagem com o endereço de hardware de sua interface de rede. O router, agora, possui tudo o que necessita para transmitir o pacote ao seu destino final. O *frame* gerado pela interface *E1* do router possui o endereço de hardware de origem (interface E1) e o endereço de hardware de destino (interface de rede instalada no *Host B*). O ponto mais importante aqui é notar que, mesmo que os endereços de hardware (de origem e de destino) do *frame* mudem a cada interface que é atravessada, os endereços IPs de origem e de destino nunca são alterados, ou seja, o pacote de dados nunca é alterado. Apenas sua moldura (o *frame*) sofre alterações;
13. O *Host B* recebe o *frame* e procede com a sua checagem (CRC). Caso não existam problemas, ele é descartado e o pacote é passado para o protocolo de camada de rede responsável pela operação (IP). O protocolo IP, então, checa o endereço IP de destino. Uma vez que o endereço IP checado coincida com o endereço IP da interface instalada no *Host B*, o protocolo IP analisa o campo *protocolo* do pacote para determinar qual o seu propósito;

14. Uma vez determinado que o pacote é uma requisição ICMP, o *Host B* gera um novo pacote ICMP com o endereço de destino sendo o endereço IP do *Host A*;
15. O processo, então, reinicia na direção oposta, até atingir seu destino final, o *Host A*.

No exemplo ilustrado anteriormente, a tabela de roteamento (*routing table*) do router já possuía os endereços IPs de ambas as redes, uma vez que elas estavam diretamente conectadas ao router em questão. O que acontece, então, se adicionarmos três outros routers? A figura 7.3 ilustra uma rede composta de quatro routers: 2500A, 2500B, 2500C e 2621A. Esses routers, por default, contêm em suas *routing tables* apenas os endereços IPs de redes diretamente conectados a eles.

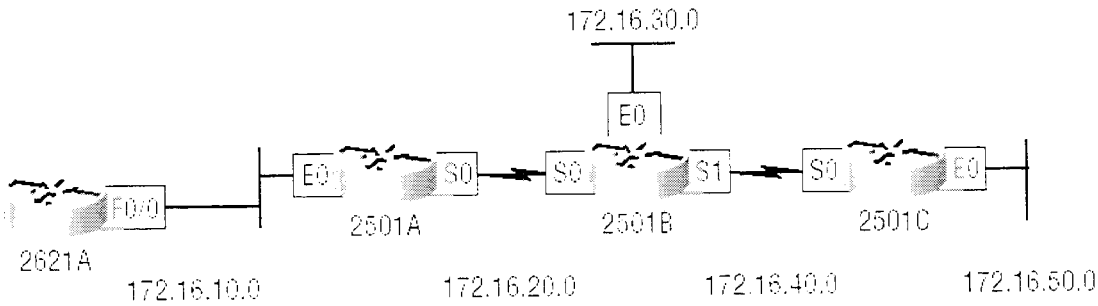


Figura 7.3: Uma rede um pouco mais complexa.

Na figura anterior, observamos três routers da linha 2500 conectados através de uma WAN (conexões seriais *S0-S0* e *S1-S0*) e o router 2621 conectado ao router 2500A através de uma rede Ethernet. Cada router possui também uma rede local (Ethernet) conectada.

O primeiro passo é a configuração das interfaces ativas de cada um dos routers. A tabela a seguir nos mostra o esquema de endereçamento IP utilizado na configuração de cada rede (note que os endereços apresentados foram aleatoriamente escolhidos. Esses endereços podem, e devem, variar caso a caso). Vamos primeiro acompanhar como cada interface é devidamente configurada, para depois verificarmos como configurar o roteamento IP. Cada endereço de rede apresentado na tabela a seguir possui uma máscara de rede de 24-bits (255.255.255.0):

Router	Rede	Interface	Endereço IP
2621A	172.16.10.0	F0/0	172.16.10.1
2501A	172.16.10.0	E0	172.16.10.2
2501A	172.16.20.0	S0	172.16.20.1
2501B	172.16.20.0	S0	172.16.20.2
2501B	172.16.30.0	E0	172.16.30.1
2501B	172.16.40.0	S1	172.16.40.1
2501C	172.16.40.0	S0	172.16.40.2
2501C	172.16.50.0	E0	172.16.50.1

O processo de configuração de um router é relativamente simples, pois basta configurar os endereços IPs para cada interface (é importante, em um ambiente de produção, que você defina uma tabela como a apresentada na página anterior para auxiliá-lo no processo de configuração e para posterior documentação das redes criadas) e, logo em seguida, aplicar o comando *no shut* em cada interface configurada. O processo ficará um pouco mais complexo mais adiante, mas, por ora, vamos configurar os endereços IPs para cada interface.

7.2.1 Configuração do Router 2621A

Para configurar o router 2621A, basta definir um endereço IP para a interface *FastEthernet 0/0*. O processo de configuração de um nome para o router (*hostname*) facilita a identificação de cada um em uma rede. Observe nas ilustrações a seguir, que o processo de configuração, em si, é bastante simples, e se resume em algumas poucas linhas:

```
Router>en
Router#config t
Router(config)#hostname 2621A
2621A(config)#interface f0/0
2621A(config-if)#ip address 172.16.10.1 255.255.255.0
2621A(config-if)#no shut
```

Para verificação da tabela de roteamento (*routing table*) criada, utilize o comando *sh ip route*.

```
2621A#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
       user static route, o - ODR, P - periodic downloaded
       static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, FastEthernet0/0
```

Note que apenas a rede configurada é apresentada na tabela, o que significa que o router 2621A, até o momento, sabe como alcançar apenas a rede 172.16.10.0. Observe também que a sigla "*C*" precede o endereço de rede apresentado, indicando que se trata de uma rede diretamente conectada ao router. Note os outros códigos disponíveis: S-Static, I-IGRP, R-RIP, M-mobile, B-BGP, D-EIGRP, EX-EIGRP external, O-OSPF, etc.

Note também que, mais uma vez, a informação da máscara de rede aparece no formato */24*.

7.2.2 Configuração do Router 2501A

Para configurar o router 2501A, duas interfaces precisam ser configuradas: *Ethernet0* e *Serial0*. Os comandos a seguir configuram a interface S0 para a rede 172.16.20.0 e a interface E0 para a rede 172.16.10.0.

```
Router>en
Router#config t
Router(config)#hostname 2501A
2501A(config)#interface e0
2501A(config-if)#ip address 172.16.10.2 255.255.255.0
2501B(config-if)#no shut
2501A(config-if)#interface s0
2501A(config-if)#ip address 172.16.20.1 255.255.255.0
2501A(config-if)#no shut
```

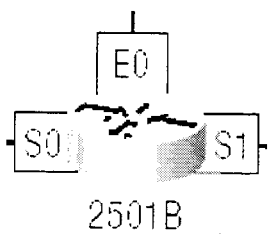
O comando *sh ip route* apresenta a tabela de roteamento do roteador 2501A.

```
2501A#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
       user static route, o - ODR, P - periodic downloaded
       static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.20.0 is directly connected, Serial0
C       172.16.10.0 is directly connected, Ethernet0
```

Note que o router 2501A sabe como alcançar as redes 172.16.10.0 e 172.16.20.0. Os routers 2621A e 2501A já podem se comunicar, pois se encontram na mesma rede local (LAN) - não há conexões WAN entre os dois routers.

7.2.3 Configuração do Router 2501B

A configuração do router 2501B não é muito diferente, a não ser pelo fato de que é preciso prover sincronização através do comando *clock rate* para ambas as interfaces DTE conectadas às interfaces seriais. Três interfaces precisam ser configuradas: *Serial0, Ethernet0* e *Serial1*.




```
Router>en
Router#config t
Router(config)#hostname 2501B
2501B(config)#interface e0
2501B(config-if)#ip address 172.16.30.1 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#interface s0
2501B(config-if)#ip address 172.16.20.2 255.255.255.0
2501B(config-if)#clock rate 64000
2501B(config-if)#no shut
2501B(config-if)#interface s1
2501B(config-if)#ip address 172.16.40.1 255.255.255.0
2501B(config-if)#clock rate 64000
2501B(config-if)#no shut
```

O comando *sh ip route* apresenta a saída ilustrada a seguir. Note que o router 2501B sabe como alcançar as redes 172.16.20.0, 172.16.30.0 e 172.16.40.0, que são as redes diretamente conectadas a ele:

```
2501B#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
       user static route, o - ODR, P - periodic downloaded
       static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.40.0 is directly connected, Serial1
C       172.16.30.0 is directly connected, Ethernet0
C       172.16.20.0 is directly connected, Serial0
```

O router 2501A e o router 2501B podem se comunicar, uma vez que se encontram na mesma rede WAN. Entretanto, o router B não pode se comunicar com o router 2621A, pois ele não tem informações em sua *routing table* sobre como alcançar a rede 172.16.10.0. O router 2501A pode "pingar" uma vez que temos na rede os routers 2621A e 2501B, entretanto, os routers 2501B e 2621A não "se enxergam", pois não existem rotas definidas para eles nas tabelas de roteamento dos respectivos roteadores.

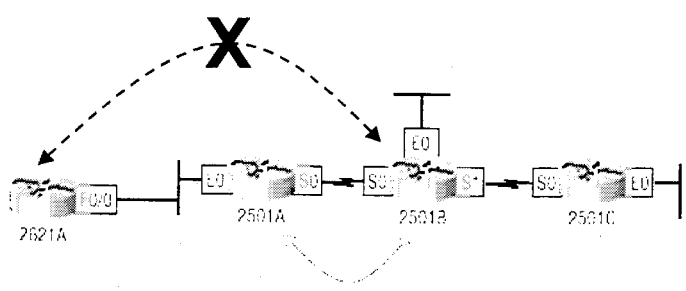


Figura 7.4: Operação da rede até o momento.

7.2.4 Configuração do Router 2501C

A configuração do router 2501C é muito parecida com a do router 2501A, apenas alterando-se os endereços de rede.

A interface E0 é associada à rede 172.16.50.0 e a interface *Serial0*, à rede WAN 172.16.40.0.

```
Router>en
Router#config t
Router(config)#hostname 2501C
2501C(config)#interface e0
2501C(config-if)#ip address 172.16.50.1 255.255.255.0
2501C(config-if)#no shut
2501C(config-if)#interface s0
2501C(config-if)#ip address 172.16.40.2 255.255.255.0
2501C(config-if)#no shut
```

O comando *sh ip route* apresenta a saída ilustrada a seguir. Note que o router 2501C sabe como alcançar as redes 172.16.40.0 e 172.16.50.0, que são as redes diretamente conectadas a ele.

```
2501C#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
       user static route, o - ODR, P - periodic downloaded
       static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.50.0 is directly connected, Ethernet0
C       172.16.40.0 is directly connected, Serial0
```

O router 2501C pode se comunicar diretamente com o router 2501B uma vez que participam da mesma rede WAN. Entretanto, por default, o router C não tem conhecimento de nenhum outro router ou rede.

7.3 Roteamento IP

A rede ilustrada anteriormente encontra-se devidamente configurada com relação ao endereçamento IP. As redes que não estão diretamente conectadas aos routers, entretanto, ainda não podem se comunicar. Os routers "aprendem" as rotas através da consulta às suas tabelas de roteamento (*routing tables*). Se um pacote é endereçado a uma rede cujo endereço não se encontra nessa tabela **o pacote é simplesmente descartado**. Não há envio de mensagens de *broadcast* ou qualquer outro

esquema utilizado para se descobrir tal rota. Como, então, configurar os routers da rede sugerida para que suas tabelas incluam os endereços das redes remotas?

Existem diferentes maneiras de se conseguir isso, utilizados de acordo com a situação. O entendimento dos diferentes modos de roteamento IP é essencial para que a escolha do melhor seja efetuada. Os diferentes modos de roteamento que podem ser utilizados são, basicamente, três: *estático, dinâmico* e *default*. Iniciaremos com a implementação de roteamento estático na rede ilustrada anteriormente. O motivo de começarmos com esse método é simples: a definição e implementação de rotas estáticas exige um profundo entendimento da rede como um todo.

7.3.1 Roteamento Estático

Vantagens:

- Redução do *overhead* na CPU do router;
- Não há utilização de largura de banda entre os routers;
- Segurança (uma vez que o administrador possui total controle do processo de roteamento).

Desvantagens:

- O administrador precisa, efetivamente, possuir um profundo conhecimento global da rede;
- Se uma rede for adicionada à *internetwork*, o administrador deve, manualmente, adicionar a rota de como alcançá-la a cada um dos routers;
- Não é viável a redes de grande porte (veremos o porquê).

A sintaxe do comando utilizado para se configurar rotas estaticamente é a seguinte:

```
ip route [rede_destino] [máscara] [endereço_do_próximo_ponto ou
interface_de_saída] [distância_administrativa] [permanent]
```

Onde:

- **ip route**: Comando utilizado para designar rotas estaticamente;
- **rede_destino (*destination network*)**: Endereço da rede que você está adicionando à tabela de roteamento;
- **máscara (*mask*)**: Máscara de rede em uso na rede;
- **endereço do próximo salto (*next hop address*)**: Endereço do ponto que receberá o pacote e o enviará à rede destino. Trata-se da interface do router de próximo ponto, que se encontra

diretamente conectado ao router que está sendo configurado e que possui conhecimento de como chegar à *rede_destino*;

- **interface de saída (*exit interface*)**: Pode ser utilizada em lugar do endereço do próximo ponto apenas em conexões seriais ponto a ponto (o que, normalmente, caracteriza uma rede WAN). Esse comando não funciona em uma LAN, como uma interface Ethernet, por exemplo;
- **distância administrativa (*administrative distance/AD*)**: Por default, rotas estáticas possuem uma distância administrativa de *1*. Esse valor pode ser alterado adicionando-se um valor ao final do comando (veremos distâncias administrativas com um maior nível de detalhamento mais adiante);
- **permanent**: Caso uma interface esteja desativada ou o router não possa se comunicar com o router no próximo ponto após um determinado período de tempo, a rota é automaticamente descartada da tabela de roteamento. A utilização da opção *permanent* mantém os dados na tabela de roteamento, não importa o que aconteça.

7.3.1.1 Configuração de Roteamento Estático no Router 2621A

Cada tabela de roteamento inclui, automaticamente, todas as redes diretamente conectadas. Para que seja possível entre as demais redes pertencentes à sua *internetwork*, a tabela de roteamento deve incluir informação que define onde as outras redes estão localizadas e como alcançá-las.

Em nossa rede sugerida, temos cinco redes: 172.16.10.0, 172.16.20.0, 172.16.30.0, 172.16.40.0 e 172.16.50.0. O router 2621A, por sua vez, encontra-se conectado apenas à rede 172.16.10.0. Para que o router 2621A seja capaz de encaminhar pacotes para todas as redes, os seguintes endereços de rede devem ser incluídos em sua tabela de roteamento:

172.16.20.0
172.16.30.0
172.16.40.0
172.16.50.0

Na seqüência, é ilustrado o processo de adição de tais rotas na tabela de roteamento do router 2621A. Para esse router ser capaz de encontrar redes remotamente conectadas - dados descrevendo tais redes, máscara de rede utilizada e para onde enviar os pacotes - devem ser adicionados à tabela de roteamento. Note que cada rota estática envia os pacotes para o endereço 172.16.10.2, que é o endereço do próximo salto (interface e0 do router 2501A), relativo ao router 2621A.

```
2621A(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2
2621A(config)#ip route 172.16.30.0 255.255.255.0 172.16.10.2
2621A(config)#ip route 172.16.40.0 255.255.255.0 172.16.10.2
2621A(config)#ip route 172.16.50.0 255.255.255.0 172.16.10.2
```

Após a configuração do router, você pode utilizar o comando *show ip route* ou *show running-config* para verificar as rotas configuradas.

```
2621A#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 -
IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
       user static route, o - ODR, P - periodic downloaded
       static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
S       172.16.50.0 [1/0] via 172.16.10.2
S       172.16.40.0 [1/0] via 172.16.10.2
S       172.16.30.0 [1/0] via 172.16.10.2
S       172.16.20.0 [1/0] via 172.16.10.2
C       172.16.10.0 is directly connected, FastEthernet0/0
```

O router 2621A possui agora todas as informações necessárias para se comunicar com as redes remotamente conectadas. Entretanto, se os outros routers da rede não possuírem essa mesma informação, os pacotes serão descartados ao alcançarem o router 2501A.

7.3.1.2 Configuração de Roteamento Estático no Router 2501A

O router 2501A encontra-se conectado às redes 172.16.10.0 e 172.16.20.0. Para o router 2501A ser capaz de rotear pacotes para todas as redes, os seguintes endereços de rede devem ser incluídos em sua tabela de roteamento:

172.16.30.0
172.16.40.0
172.16.50.0

A seguir, ilustramos o processo de configuração de tais rotas no router 2501A.

```
2501A(config)#ip route 172.16.30.0 255.255.255.0 172.16.20.2
2501A(config)#ip route 172.16.40.0 255.255.255.0 172.16.20.2
2501A(config)#ip route 172.16.50.0 255.255.255.0 172.16.20.2
```

Uma vez que todos os outros routers da rede possuam o mesmo conteúdo em suas tabelas de roteamento, o router 2501A poderá se comunicar com todas as redes remotamente conectadas. A verificação, novamente, pode ser feita através do comando *sh ip route*.

```
2501A#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route,
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
S       172.16.50.0 [1/0] via 172.16.20.2
S       172.16.40.0 [1/0] via 172.16.20.2
S       172.16.30.0 [1/0] via 172.16.20.2
C       172.16.20.0 is directly connected, Serial0
C       172.16.10.0 is directly connected, Ethernet0
```

7.3.1.3 Configuração de Roteamento Estático no Router 2501B

O router 2501B encontra-se conectado às redes 172.16.20.0, 172.16.30.0 e 172.16.40.0. Para o router 2501B ser capaz de rotear pacotes para todas as redes, os seguintes endereços devem ser incluídos em sua tabela de roteamento:

172.16.10.0
172.16.50.0

Eis o processo de configuração de tais rotas no router 2501B.

```
2501B(config)#ip route 172.16.10.0 255.255.255.0 172.16.20.1
2501B(config)#ip route 172.16.50.0 255.255.255.0 172.16.40.2
```

Note que, para chegar à rede 10, o router 2501B deve enviar os pacotes para o router 2501A (172.16.20.1), enquanto que para alcançar a rede 50 ele envia os pacotes para o router 2501C (172.16.40.2). Basta observar os endereços do próximo salto. Para checagem da tabela:

```
2501B#sh ip route
Codes: C - connected, S - static, R - RIP, M -
mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
       E1 - OSPF external type 1, E2 - OSPF external
type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS
level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U
       - per-user static route, o - ODR, P - periodic
       downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
S       172.16.50.0 [1/0] via 172.16.40.2
C       172.16.40.0 is directly connected, Serial1
C       172.16.30.0 is directly connected, Ethernet0
C       172.16.20.0 is directly connected, Serial0
S       172.16.10.0 [1/0] via 172.16.20.1
```

7.3.1.4 Configuração de Roteamento Estático no Router 2501C

O router 2501C encontra-se conectado às redes 172.16.40.0 e 172.16.50.0. Para ele rotear pacotes para todas as redes, os seguintes endereços de rede devem ser incluídos em sua tabela de roteamento:

172.16.10.0
172.16.20.0
172.16.30.0

A seguir, ilustramos o processo de configuração de tais rotas no router 2501C.

```
2501C(config)#ip route 172.16.10.0 255.255.255.0 172.16.40.1
2501C(config)#ip route 172.16.20.0 255.255.255.0 172.16.40.1
2501C(config)#ip route 172.16.30.0 255.255.255.0 172.16.40.1
```

E para verificação da tabela:

```
2501C#sh ip route
Codes: C - connected, S - static, R - RIP, M -
mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
       E1 - OSPF external type 1, E2 - OSPF external
type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS
level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U
       - per-user static route, o - ODR, P - periodic
       downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.50.0 is directly connected, Ethernet0
C       172.16.40.0 is directly connected, Serial0
S       172.16.30.0 [1/0] via 172.16.40.1
S       172.16.20.0 [1/0] via 172.16.40.1
S       172.16.10.0 [1/0] via 172.16.40.1
```

Uma vez finalizada a configuração das rotas no router 2501C, todos os routers da rede proposta devem possuir em suas tabelas de roteamento **exatamente o mesmo conteúdo**. Isso significa que uma comunicação total entre os routers da rede pode, agora, ser atingida. Entretanto, caso uma rede seja adicionada à *internetwork*, as tabelas de roteamento de todos os routers devem ser reconfiguradas para que contenham o endereço da rede adicionada. Em uma rede de pequeno porte, como a sugerida, isso não seria problema. Já em uma de grande porte, isso seria praticamente inviável.

7.3.1.5 Análise das Tabelas de Roteamento

A figura 7.5 mostra que todas as tabelas de roteamento contêm, agora, as mesmas informações sobre a nossa rede. Observe que, apesar de as rotas

em todas as tabelas serem exatamente as mesmas, o modo como foram inseridas na tabela de roteamento difere de router para router.

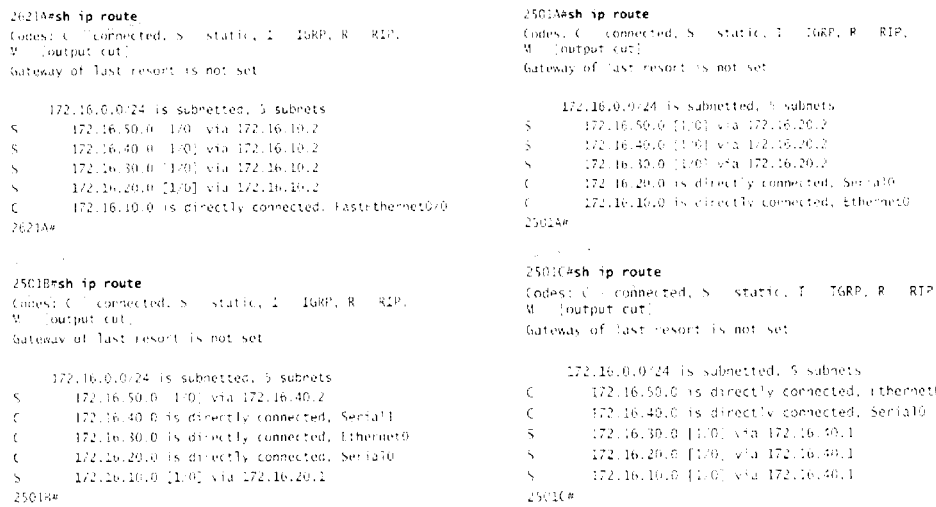


Figura 7.5: Tabelas de roteamento dos 4 routers, convergidas após configuração de roteamento.

Algumas rotas foram estaticamente configuradas *(S)*, enquanto outras, por se tratarem de redes diretamente conectadas, são incorporadas à tabela automaticamente, sem a necessidade de incluí-las manualmente *(C)*.

7.3.2 Roteamento Default

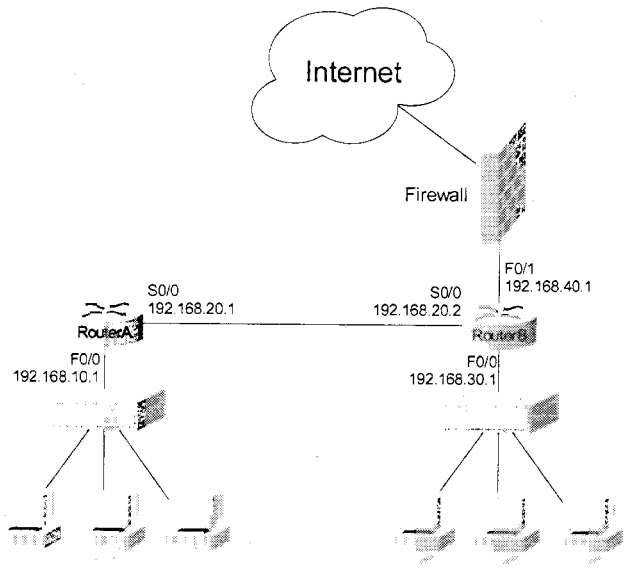
Roteamento default é usado no envio de pacotes para redes que não se encontrem na tabela de roteamento. Lembra-se da regra geral? Se o router não conhece o caminho (rota) para o destino, o pacote é descartado. Porém, usando-se roteamento default, podemos instruir o router que, em vez de simplesmente descartar o pacote com destino desconhecido, o encaminhe para uma interface específica de saída (por exemplo, uma interface com saída para a Internet ou conectada a um router que talvez conheça a rota para aquele destino).

Rotas default, se usadas sozinhas, apenas devem ser configuradas em redes chamadas *stub*, ou seja, redes que possuam apenas uma interface de saída. Nada impede que rotas default sejam usadas em routers com mais de uma interface de saída, porém, não se deve usar **apenas** roteamento default nesse caso. Uma combinação de roteamento default com um dos outros dois tipos (estático ou dinâmico) pode funcionar perfeitamente bem. Isso porque routers usam apenas a rota default em último caso. Se existir uma rota mais específica, esta será preferida. Por esse motivo, rotas default são também conhecidas como "rotas de último recurso" (*last resort gateway*).

A sintaxe da configuração de uma rota default é:

```
ip route 0.0.0.0 0.0.0.0 [endereço do
próximo salto / interface de saída]
```

Vamos supor uma rede como a ilustrada a seguir: temos duas redes locais conectadas entre si através dos routers RouterA e RouterB. Note que apenas RouterB possui uma saída para a Internet através da interface local *FastEthernet0/1*. Como configurar o roteamento para esses routers usando apenas os conhecimentos que vimos até o momento?



Antes de mais nada, vamos identificar as redes que temos em nosso problema:

```
192.168.10.0  192.168.20.0  192.168.30.0  192.168.40.0
```

Essas são as quatro redes que temos. Portanto, para que o roteamento ocorra de forma satisfatória, nossos dois routers deveriam conhecer essas quatro redes, ao menos. Analisando o RouterA e lembrando o que já vimos sobre roteamento, sabemos que ele já possui em sua tabela as redes que se encontram diretamente conectadas a ele, no caso, as redes 192.168.10.0 (F0/0) e 192.168.20.0 (S0/0). Logo, faltam, duas redes para ele: 192.168.30.0 e 192.168.40.0. Vamos adicioná-las:

```
RouterA(config)#ip route 192.168.30.0 255.255.255.0
192.168.20.2
RouterA(config)#ip route 192.168.40.0 255.255.255.0
192.168.20.2
```

O RouterB, por sua vez, já conhece as redes 192.168.20.0 (S0/0), 192.168.30.0 (F0/0) e 192.168.40.0 (F0/1). Falta, portanto, apenas a rede 192.168.10.0. Vamos adicioná-la:

```
RouterB(config)#ip route 192.168.10.0 255.255.255.0
```

```
192.168.20.1
```

Problema resolvido... Será? Bom, as duas LANs conseguem se comunicar, não há dúvidas sobre isso - uma vez que ambos os routers possuem todas as entradas necessárias em suas tabelas de roteamento. Porém, o que será que acontece quando um usuário de qualquer uma das duas redes locais tenta acessar um endereço na Internet, como *www.yahoo.com* (vamos supor que o endereço IP desse endereço Web seja 216.109.117.207)? Nossos routers possuem as redes de 192.168.10.0 a 192.168.40.0 em suas tabelas, mas nada a respeito do endereço que precisamos para esse acesso (216.109.117.207). Resumindo, o pacote do usuário que está tentando acessar o endereço mencionado não vai chegar a lugar nenhum já que nem o RouterA nem o RouterB possuem a rota para ele em suas tabelas. Conseqüentemente, o pacote será descartado.

Bom, podemos adicionar o endereço do Yahoo na tabela, não podemos? Sim, poderíamos fazê-lo, sem problemas. Mas e se outro usuário tentasse acessar outro endereço na Net, como <*www.google.com*> (64.233.161.99)? E se amanhã um outro tentasse checar as notícias em um site como o *UOL* e assim por diante? Veja que para que isso funcionasse, teríamos de passar o resto de nossas vidas inserindo dados nas tabelas de roteamento destes dois routers. Inviável! Para resolver o problema, que tal informarmos aos dois routers que, em qualquer tentativa de acesso a uma rede que não se encontre nas tabelas de roteamento, enviarem o pacote para o *firewall* (e este, para a Internet)? Isso é possível através do uso de rotas default. Para que isso funcione, basta adicionar as linhas seguintes aos respectivos routers:

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 serial0/0
```

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 fastethernet0/1
```

Observe que as próprias interfaces foram usadas como endereço do próximo salto em cada um dos routers. No caso do RouterA, a interface S0/0, que o conecta ao RouterB. No RouterB, foi usada a interface que o conecta ao firewall (F0/1). Os endereços IPs dos próximos saltos também poderiam ter sido usados, sem problemas (supondo que eles sejam conhecidos, no nosso cenário, por exemplo, não temos o endereço do firewall).

Agora, quando um usuário conectado à LAN do RouterA tentar acessar um endereço na Internet, o router irá verificar que o endereço destino não se encontra em sua tabela de roteamento e irá encaminhá-lo para o RouterB. Este, por sua vez, repetirá o processo e, usando a

rota default, encaminhará o pacote para o *firewall* (que o encaminhará para a Internet).

Se checarmos as tabelas, eis o que veremos:

```
RouterA#sh ip route

Gateway of last resort is Serial0/0 to network 0.0.0.0

S       192.168.40.0 [1/0] via 192.168.20.2
S       192.168.30.0 [1/0] via 192.168.20.2
C       192.168.20.0 is directly connected, Serial0/0
C       192.168.10.0 is directly connected, FastEthernet0/0
S*      0.0.0.0 [1/0] via Serial0/0

RouterB#sh ip route

Gateway of last resort is FastEthernet0/1 to network 0.0.0.0

S       192.168.40.0 is directly connected, FastEthernet0/1
S       192.168.30.0 is directly connected, FastEthernet0/0
C       192.168.20.0 is directly connected, Serial0/0
C       192.168.10.0 [1/0] via 192.168.20.1
S*      0.0.0.0 [1/0] via FastEthernet0/1
```

Note que, na saída do comando *sh ip route*, o *gateway of last resort* agora aparece configurado. Note também que a rota aparece identificada por um *S**, demonstrando que se trata de uma rota default. Agora sim, problema resolvido.

Nota: *Mais um comando deve ser levado em conta quando rotas default são configuradas: o comando ip classless. Todos os routers Cisco trabalham com redes classfull por default, ou seja, eles esperam que uma máscara de rede seja configurada para cada interface. Quando um router recebe um pacote para uma sub-rede destino que não se encontra na tabela de roteamento, ele descartará esse pacote, por default.* ***Se você está usando rotas default, você precisa utilizar o comando ip classless, uma vez que nenhuma sub-rede remota constará na tabela de roteamento.*** *Dos sistemas IOS 12.x em diante, o comando ip classless encontra-se ativado por default. Se você utilizar rotas default em routers rodando versões mais antigas do IOS, esse comando precisa ser digitado.*

7.3.3 Roteamento Dinâmico

Vantagens:

- Simplifica o gerenciamento da rede;
- Viável em redes de grande porte.

Desvantagens:

- Utiliza largura de banda nos links entre routers;
- Requer processamento pela CPU do router;
- Menor controle da *internetwork*.

Como você deve ter imaginado, existe, sim, um modo mais prático de se gerenciar uma rede composta de vários routers. Esse modo é conhecido como roteamento dinâmico (*dynamic routing*).

O processo de roteamento dinâmico utiliza protocolos para encontrar e atualizar tabelas de roteamento de routers. Esse modo é muito mais simples que o roteamento estático, porém, você paga por essa simplicidade. O roteamento dinâmico utiliza largura de banda (*bandwidth*) em links *inter-routers*, além de exigir que o processamento seja feito pela CPU do router.

Um protocolo de roteamento (*routing protocol*) define as regras a serem utilizadas por um router quando este se comunica com routers vizinhos. Os quatro protocolos de roteamento que discutiremos (cobrados no exame CCNA) são o RIP (*Routing Information Protocol*), o IGRP (*Interior Gateway Routing Protocol*), o OSPF (*Open Shortest Path First*) e o EIGRP (*Enhanced Interior Gateway Routing Protocol*).

Os protocolos de roteamento utilizados em *internetworks* pertecem a uma de duas categorias: IGP (*Interior Gateway Protocol*) e EGP (*Exterior Gateway Protocol*). Protocolos IGP são usados para troca de informações entre routers pertencentes a um mesmo Sistema Autônomo (AS - *Autonomous System*), que é uma coleção de redes sob um mesmo domínio administrativo. Já protocolos EGP são utilizados para comunicação entre routers pertencentes a ASs distintos. Um exemplo de protocolo que se encaixa na categoria EGP seria o BGP-4 (*Border Gateway Protocol*) - que não faz parte dos estudos para a prova CCNA, mas para o exame CCNP Routing.

7.3.3.1 Distâncias Administrativas (Administrative Distances)

Quando configurando protocolos de roteamento, deve-se atentar para um valor chamado Distâncias Administrativas (ADs), que são métricas utilizadas para classificar a confiabilidade das informações roteadas recebidas por um router, vindas de um router vizinho. A Distância Administrativa é representada por um número inteiro compreendido entre 0 e 255, 0 sendo a rota mais confiável e 255 significando que determinada rota é inalcançável. A tabela a seguir ilustra as Distâncias

Administrativas Padrão que os routers Cisco utilizam para determinar qual rota utilizar para alcançar uma rede remota:

Origem da Rota	Distância Administrativa Padrão
Interface diretamente conectada	0
Rota estática	1
EIGRP summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Desconhecido	255

Se uma rede encontra-se diretamente conectada, esta sempre utilizará a interface conectada nela. Se um administrador configurar rotas estáticas, o router "acreditará" nelas e não em rotas dinamicamente "aprendidas". Os valores das ADs podem ser alterados. A tabela ilustra os valores default. No caso do valor de uma AD ser 255, essa rota nunca será escolhida. Resumindo, quanto menor for o valor da AD, mais confiável será a rota.

Exemplificando, se em um mesmo roteador tivermos rotas estáticas configuradas e, simultaneamente, roteamento dinâmico sendo realizado por um determinado protocolo de roteamento, as rotas "aprendidas" dinamicamente somente serão utilizadas se ocorrer um problema com as rotas estáticas.

Existem três classes quando falamos em protocolos de roteamento:

- **Distance Vector**: Os protocolos de roteamento classificados nessa categoria utilizam a distância à rede remota para definição do melhor caminho. Cada vez que um pacote passa por um router, chamamos de *hop* (salto). No caso de protocolos de roteamento da classe *distance vector*, o menor número de "saltos" até determinada rede remota determina a melhor rota. Ou seja, são protocolos que se baseiam na contagem de "saltos" (*hop count*) para definição e escolha da melhor rota. Exemplos de protocolos que pertencem a essa classe são RIP e IGRP;

Nota: IGRP é classificado como distance vector mesmo usando largura de banda e atraso da linha como métricas default e não a contagem de saltos.

- **Link State**: Tipicamente conhecidos como "caminho mais curto antes" (*Shortest Path First*), cada router cria três diferentes tabelas. Uma dessas tabelas mantém informações sobre redes diretamente conectadas, outra determina a topologia de toda a rede e a última é a tabela de roteamento. Routers que utilizam protocolos *link state* conhecem a rede como um todo mais profundamente que qualquer protocolo baseado em *distance vector*. Um exemplo de protocolo de roteamento que pertence a essa classe é o OSPF (*Open Shortest Path First*);
- **Hybrid**: Trata-se de protocolos de roteamento que possuem características de ambas as classes anteriores. Um exemplo de protocolo que pertence a essa classe é o EIGRP.

de protocolo que pertence a essa classe é o EIGRP.

Não existe apenas uma solução que possa ser considerada a melhor uso no dia-a-dia. A escolha do melhor protocolo deve ser uma a baseada em estudos de operações cotidianas e conhecimento das terísticas de cada um deles. Uma vez que você entenda como as entes classes de protocolo funcionam, você poderá, então, fazer a or opção.

.2 Protocolos Baseados no Algoritmo Distance Vector

goritmo de roteamento *distance vector* envia as tabelas de roteamento pletas para os routers vizinhos, que então combinam as tabelas idas com as tabelas que já possuem e completam o mapa da rede. processo é conhecido como *routing by rumour*, pois o router recebe atualização do router vizinho e a aceita, sem nenhum tipo de icação.

É possível uma rede que possua diversos links para uma mesma remota. Nesse caso, a distância administrativa é o primeiro fator a hecado na determinação da rota preferencial. Se o valor das ADs m os mesmos, outras métricas são utilizadas pelos protocolos dores para determinar o melhor caminho para a rede remota.

O RIP, por exemplo, utiliza apenas a contagem de saltos (*hop count*) determinação da melhor rota para uma rede remota. Se o RIP rar-se com mais de um link para a mesma rede remota com a ma contagem de saltos, ele executará automaticamente o que namos de *round-robin load balance*, ou seja, distribuirá

alternadamente a carga entre os links de igual custo (mesmo número de saltos, no caso). **O RIP pode realizar balanceamento de carga para até 6 links com mesmo custo.**

Entretanto, um problema com esse tipo de métrica aparece quando dois ou mais caminhos para uma mesma rede remota possuem a mesma contagem de saltos, porém, diferentes largura de banda. A figura 7.6 ilustra dois caminhos para a rede remota 192.168.20.0. Observe que R1 encontra-se conectado a um link E1 com uma largura de banda de 2.048Mbps e a um link de 56K. A escolha mais sábia seria o caminho R1-R5-R6-R4, que possui uma largura de banda relativa evidentemente maior que o caminho R1-R2-R3-R4. Entretanto, uma vez que a contagem de saltos é a única métrica utilizada pelo protocolo RIP, ambos os caminhos serão vistos por esse protocolo como tendo o mesmo custo: três saltos (ou hops). Assim sendo, haverá um balanceamento de carga automático entre esses dois caminhos desiguais, o que resultará em problemas de congestionamento, posteriormente. Esse problema é chamado de *pinhole congestion*.

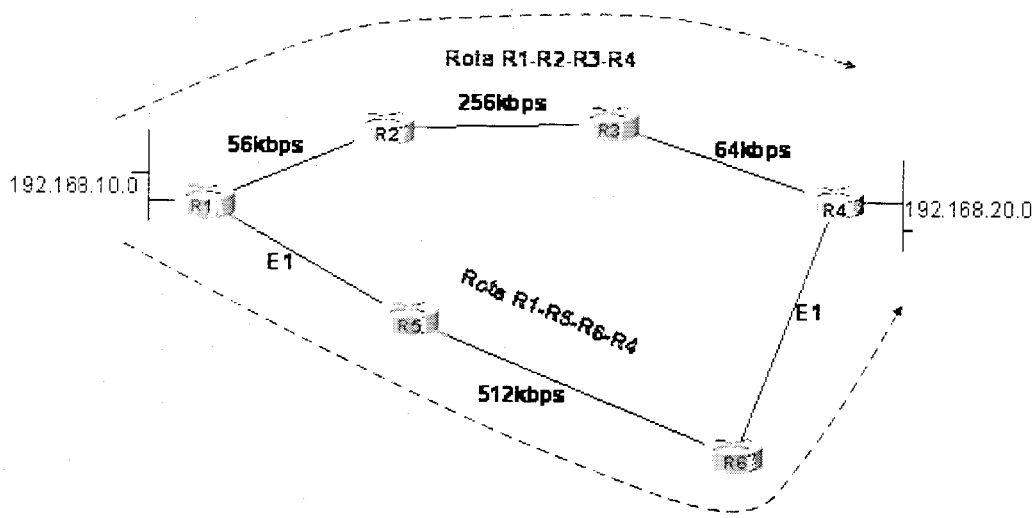


Figura 7.6: Pinhole congestion.

7.3.3.2.1 Estudo de uma Rede Baseada em Protocolos Distance Vector

É importante entender o que ocorre quando um protocolo de roteamento *distanc vector* é ativado. Na figura 7.7 observamos, em primeira instância, que os quatro routers, no início do processo, possuem em suas tabelas de roteamento apenas informações sobre redes diretamente conectadas. Uma vez que o protocolo de roteamento *distance vector* é ativado em cada um dos routers, as tabelas de roteamento são atualizadas com todas as informações reunidas dos routers vizinhos. Cada router envia sua tabela de roteamento completa

através de cada interface ativa nele. As informações de cada tabela incluem o endereço da rede, a interface de saída para esse endereço e a contagem de saltos para essa rede. Note que, para redes diretamente conectadas, o número da contagem é *0*.

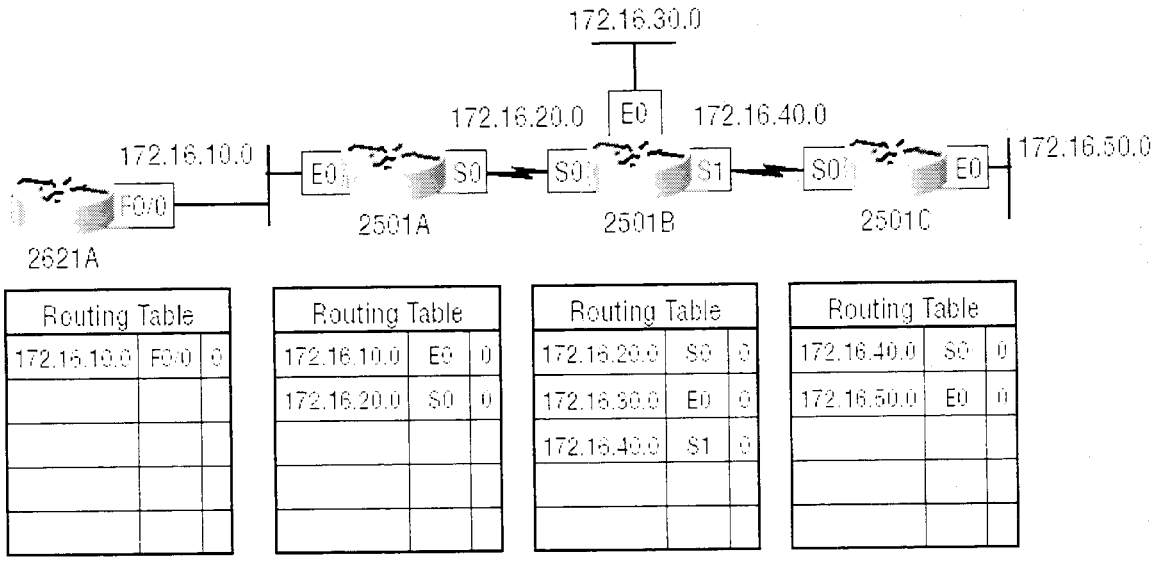


Figura 7.7: Situação inicial, antes da convergência.

Na figura 7.8, já representando um segundo momento, temos as tabelas atualizadas, com informações sobre todas as redes da internetwork. Nesse ponto, as tabelas de roteamento são tidas como convergidas. Quando os routers estão em convergência, nenhuma informação é transmitida. Eis o porquê de o tempo de convergência ser crítico. Um dos maiores problemas com o protocolo RIP é seu intervalo de convergência demasiado alto.

As tabelas de roteamento de cada router mantêm informações sobre o endereço da rede remota, a interface pela qual o router enviará pacotes para alcançar essa rede e a métrica utilizada (*hop count*, no caso).

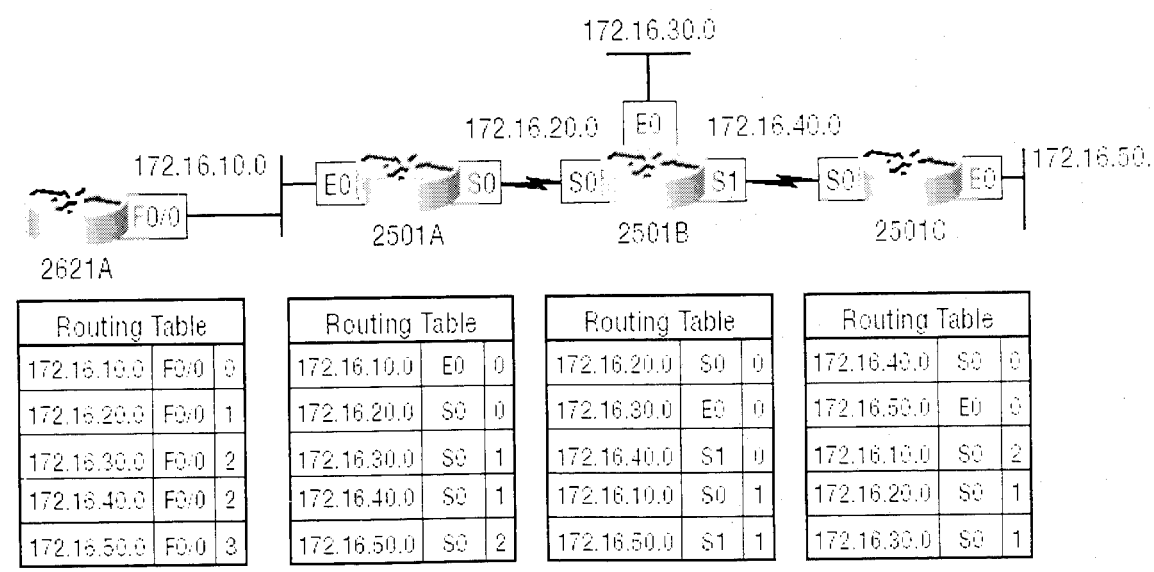


Figura 7.8: Tabelas de roteamento após convergência.

7.3.3.2.2 Loops de Roteamento (Routing Loops)

Protocolos de roteamento *distance vector* mantêm registros de todas as mudanças ocorridas na rede através do *broadcast* periódico de atualizações das tabelas de roteamento para todas as interfaces ativas. Esse processo funciona bem, apesar de consumir largura de banda e utilização da CPU do router. Entretanto, se uma queda na rede ocorre, é possível que aconteçam problemas. A lenta convergência dos protocolos de roteamento *distance vector* pode causar atualizações inconsistentes nas tabelas de roteamento e loops podem vir a ocorrer.

Loops de roteamento (*routing loops*) podem ocorrer quando os routers existentes na rede não são atualizados simultaneamente. Imagine, na figura 7.9, que a interface para a rede 5, por algum motivo, falhe. Todos os routers na rede ilustrada sabem sobre a rede 5 pelo router E. O router A, em suas tabelas, possui as rotas para a rede 5 através dos routers B, C e E. Quando a rede 5 falha, o router E avisa o router C. Isso faz com que o router C pare de rotear pacotes para a rede 5 através do router E. Porém, os routers A, B e D ainda não sabem sobre a situação da rede 5, portanto, continuam enviando suas tabelas para atualização. O router C irá, eventualmente, enviar sua tabela atualizada e fará com que o router B pare de rotear pacotes para a rede 5, mas os routers A e D ainda não foram atualizados. Para eles, a rede 5 encontra-se disponível através do router B com uma métrica de 3 saltos.

O router A envia uma mensagem regular a cada 30 segundos (no caso do RIP estar sendo usado como protocolo de roteamento) avisando que está ativo, e as rotas que ele conhece - que incluem o caminho para a rede 5. Os routers B e D, então, recebem as boas novas de que a rede 5 pode ser alcançada através do router A e enviam mensagens avisando que a rede 5 está disponível. Qualquer pacote destinado à rede 5 irá então passar pelo router A, dele para o router B e depois novamente para o router A. Isso é chamado de *routing loop*.

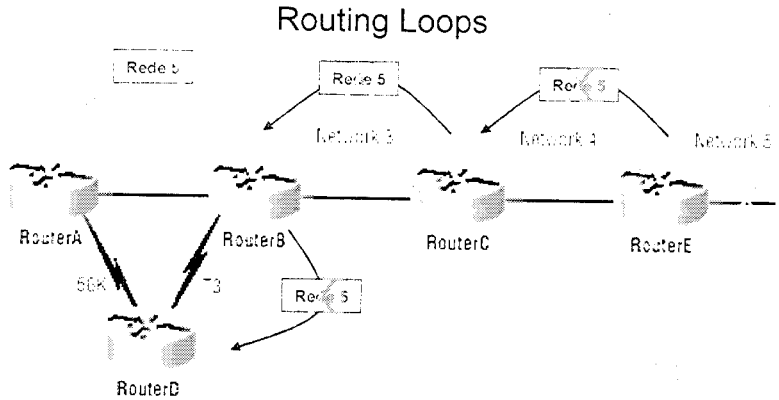


Figura 7.9: Exemplo de um loop de roteamento.

7.3.3.2.3 Mecanismos Existentes para Minimizar a Ocorrência de Loops

- **Maximum Hop Count**: O problema descrito anteriormente é chamado de contagem ao infinito (*counting to infinity*) e é causado pela transmissão de informações distorcidas sobre a real situação da rede. Sem algum tipo de intervenção, a contagem de saltos aumenta cada vez que um pacote passa por um router dentro do loop. Uma maneira de se resolver esse problema é definindo um número máximo de saltos que um pacote de dados deve atravessar antes de ser descartado. Chamamos isso de *maximum hop count*. Protocolos *distance vector* como o RIP permitem uma **contagem de saltos até 15.** Qualquer rede que requeira 16 saltos para ser alcançada é tida como inalcançável. Em outras palavras, após um loop de 15 saltos, a rede 5 será considerada inativa. Essa é uma solução remediadora, pois o *loop* não é eliminado. Os pacotes continuarão atravessando o *loop*, porém, agora, serão descartados após 15 saltos, não permanecendo no loop indefinidamente;
- **Split Horizon**: Outra solução para o problema de loops é chamado *split horizon*. Esse método reduz a transmissão de informações incorretas pela rede, assim como o *overhead* em redes baseadas em *distance vector* através da imposição da regra "a informação não pode ser enviada de volta na mesma direção em que foi recebida". Isso preveniria o router A de enviar a atualização de tabela de roteamento recebida do router B de volta ao router B.

***Nota**: O recurso split-horizon já é habilitado por default quando um protocolo do tipo vetor de distância é ativado em um router. Porém, se por algum motivo você desejar desativar este recurso (não recomendado), use o comando* no *ip split-horizon.*

- **Route Poisoning**: Outro modo de se prevenir a ocorrência de inconvenientes causados pela propagação de informações errôneas pela rede é conhecido como *route poisoning*. Por exemplo, quando a rede 5 falha, o router E inicia o processo de envenenamento de rota (*route poisoning*) através da inserção, em sua tabela de roteamento, do valor 16 para a rede 5, ou seja, **inalcançável**. Uma vez efetuada essa operação de envenenamento, o router C não mais estará suscetível a atualizações incorretas sobre a rota para a rede 5. Quando o router

C recebe o envenenamento de rota do router E, ele envia uma atualização chamada *poison reverse* (veneno reverso) de volta ao router E. Isso assegura que todas as rotas no segmento tenham recebido a informação sobre a rota envenenada;

- **Holddowns**: Finalmente, temos os chamados *holddowns*. Eles previnem que uma mensagem regular de atualização reative uma rota que, na verdade, encontra-se inalcançável por algum motivo. Também agem na prevenção de mudanças repentinas nas rotas, disponibilizando certo tempo para que uma rota que se encontre desativada por algum motivo torne-se ativa ou para que a rede se estabilize antes de decidir pela melhor rota. *Holddowns* também informam os routers para "reter", por um período específico de tempo, quaisquer mudanças que possam vir a afetar rotas recém-desativadas. Isso previne rotas, de fato, inoperantes de serem prematuramente restauradas nas tabelas de outros routers.

Quando um router recebe uma atualização de um router vizinho indicando que uma rede anteriormente acessível tornou-se inalcançável, o timer do *holddown* inicia sua contagem (esse timer determina quanto tempo essa informação ficará "retida" antes de ser repassada). Se uma nova atualização chegar de um router vizinho com uma melhor métrica, o *holddown* é removido e a atualização, repassada. Entretanto, se uma atualização é recebida de um router vizinho antes da expiração do timer e esta possuir uma métrica menor que a anterior, a atualização é ignorada e o timer continua ativado. Isso permite mais tempo para a rede convergir. *Holddowns* utilizam o que chamamos de *triggered update* – que reinicia o timer – para alertar routers vizinhos sobre mudanças na rede. Diferentemente de mensagens de atualização de routers vizinhos, *triggered updates* geram uma nova tabela de roteamento que é imediatamente enviada aos routers vizinhos uma vez que uma mudança foi detectada na rede. Três são as ocasiões em que *triggered updates* reiniciam o timer do *holddown*:

1. O timer do *holddown* expira;
2. O router recebe uma requisição de processamento proporcional ao número de links na *internetwork*;
3. Outra atualização é recebida indicando que a situação da rede foi alterada.

7.3.3.2.4 Características do Protocolo RIP

- Envia a tabela de roteamento completa para todas as interfaces a cada 30 segundos;
- Utiliza apenas a contagem de hops como métrica;

- Limita a contagem máxima de hops a 15, ou seja, não é viável em redes de grande porte ou com muitos routers.

Nota: *Lembre-se que, quando falamos da limitação de 15 saltos do RIP, nos referimos a 15 saltos consecutivos, em linha! Não quer dizer que uma rede com 15 routers não possa usar o protocolo. Este é um conceito importante.*

- O RIP versão 1 utiliza roteamento *classful*, ou seja, todos os dispositivos conectados à rede devem estar sob a mesma máscara de rede.

7.3.3.2.5 Temporizadores do Protocolo RIP (RIP Timers)

RIP utiliza quatro diferentes tipos de timers para regular sua performance:

- **Route Update Timer**: Estabelece um intervalo (geralmente 30 segundos) entre as atualizações regulares, nas quais os routers enviam uma cópia completa de suas tabelas de roteamento para todos os routers vizinhos;
- **Route Invalid Timer**: Determina a quantidade de tempo que deve correr (normalmente 180 segundos) antes de um router determinar que uma rota tornou-se inválida. Essa conclusão será atingida se não ocorrerem updates sobre uma determinada rota até o fim desse período;
- **Route Holddown Timer**: Informa aos routers para "reter", por um período específico de tempo (180 segundos, normalmente), quaisquer mudanças que possam vir a afetar rotas recém-desativadas. Isso previne rotas inoperantes de serem prematuramente restauradas nas tabelas de outros routers;
- **Route Flush Timer**: Estabelece o tempo (normalmente 240 segundos) entre uma rota tornar-se inválida e sua remoção da tabela de roteamento. Antes de eliminar uma rota de sua tabela de roteamento, o router avisa os routers vizinhos que determinada rota encontra-se inativa. O valor do *Invalid Timer* deve ser sempre menor que o do *Flush Timer*. Isso assegura ao router tempo suficiente para atualizar os routers vizinhos sobre a rota inválida, antes que sua tabela de roteamento seja atualizada.

Nota: *Os valores padrão dos timers anteriormente descritos devem ser memorizados para o exame CCNA. Um modo fácil de memorizá-los é o seguinte:*

RUT = 30 | RIT = RUT x 6 | RHT = RUT x 6 | RFT = RUT x 8

7.3.3.2.6 Configurando RIP

A configuração do RIP em um router é extremamente simples e direta. Eis o porquê de termos visto roteamento estático antes: se você domina esse roteamento, a configuração de um router para roteamento dinâmico será muito mais fácil.

No exemplo a seguir, configuramos RIP no router 2501B de nossa rede sugerida. Observe que, primeiramente, devemos excluir as rotas estáticas estabelecidas antes (comando *no ip route*) - caso isso não seja feito, o router continuará aceitando a configuração de rotas dinâmicas, porém, **como rotas estáticas possuem uma distância administrativa (AD) default de 1** e o protocolo RIP possui uma AD de **120**, as rotas estáticas serão sempre preferidas pelo router.

```
2501B#config t
2501B(config)#no ip route 172.16.10.0 255.255.255.0 172.16.20.1
2501B(config)#no ip route 172.16.50.0 255.255.255.0 172.16.40.2
2501B(config)#router rip
2501B(config-router)#network 172.16.0.0
2501B(config-router)#^Z
```

Em seguida, utiliza-se o comando *router rip* para entrar no modo de configuração de roteamento (*config-router*). O comando *network* informa ao router qual rede a ser propagada (172.16.0.0, no caso). Note que as sub-redes a serem anunciadas não são informadas, apenas a rede em si (*classful*). O protocolo RIP identificará as sub-redes existentes através das máscaras configuradas nas interfaces do router em questão, porém, lembre-se que RIP é um protocolo *classful*, não propagando, portanto, informações de máscara para a rede.

***Nota**: Observe que o comando* Ctrl+Z *(^Z) foi utilizado ao final do processo de configuração para retornar diretamente ao modo privilegiado (#).*

O processo de configuração RIP não se altera para os outros routers, com exceção das rotas estáticas que devem ser deletadas. **Como RIP é um protocolo *classful*,** a única rede a ser informada será a 172.16.0.0.

```
2501B#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - [output cut]
Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
R       172.16.50.0 [120/1] via 172.16.40.2, 00:00:26, Serial1
C       172.16.40.0 is directly connected, Serial1
C       172.16.30.0 is directly connected, Ethernet0
C       172.16.20.0 is directly connected, Serial0
R       172.16.10.0 [120/1] via 172.16.20.1, 00:00:04, Serial0
2501B#
```

120 = AD do RIP
1 = número de saltos até a rede em questão

Note na saída do comando *sh ip route* (na figura anterior) que agora temos duas rotas (em destaque) adicionadas automaticamente à tabela de roteamento pelo protocolo RIP (naturalmente isso apenas funciona se os outros routers também já estiverem configurados com o protocolo).

7.3.3.2.7 Limitando a Propagação do RIP

Você pode não desejar que sua rede RIP seja anunciada por toda a sua LAN ou WAN. Por exemplo, não há vantagens em anunciar sua rede RIP para a Internet. Existem alguns mecanismos que evitam que indesejadas atualizações RIP se propaguem por toda a sua LAN ou WAN. O modo mais fácil de fazer isso é através do comando *passive-interface*. Esse comando evita que uma atualização RIP seja propagada por uma determinada interface, porém, essa mesma interface continua a receber atualizações RIP (torna-se passiva!). Eis um exemplo de como utilizar o comando:

```
Router#config t
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#passive-interface serial 0
```

O comando anterior evita que atualizações geradas pelo RIP sejam propagadas pela interface *serial 0*, contudo, esta mesma interface ainda pode receber atualizações RIP.

7.3.3.2.8 RIP e Updates Inteligentes

A partir da versão 12.0(1)T do IOS, o protocolo RIP (ambas as versões) pode ser configurado para operar usando *triggered-updates* através do comando *ip rip triggered* (veja exemplo a seguir). O objetivo dessa "extensão" é solucionar dois sérios problemas causados pelo uso do protocolo RIP quando usado em links seriais ponto a ponto:

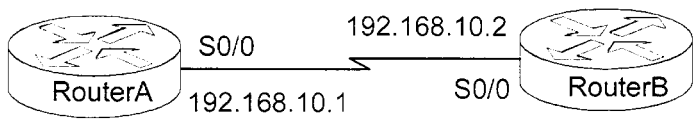
- Em caso de conexões discadas (como ISDN), os updates periódicos (que ocorrem em intervalos de 30s) podem impedir que a conexão seja desfeita;
- Mesmo em conexões WAN dedicadas, a sobrecarga ocasionada pelos updates periódicos podem comprometer a transmissão dos dados, especialmente em links de menor capacidade.

O uso do comando *ip rip triggered* faz com que os updates para links seriais ponto a ponto apenas sejam enviados quando um dos quatro eventos listados a seguir ocorrerem:

- O Router recebe uma requisição de update, o que faz com que sua tabela seja enviada;

- A informação recebida por outra interface modifica a base de dados de roteamento, resultando na propagação apenas das últimas mudanças ocorridas;
- A interface muda seu status para *Up* ou para *Down*, o que faz com que apenas parte da tabela de roteamento seja propagada;
- O router é inicializado, o que resulta na propagação de sua completa base de dados de roteamento.

Vamos supor a rede a seguir:



Eis como o comando *ip rip triggered* poderia ser configurado em ambos os routers:

```
RouterA(config)#interface Serial0/0
RouterA(config-if)#ip address 192.168.10.1 255.255.255.0
RouterA(config-if)#ip rip triggered
RouterA(config-if)#router rip
RouterA(config-router)#network 192.168.10.0

RouterB(config)#interface Serial0/0
RouterB(config-if)#ip address 192.168.10.2 255.255.255.0
RouterB(config-if)#ip rip triggered
RouterB(config-if)#router rip
RouterB(config-router)#network 192.168.10.0
```

Note que o comando é aplicado na interface serial. Este comando **apenas** funciona em interfaces seriais ponto a ponto, e a interface serial configurada com este comando deixa de enviar os updates periódicos do protocolo.

***Observação**: Dificilmente esse último comando (ip rip triggered) será cobrado no exame. Não há uma garantia, entretanto.*

7.3.3.2.9 RIP Versão 2 (RIPv2)

O protocolo RIP possui duas versões. A versão que acabamos de analisar é a versão 1 do protocolo, bastante limitada, como vimos. Existe a versão 2, que corrige algumas limitações da primeira versão. Vamos falar rapidamente dela.

RIPv2 não é muito diferente do RIPv1, no sentido de que continua sendo um protocolo essencialmente *distance vector* e segue usando a contagem de saltos como métrica. O RIPv2 também envia sua tabela

completa de roteamento periodicamente e, finalmente, os timers vistos para RIPv1 valem também para o RIPv2. O valor da distância administrativa também permanece inalterado (120). Então, o que muda?

Apesar das semelhanças, a versão 2 do protocolo possui algumas diferenças, que aumentam sua escalabilidade e o tornam mais adequado para redes de grande porte.

Olhando a tabela a seguir, poderemos notar as diferenças que fazem do RIPv2 um protocolo mais robusto que a versão 1. Basicamente, RIPv2 suporta VLSM, ou seja, ele propaga as informações de máscara de rede em suas atualizações.

	RIPv1	RIPv2
Tipo	Distance-vector	Distance-vector
Métrica	Contagem de saltos (Max. 15)	Contagem de saltos (Max. 15)
Anúncios	Classful	Classless
VLSM	NÃO	SIM
Redes descontíguas	NÃO	SIM
Autenticação	NÃO	SIM
Propagação	Periódica (broadcast)	Periódica (Multicast 224.0.0.9)
CIDR	NÃO	SIM

Para configurar RIPv2 em um router Cisco:

```
RouterA#config t
RouterA(config)#router rip
RouterA(config-router)#version 2
RouterA(config-router)#network 10.0.0.0
```

Pronto! Como você pode ver, nada muito diferente da versão 1. É interessante ressaltar que a versão 2 do protocolo RIP é inteiramente compatível com a versão 1.

7.3.3.2.10 Verificação das Configurações RIP

Os seguintes comandos podem ser usados para verificação das configurações RIP:

- **sh running**: Apresenta toda a configuração presente no router, incluindo as configurações do protocolo RIP;
- **sh ip route**: Apresenta a tabela de roteamento completa;
- **sh ip route rip**: Apresenta apenas as rotas informadas pelo protocolo RIP;
- **sh ip rip database**: Apresenta o conteúdo da base de dados privativa do protocolo RIP. Disponível apenas quando o modo *triggered* encontra-se habilitado (esse comando apenas é aceito do IOS versão 12.0(1)T em diante e não deve ser cobrado no exame CCNA).

7.3.3.2.11 Características do Protocolo IGRP

- Proprietário Cisco (apenas routers Cisco podem utilizar IGRP);
- Contagem máxima de saltos = 255, com default em 100 (útil em redes de grande porte);
- Utiliza largura de banda (*bandwidth*) e atraso da linha (*delay of the line*) como métricas default (*composite metric*);
- Permite que outras métricas como *reliability, load* e *maximum transmit unit* (MTU) sejam utilizadas.

7.3.3.2.12 Temporizadores do Protocolo (IGRP Timers)

O protocolo IGRP foi criado pela Cisco para superar as limitações impostas pelo RIP, como o limite de 15 para a contagem de hops. Apenas routers Cisco podem utilizar IGRP para roteamento, pois esse protocolo foi desenvolvido pela Cisco.

O IGRP utiliza quatro diferentes tipos de timers para regular sua performance:

- **Route Update Timer**: Estabelece um intervalo (default = 90 segundos) entre as atualizações regulares, nas quais os routers enviam uma cópia completa de suas tabelas de roteamento para todos os routers vizinhos;
- **Route Invalid Timer**: Determina a quantidade de tempo que deve correr (default = 3 x *Update Timer*) antes de um router determinar que uma rota tornou-se inválida;
- **Holddown Timers**: Especifica o período de *holddown* (default = 3 x *Update Timer* + 10 segundos);
- **Route Flush Timer**: Estabelece o tempo (default = 7 x *Update Timer*) entre uma rota tornar-se inválida e sua remoção da tabela de roteamento. Antes de eliminar uma rota de sua tabela de roteamento, o router avisa aos routers vizinhos que determinada rota encontra-se inativa. O valor do *Invalid Timer* deve ser sempre menor que o do *Flush Timer*. Isso assegura ao router tempo suficiente para atualizar os routers vizinhos sobre a rota inválida antes que sua tabela de roteamento seja atualizada.

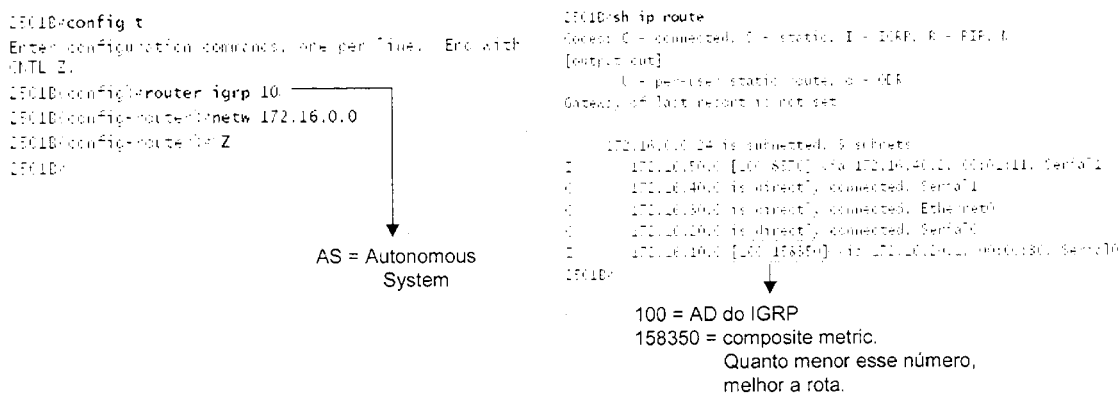
***Nota**: Os valores padrão dos timers anteriormente descritos devem ser memorizados para o exame CCNA. Um modo mais fácil de memorizá-los é:*

RUT = 90 | RIT = RUT x 3 | HDT = RUT x 3 + 10 | RFT = RUT x 7

7.3.3.2.13 Configurando IGRP

A configuração do IGRP em um router é bastante semelhante à do RIP, com uma importante diferença: você precisa informar o número do sistema autônomo (AS = *Autonomous System*). Todos os routers dentro de um mesmo sistema autônomo devem utilizar o mesmo número AS ou eles não se comunicarão com informações de roteamento.

Na ilustração a seguir, configuramos IGRP no router 2501B de nossa rede sugerida. Em seguida, utilizamos o comando *router igrp 10* para entrar no modo de configuração de roteamento (*config-router*), onde 10 é o número do sistema autônomo. O comando *network*, como no RIP, informa ao router qual rede a ser propagada (172.16.0.0, no caso).



O processo de configuração IGRP não se altera para os outros routers.

***Nota**: É de extrema importância para o exame CCNA que o candidato saiba interpretar linhas da saída do comando sh ip route. No exemplo anterior, a letra "I" indica que essa rota foi "aprendida" pelo protocolo IGRP, e os valores entre colchetes indicam a distância administrativa desse protocolo e a métrica da rota em questão.*

7.3.3.2.14 Balanceando Carga (Load Balancing) com IGRP

IGRP pode **balancear a carga entre quatro links desiguais**. Redes RIP devem ter a mesma contagem de saltos para balancear carga. Já o IGRP utiliza a largura de banda (*bandwidth*) para determinar como balancear a carga.

No balanceamento de carga entre links desiguais, o comando *variance* controla o balanceamento entre a melhor e a pior métrica aceitável. Outros dois comandos são utilizados para ajudar no controle da distribuição de tráfego entre rotas IGRP que dividem a carga:

traffic share balanced e *traffic share min*

```
Router(config)#router igrp 100
Router(config-router)#variance ?
 <1-128> Metric variance multiplier

Router(config-router)#traffic-share ?
  balanced  Share inversely proportional to metric
  min       All traffic shared among min metric paths
```

A saída anterior ilustra o comando *variance*, que é o multiplicador de métrica. A saída do comando *traffic share* nos apresenta duas opções: *balanced* e *min*. A opção *balanced* informa o protocolo IGRP para compartilhar a carga de modo inversamente proporcional às métricas, enquanto a opção *min* informa o protocolo IGRP para utilizar no processo de balanceamento apenas as rotas de menor custo.

7.3.3.2.15 Verificação das Configurações IGRP

O primeiro comando a ser considerado para verificação das configurações seria o *sh ip route*. Como ele já foi ilustrado nas páginas anteriores, não falaremos dele aqui.

Outro comando bastante útil é o *sh protocols*, pois **apresenta os endereços de rede configurados em cada interface.**

O comando *sh ip protocols* apresenta em sua saída os protocolos de roteamento configurados em um router. O comando *sh ip proto* também apresenta os valores dos timers utilizados pelos protocolos roteadores configurados. Outras informações incluídas na saída do comando *sh ip proto* são: AS, redes sendo propagadas, gateways e ADs (Distâncias Administrativas).

O comando *debug ip rip* envia as atualizações propagadas e recebidas pelo router para a console (se você estiver efetuando uma sessão Telnet, você deverá digitar o comando *terminal monitor* para ser capaz de receber a saída dos comandos de *debug*). Essa é uma grande ferramenta para identificação de problemas. Para desligar o modo *debug*, use o comando *undebug all* ou *no debug all*. A abreviação *un all* também pode ser usada.

Com o comando *debug ip igrp* você tem duas opções: *events* e *transactions*.

O comando *debug ip igrp events* apresenta um resumo das informações de roteamento IGRP que estão sendo propagadas pela rede. Dados como origem e destino de cada atualização, assim como o número de routers em cada uma são apresentadas. Informações sobre rotas individuais **não** são apresentadas por esse comando.

Finalmente, o comando *debug ip igrp transactions* apresenta requisições de atualizações feitas por routers vizinhos e as atualizações enviadas pelo seu router para esses routers.

Utilize *un all* para desativar o modo *debug*.

Nota: *É muito importante saber como verificar as configurações de um router, as informações trazidas por cada comando e o que os comandos debug apresentam ao usuário.*

7.3.3.3 Protocolos Baseados no Algoritmo Link State – O Protocolo OSPF

A sigla OSPF, em inglês, é acrônimo para *Open Shortest Path First*. Porém, a tradução não significa "Abra o Caminho Mais Curto Antes"! Muitas publicações erroneamente o traduzem assim, mas está errado. O *Open* que precede *Shortest Path First* significa que este é um protocolo aberto, isto é, de domínio público - padronizado pelo IETF[1], ou seja, é um protocolo independente de fabricantes e não-proprietário (assim como o RIP). Isso é particularmente interessante se você está considerando um protocolo para redes heterogêneas. Os protocolos IGRP e EIGRP (*Enhanced IGRP*), por exemplo, são proprietários Cisco, ou seja, apenas dispositivos Cisco podem compreendê-los.

As especificações do protocolo OSPF são definidas pela RFC[2] 1247 e podem ser consultadas acessando-se as páginas web <http://www.ietf.org/rfc.html> ou <http://www.rfc.net>.

O protocolo OSPF possui duas características básicas. A primeira é que ele é de acesso público (*open*). A segunda é que ele utiliza-se do algoritmo SPF, também conhecido como algoritmo de *Dijkstra*. A principal vantagem disso é que os cálculos realizados pelo algoritmo levam em conta a largura de banda na procura pela melhor rota, diferentemente dos protocolos *distance vector*.

Como vimos anteriormente, os protocolos baseados em algoritmos do tipo vetor de distância possuem muitas limitações que podem vir a ser um problema quando implementados em redes de médio e grande porte. Um dos problemas ilustrados é relacionado ao modo como as atualizações são percebidas e propagadas pela rede. Ambos os protocolos RIP e IGRP fazem isso através do *broadcast* da tabela completa de roteamento em intervalos de tempo predeterminados (30 segundos para o RIP e 90 segundos para o IGRP). Isso significa que, mesmo que não ocorram mudanças na rede,

[1] *Internet Engineering Task Force.*

[2] *Request For Comment* <www.rfc.net>.

após 30 segundos (ou 90, no caso do IGRP) a tabela completa de roteamento será enviada via *broadcast* para todas as interfaces ativas. Isso é um desastre em uma rede de grande porte. Imagine uma tabela de roteamento gigantesca, com mais de 800 entradas, por exemplo, sendo propagada a cada 30 segundos por todas as portas ativas de um router e, assim, sucessivamente, por todos os routers da rede. A quantidade de tráfego "secundário" (tráfego que não contempla dados de usuários) nessa rede seria ridiculamente grande, inviabilizando a sua operação - tanto financeira quanto tecnicamente.

Com o protocolo OSPF, a coisa muda um pouco de figura. Esse protocolo já foi criado tendo-se em vista redes de grande porte. Ele não trabalha com propagação via *broadcast*, mas via *multicast*, ou seja, apenas routers que estejam rodando esse protocolo receberão as atualizações necessárias. Uma interface que não possua um router rodando OSPF conectada a ela não receberá as mensagens de atualização via *multicast*. Outra grande vantagem: atualizações incrementais, ou seja, quando houver uma alteração na rede (por exemplo, uma nova rede foi detectada), apenas a informação adicional será propagada via *multicast* para os routers vizinhos e não mais a tabela completa, como faziam o RIP e o IGRP. Isso significa maior agilidade e uma grande economia de largura de banda. Existem muitas outras diferenças, que veremos mais adiante.

O protocolo OSPF permite a hierarquização de uma rede através da sua divisão em diversas áreas. O tráfego entre essas áreas é realizado pelo roteador de borda de área (*Area Border Router* - ABR). O exame CCNA foca apenas em OSPF *single area*, portanto não vamos nos aprofundar no comportamento interárea do OSPF. Mesmo assim, quando falamos de áreas e OSPF, é importante ter alguns conceitos bem sedimentados:

- A área 0 (zero) **sempre** deve existir em redes com mais de uma área. Essa área, em uma rede OSPF, é conhecida como *backbone area*;
- Todas as outras áreas devem se conectar à área 0. Essa regra deve **sempre** ser obedecida, ou a rede OSPF não funcionará a contento;
- Para interconectar uma área que não está diretamente conectada à área 0, deve-se usar o artifício dos "virtual-links", que nada mais são do que túneis, para "enganar" o protocolo e fazê-lo pensar que a área em questão encontra-se diretamente conectada à área 0. Mesmo isso sendo possível, é uma solução pobre e deve ser usada apenas como uma medida temporária para remediar o problema, nunca como uma solução definitiva;

- Como os routers pertencentes à área 0 (*backbone*) normalmente terão um processamento mais elevado, é sensato que os routers escolhidos para fazer parte dessa área tenham porte e capacidade adequados.

A figura 7.10 ilustra um exemplo de uma rede OSPF.

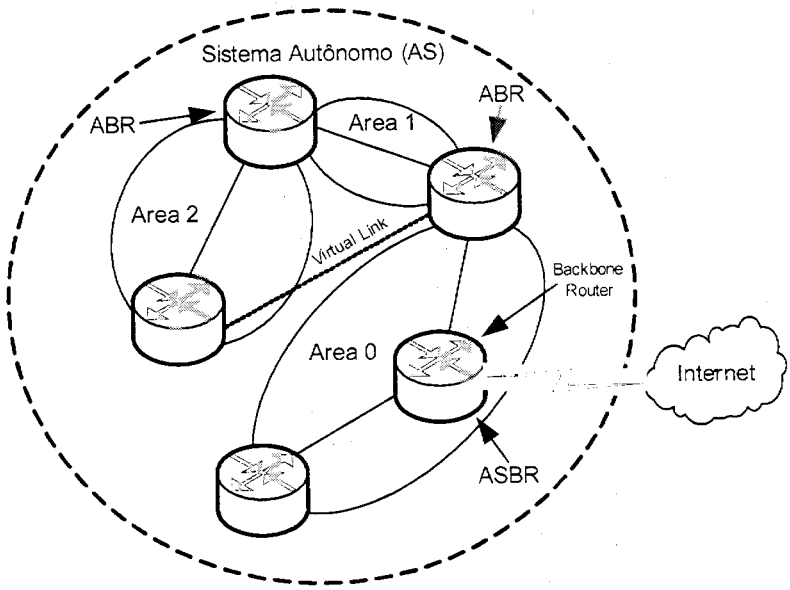


Figura 7.10: Ilustração de uma rede OSPF.

A tabela a seguir realiza uma rápida comparação entre os protocolos RIP (v1 e v2), IGRP e OSPF:

Característica	RIP	RIPv2	IGRP	OSPF
Tipo de protocolo	Distance Vector	Distance Vector	Distance Vector	Link State
Suporte à VLSM (classless routing)	NÃO	SIM	NÃO	SIM
Auto summarization	SIM	SIM	SIM	NÃO
Manual summarization	NÃO	SIM	NÃO	SIM
Suporte a redes descontíguas	NÃO	SIM	NÃO	SIM
Tipo de propagação	Broadcast	Multicast	Broadcast	Multicast
Métrica utilizada	Saltos	Saltos	Composta[3]	Largura de banda

[3] IGRP usa uma composição de métricas, entre elas largura de banda, delay (essa duas sendo as defaults), load, reliability, entre outras.

Característica	RIP	RIPv2	IGRP	OSPF
Limite de saltos (hop count)	15	15	255	N/A
Convergência	Lenta	Lenta	Lenta	Rápida
Suporte à autenticação	NÃO	SIM	NÃO	SIM
Suporte à hierarquização	NÃO	NÃO	NÃO	SIM
Tipo de atualização	Updates periódicos	Updates periódicos	Updates periódicos	"Event Triggered"
Algoritmo adotado	Bellman-Ford	Bellman-Ford	Proprietário (Cisco)	SPF (Dijkstra)

O protocolo OSPF possui ainda muitas outras características, não listadas na tabela anterior, que contribuem para que ele seja um protocolo rápido, confiável e robusto, empregado em milhares de redes, globalmente.

A seguir, uma tabela com a terminologia adotada pelo protocolo OSPF.

Adjacência	Uma adjacência é formada quando dois routers vizinhos (*neighbors*) acabaram o processo de troca de informações e possuem a mesma tabela topológica. As bases de dados encontram-se sincronizadas e ambos vêem as mesmas redes.
Área	Grupo de routers que partilham do mesmo ID de área. Cada router na mesma área possui uma cópia idêntica da tabela topológica. A área é definida por interface, no momento da configuração do router.
Sistema Autônomo (AS)	Grupo de roteadores que partilham as mesmas características de roteamento, normalmente, dentro de uma mesma organização.
Backup Designated Router (BDR)	O backup do *Designated Router* (DR). Caso o DR falhe, o BDR assumirá suas funções imediatamente.
Custo	A métrica usada pelo protocolo OSPF. A Cisco adota o custo como sendo o inverso da largura de banda disponível, assim, quanto menor a largura de banda, maior o custo e vice-versa.
Database Descriptor	Também conhecido por DBDs ou DDPs (*Database Descriptor Packets*). São datagramas trocados pelos *neighbors* durante o *exchange state*. Os DDPs contém os LSAs (*Link State Advertisement*).

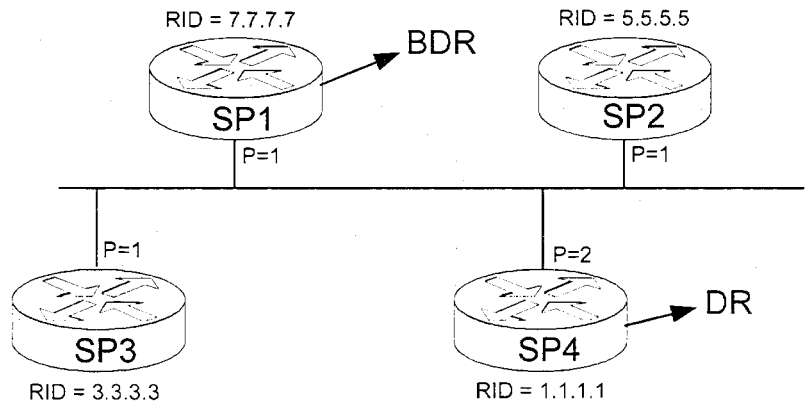
Designated Router (DR)	Router responsável por estabelecer as adjacências com todos os *neighbors* em uma rede multiacesso, como Ethernet ou Frame-Relay. O DR garante que todos os routers no link multiacesso tenham a mesma tabela topológica (multicast 224.0.0.6).
Exchange State	Método através do qual dois routers vizinhos descobrem o mapa da rede. Quando dois routers tornam-se adjacentes, eles devem primeiro trocar DDPs para garantir que possuem a mesma tabela topológica.
Full State	Estado no qual os routers adjacentes devem possuir uma cópia exata da tabela topológica.
Exstart	Estado no qual os routers vizinhos determinam o número de seqüência dos DDPs e estabelecem uma relação mestre-escravo.
Init	Estado no qual um pacote *hello* foi enviado pelo router, que está no aguardo de uma resposta para estabelecer uma comunicação de duas vias.
Internal Router	Um router que possui todas as suas interfaces na mesma área.
Link State Advertisement (LSA)	Um datagrama contendo as descrições dos links e seu estado de um determinado router. Existem diferentes tipos de LSA para descrever diferentes tipos de links.
Link State Database	Também conhecido como mapa topológico (*topology map*). Trata-se de um mapa de todos os routers, seus links e seu estado. Também contempla um mapa de todas as redes e todos os caminhos para cada uma delas.
Link State Request (LSR)	Quando um router recebe um DDP completo, com o LSA, ele compara o LSA contra a base de dados topológica. Se nela não houver informação do LSA ou se a informação for mais antiga que o DDP, o router solicitará informações adicionais.
Link State Update (LSU)	Atualização enviada em resposta ao LSR. Trata-se do LSA que foi solicitado.
Neighbor Table	Uma tabela montada a partir do *hello* recebido do router vizinho. O pacote *hello* transporta consigo uma lista dos vizinhos (*neighbors*).
Priority	Forma de tornar um router um DR ou BDR, manualmente.

SPF tree	Uma "árvore" da rede topológica formada após o algoritmo SPF ter sido rodado. O algoritmo automaticamente elimina da base de dados os caminhos alternativos e cria um mapa com os caminhos mais curtos – livre de loops – para todas as redes. O router fica na raiz da rede, já que a mesma é percebida segundo a sua perspectiva.
Topology table	O mesmo que *link state database*. Essa tabela contém todos os links para a rede.
Broadcast Multi-Access	Redes como Ethernet permitem que múltiplos dispositivos sejam conectados na mesma rede, provendo também a possibilidade de pacotes broadcast (um pacote que atinge muitos dispositivos nessa rede). OSPF rodando em redes broadcast precisam ter routers DR e BDR eleitos.
Non-Broadcast Multi-access	Redes como Frame-Relay, ATM e X25 permitem multi-access, porém, não são redes broadcast. Logo, esses tipos de rede podem necessitar de configurações especiais para que OSPF funcione a contento. Aqui também existe a necessidade de eleição de um BR e BDR.

Como já foi mencionado, em uma rede OSPF a área 0 (*backbone area*) deve existir, e todas as outras áreas devem conectar-se diretamente à área 0 através do *Area Border Router* (ABR). Basicamente, o ABR é um router que possui pelo menos uma interface na área 0 e as demais em quaisquer outras áreas. Ele é o ponto de conexão entre as outras áreas e o *backbone* (área 0).

7.3.3.3.1 Designated Router/Backup Designated Router

O protocolo OSPF, quando operando em redes multiacesso (como redes Ethernet), utiliza o artifício de eleger um router como DR e outro como Backup DR (BDR). Basicamente, a eleição do router DR e BDR usa os datagramas *hello* enviados por cada um dos routers presentes na rede multiacesso para examinar o valor da prioridade de cada router. O router com a maior prioridade é eleito o DR para seu segmento e o com a segunda maior prioridade, o BDR. Se os valores de prioridade nos routers, no entanto, forem os defaults (1) ou iguais, o Router ID (RID) de cada um é usado para o desempate. Lembrando que o RID é, basicamente, o maior valor IP configurado no router ou o IP de uma interface *loopback* (virtual) - se cabível. A figura a seguir ilustra o processo.



Observe que todos os routers, com exceção do *SP4*, possuem prioridade configurada de 1 (default). *SP4*, por sua vez, possui prioridade configurada para 2, sendo, portanto, eleito o DR para seu segmento (maior prioridade). Os outros três routers possuem o mesmo valor de prioridade, porém, o RID de *SP1* é maior que o dos routers *SP2* e *SP3*; logo, *SP1* é eleito BDR (observe que se o valor de prioridade de *SP4* fosse também igual a 1, *SP1* seria o DR e *SP2*, o BDR).

Caso seja necessário excluir um router do processo de seleção de DR/BDR, basta configurar sua prioridade para "0". Seu estado na rede OSPF multiacesso passaria a ser "DROTHER", neste caso.

A configuração de prioridades em um router OSPF deve ser feito por interface, já que um mesmo router pode encontrar-se conectado a mais de um segmento multiacesso (um router com duas interfaces Ethernet, por exemplo). O comando para configurar a prioridade OSPF em uma interface é ilustrado a seguir.

```
MG#conf t
MG(config)#int f0/0
MG(config-if)#ip ospf priority 2
```

Um ponto adicional que vale ser mencionado: Quando um router é inserido em um ambiente multiacesso (vamos supor que o router *SP4* tenha sido o último a ser incluído na rede) e já existe um DR para esse segmento (no caso, como o router *SP4* não "existia", *SP1* era o DR), o router *SP4* **não será** eleito DR, ao menos até que uma mudança na rede ocorra. Isso ajuda a manter a convergência da rede OSPF menos sujeita a interferências externas.

7.3.3.3.2 Formação da Árvore SPF (SPF Tree)

Dentro de uma área, cada router calcula o melhor (mais curto) caminho para todas as redes pertencentes à mesma área. Esse cálculo é baseado nas informações coletadas na base de dados topológica e um algoritmo chamado SPF (*Shortest Path First*), também conhecido como *Dijkstra*

(nome dado em homenagem ao matemático que criou esse algoritmo). Imagine cada router em uma área construindo uma árvore - como uma árvore genealógica - onde o router é a raiz e todas as outras redes são arranjadas nos galhos remanescentes. Essa seria a árvore SPF (SPF tree) usada pelo router para inserção de rotas na tabela de roteamento.

É importante frisar que essa árvore contém apenas redes contidas na mesma área na qual o router se encontra. Se um router pertence a múltiplas áreas, então múltiplas árvores serão formadas, uma para cada área. Um dos critérios adotados durante o processo de seleção do algoritmo SPF é o custo de cada caminho em potencial para uma dada rede. Mas esse cálculo não se aplica para rotas de outras áreas.

A métrica usada pelo protocolo OSPF é o custo. Um custo é associado a cada interface de saída incluída em uma árvore SPF. O custo total de um dado caminho é a soma dos custos das interfaces de saída, conforme o caminho evolui. Para cálculo do custo por interface, a Cisco adota a fórmula 10^8 / *largura de banda*, sendo que a largura de banda é o valor configurado no parâmetro *bandwidth* para a interface. Utilizando essa lógica, uma interface *FastEthernet* operando a 100Mbps teria um custo OSPF de 1, enquanto uma interface Ethernet operando a 10Mbps teria um custo de 10 (uma interface configurada com *bandwidth* de 64Kbps teria um custo de 1563, apenas por curiosidade). O valor do custo pode ser sobrescrito, entretanto, usando-se o comando *ip ospf cost*. O custo pode ser manipulado alterando-se o valor para algo entre 1 e 65.535.

Nota: *Como já mencionado, OSPF usa multicast para enviar atualizações para a rede. Os endereços utilizados são:*
224.0.0.5*: Endereço multicast para todos os routers OSPF (AllOSPFRouters)*
224.0.0.6*: Endereço multicast usado para todos os OSPF Designated Routers*

7.3.3.3.3 Configurando OSPF em uma Rede Cisco

Lembramos mais uma vez que ao exame CCNA apenas importa o conhecimento de redes OSPF *single area*, ou seja, não precisamos nos preocupar com OSPF *multi-area*.

7.3.3.3.4 Configuração do Protocolo OSPF

Para ativar o protocolo OSPF em um router, eis o comando:

```
Marco(config)#router ospf ?
  <1-65535>
```

O valor compreendido entre 1 e 65.535 identifica o processo OSPF que será ativado no router em questão. O interessante aqui é notar que o valor é de processo, e nada tem a ver com sistema autônomo (como é o caso do IGRP). Routers diferentes podem possuir processos OSPF diferentes e mesmo assim formar adjacências, ou seja, o valor que for escolhido aqui não faz diferença se você não precisar de mais de um processo OSPF ativado em seu router. Isso mesmo! Você pode ter várias instâncias do serviço (processo) OSPF ativado em um mesmo router! Para quê? Existem algumas razões para isso, mas não vou entrar em detalhes, já que isso nada tem a ver com o exame CCNA.

Seguindo em nosso exercício de configuração, vamos à próxima etapa:

```
Marco(config)#router ospf 64
Marco(config-router)#network 192.168.10.0 0.0.0.255 area ?
 <0-4294967295>   OSPF area ID as a decimal value
 A.B.C.D          OSPF area ID in IP address format

Marco(config-router)#network 192.168.10.0 0.0.0.255 area 0
```

Mais uma vez, o ID do processo é completamente irrelevante. Pode ser o mesmo em todos os routers da rede ou diferente em cada um deles, não faz a menor diferença. Os parâmetros do comando *network* são o valor da rede (192.168.10.0), seguido do *wildcard mask* (0.0.0.255) e, finalmente, da identificação da área a qual a rede em questão pertence (no caso, área 0). É importante frisar que a combinação do endereço de rede e do *wildcard mask* identifica a interface na qual o processo OSPF estará operando e também será incluído nos updates LSA, ou seja, o protocolo OSPF, diferentemente dos protocolos já vistos até o momento (RIP e IGRP), é ativado por interface e não no router todo. Basicamente, o protocolo irá procurar no router por interfaces pertencentes à rede 192.168.10.0 e colocará todas as que encontrar dentro da área 0, conforme configurado.

Outro ponto que merece destaque: o valor da área pode ser escrito tanto em formato numérico simples (1, 2, 3, 0 etc.) quanto em formato IP (0.0.0.0, para área 0, por exemplo).

7.3.3.3.5 Verificando a Configuração OSPF

Existem diversas maneiras de verificar se o protocolo OSPF foi configurado e está operando corretamente. De todas elas, as variações do comando *show* encabeçam a lista, com certeza.

```
Marco#show ip route

Gateway of last resort is not set
O    192.168.30.0/24 [110/65] via 192.168.10.1, 00:01:02,
Serial0/0
C   192.168.10.0/24 is directly connected, Serial0/0
O   192.168.20.0/24 [110/128] via 192.168.10.1, 00:01:02,
Serial0/0
O   192.168.40.0/24 [110/138] via 192.168.10.1, 00:01:02,
Serial0/0
```

Como podemos observar, essa saída mostra três redes identificadas pelo protocolo OSPF (isso pode ser evidenciado tanto pelo "O" que precede as rotas quanto pela distância administrativa de 110 de cada uma delas).

```
Marco#show ip ospf
Routing Process "ospf 64" with ID 192.168.10.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 3d01h ago
        SPF algorithm executed 2 times
```

```
    Area ranges are
    Number of LSA 1. Checksum Sum 0x00E570
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Note o valor do OSPF router ID (RID) de 192.168.10.1. O protocolo OSPF sempre usa o maior IP configurado no router ou o IP da interface *loopback*, se uma estiver configurada no router (o valor mais alto das *loopbacks*, se mais de uma existir, claro).

```
Marco#sh ip ospf data

            OSPF Router with ID (192.168.10.1) (Process ID 64)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link Count
192.168.10.1    192.168.10.1    1649        0x80000085 0x00E570 2
```

A saída desse comando mostra o link ID (lembre-se que uma interface é também um link, quando falamos de OSPF), o RID do router e o processo OSPF ativo nele.

```
Marco#sh ip ospf int
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.10.1/24, Area 0
  Process ID 64, Router ID 192.168.10.1, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.10.1, Interface address
192.168.10.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

O comando *sh ip ospf interface*, ilustrado anteriormente, apresenta todas as informações OSPF relacionadas às interfaces. As informações apresentadas incluem:

- Endereço IP da interface;
- Área OSPF à qual ela pertence;
- ID do processo OSPF;
- Router ID (RID);
- Tipo de rede (*point-to-point, point-to-multipoint*);
- Custo;
- Prioridade;
- Informações sobre DR/BDR, se aplicável;
- Valores dos timers HELLO e DEAD;
- Informações sobre adjacências.

Outros comandos úteis para verificação OSPF:

- **show ip ospf neighbor**: Esse é um comando particularmente interessante, já que resume informações do router OSPF vizinho, assim como o status da adjacência. Se existir um BR ou um BDR, essa informação também será apresentada;
- **show ip protocols**: Esse comando é útil independentemente de qual protocolo você esteja utilizando: OSPF, RIP, IGRP, BGP etc. Ele provê um resumo das operações e status dos protocolos ativos no router.

7.3.3.3.6 Uso de Interfaces Loopback em Redes OSPF

Como já foi mencionado, o router ID de um router rodando o protocolo OSPF será o maior IP configurado em uma interface física ou o IP da interface *loopback*, se esta encontrar-se configurada. A *loopback* é uma interface virtual, existente apenas no software do router e, por ser virtual, ela nunca está *down*. O objetivo de configurar uma interface *loopback* quando se está usando OSPF é exatamente forçar o router a adotar como RID o IP dessa interface e, como ela nunca vai estar como *down*, o router nunca irá trocar seu router ID. Isso não seria verdade se você não configurasse uma *loopback* e seu router adotasse o endereço da interface serial, por exemplo, como RID (supondo que ele fosse o IP mais alto configurado no router). Imagine se a interface em questão perdesse a conectividade, por algum motivo. Seu router perderia momentaneamente o RID e adotaria o valor da interface com endereço IP imediatamente inferior ao da serial. Isso pode causar problemas de inconsistência na rede.

Para configurar uma interface ***loopback***:

```
Marco(config)#interface loopback0
Marco(config-if)#ip address 1.1.1.1 255.255.255.255
```

Portanto, a partir deste momento, o RID deste router passa a ser 1.1.1.1 (endereço da interface *loopback0*):

```
Marco#sh ip ospf data

            OSPF Router with ID (1.1.1.1) (Process ID 64)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link Count
192.168.10.1    192.168.10.1    1649        0x80000085 0x00E570 2
```

***Nota**: Observe que, mesmo que o endereço IP da interface FastEthernet seja numericamente maior que o da loopback0, o da loopback é o usado para definição do RID. Sempre o endereço IP de uma interface loopback será preferido ao de qualquer outra interface, independentemente do valor delas.*

7.3.3.3.7 Identificando Problemas em Redes OSPF

Como qualquer outro protocolo, OSPF pode causar dor de cabeça se não for bem implementado. Se você notar problemas após configurar seus routers, observe se:

- Os timers do OSPF (*hello* e *dead*) estão consistentes através da rede (os defaults são 10 e 40, respectivamente);

***Nota**: Lembre-se dos valores desses timers: Hello Timer: 10 segundos / Hold Timer: 40 segundos (por default).*

- Existem outros protocolos configurados? Lembre-se de que IGRP, por exemplo, tem uma distância administrativa (AD) de 100, enquanto a do OSPF é 110, ou seja, rotas descobertas via IGRP serão preferidas sempre. Cheque também se existem rotas estáticas configuradas, já que estas sempre serão as preferidas por default;
- Existe consistência nas áreas configuradas;
- Os parâmetros do comando *network* foram corretamente inseridos, lembrando sempre que devemos usar o *wildcard mask*, e não o formato padrão de máscaras, com OSPF.

7.3.3.4 Protocolos Híbridos – O Protocolo EIGRP da Cisco

O EIGRP é um protocolo do tipo *classless*, com algumas características tanto de *distance vector* como de *link state* (por isso o termo híbrido). O

EIGRP, como o próprio nome sugere, é uma versão tonificada do protocolo que já estudamos, o IGRP. Assim como o IGRP, o EIGRP usa o conceito de sistema autônomo para descrever um grupo de routers que rodam um mesmo tipo de protocolo de roteamento, compartilhando informações de roteamento. Entretanto, diferentemente de seu "irmão", o EIGRP é capaz de lidar com máscaras de rede, tornando possível a ele a adoção de práticas como VLSM, CIDR e sumarização de rotas. O EIGRP também oferece suporte à autenticação, aumentando a segurança da rede.

O EIGRP é classificado como híbrido, pois mantém tanto qualidades de um protocolo *link state*, quanto de um *distance vector*. O protocolo, por exemplo, não usa o artifício dos *link state packets* (LSPs), como faz o OSPF, enviando em seu lugar tradicionais atualizações de vetor de distância contendo informações sobre as redes e o custo para alcançá-las, sob a perspectiva do router que está enviando essas informações. No entanto, o EIGRP também possui características de protocolos *link state*, como a sincronização das tabelas entre os routers vizinhos e o envio de atualizações para eles somente quando alguma mudança na rede ocorrer (*update incremental*). Isso tudo faz com que o protocolo EIGRP seja apropriado para uso em redes de grande porte. O EIGRP possui uma limitação de saltos de 224, e não 255 como seu "irmão", o IGRP.

Entre as principais vantagens em se adotar o EIGRP e não outros protocolos, eis algumas:

- Suporta múltiplos protocolos de camada 3 (IP, IPX, *AppleTalk*), enquanto o OSPF suporta apenas IP;
- É um protocolo *classless*, portanto suporta VLSM e CIDR;
- Suporta sumarização e redes não-contíguas;
- É eficiente em sua operação, sendo sua convergência substancialmente mais rápida que a de outros protocolos (inclusive o OSPF);
- Utiliza o algoritmo DUAL (*Diffusion Update Algorithm*), que inibe a formação de loops e é bastante eficiente.

Nota: *A Cisco algumas vezes refere-se ao protocolo EIGRP como distance vector, advanced distance vector ou híbrido.*

7.3.3.4.1 O Processo de Descoberta dos Routers Vizinhos

Antes de um router rodando EIGRP poder trocar informações de roteamento com outro, eles devem tornar-se vizinhos. Existem basicamente três condições para que essa relação ocorra:

- Pacotes *hello* ou ACK são recebidos;
- Ambos os routers encontram-se dentro do mesmo sistema autônomo (AS);
- Ambos possuem os parâmetros usados para cálculo de métricas (K values) idênticos.

Como já vimos com o OSPF, protocolos que se encaixam na classificação de *link state* tendem a usar datagramas *hello* para estabelecer a relação de vizinhança, uma vez que eles normalmente não enviam atualizações periódicas e que existem alguns mecanismos que ajudam os routers vizinhos a identificar quando um novo router foi incluído à rede ou quando um antigo vizinho foi removido ou encontra-se inacessível. Com o EIGRP não é diferente. Para que a relação de vizinhança seja mantida, o router deve seguir recebendo datagramas *hello* de seus vizinhos. Se isso falhar, o protocolo entenderá que o vizinho não se encontra mais acessível.

Routers EIGRP que não pertençam ao mesmo sistema autônomo não trocam informações de roteamento diretamente e não formam relações de vizinhança entre si.

O único caso em que o EIGRP divulga sua tabela de roteamento completa é quando um router identifica um novo router EIGRP vizinho e forma uma adjacência com ele através da troca dos datagramas *hello*. Quando isso ocorre, cada um dos dois routers propaga sua tabela de roteamento completa para o outro. Uma vez que ambos tenham aprendido as rotas de cada vizinho, apenas mudanças na tabela de roteamento são propagadas (updates incrementais). A tabela 7.1 lista alguns termos pertinentes ao universo EIGRP.

Feasible distance (FD)	Esta seria a melhor métrica para uma rede remota, incluindo a métrica até o vizinho que a está propagando. Esta é, na verdade, a rota encontrada na tabela de roteamento, já que ela é considerada o melhor caminho para a rede remota. A métrica de um feasible distance é a métrica reportada pelo router vizinho (conhecida também como "distância reportada" ou reported distance), acrescida da métrica para se chegar até o vizinho que está propagando a rota.
Reported distance ou Advertised distance (AD)	Métrica de uma rede remota, do modo como o router vizinho a enxerga. Trata-se da métrica para a rede remota existente na tabela de roteamento do router vizinho.
Neighbor table	Uma lista de todos os routers vizinhos, incluindo o endereço IP deles, interface de saída, valores dos timers, e tempo que o vizinho em questão encontra-se na tabela.

Topology table	Tabela contendo todos os caminhos propagados pelos routers vizinhos para todas as redes conhecidas. Basicamente é uma lista com todos os successors, feasible successors, feasible distance, advertised distance e a interface de saída. O algoritmo do EIGRP (DUAL) age sobre esta tabela para determinar os successors e os feasible successors para, então, montar a tabela de roteamento.
Successor	Router de próximo ponto que satisfaz a *feasible condition*. Ele é escolhido entre os FSs (*feasible successors*) como tendo a menor métrica para a rede remota.
Feasible successor (FS)	Um router vizinho que reporte uma *advertised distance* (AD) menor que a *feasible distance* (FD) do router torna-se um *feasible successor*.
Feasible condition (FC)	Quando um router vizinho reporta um caminho (AD) com uma métrica menor que a FD do router em questão, a condição FC é alcançada.
Reliable Transport Protocol (RTP)	Requerimento de que todos os datagramas devem ser entregues com garantia e em seqüência.

Tabela 7.1: Principais terminologias EIGRP.

***Nota**: Um feasible successor nada mais é que uma rota alternativa para a mesma rede remota, armazenada na tabela topológica. Já um successor é a rota primária, armazenada em ambas as tabelas topológica e de roteamento. Esse é um dos artifícios usados pelo algoritmo do EIGRP (DUAL) para garantir a integridade da tabela de roteamento, mantendo-a livre de loops.*

7.3.3.4.2 Reliable Transport Protocol (RTP)

O EIGRP usa um protocolo proprietário chamado RTP para gerenciar o fluxo de informações entre routers EIGRP. Como o próprio nome sugere, trata-se de um protocolo que garante a integridade dessas informações.

Quando o EIGRP envia tráfego *multicast*, ele usa o endereço de classe D 224.0.0.10 (lembre-se disso!). Como já mencionado, cada router EIGRP sabe quem são seus vizinhos e a cada *multicast* enviado, uma lista com os vizinhos ativos é mantida. Se após um *multicast* um vizinho não responde, o EIGRP alternará para *unicast* e continuará tentando obter uma resposta daquele vizinho específico. Se após 16 tentativas *unicast* ainda não houver resposta, o vizinho é tido como *dead*.

7.3.3.4.3 Diffusing Update Algorithm (DUAL)

O EIGRP usa o algoritmo DUAL para selecionar e manter em sua tabela de roteamento a melhor rota para uma rede remota. As principais funções desse algoritmo são:

- Determinação de uma rota alternativa, se cabível;
- Suporte a VLSM e CIDR;
- Identificação dinâmica de rotas;
- Procurar identificar uma rota alternativa, caso nenhuma seja encontrada.

O algoritmo DUAL provê ao EIGRP um dos melhores tempos de convergência entre todos os protocolos existentes. Os pontos-chave para a velocidade de convergência são dois, basicamente:

1) Routers rodando EIGRP mantêm uma cópia de todas as rotas conhecidas por routers vizinhos, que são usadas para o cálculo do melhor custo para cada uma das redes remotas. Se uma rota tornar-se inacessível por qualquer motivo, basta consultar a tabela topológica em busca da melhor rota alternativa;
2) Se não houver uma rota alternativa na tabela topológica local, o router EIGRP contatará seus vizinhos perguntando se algum deles possui uma rota alternativa para a rede em questão (esse é o processo de *query* do EIGRP). Podemos ver que o protocolo EIGRP é bastante desinibido: se ele não conhece, pergunta. Simples assim!

7.3.3.4.4 Conceito de Redes Descontíguas

O EIGRP, assim como o RIPv2, oferece suporte a redes descontíguas. O que é, afinal, uma rede descontígua? Basicamente o termo é adotado para duas ou mais sub-redes de uma rede *classful*, conectadas entre si através de uma rede *classful* diferente. A figura 7.11 ilustra o conceito.

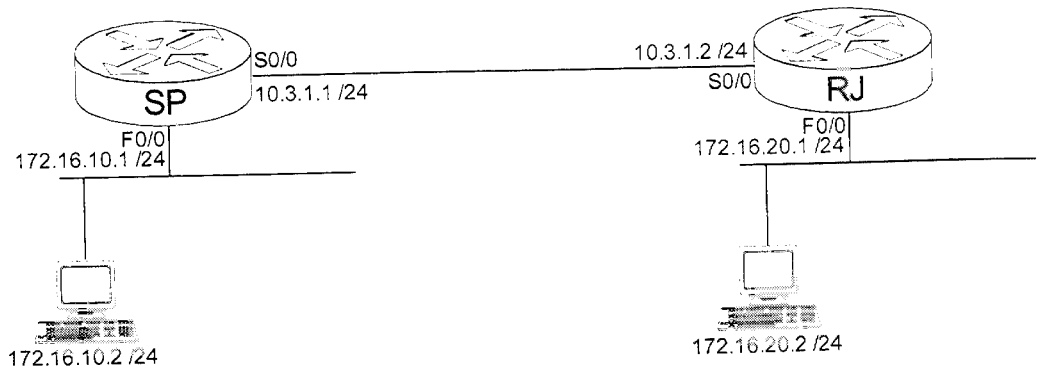


Figura 7.11: Exemplo de uma rede descontígua.

Note, na figura 7.11, que temos as sub-redes 172.16.10.0 e 172.16.20.0 conectadas entre si através da sub-rede 10.3.1.0. Por padrão, cada router pensa possuir apenas a rede 172.16.0.0 (auto-sumarização *classful*). É bastante importante chamar a atenção aqui para o fato de que redes descontíguas, como a apresentada na figura 7.11, não podem funcionar com os protocolos RIPv1 ou IGRP, já que estes apenas suportam redes *classful*. O roteamento simplesmente não funcionaria (ambos os routers não saberiam o que fazer quando o destino é a rede 172.16.10.0 ou 172.16.20.0, já que eles apenas enxergariam a rede *classful* 172.16.0.0). Mesmo os protocolos RIPv2 e EIGRP não suportam essas redes por default - já que o recurso de auto-sumarização encontra-se habilitado em ambos. É preciso desativar o recurso nesses dois protocolos.

***Nota**: O RIPv2 e o EIGRP suportam redes descontíguas, mas não por default. O OSPF, por sua vez, suporta redes descontíguas por default já que esse protocolo não auto-sumariza as redes no limite da rede-mãe (classful).*

Portanto, para que o roteamento em redes descontíguas funcione a contento usando-se o protocolo EIGRP, o recurso *auto-summary* deve ser desativado (ele vem ativado por default). Para isso, basta usar o comando *no auto-summ* dentro do prompt *config-router*.

Tabelas do EIGRP

Basicamente, o protocolo mantém três tabelas em um router:

- **Neighbor table**: Armazena informações sobre os routers vizinhos;
- **Topology table**: Armazena as informações sobre rotas propagadas por cada *neighbor*;
- **Routing table**: Armazena as rotas que estão efetivamente em uso num dado momento.

7.3.3.4.5 Métricas EIGRP

O protocolo EIGRP usa praticamente as mesmas métricas adotadas pelo seu "irmão", o IGRP. São elas:

Símbolo	Valor
K1	Bandwidth
K2	Load
K3	Delay
K4	Reliability
K5	MTU

Nota: As métricas default para EIGRP são K1 e K3 (Bandwidth e Delay), assim como no IGRP. Os valores dos "Ks" devem ser consistentes na rede inteira ou o protocolo não irá sincronizar.

Assim como o IGRP, o EIGRP também pode prover balanceamento de carga em até quatro links com métricas diferentes (*unequal cost load balance*); entretanto, é possível alcançar um balanceamento de carga com até seis links usando-se o comando *maximum-paths*:

```
Router(config)#router eigrp 10
Router(config-router)#maximum-paths 6
```

7.3.3.4.6 Configuração EIGRP

Usando a rede proposta na figura 7.11, vamos configurar o EIGRP para os routers SP e RJ, sabendo-se que ambos encontram-se inseridos no mesmo sistema autônomo de número 100:

```
SP(config)#router eigrp 100
SP(config-router)#network 172.16.0.0
SP(config-router)#network 10.0.0.0
```

Vamos supor que você não queira que as atualizações EIGRP sejam transmitidas pela interface F0/0. Para isso, use o comando:

```
SP(config-router)#passive-interface f0/0
```

Pronto, o EIGRP encontra-se configurado no router SP! Mas espere um pouco! Se fizermos apenas isso, teremos um problema, já que nossa rede é descontígua, lembra-se? Do modo como a coisa foi feita, apenas a rede *classful* (172.16.0.0) será propagada, e isso de nada vai adiantar (ambos os lados da rede possuem 172.16.0.0). Para resolver esse pequeno impasse, temos que desativar o recurso *auto-summ* do EIGRP:

```
SP(config-router)#no auto-summary
```

Agora sim, nosso router de SP está finalizado. Vamos ao router RJ. Como vocês devem imaginar, não será muito diferente:

```
RJ(config)#router eigrp 100
RJ(config-router)#network 172.16.0.0
RJ(config-router)#network 10.0.0.0
RJ(config-router)#passive-interface f0/0
RJ(config-router)#no auto-summary
RJ(config-router)#end
```

7.3.3.4.7 Verificação EIGRP

Para verificar o funcionamento do protocolo em um router, existem muitos comandos (alguns inclusive já vistos). Eis os principais:

```
Marco#sh ip route
[output cut]
Gateway of last resort is not set
D 192.168.30.0/24 [90/2172416] via 192.168.20.2,00:04:36, Serial0/0
C 192.168.10.0/24 is directly connected, FastEthernet0/0
D 192.168.40.0/24 [90/2681856] via 192.168.20.2,00:04:36, Serial0/0
C 192.168.20.0/24 is directly connected, Serial0/0
D 192.168.50.0/24 [90/2707456] via 192.168.20.2,00:04:35, Serial0/0
```

Note que as rotas trazidas pelo EIGRP são prefixadas pela letra "D", de DUAL. Observe também o valor da distância administrativa do protocolo: 90.

```
Marco#show ip eigrp neighbor
 Address      Interface Holdtime Uptime   SRTT  RTO  Q  Seq Type
                        (sec)            (ms)      Cnt Num
 192.168.40.1     Se0    12      00:13:24  26   200  0  7
```

- **Holdtime**: Indica o tempo que esse router irá aguardar por um pacote *hello* do vizinho especificado;
- **Uptime**: Indica há quanto tempo a adjacência foi estabelecida;
- **SRTT (*Smooth Round Trip Time*)**: Indica quanto tempo leva para alcançar o vizinho em questão e retornar;
- **RTO (*Retransmission Time Out*)**: Tempo que o protocolo aguarda antes de retransmitir um pacote da fila de retransmissão para o vizinho em questão;
- **Q**: Indica se existem mensagens excepcionais na fila de transmissão. Números altos aqui podem indicar um problema;
- **Seq**: Indica o número de seqüência do último update do vizinho em questão. Usado para manter a sincronização e evitar duplicidade de informação ou pacotes fora de seqüência.

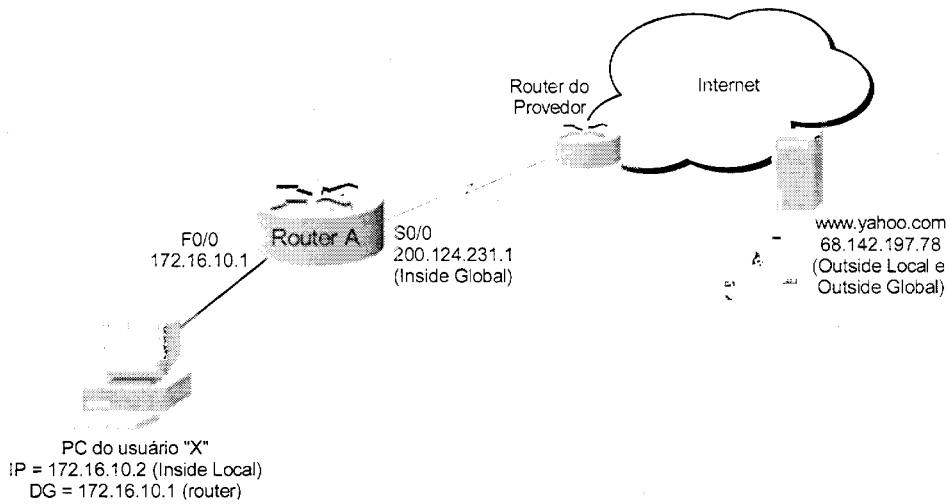
```
Marco#show ip eigrp topology
Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
       r - reply Status, s - sia Status
P 192.168.40.0/24, 1 successors, FD is 2169856
     via Connected, Serial0
P 192.168.50.0/24, 1 successors, FD is 281600
     via Connected, Ethernet0
P 192.168.10.0/24, 1 successors, FD is 2707456
     via 192.168.40.1 (2707456/2195456), Serial0/0
P 192.168.30.0/24, 1 successors, FD is 2172416
     via 192.168.40.1 (2172416/28160), Serial0/0
P 192.168.20.0/24, 1 successors, FD is 2681856
     via 192.168.40.1 (2681856/2169856), Serial0/0
```

Note que cada rota é precedida pela letra "P". Isso significa que essa rota encontra-se em estado passivo (*passive-state*). Rotas em estado ativo (*active-state*) indicam que o router perdeu o caminho para aquela rede e está procurando uma rota alternativa. Note também que cada entrada na tabela possui um *feasible distance* (FD) para cada rede remota, além do vizinho através do qual os pacotes serão enviados para seu destino final. Temos também, para cada entrada, dois valores entre parênteses - ex.: *(2707456/2195456)*. O primeiro valor indica o *feasible distance*, enquanto o segundo indica a distância propagada (*advertised distance* - AD) para a rede remota.

***Nota**: É importante lembrar-se de que o estado ativo (ative-state) indica que a rota em questão não se encontra mais na tabela de roteamento e que o protocolo EIGRP está "indagando" (querying) os routers vizinhos para descobrir se existe um caminho alternativo para a rota "perdida". Quando a rota encontra-se em estado passivo (passive-state), tudo está normal (aparentemente, ao menos), e ela encontra-se inserida na tabela de roteamento.*

7.4 Traduzindo Endereços com NAT (Network Address Translation)

Como vimos anteriormente, existem intervalos de endereços IPs que são reservados para uso privativo, ou seja, essas redes simplesmente não são roteadas através de uma rede de domínio público, como a Internet. Suponha que sua rede tenha o layout proposto a seguir:



No exemplo anterior, nosso usuário (o senhor "X") usa uma máquina que tem como *Default Gateway* (DG) o router "A", ou seja, para todo e qualquer acesso fora de sua rede, o PC do Sr. "X" irá usar o router como porta de saída.

Vamos supor que o Sr. "X" abre seu navegador Internet (*browser*) e digita *www.yahoo.com*. Usando um servidor DNS, esse endereço será convertido em um IP (no caso, um dos IPs do Yahoo: 68.142.197.78). Como esse endereço não se encontra na rede local (não pertence à rede 172.16.x.x), o pacote com a solicitação da página será enviado ao router. O router, por sua vez, terá uma rota default configurada, informando que tudo aquilo que ele não tiver em sua tabela de roteamento (o endereço IP do servidor do Yahoo, por exemplo) deve sair pela interface Serial 0/0 (o comando para configuração dessa rota, como já vimos, seria ip route 0.0.0.0 0.0.0.0.0 serial 0/0).

Excelente! Temos então um pacote IP com o endereço do PC do Sr. "X" como origem e o endereço do servidor do Yahoo como destino, sendo enviado pelo router "A" para o próximo ponto: o router do provedor Internet. Esse é o router que, de fato, possui em sua tabela a rota para o servidor do Yahoo. Afinal, ele sim é um roteador de Internet. Nosso router "A" não precisa conhecer as rotas da Internet (milhares), já que ele pode apenas configurar uma rota default e deixar que o router de seu provedor cuide do roteamento dentro da Internet.

O router do provedor irá identificar a rota para o servidor do Yahoo (68.142.197.78) e encaminhar o pacote para o caminho correspondente, até que, eventualmente, o pacote de nosso amigo Sr. "X" chegue ao seu destino.

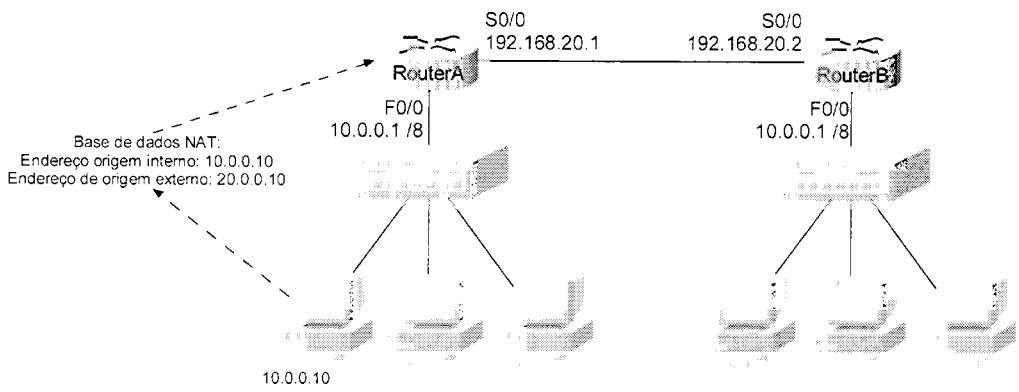
Bom, até aqui nenhum problema, certo? Conseguimos chegar até nosso destino, mesmo adotando um endereço reservado (172.16.10.2). Qual o problema, então, em adotar esse tipo de endereço? O problema é a volta da informação. O caminho de ida ocorre sem maiores complicações, pois estamos roteando para um endereço de Internet público (68.142.197.78, no caso). No retorno do pacote (a resposta do servidor do Yahoo para o PC do Sr. "X") é que a coisa complica.

Lembre-se de que, no retorno, os endereços são trocados. O que era origem vira destino e vice-versa. Portanto, partindo do servidor do Yahoo, o pacote de resposta será enviado com o endereço IP de destino da máquina do Sr. "X": 172.16.10.2. Assim que esse pacote entrar na Internet, ele será descartado, já que esse é um endereço reservado para uso privado e não pode ser roteado pelos roteadores da Internet. Resumindo, o PC de nosso amigo sofrerá um belo *time out* e a esperada página de entrada do portal Yahoo nunca aparecerá.

Como resolver esse impasse? Precisamos configurar nosso Router "A" para que ele realize uma troca dos endereços de origem assim que um pacote atravessar a interface com conexão à Internet (S0/0, no caso). Basicamente, informaremos ao router para retirar o endereço de

origem inválido (rede 172.16.0.0) e colocar, em seu lugar, um endereço roteável na Internet (podendo ser o da própria interface S0/0, por exemplo). Isso é NAT, conforme definido pela RFC 1631.

Além de permitir o acesso a redes públicas, o NAT também aumenta a segurança da rede privada, uma vez que mascara da Internet os endereços IP internos (quem capturar um pacote do Sr. "X" verá que a sua origem é o endereço da interface serial 0/0 e nunca saberá qual o real endereço do PC do Sr. "X"). O NAT também pode ser usado em outras ocasiões. Suponha que você deseje que duas redes concebidas usando o mesmo endereço privado de rede (por exemplo: 10.0.0.0) se comuniquem. Lembre-se de que routers não roteiam para um mesmo endereço de rede - uma questão de definição. O NAT pode ser usado para traduzir o endereço de uma das redes para um outro padrão de endereçamento, tornando a comunicação possível (veja a seguir).



No exemplo anterior, todos os endereços IPs da rede à esquerda serão percebidos pela rede à direita como sendo originados na rede 20.0.0.0. É uma forma de solucionar o problema através do uso do NAT.

Existem basicamente três tipos de NAT:

- **NAT estático**: Provê o mapeamento de um para um, ou seja, para cada endereço IP privado, existe um endereço IP válido para a conexão com a internet;
- **NAT dinâmico**: Provê um mapeamento de endereços não-válidos para válidos, porém, sem a necessidade de possuirmos um endereço válido para cada endereço inválido. Nesse caso, trabalha-se com um intervalo de endereços válidos (*pool*), que é alocado conforme necessidade;
- **Overloading**: Essa modalidade de NAT permite que poucos ou até mesmo apenas um endereço válido seja usado para todas as máquinas com endereços inválidos. Isso é possível, pois, no processo de troca, o NAT armazena o valor da porta TCP origem juntamente com o IP que está sendo trocado, e

usa isso como um identificador para recolocar o endereço original - não-válido - no retorno do pacote para que este finalmente chegue ao PC origem. Por esse motivo, esse método também é conhecido como PAT - *Port Address Translation.*

Eis um exemplo de configuração para nossa rede sugerida (para que, finalmente, o Sr. "X" consiga acessar a página do Yahoo!). Vamos adotar a modalidade *overloading*, até mesmo por essa ser a mais comumente usada:

```
RouterA(config)#int f0/0
RouterA(config-if)#ip nat inside
RouterA(config-if)#int S0/0
RouterA(config-if)#ip nat outside
RouterA(config-if)#exit
RouterA(config)#access-list 10 permit 172.16.0.0 0.0.255.255
RouterA(config)#ip nat pool internet 200.124.231.1
200.124.231.1 prefix 24
RouterA(config)#ip nat inside source list 10 pool internet
overload
```

Como complemento à terminologia, a Cisco define quatro tipos de endereços IPs quando o assunto é NAT:

- **Inside local address**: O endereço IP associado a um host dentro da rede local (*inside*). Esse endereço, provavelmente, não é um endereço IP válido para roteamento na Internet (ex.: 172.16.10.1);
- **Inside global address**: Um endereço IP válido para roteamento na Internet (ou não, dependo do que se deseja obter com o NAT) que representa um ou mais IPs internos à rede (*inside local*) para o mundo externo (no exemplo anterior, seria o IP 200.124.231.1);
- **Outside local address**: Endereço IP de um host externo à rede organização (*outside*), do modo como ele é percebido localmente, pelas máquinas da rede local;
- **Outside global address**: Qualquer endereço IP externo à organização, do modo como ele é percebido pela Internet.

  Basicamente, **local** é usado para definição do ponto de vista interno à rede local, enquanto **global** é usado para definir o ponto de vista externo à rede local;
- **Local address**: Qualquer endereço IP que é interno à rede local estando, portanto, sujeito à tradução;
- **Global address**: Qualquer endereço IP externo à rede local.

Como podemos ver, não é muito complicado. A interface local (F0/0) é nossa *NAT inside*, enquanto a interface com acesso à Internet (S0/0) é nossa interface *NAT outside*. Criamos a *access-list 10* para definir qual o intervalo válido para conversão dos IPs (no caso, a rede 172.16.x.x) e, finalmente, o intervalo dos endereços que serão usados para conversão (endereços válidos para a Internet). No caso, o intervalo é de apenas um IP, o da própria serial.

7.5 Sumarização de Rotas Usando EIGRP e OSPF

Veremos agora comandos usados para criação de rotas sumarizadas em um router rodando o protocolo EIGRP ou OSPF. A teoria de sumarização já foi vista em capítulo anterior, juntamente com a teoria sobre sub-redes.

Mesmo que o processo de sumarização de rotas no OSPF possa ocorrer de algumas maneiras distintas, focaremos no comando mais comum, que sumariza redes de diversas áreas OSPF na área 0 (*backbone*). É sempre bom lembrar, porém, que o exame CCNA apenas foca em OSPF funcionando em uma única área (*single area OSPF*).

Vamos adotar a rede ilustrada na figura 7.12 para nosso cenário de sumarização.

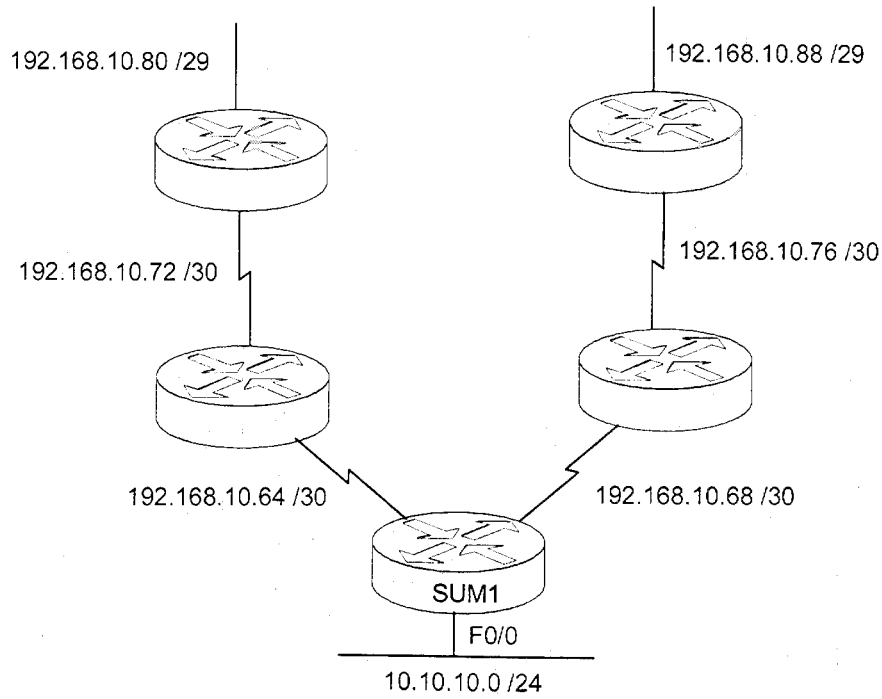


Figura 7.12: Modelo da rede a ser aplicada sumarização usando EIGRP.

Como podemos notar, temos seis sub-redes 192.168.10.x, sendo que duas delas são /29 (255.255.255.248) e as quatro restantes (conexões

WAN), /30 (255.255.255.252). No exercício que segue, iremos sumarizar essas seis sub-redes em apenas um endereço de rede e divulgando essa rota sumarizada para dentro da rede 10.10.10.0 (conectada ao router SUM1 através da interface F0/0).

O primeiro passo, como já vimos, é descobrir como sumarizar essas redes. Temos que sumarizar as redes no intervalo 192.168.10.64 a 192.168.10.88, conforme a figura 7.13 nos mostra. O cálculo que podemos usar é simples. Vamos subtrair uma rede da outra (matemática simples): x.x.x.*88* - x.x.x.*64* = *24*. Lembra-se dos "blocos" válidos que podemos usar (4, 8, 16, 32, 64 etc.)? No nosso caso, o bloco 32 deve ser usado, já que o imediatamente inferior (16) seria muito pequeno para acomodar todas as redes requeridas (de .64 a .88).

Já que temos nosso bloco, o próximo passo é fazer o bom e velho cálculo:

256 - 32 = *224*

Portanto, a máscara de nossa rede sumarizada seria 255.255.255.*224*! Simples, não é verdade?

Sendo que nosso bloco é 32, imediatamente identificamos que a primeira rede desse bloco deve ser um múltiplo desse número ou, no nosso caso, 192.168.10.64. Já temos a máscara e o endereço de rede da rota sumarizada: 192.168.10.64 /27. Basta agora configurá-la em nosso router SUM1, na interface F0/0, para que a rede 10.10.10.0 receba apenas a rota sumarizada e não as seis rotas mencionadas anteriormente:

```
SUM1#config t
SUM1(config)#router eigrp 10
SUM1(config-router)#network 192.168.10.0
SUM1(config-router)#network 10.0.0.0
SUM1(config-router)#no auto-summary
SUM1(config-router)#interface fastethernet 0/0
SUM1(config-if)#ip summary-address eigrp 10 192.168.10.64
255.255.255.224
```

***Nota**: A propagação de rotas manualmente sumarizadas tem prioridade sobre a propagação de rotas automaticamente sumarizadas.*

E, se desejássemos fazer o mesmo, mas usando o protocolo OSPF:

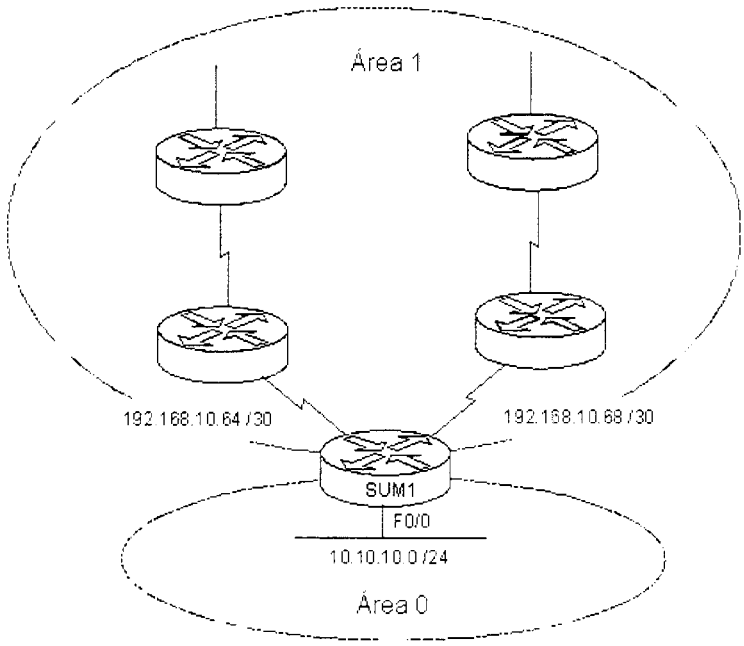


Figura 7.13: Modelo da rede a ser aplicada sumarização usando OSPF.

```
SUM1#config t
SUM1(config)#router ospf 1
SUM1(config-router)#network 192.168.10.64 0.0.0.3 area 1
SUM1(config-router)#network 192.168.10.68 0.0.0.3 area 1
SUM1(config-router)#network 10.10.10.0 0.0.0.255 area 0
SUM1(config-router)#area 1 range 192.168.10.64 255.255.255.248
```

Observe que, para o protocolo OSPF, o comando *no auto-summary* não é requerido, já que ele não realiza sumarização por default (como faz o EIGRP). Neste exemplo, o router SUM1 é um *Area Border Router* (ABR).

7.6 Sumarização de Rotas Usando RIPv2

Para fazer sumarização manual usando o protocolo RIPv2, basta usar o comando *ip summary-address rip*, como no exemplo a seguir:

```
Router(config)#int Ethernet0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip summary-address rip 10.2.0.0 255.255.0.0
```

Assim como no EIGRP, rotas manualmente sumarizadas terão prioridade sobre rotas automaticamente sumarizadas.

Questões de Revisão – Roteamento IP

1. Qual a categoria do protocolo de roteamento RIP?

a) Routed information
b) Link together
c) Link state
d) Distance vector

2. Qual a categoria do protocolo de roteamento IGRP?

a) Routed information
b) Link together
c) Link state
d) Distance vector

3. Qual comando deve ser digitado no prompt do router para verificar a freqüência de broadcast IGRP?

a) sh ip route
b) sh ip protocol
c) sh ip broadcast
d) debug ip igrp

4. Qual a métrica de roteamento utilizada pelo RIP?

a) Count to infinity
b) Hop count
c) TTL
d) Bandwidth, delay

5. Qual comando é usado para evitar que atualizações de roteamento sejam propagadas por uma determinada interface?

a) Router(config-if)#no routing
b) Router(config-if)#passive-interface
c) Router(config-router)#passive-interface s0
d) Router(config-router)#no routing updates

6. Quais as métricas de roteamento default utilizadas pelo protocolo IGRP?

a) Count to infinity
b) Hop count
c) TTL
d) Bandwidth
e) Delay

7. O que a métrica de 16 saltos representa em uma rede RIP?

a) 16ms até o próximo salto.
b) O número total de routers presentes na rede.
c) Número de saltos até o destino.
d) Destino inalcançável.
e) Último salto verificado antes de a contagem reiniciar.

8. Para que servem os holddowns?

a) Para impedir a passagem de uma atualização para o próximo hop.
b) Para prevenir que mensagens regulares de atualização reativem uma rota que se encontra, na verdade, desativada.
c) Para prevenir que mensagens regulares de atualização reativem uma rota que acaba de ser ativada.
d) Para prevenir que mensagens irregulares de atualização reativem uma rota que se encontra desativada.

9. O que é a regra do split horizon?
   a) A regra do split horizon rege que um router não deve enviar de volta a informação recebida de outro router através da mesma interface, prevenindo a ocorrência de loops de roteamento.
   b) A regra do split horizon rege que, quando um barramento de rede (horizonte) de grande porte existir, ele deve dividir (split) o tráfego dessa rede.
   c) A regra do split horizon previne atualizações regulares de serem propagadas para um link desativado.
   d) A regra do split horizon previne atualizações regulares de reabilitarem uma rota que se encontra desativada.

10. O que faz o poison reverse?
   a) O mecanismo de poison reverse envia de volta a informação recebida por router como uma poison pill, bloqueando assim atualizações regulares.
   b) É a informação recebida de um router que não pode ser enviada de volta ao router que a originou.
   c) Previne atualizações regulares de reabilitarem uma rota que acaba de ser ativada.
   d) O mecanismo de poison reverse faz com que um router configure a métrica de um link desativado para counting to infinity.

11. Qual é a distância administrativa default para o IGRP?
   a) 90
   b) 100
   c) 120
   d) 220

12. Qual das seguintes é a sintaxe correta para se configurar uma rota default?
   a) route ip 172.0.0.0 255.0.0.0 s0
   b) ip route 0.0.0.0 0.0.0.0 172.16.20.1
   c) ip route 0.0.0.0 255.255.255.255 172.16.20.1
   d) route ip 0.0.0.0 0.0.0.0 172.16.10.1150
   e) ip route 0.0.0.0 0.0.0.0

13. Qual dos seguintes é um protocolo de roteamento do tipo link state?
   a) RIPv2
   b) EIGRP
   c) OSPF
   d) IGRP
   e) BGP4

14. Quais dos comandos a seguir estão disponíveis para suportar redes RIP?
   a) sh ip route
   b) sh ip rip proto
   c) sh rip network
   d) debug ip rip

15. Qual das seguintes afirmações é verdadeira sobre protocolos do tipo distance vector?

a) Enviam atualizações incrementais a cada 60 segundos.
b) Enviam sua tabela de roteamento completa em intervalos regulares.
c) Enviam sua tabela de roteamento parcial em intervalos regulares.
d) Enviam atualizações incrementais quando uma mudança na rede é percebida.

16. Qual comando do IOS pode ser usado para visualizar, na tabela de roteamento, apenas as rotas estáticas?

a) sh ip config stat
b) sh ip static routes
c) sh ip route sta
d) sh ip table/static routes

17. Para que a distância administrativa é usada no processo de roteamento?

a) Determinação de qual deve ser o router gerenciador da rede.
b) Criação de um banco de dados.
c) Classificação da confiabilidade da origem, expressa por um valor numérico entre 0 e 255.
d) Classificação da confiabilidade da origem, expressa por um valor numérico entre 0 e 1023.

18. Quando olhamos uma tabela de roteamento, o que o "S" significa?

a) Rota diretamente conectada.
b) Rota dinamicamente descoberta.
c) Rota estaticamente configurada.
d) Rota preferencial.
e) Rota-raiz (seed route).

19. Qual das afirmações a seguir é verdadeira sobre o processo de roteamento IP?

a) O endereço IP de destino é alterado a cada salto.
b) O endereço IP de origem é alterado a cada salto.
c) O frame não é alterado a cada salto.
d) O frame é alterado a cada salto, mas o pacote IP, não.

20. Quais das seguintes afirmações são verdadeiras com relação à criação de rotas estáticas?

a) O parâmetro de máscara é opcional.
b) O parâmetro de próximo salto ou interface de saída é requerido.
c) A distância administrativa é requerida.

d) A distância administrativa é opcional.
e) n.d.a.

21. Qual o propósito da estrutura hierárquica oferecida pelo protocolo OSPF?

a) Reduzir a complexidade da configuração do router.
b) Acelerar o processo de convergência.
c) Confinar a instabilidade da rede a áreas específicas.
d) Reduzir o volume de atualizações propagadas pela rede.
e) Reduzir a latência da rede.

22. Você, como administrador de uma rede, precisa escolher um protocolo de roteamento que:

- Possua escalabilidade
- Suporte VLSM
- Mantenha o tráfego de atualizações a um mínimo
- Suporte roteadores de múltiplos fabricantes

Qual das alternativas a seguir seria a mais indicada?

a) RIPv2
b) IGRP
c) EIGRP
d) IS-IS
e) OSPF

23. Quais os protocolos de roteamento que suportam balanceamento de carga por até quatro links com métricas desiguais?

a) RIPv2
b) RIPv1
c) IGRP
d) OSPF
e) EIGRP

24. Quais as métricas default adotadas pelo protocolo EIGRP?

a) K1=1, K2=1, K3=0, K4=1, K5=0
b) K1=1, K2=0, K3=1, K4=1, K5=0
c) K1=1, K2=0, K3=0, K4=1, K5=0
d) K1=1, K2=0, K3=1, K4=0, K5=0
e) K1=0, K2=1, K3=0, K4=1, K5=0

25. O que o estado *active* de uma rota na tabela topológica indica quando usamos o comando sh ip eigrp topo?

a) A rota em questão não se encontra mais na tabela de roteamento e o router está pesquisando com seus vizinhos se algum deles conhece um caminho alternativo para essa rota.
b) A rota em questão está ativa e disponível.
c) O protocolo acaba de descobrir essa rota e a está incluindo na tabela de roteamento.
d) A rota em questão está ativa, porém, indisponível.

26. Qual comando EIGRP apresenta os feasible distances?

a) sh ip ro eigrp
b) sh ip eigrp neigh
c) sh ip eigrp topo
d) sh ip eigrp

27. Com relação ao protocolo OSPF, quais os critérios para eleição dos routers DR e BDR?

a) O router com o maior número de interfaces é eleito o DR e o segundo router com mais interfaces, o BDR.
b) O router com a maior prioridade OSPF é eleito o DR.
c) Em caso de empate, o RID é usado.
d) Um router com prioridade OSPF = "0" é considerado inelegível.
e) O maior IP nas interfaces é usado para definir o RID de um router. No caso de haver uma interface loopback configurada, o IP desta será o usado, mesmo que ele seja menor que os IP de outras interfaces do router.

28. Uma empresa possui 25 usuários e decide conectar a rede existente à Internet. A empresa deseja que todos os usuários tenham acesso à Internet simultaneamente, porém, ela possui apenas um endereço público (roteável na Internet). O que deve ser configurado para que todos os 25 usuários consigam acesso à Internet simultaneamente usando este único IP público?

a) NAT estático
b) NAT global
c) NAT dinâmico
d) NAT estático com apoio de listas de acesso
e) NAT dinâmico com overload

29. Em uma rede OSPF, o que é o ABR?

a) Um router que possui ao menos uma de suas interfaces na área 0 e outra em qualquer outra área.
b) Um router que fica na borda do sistema autônomo.
c) Um router que fica contido na área 0.
d) Um router que serve de base para um link virtual.

30. Quais dos protocolos listados a seguir suportam autenticação?

a) OSPF
b) RIP
c) IGRP
d) RIPv2
e) EIGRP

31. Em uma rede com os protocolos EIGRP, OSPF, RIPv2 e IGRP simultaneamente ativos, as rotas preferidas serão as trazidas por qual protocolo?

a) OSPF
b) EIGRP
c) RIPv2
d) IGRP

32. Baseando-se na saída a seguir responda: Qual o protocolo de roteamento em atividade nesta rede?

```
Marco#sh ip route
[output cut]
? 192.168.30.0/24 [90/2172416] via 192.168.20.2,00:04:36,
Serial0/0
```

a) Não é possível responder, pois o indicador de protocolo aparece como "?".
b) RIPv2
c) IGRP
d) OSPF
e) EIGRP

Respostas das Questões de Revisão – Roteamento IP

1. **D**. O RIP usa o algoritmo de roteamento distance vector e utiliza somente a contagem de saltos (hop count) como métrica para determinar a melhor rota em uma rede.

2. **D**. O IGRP é um protocolo proprietário Cisco do tipo distance vector.

3. **B**. O comando show ip protocol mostrará os protocolos de roteamento ativos, assim como os timers configurados para cada um deles.

4. **B**. O RIP utiliza somente a contagem de saltos para determinar o melhor caminho para uma rede remota.

5. **C**. O comando passive interface evita que atualizações sejam enviadas por uma determinada interface.

6. **D**, E. Bandwidth e delay of the line são as métricas default usadas pelo IGRP para determinar o melhor caminho para uma rede remota.

7. **D**. O RIP permite uma contagem de até 15 hops; 16 hops define um ponto inalcançável.

8. **B**. Holddowns evitam que mensagens regulares de atualização reabilitem uma rota que se encontra desativada.

9. **A**. Split horizon não informará uma rota recebida por um router vizinho de volta a ele, pela mesma interface na qual a rota foi recebida. Isso ajuda a reduzir o risco de loops em uma rede baseada em protocolos distance vector.

10. **D**. Poison reverse é utilizado para comunicar a um router que determinada rede encontra-se inalcançável, e que a contagem de saltos para essa rede está configurada para infinito ou inalcançável.

11. **B**. A distância administrativa default para IGRP é 100; para o RIP a distância administrativa default é 120.

12. **B**. A configuração de uma rota IP default utiliza uma série de zeros (wildcard) para definir a rede de destino (qualquer rede que não se encontre na tabela de roteamento, basicamente), seguidos pelo endereço do próximo salto ou da interface de saída.

13. **C**. OSPF é um protocolo IP verdadeiramente link state. Utiliza somente a largura de banda (custo) como métrica para encontrar o melhor caminho para uma rede remota.

14. **A, D**. O comando show ip route e debug ip rip são usados para dar suporte e verificar redes RIP.

15. **B**. Protocolos de roteamento do tipo *distance vector* enviam suas tabelas de roteamento completas para todas as interfaces ativas em intervalos regulares de tempo. Em uma rede RIP isso ocorre a cada 30 segundos, enquanto em uma rede IGRP isso ocorre a cada 90 segundos, por default.

16. **C**. O comando show ip route static apresenta apenas as rotas estaticamente configuradas na tabela de roteamento IP.

17. **C**. Distância administrativa é usada em roteamento para classificar a confiabilidade de uma rota. 0 é a mais alta classificação (maior confiabilidade), sendo usada para redes diretamente conectadas.

18. **C**. Rotas estaticamente configuradas são representadas na tabela de roteamento pela letra "S".

19. **D**. No roteamento IP o frame é substituído a cada hop à medida que o pacote atravessa um dispositivo de camada 2. O pacote IP, entretanto, não sofre nenhuma modificação durante o processo.

20. **B, D**. Quando configuramos rotas estáticas, a rede de destino seguida da máscara e do endereço do próximo hop ou a interface de saída para aquele router devem ser informados. A distância administrativa é um parâmetro opcional.

21. **B, C, D**. A função das áreas em uma rede OSPF é manter os problemas inerentes a elas dentro de cada uma. Isso evita que atualizações sejam propagadas pela rede toda cada vez que uma mudança ocorre em uma área. Por esse mesmo motivo, o tempo de convergência é reduzido.

22. **E**. Apenas o protocolo OSPF cobre todos os requisitos pedidos.

23. **C, E.** Ambos os protocolos Cisco (IGRP e EIGRP) disponibilizam o recurso de balanceamento de carga por até quatro links desiguais (até seis, no caso do EIGRP).

24. **D.** K1=1 e K3=1 (bandwidth e delay) são as métricas default usadas pelo protocolo EIGRP.

25. **A.** Quando uma rota encontra-se em modo *active* na tabela topológica, o router não mais conhece um caminho para chegar à rede em questão.

26. **C.** O comando sh ip eigrp topology apresenta, entre outras informações, os valores das feasible distances.

27. **B, C, E.** Apesar da alternativa "D" possuir uma informação correta, não foi isso o que foi perguntado.

28. **E.** O modo *NAT* overload permite que apenas um IP seja usado por várias máquinas na rede para acessar uma rede remota. Isso á atingido através do mecanismo chamado PAT (Port Address Translation).

29. **A.** Um ABR (Area Border Router) é um router que possui ao menos uma de suas interfaces na área 0 e outra(s) em qualquer outra área.

30. **A, D, E.** RIPv2, OSPF e EIGRP oferecem suporte à autenticação

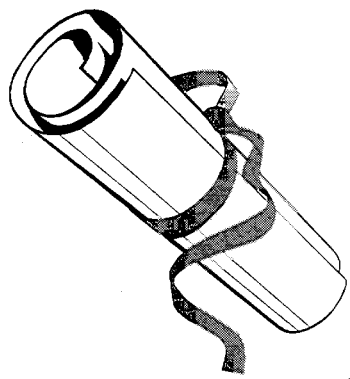
31. **B.** O EIGRP possui uma distância administrativa (90) menor que a dos outros protocolos, portanto, suas rotas serão preferidas.

32. **E.** Na saída podemos identificar que o protocolo usado é o EIGRP observando a distância administrativa ([*90*/2172416]).

Relação dos Comandos Analisados

Comando	Descrição
ip route 123.123.123.0 255.255.255.0 10.0.0.1	Cria uma rota estática para a rede 123.123.123.0 através do próximo salto 10.0.0.1
sh ip route	Apresenta toda a tabela de roteamento ativa no router em questão
sh ip route sta	Apresenta somente as rotas estáticas presentes na tabela
sh ip route rip	Apresenta apenas as rotas aprendidas pelo protocolo RIP

Comando	Descrição
sh ip route eigrp	Apresenta apenas as rotas aprendidas pelo protocolo EIGRP
sh ip route ospf	Apresenta apenas as rotas aprendidas pelo protocolo OSPF
router rip	Ativa o protocolo RIP no router
router ospf 64	Ativa o processo OSPF número 64 no router
router eigrp 64	Ativa o protocolo EIGRP para o sistema autônomo 64
router igrp 64	Ativa o protocolo IGRP para o sistema autônomo 64
sh ip eigrp topo	Apresenta a tabela topológica do EIGRP
router rip | version 2	Ativa o protocolo RIPv2 no router
ip route 0.0.0.0 0.0.0.0 s0/0	Cria uma rota estática default usando a interface s0/0 como default gateway
router ospf 64 | netw 12.0.0.0 0.0.0.255 area 0	Insere a interface com endereço de rede 12.0.0.0 na área OSPF "0" (*backbone*)
interface loopback 0	Cria a interface virtual Loopback0 no router
sh ip eigrp neigh	Apresenta informações sobre os routers EIGRP vizinhos
no auto-summary	Desativa a sumarização automática nos protocolos IGRP, EIGRP e RIPv2
sh ip ospf adj	Apresenta informações sobre as adjacências OSPF estabelecidas
ip nat inside	Define a interface interna no processo de NAT
ip nat outside	Define a interface externa no processo de NAT
overload	Informa ao processo NAT para ativar o recurso *overload* na tradução de endereços
ip summary-address eigrp 10 192.168.10.0 255.255.255.0	Habilita sumarização EIGRP do endereço apresentado
ip summary-address rip 192.168.10.0 255.255.255.0	Habilita sumarização RIPv2 do endereço apresentado



8 Gerenciamento de uma Rede Cisco

8.1 Tópicos Abordados

- Backup e Recuperação do Sistema IOS;
- Backup e Recuperação da Configuração do Router;
- Reunião de Informações sobre Dispositivos Vizinhos através dos Recursos CDP e Telnet;
- Resolução de Hostnames;
- Configuração dos Serviços DHCP e DNS em um Roteador Cisco
- Teste da Rede Através dos Recursos Ping e Trace.

Neste capítulo veremos como gerenciar routers Cisco em uma rede de grande porte.

O sistema IOS e arquivos de configuração residem em diferentes localizações em um dispositivo Cisco, e é importante o entendimento de onde esses arquivos se encontram e como eles funcionam.

Analisaremos também neste capítulo os componentes de um roteador, a sua seqüência de inicialização (*boot sequence*), o *configuration register* e seu uso na recuperação de senhas esquecidas ou perdidas.

8.2 Componentes Físicos e Lógicos de um Roteador Cisco

Antes de configurar e atuar na resolução de problemas (*troubleshooting*) de uma internetwork Cisco, você deve conhecer os principais componentes de um router Cisco, assim como entender qual a função de cada um:

- **Bootstrap**: Armazenado no microcódigo da ROM, o *bootstrap* é utilizado na inicialização de um router, para ativá-lo. Ele se encarrega do *boot* do router e do carregamento do IOS.
- **POST (*Power-On Self Test*)**: Também armazenado no microcódigo da ROM, o *POST* é utilizado na checagem básica de hardware do router e determina quais interfaces encontram-se presentes.
- **ROM Monitor**: Armazenado no microcódigo da ROM, o ROM Monitor é usado na identificação de problemas e testes de fabricação.
- **Mini-IOS**: Também chamado de *RXBOOT* ou *bootloader*, o *Mini-IOS* é uma versão reduzida do IOS alojada na ROM que pode ser usado na ativação de uma interface e no carregamento do sistema IOS no FLASH. O *Mini-IOS* também pode desempenhar outras tarefas de manutenção.
- **DRAM**: Usado no armazenamento (*buffer*) de pacotes, tabelas de roteamento e outras estruturas de dados que permitem ao router funcionar adequadamente. A configuração ativa (*Running-Config*) é armazenada na DRAM e, em alguns routers, o IOS pode ser rodado diretamente da DRAM.
- **ROM**: Usado para inicializar o router e na sua manutenção.
- **FLASH**: Usado para armazenamento do sistema IOS. O conteúdo da memória FLASH não é perdido quando um router é reiniciado.
- **NVRAM**: Usada no armazenamento da configuração (*Startup-Config*) em routers e switches. Seu conteúdo também é mantido, mesmo que um router seja desligado.
- **Configuration Register:** Define como um router será inicializado e outros parâmetros. A configuração ativa pode ser vista através do comando *show version*.

8.2.1 O Configuration Register

Todos os routers Cisco possuem um software registrador de 16-bits, que fica armazenado na NVRAM. Por default, o *configuration register* é configurado para carregar o sistema IOS do FLASH e para procurar o *startup-config* na NVRAM.

Podemos fazer uma analogia do *configuration register* com um *dip switch* físico, daqueles encontrados na parte traseira de modems externos ou em placas-mãe de PCs comuns (veja a figura 8.1). A posição

ON do *dip switch* equivale ao "1" no *configuration register* e a posiçãc *OFF*, ao "0". Basicamente, o *configuration register* de um router é um *dip switch* virtual. Pense no *configuration register* como um *dip switch* de 16 posições. Conforme elas são combinadas - alternando-se *ON* e *OFF* ("0s" e "1s") - um resultado diferente é obtido.

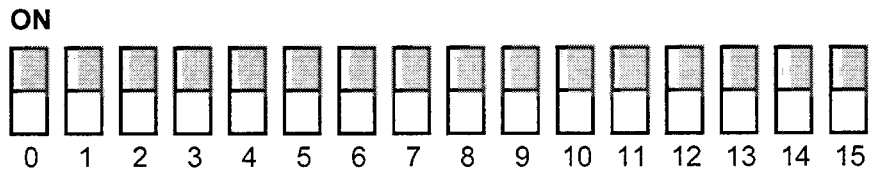


Figura 8.1: Modelo de um dip switch físico.

Os 16 bits do *configuration register* correspondem ao intervalo 0-15, lidos da esquerda para a direita (veja esquema a seguir). A configuração default encontrada nos routers Cisco é *0x2102*. Note que cada grupo de 4 bits (os quadrantes no esquema) é lido em notação binária com valores 1, 2, 4 e 8, da direita para a esquerda, pois o registrador faz uso do sistema hexadecimal (o *"0x"* que antecede o seu valor indica que o número que segue encontra-se em notação hexadecimal). Basta pensar: quantos bits são necessários para representar 16 algarismos (sistema hexadecimal)? A resposta seria 4, pois $2^4 = 16$. Esse é o motivo dos 16 bits serem agrupados de 4 em 4. Cada grupo de 4 corresponde a um possível algarismo em notação hexadecimal.

O esquema a seguir ajuda a compreender essa linha de pensamento. Vamos utilizá-lo para analisar o valor padrão do registrador em roteadores: 0x2102. Repare que o valor 0x2102 significa que os bits 13, 8 e 1 encontram-se *ON* (veja esquema). Seria, portanto, como ter em mãos um *dip switch*, e colocar as suas chaves 13, 8 e 1 no modo *ON* (veja figura 8.2).

	1° quadrante				2° quadrante				3° quadrante				4° quadrante			
	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
	8	4	2	1	8	4	2	1	8	4	2	1	8	4	2	1
Valor do Configuration Register **0x**	0	0	**2**	0	0	0	0	**1**	0	0	0	0	0	0	**2**	0
Número do bit	15	14	**13**	12	11	10	9	**8**	7	6	5	4	3	2	**1**	0
Notação binária	0	0	**1**	0	0	0	0	**1**	0	0	0	0	0	0	**1**	0

Novamente, se pensarmos em um *dip switch* físico, eis como faríamos:

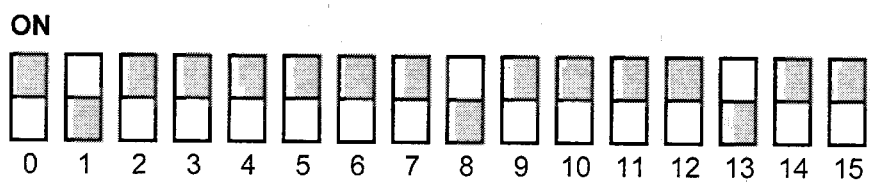


Figura 8.2: Um dip switch físico mapeado para o registrador default de um router (0x2102).

A tabela a seguir ilustra os significados dos bits. Note que **o bit 6 pode ser utilizado para que se ignore o conteúdo da NVRAM.** Esse recurso auxilia na recuperação de senhas, como veremos mais adiante, bastando alterar o valor do registrador para *0x2142*. Dessa forma, o router ignora o conteúdo da NVRAM (o que significa ignorar também todas as senhas que se encontravam configuradas).

00-03	0X0000-0X000F	Campo de boot (veja tabela a seguir).
6	0X0040	Ignora o conteúdo da VRAM.
7	0X0080	Habilita o bit OEM.
8	0X0100	Desabilita o <BREAK>.
10	0X0400	Broadcast IP com "0s".
11/dez	0X0800-0X1000	Velocidade da linha do console.
13	0X2000	Inicializa via software presente na ROM, caso a inicialização via rede falhe.
14	0X4000	Broadcasts IP sem valores da rede.
15	0X8000	Habilita mensagens de diagnóstico e ignora o conteúdo da NVRAM.

O campo de *boot* (*boot field*), que consiste do intervalo de bits 0-3 no *configuration register*, controla a seqüência de inicialização (*boot*) do router. A seguir, descrevemos os bits do campo de *boot*:

Campo de boot	Significado	Utilização
00	Modo ROM monitor	Para inicialização em modo ROM monitor, configure o *configuration register* para 2100. O prompt *rommon>* será apresentado.
01	Inicializa com imagem da ROM	Para inicializar o router a partir de uma imagem do IOS armazenada na ROM, configure o *configuration register* para 2101. O prompt *(boot)>* será apresentado.
02-F	Especifica um nome de arquivo de boot default	Qualquer valor de 2102 a 210F informa ao router para utilizar os comandos de inicialização especificados na NVRAM.

8.2.1.1 Conversão Binário – Hexadecimal

Eis um rápido tutorial para o entendimento do funcionamento da conversão binário-hexadecimal:

Nota: Este é um assunto que foi incorporado ao exame CCNA em sua nova versão. Além disso, é uma boa idéia entender os conceitos apresentados para total domínio do configuration register.

Peguemos como exemplo o número binário *111010010*.

1. Para começar, devemos entender que números hexadecimais são números de base 16, ou seja, apenas um número hexadecimal representa valores que vão de 0 a 15. Como a representação "15" existe apenas para números decimais, números hexadecimais representam os números decimais 10,11,12,13,14 e 15 respectivamente por A, B, C, D, E, F. Portanto, teremos os números hexadecimais representados por 0,1,2,3,4,5,6,7,8,9, A, B, C, D, E, F (veja tabela a seguir).

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

2. Pensando em binários, de quantos bits precisamos para representar um número no intervalo 0-15? 4 bits, certo? Pense: $(1*2)^0 + (1*2)^1 + (1*2)^2 + (1*2)^3 = 1+2+4+8 = 15$.
3. Pensando assim, para converter qualquer número binário para hexadecimal, basta que os agrupemos de 4 em 4, **sempre partindo da direita para a esquerda!**
4. Portanto, em nosso exemplo, *111010010*, agrupe-os assim: *0001 1101 0010* (acrescente os zeros faltantes ao último grupo, como fiz aqui).
5. Agora, para determinar o número em hexadecimal, basta fazer a conversão de cada um dos grupos: *0+0+0+1 8+4+0+1 0+0+2+0 = 1 13 2*.
6. Não temos *"13"* em hexadecimal, portanto, devemos convertê-lo para uma das letras correspondentes: A=10, B=11, C=12, D=13, E=14, F=15.
7. Finalmente, o número *111010010* convertido para hexadecimal seria *1 D 2*.

Eis um exercício rápido, apenas para sedimentar o que foi visto aqui. Suponhamos que eu deseje ativar os bits 0, 2, 7, 9, 11 e 15. Como ficaria o valor do meu registrador?

	1° quadrante				2° quadrante				3° quadrante				4° quadrante			
	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
	8	4	2	1	8	4	2	1	8	4	2	1	8	4	2	1
Valor do Configuration Register **0x**	**8**	0	0	0	**8**	0	**2**	0	**8**	0	0	0	0	**4**	0	**1**
Número do bit	**15**	14	13	12	**11**	10	**9**	8	**7**	6	5	4	3	**2**	1	**0**
Notação binária	**1**	0	0	0	**1**	0	**1**	0	**1**	0	0	0	0	**1**	0	**1**

Usando o mesmo esquema já apresentado, fica fácil visualizar. O novo valor seria:

No primeiro quadrante, temos apenas *8*. No segundo, 8 + 2 = *10*. O número 10 em notação hexadecimal seria "*A*". No terceiro quadrante temos apenas *8*, e finalmente, no último quadrante temos 4 + 1 = *5*. Portanto, nosso registrador ficaria 0x*8A85*.

8.2.1.2 Verificação do Valor do Configuration Register

Você pode checar o valor em uso do *configuration register* através do comando *show version*, conforme ilustrado a seguir. A última informação (em destaque) é o valor do *configuration register* ativo. Nesse exemplo, o valor é *0x2102*, que é o valor default. Note também que a saída do comando *show version* nos informa a versão do sistema IOS em uso (12.3(8)T6, no caso).

```
Router>sh ver
Cisco IOS Software, 1841 Software (C1841-SPSERVICESK9-M),
Version 12.3(8)T6, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Tue 28-Dec-04 14:48 by hqluong

[...]

Configuration register is 0x2102
```

8.2.1.3 Alterando o Configuration Register

Você pode alterar o valor do *configuration register* para modificar parâmetros que estabelecem como o router inicializa e opera, como segue:

- Colocar o sistema para Modo Monitor;
- Selecionar uma fonte para inicialização e um nome de arquivo boot default;
- Habilitar e desabilitar o recurso <*BREAK*>;

- Controlar endereços de *broadcast*;
- Definir a velocidade (*baud rate*) da linha Console;
- Carregar o sistema IOS da ROM;
- Habilitar inicialização via servidor TFTP.

Nota: *Antes de alterar os valores do configuration register, certifique-se de que a configuração atual esteja anotada. Use o comando show version para obter essa informação.*

Para alterar o valor do *configuration register*, utilize o comando *config-register*. No exemplo a seguir, os comandos digitados informam ao router para inicializar no modo *ROM MONITOR*. Em seguida, o valor do *configuration register* (que apenas terá efeito após reinicialização do router) é apresentado:

```
Router>en
Router#config t
Router(config)#config-register 0x0101
Router(config)#^Z

Router#sh ver
Cisco IOS Software, 1841 Software (C1841-SPSERVICESK9-M),
Version 12.3(8)T6, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Tue 28-Dec-04 14:48 by hqluong

[...]

Configuration register is 0x2102 (will be 0x0101 at next reload)
```

8.3 Recuperação de Senhas

Como o procedimento para recuperação de senhas pode variar levemente de um modelo de roteador para outro, ilustraremos aqui os procedimentos para dois modelos bastante comuns. O importante aqui é lembrar-se de que, mudando o valor do registrador para *0x2142*, você faz com que o router ignore totalmente a configuração gravada na NVRAM. Lembre-se disso, pois pode ser cobrado no exame!

8.3.1 Routers da Série 2600 e de Outras Séries Mais Novas

Desligue o router, ligue-o novamente e pressione a tecla *Break* (*Ctrl* + *C* ou *Ctrl* + *Break*) nos 60 segundos iniciais.

No prompt apresentado (algo como *rommon>*), digite o comando *confreg 0x2142*, que fará com que o router **ignore a configuração na NVRAM,** indo direto para a RAM.

Digite o comando *reset* para reinicializar o router. Como nenhum arquivo de configuração encontra-se armazenado na RAM, o router começará do zero (*setup mode*). Opte por não entrar no modo *setup* e, uma vez no modo de comando, digite *enable* para entrar em modo privilegiado. Nesse ponto, você tem duas opções: se a senha perdida for a *enable*, basta digitar o comando *show startup-config* e identificar a senha na saída apresentada, uma vez que ela não é criptografada. Se esse for o caso, anote a senha, **mude o registrador de volta para o valor original**, reinicie o router e pronto. Caso você tenha configurado a senha *enable secret*, isso não resolverá, uma vez que essa senha é criptografada. Nesse caso, copie a configuração da NVRAM para a RAM (*copy start run*), entre no modo de configuração global (*config t*) e **defina uma nova senha *enable secret***. Mude, então, o registrador para o valor inicial (para procurar a configuração na NVRAM), **copie a configuração da RAM para a NVRAM** (*copy run start*), reinicie o router e pronto.

8.3.2 Routers da Série 2500 e Mais Antigos

Para routers da série 2500, os procedimentos para recuperação de senha são muito parecidos com os descritos anteriormente, com algumas exceções:

Na linha 2500, ao se efetuar o *Break*, deve-se, no prompt apresentado (algo como > somente) digitar o comando *o*. Feito isso, um menu será apresentado na tela listando as opções para configuração do *configuration register*. Para alterar a configuração, utilize o comando *o/r*, seguido do novo valor:

```
>o/r 0x2142
```

Após alterado o valor do *configuration register*, utilize o comando *i* para reinicializar o router. A partir desse ponto, os passos a seguir são exatamente os mesmos descritos para a linha 2600.

Não se esqueça de configurar o *configuration register* com o valor original após os procedimentos para recuperação de senha terem sido efetuados. Do contrário, o router pode não funcionar a contento.

***Nota**: Apesar de muitos dizerem o contrário, é possível a recuperação de senhas dos switches da série Catalyst 1900. Para tal, basta desligar o seu cabo de força e religá-lo pressionando a*

tecla MODE por 2 segundos. No menu que lhe será apresentado, selecione [S] System debug interface e, em seguida, [F] Return system to factory defaults. O único problema: todas as configurações serão perdidas.

8.4 Procedimentos de Backup e Recuperação do Sistema IOS

Antes de efetuar um upgrade no sistema IOS, uma cópia da versão atual deve ser feita caso existam problemas com a imagem a ser instalada. Normalmente, *backups* são feitos em *servidores TFTP*. Por default, o sistema IOS encontra-se armazenado na FLASH do router. Descreveremos neste capítulo como analisar a quantidade de memória disponível na FLASH, os procedimentos para copiar o sistema IOS da FLASH para um servidor TFTP e, finalmente, como recuperar o sistema IOS de um servidor TFTP para a FLASH.

Antes de efetuar um upgrade no IOS de um router, devemos nos certificar de que há espaço suficiente na FLASH dele para tal operação. Você pode verificar a quantidade de memória disponível na FLASH, assim como os arquivos armazenados nela através do comando *show flash*:

```
Router#sh flash

System flash directory:
File  Length    Name/status
  1   8121064   c2500-js-l.112-18.bin
[8121064 bytes used, 8656152 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)
```

Note que o nome do arquivo, no exemplo anterior, é c2500-js-l.112-18.bin. O nome do arquivo é específico para cada plataforma e tem o seguinte significado:

- **c2500**: Indica a plataforma;
- **j**: Indica que o arquivo é uma *enterprise image* (versão corporativa);
- **s**: Indica que o arquivo contém capabilidades estendidas;
- **l**: Indica que o arquivo pode ser movido da FLASH se necessário e que ele não se encontra comprimido;
- **112.18**: Número de versão/revisão do arquivo (versão 11.2, revisão 18);
- **.bin**: Indica que o Cisco IOS é um binário executável.

A última linha da saída apresentada indica que se trata de uma FLASH com capacidade de 16MB (16.384KB). Portanto, se o arquivo que você deseja copiar para ela tem, vamos supor, um tamanho de 10MB, você saberia que há espaço suficiente para ele. Uma vez verificado que a FLASH possui espaço suficiente para acomodar a nova imagem a ser copiada, o processo de backup pode prosseguir.

Para copiar o sistema IOS para um host TFTP, utilize o comando *copy flash tftp*. Os únicos dados que lhe serão pedidos são: nome do arquivo fonte e endereço IP do host TFTP.

Antes de iniciar a operação de backup, é uma boa idéia testar a conexão entre o router e o TFTP host. Isso pode ser feito através do comando *ping*. No exemplo a seguir, ilustramos esse procedimento para um TFTP host com endereço IP 192.168.0.120:

```
Router#ping 192.168.0.120
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.120, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 4/4/8 ms
```

Após certificar-se de que a conectividade entre as pontas é satisfatória, efetue o processo de backup utilizando o comando *copy flash tftp*, conforme ilustrado a seguir. Note que, logo após a digitação do comando, o nome do arquivo armazenado na FLASH é apresentado, facilitando as coisas para você. Você pode, simplesmente, copiar o nome do arquivo apresentado e colá-lo quando requisitado.

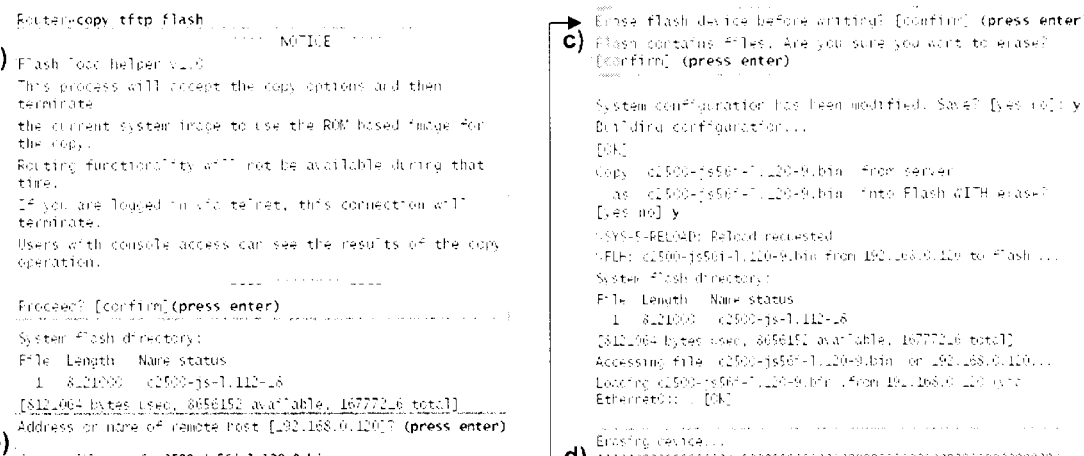
Lembre-se: *Source file name = nome do arquivo apresentado após a digitação do comando;*
Address of remote host = endereço IP do servidor TFTP

O comando *copy flash tftp* não pede que você entre com a localização de qualquer arquivo ou que você escolha onde colocar o arquivo copiado. Ele simplesmente transfere o arquivo para um diretório padrão no servidor TFTP. Caso esse diretório não exista, o processo não será concluído com sucesso.

```
Router#copy flash tftp
System flash directory:
File Length  Name/status
1    8121000 c2500-js-l.112-18.bin
[8121064 bytes used, 8656152 available, 16777216 total]
```

```
Address or name of remote host [255.255.255.255]?192.168.0.120
Source file name?c2500-js-l.112-18.bin
Destination file name [c2500-js-l.112-18.bin]?[Enter]
Verifying checksum for 'c2500-js-l.112-18.bin')file #1)
...OK
Copy '/c2500-js-l.112-18' from Flash to server
as '/c2500-js-l.112-18'? [yes/no]y
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!! [output cut]
Upload to server done
Flash copy took 00:02:30 [hh:mm:ss]
Router#
```

8.5 Recuperação de uma Imagem IOS Armazenada em um Servidor TFTP



Você pode precisar recuperar um arquivo IOS armazenado em um host TFTP para a FLASH, para substituir um arquivo que tenha sido corrompido ou para substituir a versão presente na FLASH por uma mais nova. Para recuperar um arquivo armazenado em um TFTP host, utilize o comando *copy tftp flash*. Você será prontificado a fornecer o endereço IP do servidor TFTP e o nome do arquivo que você deseja copiar para a FLASH (b).

Antes de iniciar o processo, certifique-se de que o arquivo que você deseja copiar para a FLASH se encontra no diretório default do servidor TFTP. Uma vez executado o comando, o servidor TFTP não irá perguntar onde o arquivo se encontra. Se o arquivo que você deseja copiar para a FLASH não estiver no diretório default do host TFTP, o processo não irá funcionar.

Uma vez executado o comando, uma mensagem surgirá na tela (a) informando que o router irá reinicializar e utilizar o IOS presente na ROM para efetuar essa operação.

O próximo passo é informar o endereço IP do servidor TFTP e o nome do arquivo a ser copiado (b). Uma vez que o router já tenha utilizado um servidor FTP, ele "lembrará" do seu endereço IP (b).

Uma vez informados os dados requisitados, o router irá pedir que você confirme o entendimento de que o conteúdo da memória FLASH será apagado durante o processo (c).

Uma vez confirmado, o router irá reiniciar e carregar uma versão simplificada do IOS presente na ROM, já que o IOS da FLASH não pode ser alterado se estiver em uso. Feito isso, o conteúdo da FLASH é apagado e o arquivo presente no servidor TFTP host é copiado para a FLASH. A fileira de *"e"*s indica que o conteúdo da FLASH está sendo apagado (d). Cada ponto de exclamação (*!*) indica que um segmento UDP foi transferido com sucesso (d).

Uma vez completada a operação, a seguinte mensagem deve ser apresentada:

```
[OK - 10935532/16777216 bytes]
Verifying checksum... OK (0x2E3A)
Flash copy took 0:06:14 [hh:mm:ss]
%FLH: Re-booting system after download
```

Uma vez que o novo arquivo tenha sido copiado para a FLASH e que a checagem de erro (*checksum*) tenha ocorrido sem problemas, o router é reiniciado para que o novo IOS seja executado.

***Nota**: Routers Cisco podem ser configurados para agir como servidores TFTP para uma imagem do IOS que esteja armazenada em sua FLASH. O comando que permite isso é: (config)# tftp-server system [nome-do-arquivo-IOS].*

8.6 Procedimento de Backup dos Arquivos de Configuração (Startup-config e Running-config)

Qualquer mudança que você efetua na configuração de um router fica armazenada no arquivo *running-config*, que é a configuração ativa, armazenada na RAM. Caso você não execute o comando *copy run start*, toda a configuração será perdida caso o router seja desligado ou reiniciado. Você pode desejar efetuar um backup adicional do seu arquivo de configuração, na eventualidade de o router "pifar" de vez

ou apenas para documentação. Descreveremos, a seguir, como proceder para copiar a configuração ativa para a NVRAM e para um host TFTP e como recuperar essa configuração.

Para verificar a configuração ativa (*running-config*), utilize o comando *sh run*. Esse comando informa, entre outras coisas, a versão do IOS ativa no router.

Para verificar a configuração armazenada na NVRAM (*startup-config*), utilize o comando *sh start*. Entre as informações apresentadas, você obterá o espaço de memória utilizado pelo arquivo. Se você não tem certeza se os arquivos *running-config* e *startup-config* são os mesmos e é o *running-config* que você deseja utilizar e manter, utilize o comando *copy run start* para copiá-lo da RAM para a NVRAM. Dessa forma, na próxima vez que o router for inicializado, essa será a configuração carregada.

Nota: *O comando write (ou simplesmente wr) também pode ser utilizado para essa função.*

Você pode copiar a configuração ativa para um servidor TFTP, como um segundo backup da *running-config*. Para tal, utilize o comando *copy run tftp*. Conforme discutido nas páginas anteriores, duas informações lhe serão pedidas: o endereço IP do servidor TFTP e o nome do arquivo destino (*destination filename*). Para nome do arquivo, qualquer nome pode ser escolhido, desde que o router não tenha um *hostname* configurado. Caso tenha, o nome do arquivo será, automaticamente, o nome do router (*hostname*) acrescido da extensão *-confg*.

Para ativar a configuração armazenada na NVRAM, utilize o comando *copy start run*. O conteúdo da NVRAM (*startup-config*) será copiado para a RAM, **substituindo a *running-config* anteriormente utilizada**. Um comando mais antigo também pode ser utilizado para executar essa operação: *config mem*.

Para recuperar uma configuração copiada para um TFTP host, utilize o comando *copy tftp run* (para copiar para a RAM) ou *copy tftp start* (para copiar para a NVRAM). Um comando mais antigo que também pode ser utilizado para executar essa operação é o *config net* (equivalente ao comando *copy tftp run*).

Para apagar a configuração armazenada na NVRAM (*startup-config*), utilize o comando *erase start*. Esse comando apaga a *startup-config*, ou seja, na próxima vez em que o router inicializar, ele irá para o modo *setup*.

8.7 O Protocolo CDP (Cisco Discovery Protocol)

O protocolo CDP foi criado pela Cisco para ajudar administradores de rede na coleta de informações sobre dispositivos local e remotamente conectados.

8.7.1 Obtenção dos Valores dos Timers CDP e Informações sobre Holdtime

O comando *show cdp* apresenta informações sobre dois parâmetros globais CDP que podem ser configurados em dispositivos Cisco:

- **CDP Timer**: Registra a freqüência com a qual pacotes CDP são transmitidos para todas as interfaces ativas;
- **CDP Holdtime**: Registra a quantidade de tempo que um dispositivo deve reter pacotes recebidos de dispositivos vizinhos.

Tanto routers quanto switches Cisco utilizam esses parâmetros. A saída em um router é ilustrada a seguir:

```
Router#sh cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
```

Você pode utilizar os comandos (config)#*cdp timer [valor]* e (config)#*cdp holdtime [valor]* para configurar esses parâmetros globalmente em um router e pode ativar e desativar o protocolo CDP globalmente ou em interfaces específicas através dos comandos *cdp enable* e *no cdp enable*. Veremos como fazer isso mais adiante.

O comando *sh cdp neighbor* (*sh cdp nei*) apresenta informações sobre dispositivos diretamente conectados. É importante lembrar que pacotes CDP **não atravessam um switch Cisco** e que você apenas vê aquilo que se encontra **diretamente conectado**. No caso de o comando ser digitado em um router que se encontra conectado a um switch, você não obterá informações sobre os dispositivos conectados ao switch, apenas sobre o switch em si e sobre os outros dispositivos que estejam diretamente conectados ao router em questão.

A figura 8.3 ilustra uma saída do comando *sh cdp nei* executado em um switch Catalyst modelo 1924-EN. A tabela 8.1 sumariza as informações obtidas através do comando *sh cdp nei* para cada dispositivo.

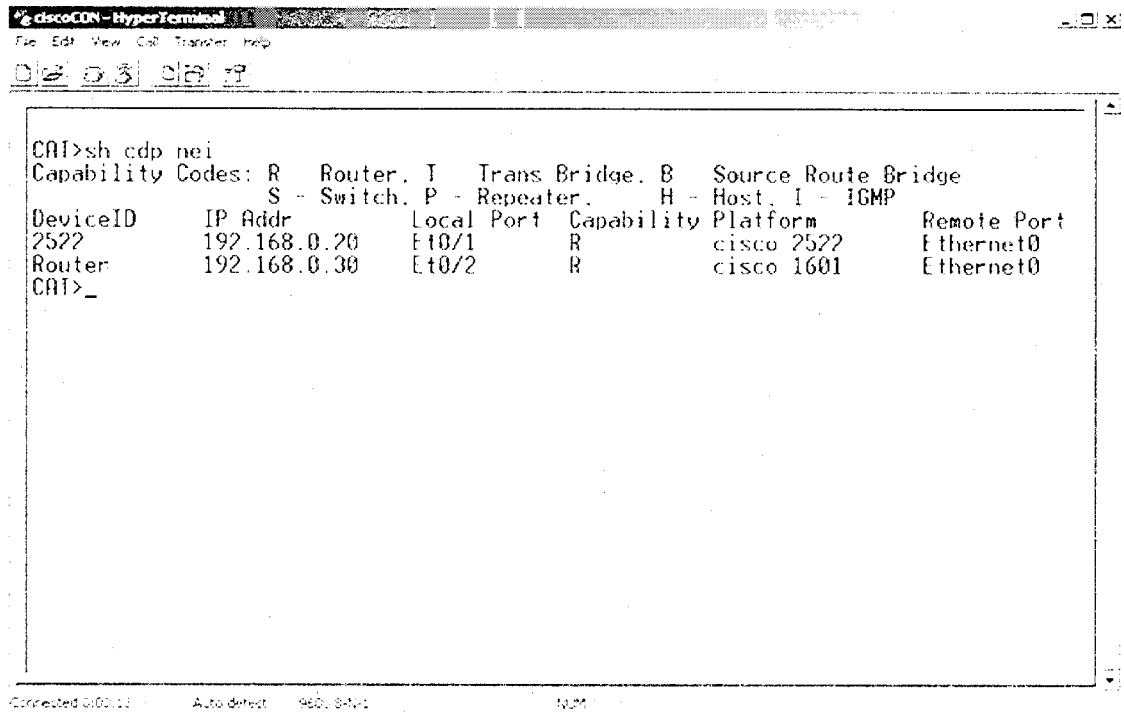


Figura 8.3: Exemplo de saída do comando sh cdp neighbors.

Campo	Descrição
Device ID	O nome (hostname) do dispositivo diretamente conectado
IP Addr	Endereço IP da porta do dispositivo vizinho
Local Port	A porta local na qual os pacotes CDP estão sendo recebidos
Holdtime	Tempo que o router deve reter os pacotes recebidos pelos dispositivos vizinhos antes de descartá-los
Capability	O tipo de dispositivo vizinho (ex.: router, switch etc.)
Platform	Identifica a série ou o modelo do dispositivo conectado (ex.: Cisco 2522)
Remote Port	A porta ou interface do dispositivo vizinho

Tabela 8.1: Sumário das informações obtidas na Figura 8.1.

Outro comando utilizado para reunir informações sobre dispositivos vizinhos é o *sh cdp nei detail* (*sh cdp nei de*), que também pode ser executado em um router ou switch. Esse comando exibe informações detalhadas sobre cada dispositivo conectado ao dispositivo em questão (um switch 1924, no caso). Entre as informações obtidas na saída desse comando - em adição às obtidas através do comando *sh cdp nei* - estão:

- *Hostname* e endereço IP de dispositivos diretamente conectados;
- Versão do sistema IOS em atividade no dispositivo vizinho.

Nota: *O comando sh cdp entry * apresenta exatamente as mesmas informações obtidas através do comando sh cdp nei de.*

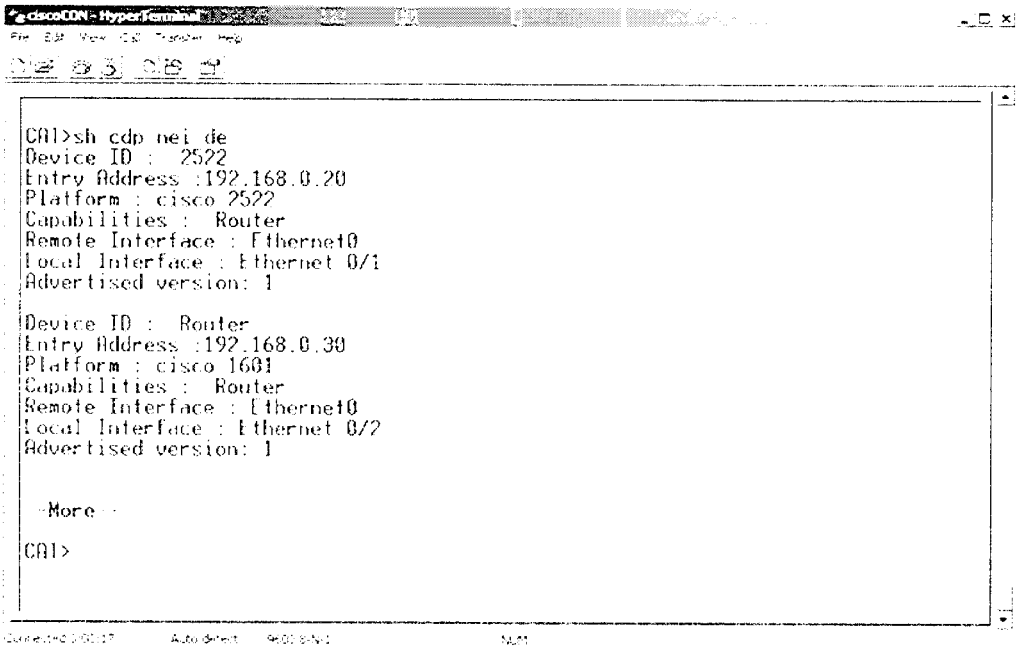


Figura 8.4: Exemplo de saída do comando sh cdp neighbors detail.

8.7.2 Obtenção de Informações sobre o Tráfego de Dados em Interfaces via CDP

O comando *sh cdp traffic* apresenta informações sobre o tráfego de dados em interfaces, incluindo o número de pacotes CDP enviados e recebidos e estatísticas sobre erros relacionados ao CDP.

O comando *sh cdp interface* (*sh cdp int*) apresenta o *status* do CDP nas interfaces de um router ou nas portas de um switch. Conforme mencionado anteriormente, é possível desativar completamente o recurso CDP através do comando *no cdp enable*. Outro comando que pode ser usado para esse fim é o *no cdp run*. Para habilitar CDP em portas ou interfaces específicas, utilize o comando *cdp enable*. **Todas as portas e interfaces têm, como default, o CDP habilitado.** Em um router, o comando *sh cdp int* apresenta informações sobre cada interface utilizando CDP, incluindo o encapsulamento utilizado e os valores do timer e do holdtime para cada interface.

Para desativar o CDP em uma interface específica de um router, utilize o comando *no cdp enable*, no modo de configuração de interface (*config-if*).

Verifique a desativação utilizando o comando *sh cdp int*. A interface para a qual o protocolo CDP foi desativado não deve constar na saída desse comando.

8.8 Configuração do Telnet (Terminal Virtual)

Telnet é um protocolo de terminal virtual, parte do conjunto de protocolos TCP/IP. Ele permite que você se conecte a dispositivos remotos, reúna informações sobre eles, configure-os e rode aplicações.

Uma vez que seus routers e switches encontrem-se configurados, você pode utilizar um programa Telnet para checagem de configuração e para configuração deles sem a necessidade do uso de cabos de console.

Para executar um programa Telnet, normalmente basta que se digite *telnet* no prompt de comando em qualquer ambiente CLI (DOS, UNIX, IOS). Entretanto, para acessar routers através desse recurso, **senhas VTY (portas virtuais) devem estar configuradas neles**.

Você não pode utilizar o CDP para reunir informações sobre dispositivos que não estejam diretamente conectados ao seu dispositivo. Entretanto, o Telnet pode ser utilizado para esse fim. Você pode se conectar a um dispositivo remoto utilizando Telnet e rodar, remotamente, comandos CDP nesse dispositivo para reunir informações sobre os dispositivos diretamente conectados a ele.

Lembre-se de que **as portas VTY em um router são configuradas por default como *login***, o que significa que **você deve ou definir uma senha para a porta VTY** ou desabilitar o comando *login* na porta VTY através do comando *no login*.

Em um router Cisco, o comando Telnet não precisa ser utilizado. Uma vez que você saiba o endereço IP do dispositivo-alvo, basta digitá-lo diretamente no prompt do IOS para que a sessão Telnet seja inicializada.

Vamos agora definir uma senha VTY para um router para que uma conexão possa ser estabelecida via Telnet. A imagem a seguir ilustra como proceder.

```
2501B#config t
Enter configuration commands, one per line. End with
CNTL/Z.
2501B(config)#line vty 0 4
2501B(config-line)#login
2501B(config-line)#password netceptions
2501B(config-line)#^Z
2501B#
%SYS-5-CONFIG_I: Configured from console by console
```

Lembre-se de que a senha VTY é uma **senha de modo usuário**. Caso você tente entrar em modo privilegiado (comando *enable*) no prompt do dispositivo remotamente conectado, o seguinte ocorrerá:

```
2501B>en
%No password set
2501B>
```

Isso é um bom recurso. Você não gostaria que qualquer pessoa se conectasse remotamente via Telnet a seu router e, depois, simplesmente digitasse *enable* e acessasse o modo privilegiado.

A senha *enable* ou *enable secret* deve estar configurada no dispositivo-alvo para que ele possa ser remotamente configurado. No caso de nenhuma senha de modo privilegiado encontrar-se configurada, a mensagem de erro ilustrada anteriormente será apresentada.

***Importante**: Para se conectar remotamente a múltiplos dispositivos simultaneamente, utilize a combinação de teclas Ctrl+Shift+6 e logo após, pressione "x" após encontrar-se em modo usuário no dispositivo remoto. Fazendo isso, você terá o prompt de seu router de volta na tela, permitindo que outra sessão Telnet seja iniciada e, assim, sucessivamente.*

8.8.1 Monitorando Conexões Telnet

```
a) 2501B#sh sessions
   Conn Host           Address         Byte    Idle    Conn Name
      1 172.16.10.2    172.16.10.2      0        0     172.16.10.2
    * 2 192.168.0.148  192.168.0.148    0        0     192.168.0.148
b) 2501B#sh users
       Line      User   Host(s)                  Idle  Location
    * 0 con 0          172.16.10.2          00:07:52
                       192.168.0.148        00:07:18
c) 2501B#disconnect
    <1-2>  The number of an active network connection
    WORD   The name of an active network connection
    <cr>
```

Para checar conexões realizadas do seu router para dispositivos remotos, utilize o comando *sh sessions* (a). Note o asterisco (*) ao lado da conexão 2. Isso significa que essa foi a última a ser estabelecida. Você pode retornar à sua última sessão pressionando *Enter* duas vezes seguidas. Outro modo de se retornar à conexão desejada é digitando-se o seu número e pressionando *Enter*.

Para listar todos os consoles ativos e portas VTY em uso no seu router, utilize o comando *sh users* (b). O "con" na saída ilustrada representa a console local. No exemplo anterior, a console encontra-se conectada a dois dispositivos (endereços IPs apresentados).

Para encerrar uma sessão Telnet (c), meios diferentes podem ser utilizados. Digitar o comando *exit* ou *disconnect* talvez seja o mais simples

de todos. Usando o comando *disconnect*, você pode especificar qual sessão deseja encerrar informando o seu número como atributo.

Caso você deseje encerrar uma sessão Telnet de um dispositivo conectado ao seu router, primeiro certifique-se de quais dispositivos encontram-se conectados através do comando *sh users*. Identifique qual porta (*line*) (veja exemplo b) da saída apresentada possui a conexão que você deseja encerrar. Identificado o número da porta (*line*), utilize o comando *clear line [número da porta]*. Certifique-se de que a conexão foi desfeita através do comando *sh users*.

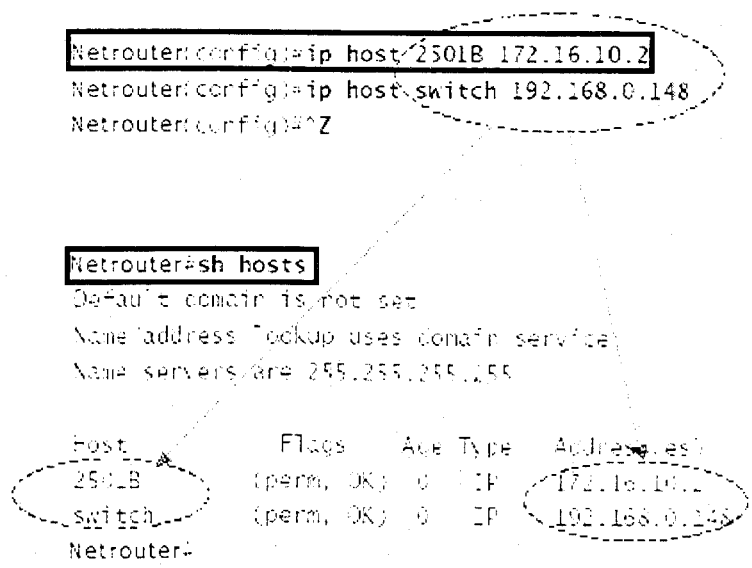
8.9 Resolução de Hostnames

Para utilizar um nome (*hostname*) no lugar de um endereço IP para se conectar a um dispositivo remoto, o dispositivo que você está utilizando para efetuar essa conexão deve ser capaz de traduzir, ou melhor, mapear esse nome para um endereço IP (façamos uma analogia ao modo de endereçamento da Web, como conhecemos hoje).

Existem dois modos para mapear nomes para endereços IPs: criando manualmente uma tabela de nomes (chamada de *host table*) ou criando um servidor de mapeamento de nomes (DNS - *Domain Name Server*), o que seria o equivalente a uma tabela de nomes dinâmica.

A *host table* irá prover o mapeamento de nomes para IP **apenas no router onde ela se encontra**. A sintaxe do comando a ser usada na criação de uma *host table* em um router é a seguinte:

```
ip host [nome] [porta_tcp] [endereço_ip]
```



A porta default é a 23 (*Telnet*). Na figura anterior ilustramos um exemplo de como o comando deve ser utilizado. No exemplo, foi feita a configuração da *host table* com duas entradas, para o mapeamento dos nomes do router 2501B e do switch.

Para ver a tabela formada, utilize o comando *sh hosts*. Na figura ilustramos a saída desse comando. O termo *perm* que aparece na coluna *Flags* significa que os dados apresentados foram manualmente adicionados. Caso o termo encontrado nessa coluna fosse *temp*, os dados teriam sido adicionados à tabela através de um servidor DNS.

Para testar a funcionalidade da tabela apresentada, tente digitar apenas o nome do dispositivo remoto no prompt do IOS. Caso a conexão seja estabelecida, a tabela torna-se operacional.

Para remover uma entrada da tabela *host* (*host table*), utilize o comando *no ip host [nome]*. O problema com esse método é que os nomes e endereços IPs correspondentes precisam ser manualmente adicionados à tabela. Se houver muitos dispositivos para os quais você deseje ter seus nomes mapeados, utilizar o método DNS pode ser muito mais produtivo.

Se você possui muitos dispositivos a serem mapeados, utilize um servidor DNS para o mapeamento de nomes. Toda vez que um dispositivo Cisco recebe um comando inválido para o IOS, ele tenta resolver o comando (ou nome) digitado através do DNS (procedimento default). Eis o que acontece quando um comando não reconhecido é digitado:

```
Router#nomequalquer
Translating "nomequalquer"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find
computer address
router#
```

Você pode desabilitar o procedimento de resolução padrão através do comando *no ip domain-lookup*, que deve ser digitado no modo de configuração global.

Caso você tenha, de fato, um servidor DNS operando em sua rede, alguns comandos devem ser digitados para que a resolução de nomes via servidor DNS funcione de acordo:

- **ip domain-lookup:** Esse comando encontra-se ativo, por default;
- **ip name-server**: Utilizado para definir o endereço IP do servidor DNS;
- **ip domain-name**: Opcional, mas sua utilização é recomendada. Acrescenta o nome do domínio ao nome digitado. Uma vez que o DNS é um sistema de domínios totalmente qualificados (*Fully Qualified Domain Name System*), é aconselhável a adoção de nomes DNS completos, no estilo *domínio.com*.

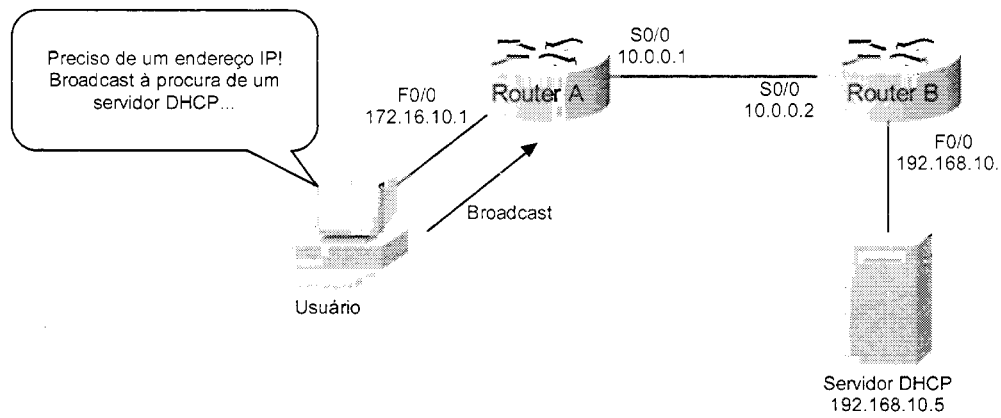
Uma vez que a configuração DNS esteja OK, sua funcionalidade pode ser testada através dos comandos *ping*, *trace* e *telnet*. Se você

conseguir "pingar" um dispositivo utilizando seu nome no lugar de seu endereço IP, sua configuração DNS está funcionando.

Utilize o comando *sh hosts* para visualizar a *host table* atualizada.

8.9.1 Configurando Routers para Lidar com Broadcasts e Multicasts

Pode ocorrer que um host em uma determinada rede necessite acessar um servidor DHCP localizado em uma rede remota. O problema quando isso ocorre é que o host usa *broadcasts* para identificar o servidor DHCP na rede, e se este não estiver na rede local, esse *broadcast* será direcionado ao router - e routers não propagam *broadcasts* por definição. Para resolver esse problema, podemos forçar o router a encaminhar qualquer mensagem *broadcast* (ou *multicast*) para um ou mais destinos específicos através do uso do comando *ip helper*, configurado na interface local. Vamos supor que nosso servidor DHCP tenha o endereço IP 192.168.10.5:



A configuração do *IP Helper* no router "A" ficaria assim:

```
RouterA#config t
RouterA(config)#int f0/0
RouterA(config-if)#ip helper-address 192.168.10.5
```

Desnecessário dizer que, para que isso funcione, a rede 192.168.10.0 deve estar presente na tabela de roteamento do RouterA (do contrário, ele descartará o pacote).

8.10 Configuração do Serviço DHCP em um Roteador Cisco

Embora existam diversas soluções de mercado para serviços DHCP bem mais robustas, o serviço de servidor DHCP embutido no Cisco IOS é bastante

útil em ambientes SOHO e em redes de pequeno porte que dependem de somente um roteador para a conexão com a Internet ou com a matriz.

Como já vimos, o papel do DHCP na rede é atribuir endereços IP automaticamente às estações de trabalho (ou outros dispositivos). Além de atribuir dinamicamente endereços IP, o DHCP pode também configurar uma gama de parâmetros TCP/IP nestas estações, como os endereços dos servidores DNS, endereço do default gateway da rede, *WINS servers*, dentre outros.

Configurar um roteador Cisco para que ele funcione como um servidor DHCP é bastante simples.

1. Certifique-se que a porta que se conecta à rede local (LAN) esteja devidamente configurada e ativada, e inicie o serviço DHCP no router:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# service dhcp
```

2. Crie o *pool* onde será especificado os endereços IP que você deseja distribuir para os hosts em sua rede:

```
Router(config)# ip dhcp pool meupooldeenderecos
```

3. Especifique os endereços que serão disponibilizados para os hosts:

```
Router(dhcp-config)# network 192.168.10.0 /24
```

4. Especifique o domínio a ser configurado nos hosts:

```
Router(dhcp-config)#domain-name nomedodominio.com
```

5. Especifique os servidores DNS (até 8 endereços podem ser configurados):

```
Router(dhcp-config)#dns-server 192.168.10.2 192.168.10.3
```

6. Especifique o endereço do default gateway da rede (até 8 endereços podem ser configurados):

```
Router(dhcp-config)#default-router 192.168.10.1 (endereço do
próprio router, no caso)
```

7. Especifique o tempo de duração do *lease*, ou seja, quanto tempo o host pode ficar com o endereço antes de rechecar com o DHCP:

```
Router(dhcp-config)#lease 7 (tempo em dias, no exemplo)
```

8. Exclua os endereços IP que não devem ser oferecidos aos hosts. No exemplo abaixo, os IPs 192.168.10.1 até 192.168.10.10 não serão oferecidos aos hosts pelo DHCP.

```
Router(config)# ip dhcp excluded-address 192.168.10.1
192.168.10.10
```

E pronto! Seu router agora responderá às solicitações DHCP de hosts na rede, e estes hosts receberão um endereço IP que pode ir de 192.168.10.11 até 192.168.10.254.

8.10.1 Monitorando o DHCP

Os seguintes comandos possibilitam o gerenciamento do serviço DHCP em um router Cisco:

- **show ip dhcp binding:** Lista os IPs já fornecidos para as estações de trabalho;
- **show ip dhcp conflict:** Lista eventuais conflitos de endereços IP;
- **show ip dhcp database:** Lista o DHCP database;
- **show ip dhcp pool:** Lista todo o conteúdo dos *pools* configurados;
- **show ip dhcp relay information trusted-sources:** Lista as informações sobre o *relay* DHCP;
- **show ip dhcp server statistics:** Mostra as estatísticas do tráfego DHCP.

Em caso de problemas, as seguintes opções para debugging estão disponíveis:

- **debug ip dhcp server events:** Muito útil para mostrar os "empréstimos" e *expirations* dos endereços IP;
- **debug ip dhcp server linkage:** Serve para diagnosticar eventos em situações onde existam relações entre dois ou mais servidores DHCP (esquema *parent/child*, tais como *radix tree*);
- **debug ip dhcp server packet:** Mostra o tráfego DHCP em tempo real.

Questões de Revisão – Gerenciamento de uma Rede Cisco

1. Qual comando apresenta o nome do host resolvido para um endereço IP em um roteador?

a) sh router
b) sho hosts
c) sh ip hosts
d) sho name resolution

2. Qual comando faz um backup da imagem do sistema (IOS) para um servidor TFTP?

a) transfer IOS to 172.16.10.1
b) copy run start
c) copy tftp flash
d) copy run tftp
e) copy flash tftp

3. Qual comando busca uma configuração armazenada em um servidor TFTP para a NVRAM do roteador?

a) transfer IOS to 172.16.10.1
b) copy run start
c) copy tftp startup
d) copy tftp run
e) copy flash tftp

4. Para restaurar a configuração existente em um host TFTP para a DRAM de um roteador Cisco na sua rede, quais os dois comandos que podem ser utilizados?

a) config netw
b) config mem
c) config term
d) copy tftp run
e) copy tftp start

5. Qual o nome da memória responsável pelo armazenamento dos buffers de pacotes e das tabelas de roteamento?

a) Flash b) RAM c) ROM d) NVRAM

6. Qual dos seguintes comandos cria uma tabela de nomes mapeados para IP em um roteador Cisco?

a) bob ip host 172.16.10.1
b) host 172.16.10.1 bob
c) ip host bob 172.16.10.1
d) host bob 172.16.10.1

7. Qual comando apresenta as conexões estabelecidas do seu roteador para um dispositivo remoto?

a) sh sess
b) sh users
c) disconnect
d) clear line

8. Qual comando apresenta as interfaces habilitadas para CDP num roteador?

a) sh cdp
b) sh cdp interface
c) sh interface
d) sh cdp traffic

9. Quais os valores default para os timers update e holdtime do CDP
   a) 240, 90 b) 90, 240 c) 180, 60 d) 60, 180

10. Para realizar uma cópia da configuração presente na DRAM d um roteador Cisco para um servidor TFTP na rede, qual comando pod ser usado?
   a) config netw c) config term e) copy start tftp
   b) config mem d) copy run tftp

11. Para alternar entre várias sessões abertas simultaneamente, qua combinação de teclas pode ser usada?
   a) Tab+"espaço"
   b) Ctrl+X, seguido da tecla "6"
   c) Ctrl+Shift+X, seguido da tecla "6"
   d) Ctrl+Shift+6, seguido da tecla "X"

12. Qual dos seguintes comandos possui exatamente a mesma funçã do comando show cdp neighbors detail?
   a) show cdp c) sh cdp neigh
   b) show cdp ? d) sh cdp entry *

13. O que o comando [Router(config)#cdp timer 90] faz?
   a) Mostra a freqüência de atualização dos pacotes CDP.
   b) Altera a freqüência de atualização dos pacotes CDP.
   c) Desativa o CDP em 90 segundos.
   d) Muda o valor do holdtime dos pacotes CDP.

14. Qual comando desabilita o CDP em uma determinada interface?
   a) no cdp run c) no cdp
   b) no cdp enable d) disable cdp

15. Qual comando é usado para mapear o caminho percorrido por um pacote através de uma rede?
   a) ping b) trace c) RIP d) SAP

16. Quais comandos podem ser utilizados com o objetivo de testar conectividade IP em uma rede?
   a) ping b) trace c) RIP d) telnet

17. Qual comando finaliza uma sessão com um dispositivo remoto?
   a) clear connection c) disconnect
   b) clear line d) clear user

18. Qual comando finaliza uma sessão estabelecida de um dispositivo remoto para o seu roteador?

a) clear connection
b) clear line #
c) disconnect
d) clear user

19. Quais das seguintes informações são apresentadas pelo comando show cdp neighbor?

a) Endereço MAC do dispositivo vizinho.
b) Descrição da porta/interface local.
c) As mesmas informações apresentadas pelo comando show version.
d) Características do dispositivo remoto.
e) As mesmas informações apresentadas pelo comando show cdp entry *.
f) O ID da porta remota .
g) O ID do dispositivo vizinho.
h) O valor do holdtime.
i) A plataforma de hardware do dispositivo vizinho.
j) A velocidade do link até o dispositivo vizinho.

20. Qual comando pode ser usado para carregar um novo IOS para um roteador?

a) copy tftp run
b) copy tftp flash
c) copy tftp start
d) copy flash tftp
e) boot system flash IOS_name

Respostas das Questões de Revisão – Gerenciamento de uma Rede Cisco

1. **B**. O comando que apresenta a tabela host - que mapeia nomes para endereços IPs - é o show host (ou show hosts).

2. **E**. Para fazer um backup do IOS - que se encontra armazenado na memória flash por default - para um servidor TFTP, o comando usado é o copy flash tftp.

3. **C**. Para recuperar uma configuração armazenada em um host TFTP para a NVRAM de um roteador, o comando a ser usado é copy tftp startup-config.

4. **A, D**. Para recuperar uma configuração armazenada em um host TFTP para a DRAM de um roteador, os comandos que podem ser usados são copy tftp running-config ou config net.

5. **B**. A RAM (ou DRAM) é usada para armazenar buffer de pacote e a tabela de roteamento, entre outras coisas.

6. **C**. O comando ip host [hostname] [ip_addresses] é usado par criar uma tabela de resolução de nomes em um roteador Cisco.

7. **A**. O comando show sessions apresenta as sessões ativas estabelecidas a partir do seu roteador.

8. **B**. O comando show cdp interface apresenta o status da interfaces habilitadas para CDP.

9. **D**. O update timer default para pacotes CDP é de 60 segundos Um dispositivo irá reter as informações CDP por 180 segundo (holdtime timer), por default.

10. **D**. Para fazer uma cópia da configuração ativa de um roteado para um servidor TFTP, o comando copy running-config tftp pode ser usadc

11. **D**. Para alternar entre múltiplas sessões abertas simultaneamente a combinação Ctrl+Shift+6 e, depois, "x" pode ser usada.

12. **D**. O comando show cdp entry * e o comando show cdp neighbors detail possuem a mesma função.

13. **B**. O comando cdp timer 90 muda a freqüência de atualização dos pacotes CDP de 60 segundos (default) para 90 segundos.

14. **B**. O comando no cdp enable desabilita o protocolo CDP em uma determinada interface.

15. **B**. O comando trace mostra o caminho que um pacote faz par alcançar uma rede remota usando timeouts ICMP.

16. **A, B, D**. Os comandos ping e trace podem ser utilizados par testar a conectividade IP em uma rede. O telnet vai um passo além, j que testa não apenas a conectividade IP, mas também a comunicação desde a camada de aplicação.

17. **C**. O comando disconnect finaliza uma sessão remota.

18. **B**. O comando clear line [#] encerra uma sessão estabelecid para o roteador em questão.

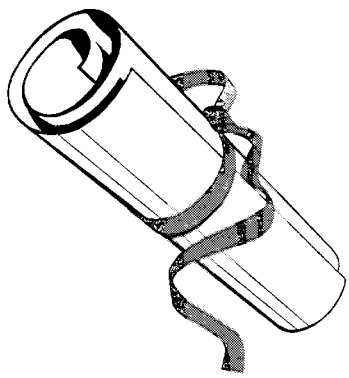
19. **B, D, F, G, H, I**. O comando show cdp neighbor fornece um série de informações: nome da interface local, o hostname do dispositiv local, interface remota usada para envio do CDP, o hostname d dispositivo vizinho, o tempo que os pacotes CDP ficam retido (holdtime) e o tipo de dispositivo.

20. **B**. Para carregar um novo IOS para um roteador, o comand copy tftp flash pode ser usado.

Relação dos Comandos Analisados

Comando	Descrição
cdp enable	Ativa CDP em uma interface específica.
cdp holdtime	Altera a freqüência do *holdtime*.
cdp run	Ativa CDP em um router.
cdp timer	Altera a freqüência do timer do CDP.
clear line	Encerra uma conexão Telnet ao seu router.
config-register	Informa ao router como inicializar e altera a configuração do registro.
copy flash tftp	Copia arquivos da FLASH para um servidor TFTP.
copy run start	Copia a configuração ativa (*running-config*) para a NVRAM (*startup-config*).
copy run tftp	Copia a configuração ativa para um servidor TFTP.
copy tftp flash	Copia um arquivo do servidor TFTP para a FLASH.
copy tftp run	Copia a configuração armazenada no servidor TFTP para a RAM.
Ctrl+Shift+6, depois X	Retorna a tela para a última conexão.
disconnect	Encerra uma conexão a um dispositivo remoto.
erase startup-config	Apaga o conteúdo da NVRAM (*startup-config*) em um router.
exit	Encerra uma conexão a um dispositivo remoto.
Ip domain-lookup	Ativa *DNS lookup*.
Ip domain-name	Adiciona um nome de domínio ao *DNS lookup*.
Ip host	Cria uma tabela host (*host table*) em um router.
Ip name-server	Define o endereço IP para até seis servidores DNS.
No cdp enable	Desativa CDP em uma determinada interface.
No cdp run	Desativa CDP no router.
No ip domain-lookup	Desativa *DNS lookup*.
No ip host	Remove um nome da *host table*.
o/r 0x2142	Altera o modo como um router 2501 inicializa.
show cdp	Apresenta os timers CDP e freqüência do *holdtime*.
show cdp entry *	Apresenta os endereços IPs e versão do IOS, em adição às informações apresentadas pelo comando *sh cdp nei*.
show cdp interface	Apresenta as interfaces com CDP ativo.
show cdp neighbor	Apresenta os dispositivos diretamente conectados e detalhes sobre eles.
show cdp neighbor detail	Mesma função do comando *show cdp entry **.

Comando	Descrição
show cdp traffic	Apresenta os pacotes CDP enviados e recebidos e erros decorrentes.
show flash	Apresenta o conteúdo da FLASH.
show hosts	Apresenta o conteúdo da tabela host.
show run	Apresenta o arquivo de configuração ativo (*running-config*).
show sessions	Apresenta as conexões via Telnet ativas.
show start	Apresenta o arquivo de configuração armazenado na NVRAM (*startup-config*).
show version	Apresenta o tipo e versão do IOS ativo, assim como os valores do registrador (*configuration register*).
tftp-server system ios-name	Cria um servidor TFTP para uma imagem do IOS armazenada na FLASH, para acesso por outros dispositivos.
ip helper-address	Informa um ou mais endereços IPs para onde os broadcasts devem ser encaminhados em forma de unicast.



9 Segurança de Redes

9.1 Tópicos Abordados

- Segurança de Redes;
- Identificação de Ameaças;
- Práticas Gerais para Mitigação de Riscos;
- Listas de Controle de Acesso (ACL):
  - Listas de Acesso IP Padrão;
  - Listas de Acesso IP Estendidas;
  - Listas de Acesso IP Avançadas
    - Nomeadas (*Named ACLs*);
    - Lock and Key ACLs;
    - Time-based ACLs;
  - Configuração, Gerenciamento e Identificação de Problemas.

9.2 Segurança de Redes

No passado, a maioria das ameaças digitais eram originadas por gênios da computação ou estudantes de computação com muito tempo livre. Conforme o tempo foi passando, o conhecimento foi sendo disseminado e, hoje, estas ameaças se multiplicaram e podem ser iniciadas por praticamente qualquer pessoa que tenha acesso à Internet. Não é novidade, portanto, que o assunto de segurança de redes venha ganhando destaque nos últimos anos. Empresas buscam especialistas em segurança para ajudá-las a conter o crescente número de ameaças

A maior preocupação hoje é a clara alteração na motivação dos criminosos virtuais. Antes motivados pelo desafio, estes agiam normalmente sozinhos. Hoje, a motivação é o ganho financeiro, alcançado por meio de acesso à informações sigilosas, desvio eletrônico de recursos, roubo de identidade, chantagem por meio de ataques coordenados à servidores vitais, dentre muitos outros. Dada a importância que este assunto tem nos dias de hoje, o exame demanda que seus candidatos conheçam a terminologia utilizada neste meio, os principais tipos de ameaças e ataques e procedimentos existentes para mitigá-los.

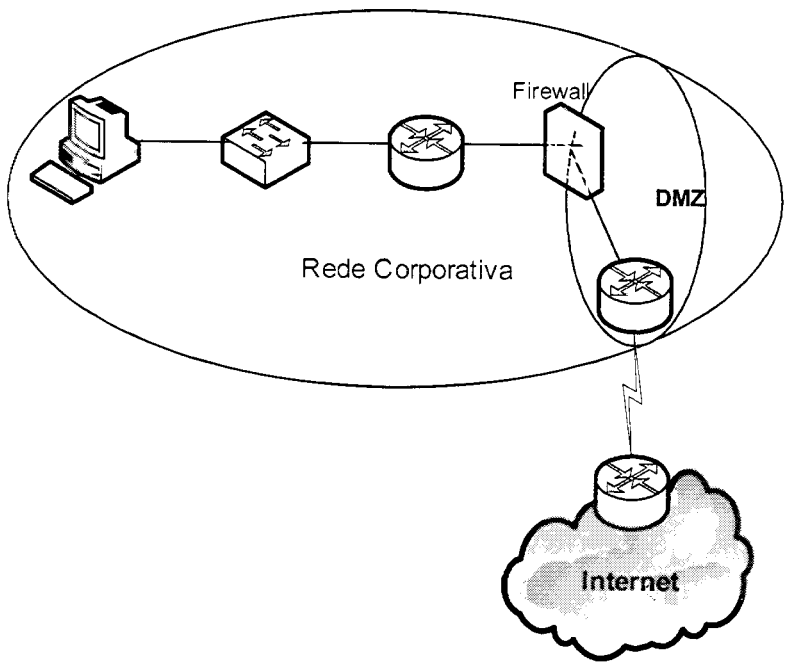


Figura 9.1: Típica conexão de uma rede corporativa ao mundo externo.

A figura 9.1 ilustra a típica conexão de uma rede corporativa com o mundo externo. A área acinzentada é chamada de DMZ (*DeMilitarized Zone*, que significa Zona Desmilitarizada). Normalmente, aloca-se na DMZ os elementos que têm acesso direto e irrestrito ao mundo externo, normalmente os primeiros alvos de ataques vindos de fora. No exemplo, o roteador que se conecta ao provedor de internet e o próprio *firewall* seriam os primeiros a serem atacados.

A função do *firewall* em uma rede é filtrar os pacotes que entram e saem da rede, de modo a evitar que pacotes contendo conteúdo nocivo atinjam a rede e causem qualquer tipo de prejuízo. Estes filtros examinam uma gama de informações em um pacote de dados, que vão desde o número da porta de comunicação até a assinatura da aplicação que esta sendo transportada. A adoção de uma topologia como esta, puramente, entretanto, pode gerar um falso senso de segurança. Alguns podem pensar que um *firewall* pode evitar qualquer tipo de ataque

originado na Internet. Mas, um único *firewall* perimetral (um *firewal* que se situa na borda da rede, como o ilustrado) não é capaz de protege uma rede corporativa de todas as ameaças vindas da Internet. Alén disso, é importante ter como fato que um considerável porcentual do ataques tem origem dentro da rede corporativa e o *firewall* seque examina estes pacotes.

Alguns dos tipos de ataques mais comuns atualmente encontram se listados a seguir:

- **Ataques Denial of Service (DoS):** Um tipo de ataque cuj propósito é parar determinados serviços ou elementos d rede. Existem ataques DoS do tipo *destroyers*, cujo propósit específico é danificar seus alvos por meio d comprometimento de seus dados ou de seu software Ataques do tipo *crashers*, por sua vez, objetivam romper conexão do host com a rede. Finalmente, temos os ataque DoS do tipo *flood*, cujo objetivo é inundar a rede com pacote tornando-a inutilizável, prevenindo qualquer tipo d comunicação útil com os servidores;
- **Ataques de Reconhecimento (*Reconnaissance Attacks*)** Este tipo de ataque pode derrubar uma rede como efeit colateral, mas seu objetivo principal é obter informaçõe importantes que possam, posteriormente, serem utilizada em um ataque de acesso (mencionado a seguir). Ur exemplo deste tipo de ataque seria descobrir os endereço IP dos servidores ou dos roteadores de uma rede, para depoi tentar identificar quais encontram-se mais vulneráveis a ur determinado tipo de ataque;
- **Ataques de Acesso (*Access Atacks*):** Ataques deste tip objetivam o roubo de dados, tipicamente buscando-s alguma vantagem financeira. Por exemplo, o acesso seguid de roubo de informações privilegiadas sobre algum corporação que possa ser vendido depois para seu concorrentes.

Vírus de computadores, cavalos de tróia, *worms*, *spywares*, *malware* scanners, *key-loggers* e outros são apenas ferramentas utilizadas par executar um dos tipos de ataques mencionados anteriormente Atualmente, a maioria dos computadores já saem de fábrica com algur tipo de software antivírus instalado.Estes softwares, basicamente carregam uma base de dados contendo informações sobre todos os víru conhecidos (conhecidas como assinaturas). Depois, observand

passivamente o tráfego que entra e sai do computador, o software antivírus é capaz de identificar os padrões utilizados pelos vírus constantes em sua base de dados e impedir que o computador seja infectado. A figura 9.2 ilustra as falhas de segurança mais comuns no mundo corporativo.

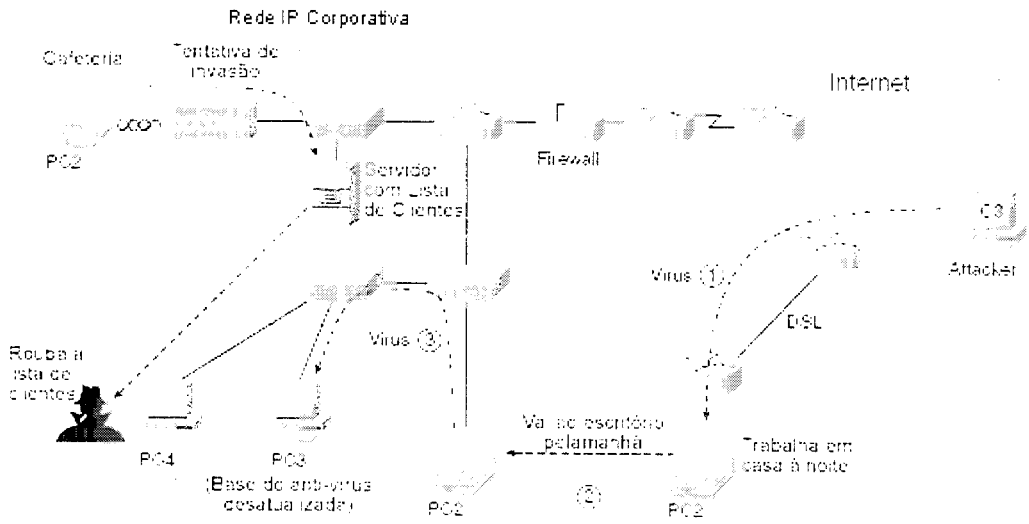


Figura 9.2: Falhas comuns de segurança em redes corporativas.

Os seguintes tipos de problemas poderiam ocorrer na rede da empresa ilustrada na figura:

- **Acesso aberto via rede Wireless (WIFI):** Na ilustração temos uma tentativa de invasão originada de alguém presente em uma cafeteria próxima que conseguiu acesso livre à rede corporativa via rede sem-fio. É comum o sinal de um ponto de acesso wireless interno à empresa atravessar suas paredes e chegar em locais externos próximos, como a cafeteria ilustrada na figura. Se a rede estiver desprotegida, qualquer um com um laptop e uma antena WIFI pode captar o sinal e ter acesso à rede. Note que, neste caso, de nada adianta existir um *firewall* na rede, já que o tráfego vindo da cafeteria jamais passará por ele;
- **Laptops infectados:** Quando um funcionário leva seu laptop para casa e o usa para acesso à internet sem possuir um software de *firewall* ou um antivírus instalado (PC2, na figura), ele pode ter seu laptop infectado por um vírus. Quando este funcinário retorna ao trabalho no dia seguinte, e conecta seu laptop à rede corporativa, o vírus é propagado para a rede, e pode infectar outros PCs, como o PC3, na figura;

- **Funcionários insatisfeitos:** Suponha a seguinte situação: o usuário que utiliza o PC4 está pensando em mudar de emprego. Ele rouba uma série de dados críticos da empresa atual e os grava em um pendrive USB. Com a capacidade dos pendrives atuais (até 8GB), isso permite que ele copie toda a base de dados dos clientes e deixe as instalações da empresa sem que ninguém desconfie de nada, já que o pendrive pode ser facilmente escondido.

Estes são apenas exemplos de ataques que podem ocorrer se nenhum tipo de política de segurança for colocada em prática. Para prevenir estes tipos de problema, a Cisco sugere um modelo de segurança que se baseia em ferramentas que automaticamente se adaptam e trabalham para defender a rede. Este modelo é chamado de *self-defending network*.

Um exemplo de ferramenta Cisco que atua sob esta arquitetura é o *Network Admission Control* ou NAC. NAC é uma ferramenta de segurança que ajuda na prevenção de dois dos ataques mencionados. Dentre outras funções, o NAC é capaz de monitorar a primeira conexão dos dispositivos na rede, seja esta rede física ou sem-fio. O NAC, por exemplo, pode impedir que um PC se conecte à rede até que a base de assinaturas do seu antivírus esteja atualizada. O NAC também pode implementar esquemas de autenticação com nome de usuário e senha, o que evitaria que a pessoa na cafeteria tivesse acesso à rede sem possuir a devida autorização. O NAC, entretanto, não consegue evitar o terceiro tipo de ameaça, que seria o furto de informações por algum funcionário da empresa.

Além dos vírus, uma série de outras ferramentas que ajudam a formar um ataque de rede existem. Vamos conhecer algumas delas.

- **Scanner:** Esta é uma aplicação que envia uma série de solicitações de conexão em várias portas UDP e TCP na tentativa de identificar que tipos de aplicações rodam na rede e, possivelmente, quais os tipos de sistemas operacionais existentes em cada host escaneado. Um exemplo de software que faz este tipo de varredura é o *LANGuard Port Scanner* que pode ser obtido gratuitamente em <http://www.tucows.com/preview/213719>. O uso deste tipo de software por um administrador de redes pode ser produtivo, já que ele listará as principais vulnerabilidades existentes em sua rede e, medidas corretivas e preventivas podem ser tomadas antes que um ataque de fato ocorra;

- **Spyware:** Os *spywares* são, basicamente, vírus que buscam informações específicas em sua máquina, rastreando tudo o que o usuário faz em seu PC e transmitindo estas informações de volta para o *attacker*, na internet;
- **Worm:** Um programa que se auto-replica rapidamente por redes corporativas ou pela internet, cujo objetivo principal é lançar ataques de DoS, particularmente, tendo servidores específicos como alvo;
- **Key-logger**: Uma espécie de vírus que grava sequências de teclas digitadas no PC e as envia para o *attacker*, na internet. Normalmente são usadas para conseguir usernames e senhas;
- **Phishing**: Consiste em clonar um determinado website (de um banco, por exemplo) e fazer com que um usuário desavisado o acesse, capturando assim dados valiosos como: *username*, senha, etc. Normalmente, ataques deste tipo ocorrem via e-mail, quando uma mensagem falsa informando que seu saldo está negativo, ou algo do gênero, apresenta um link que leva o usuário ao site falso;
- **Malware**: Nada mais que um conjunto de ferramentas maliciosas, como vírus, *spywares*, *worms*, etc.

9.2.1 Práticas para Mitigação dos Riscos

Como já foi mencionado antes, a melhor solução para evitar esses tipos de problema é a adoção de uma política efetiva de segurança em toda a rede. Já mencionei o NAC. Vamos ver outras ferramentas da Cisco igualmente importantes.

9.2.1.1 Firewalls e o Cisco Adaptative Security Appliance (ASA)

Os *firewalls* examinam todos os pacotes que entram e saem de uma determinada rede, em busca de padrões que satisfaçam algumas regras previamente configuradas. Os *firewalls* fazem essa análise observando informações de camada 3 (endereços IP de origem e destino, por exemplo), camada 4 (portas TCP e UDP, por exemplo) e camada 7, que observa os cabeçalhos de determinadas aplicações. Um *firewall*, por definição, nega todo e qualquer tráfego, a não ser aqueles explicitamente autorizados pelo administrador da rede. Como já foi dito, o *firewall* normalmente será colocado entre uma rede segura e outra não tão segura (como a Internet). Em alguns casos, uma corporação precisa ter servidores que encontrem-se acessíveis

externamente, como um servidor Web. Neste caso, estes servidores devem ficar do lado menos seguro do *firewall*, chamado de DMZ (*DeMilitarized Zone*). A DMZ, portanto, é uma zona mais exposta aos ataques externos.

Até alguns anos atrás, os *firewalls* vendidos pela Cisco eram conhecidos pela marca "PIX". A Cisco lançou recentemente uma nova geração de equipamentos de segurança (que também são usados como *firewalls*), chamada ASA (*Adaptative Security Appliance*), aposentando assim a linha PIX.

9.2.1.2 Anti-X

Uma política de segurança bem elaborada requer uma série de medidas para prevenir os diferentes tipos de ataques e problemas. A Cisco usa o termo anti-X para se referir a toda uma classe de ferramentas de segurança que podem agir na prevenção de muitos dos problemas vistos até agora, incluindo:

- **Anti-vírus:** Realizam uma varredura do tráfego de rede para prevenir a transmissão de vírus. Fundamentado em uma base de dados atualizável contendo a assinatura dos vírus conhecidos;
- **Anti-spyware:** Da mesma forma que os antivírus, previnem que *spywares* sejam transmitidos pela rede;
- **Anti-spam:** Examina os e-mails no servidor ANTES que eles sejam enviados aos usuários, identificando spams por meio de padrões pré-configurados;
- **Anti-phishing:** Monitora URLs enviadas via rede identificando URLs falsas e prevenindo o ataque de alcançar os usuários;
- **Filtros de URL:** Filtra o tráfego Web baseado em URLs, impedindo os usuários de acessar sites supostamente perigosos;
- **Filtros de e-mail:** Além de incorporar a ferramenta anti-spam, estes filtros rejeitam mensagens específicas, tendo como base a análise do conteúdo.

9.2.1.3 Ferramentas de Detecção e Prevenção de Intrusão

Alguns tipos de ataques não são facilmente identificados pelas ferramentas "anti-x". Alguns tipos de ataques são bastante sofisticados, e o simples uso de *firewalls* ou outras ferramentas mencionadas não são suficientes para impedi-los. Na área de segurança de redes, dois

tipos específicos de ferramentas podem ser usados para mitigar estes ataques mais elaborados: os Sistemas de Detecção de Intrusão (*Intrusion Detection Systems* - IDS) e os Sistemas de Prevenção de Intrusão (*Intrusion Prevention Systems* - IPS). Estas ferramentas detectam ataques observando padrões e tendências. Por exemplo, IDS e IPS podem monitorar seqüências de pacotes enviados entre hosts buscando padrões em transferências que indiquem que um *worm* está tentando se replicar pela rede. Ao primeiro sinal de ataque, estes sistemas emitem alertas visuais, sonoros ou via telefone celular para que o administrador da rede tome as devidas providências.

Estes sistemas também são capazes de isolar porções de uma rede para impedir que uma suspeita de ataque se propague. IPS e IDS agem de forma semelhante, porém, o IDS foca na análise passiva dos pacotes, alertando quando um problema em potencial é identificado. O IPS, por sua vez, atua de forma ativa, ele pode efetivamente aplicar filtros na rede que isolem o problema.

9.2.1.4 Cisco Security Agent (CSA)

O *Cisco Security Agent* (CSA) oferece proteção contra ameaças aos sistemas de computação como servidores ou desktops. Além disso, o CSA ajuda a reduzir os custos operacionais relativos à identificação, prevenção e remoção de ameaças conhecidas e desconhecidas. O interessante do *Cisco Security Agent* é que ele analisa o comportamento do dispositivo em vez de analisar apenas as ameaças conhecidas, o que não requer conhecer a estrutura do vírus ou *worm* para deter um ataque. Esta arquitetura pode identificar e prevenir as ameaças no *Dia Zero,* ou seja, quando começam a atuar.

9.2.1.5 SSH (Secure Shell)

O SSH deve ser implementado, sempre que possível, como meio de acesso aos elementos de rede no lugar do Telnet tradicional. De forma simplista, o SSH pode ser visto como uma sessão Telnet criptografada. Para ativar o recurso SSH em um dispositivo Cisco, utilize os comandos:

```
ip domain-name ccna.com.br
aaa new-model
username cisco password 0 cisco
(O comando aaa new-model faz com que o username e senha locais
configurados no router sejam utilizados na ausência de outros
parâmetros AAA)
crypto key generate rsa
ip ssh time-out 60
```

```
ip ssh authentication-retries 2
(Gera a chave criptografada para ser usada em conjunto com o SSH)
line vty 0 4
transport input SSH
(Habilita o acesso via SSH no router. Neste caso, o acesso
Telnet é desabilitado)
```

9.2.1.6 Virtual Private Networks (VPNs)

Outra ferramenta de segurança que trataremos neste tópico é conhecida por Rede Virtual Privada ou VPN. Quando temos uma conexão dedicada entre dois pontos, não temos muitas preocupações em termos de segurança, já que o circuito ponto-a-ponto nos pertence e não é compartilhado com mais ninguém. Entretanto, com a crescente oferta de banda e melhora de performance dos links da internet, muitas empresas enxergaram um modo barato de interconectar dois pontos remotos. O problema é que a internet é um meio público, ou seja, além de não pertencer à sua empresa, é compartilhado por milhões de pessoas. Para possibilitar a utilização de links internet na interconexão de localidades corporativas, VPNs são utilizadas.

VPNs resolvem dois problemas : o de segurança, uma vez que todos os pacotes enviados via VPN são criptografados, ou seja, se forem interceptados não terão valor algum, e, resolvem o problema de endereçamento e roteamento IP, já que, se utilizássemos a internet para conectar dois pontos, não teríamos como rotear pacotes de um ponto ao outro, já que não temos controle sobre os roteadores que se encontram no meio do caminho. Quando um túnel VPN é fechado entre dois pontos, para todos os efeitos, o que temos é uma conexão ponto-a-ponto, e podemos configurar rotas ou rodar o protocolo de roteamento que bem entendermos, como em uma verdadeira rede privada.

Em uma VPN, os elementos participantes (chamados de *endpoints*) necessitam autenticar-se antes que o túnel VPN seja criado, o que garante a integridade dos dados que atravessam esta arquitetura. A figura 9.3 ilustra dois tipos distintos de VPN: A VPN2 seria uma VPN ponto-a-ponto entre dois sites (matriz e filial) chamada de intranet VPN. A VPN1, por sua vez, seria uma VPN de acesso, criada por um usuário para conectar seu laptop (em casa) à rede corporativa. No primeiro caso, a VPN é mantida por tempo indeterminado, como se fosse um link ponto-a-ponto tradicional, possibilitando a comunicação entre os dois sites. No segundo caso, a VPN é estabelecida sob demanda, somente quando o usuário necessita de acesso aos recursos da rede corporativa.

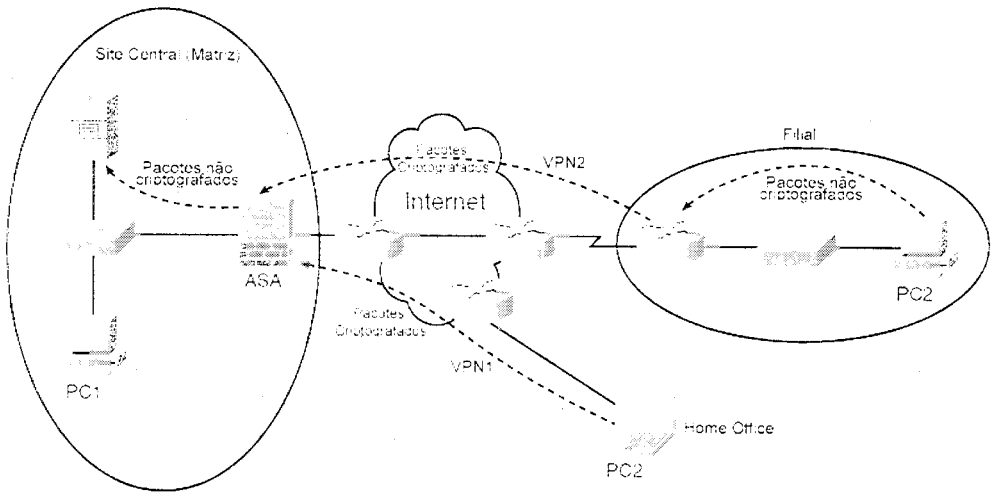


Figura 9.3: Exemplo de funcionamento de dois tipos de VPNs.

9.3 Listas de Acesso

A apropriada configuração e uso de listas de acesso pode ser um procedimento vital dentro da política de segurança de uma corporação. Listas de acesso permitem aos administradores de rede o gerenciamento de um grande fluxo através de toda a rede. Aplicando listas de acesso, administradores podem obter estatísticas sobre o fluxo de pacotes e, então, implementar políticas de segurança adequadas.

Listas de acesso podem ser utilizadas para permitir ou negar o fluxo de pacotes através de um router, permitir ou negar acesso via Telnet (VTY) para ou de um router, proteger dispositivos críticos de acessos não-autorizados e determinar o que é considerado tráfego interessante (*interesting traffic*) em uma rede, que em um ambiente de discagem sob demanda (*dial-on-demand* - DDR), por exemplo, dispara o processo de discagem para um local remoto.

Listas de acesso são, essencialmente, listas de condições que controlam o acesso. Uma vez criadas, **podem ser aplicadas tanto ao tráfego entrante (*inbound traffic*) quanto ao tráfego sainte (*outbound traffic*)**, em qualquer interface. A aplicação de listas de acesso fará com que o router examine cada pacote atravessando uma determinada interface em uma determinada direção e tome as providências apropriadas.

Algumas regras que um pacote segue quando comparado com listas de acesso:

- A comparação com cada linha da lista de acesso sempre **ocorre seqüencialmente**, ou seja, sempre se inicia na linha 1, seguindo para a linha 2 e assim sucessivamente;

- A comparação é realizada **apenas até que ocorra a identificação de uma linha da lista de acesso com o pacote.** Uma vez que essa identificação ocorra, as ações especificadas são tomadas e nenhuma comparação adicional é feita;
- Existe **um comando "negue" (*deny*) implícito (ele não aparece, mas o router o entende) no final de cada lista de acesso**. Isso significa que, caso não ocorra nenhuma identificação positiva de um determinado pacote com alguma linha da lista de acesso, ele será descartado.

Existem basicamente três tipos de lista de acesso: *standard* (padrão), *extended* (estendida) e *named* (nomeada). Uma vez criada, a lista de acesso deve ser aplicada a uma interface como entrante (*inbound*) ou sainte (*outbound*).

- **Inbound**: Os pacotes são processados pela lista de acesso assim que atravessam a interface de entrada do roteador, ou seja, **antes de serem encaminhados para a interface que o transportará ao seu destino**;
- **Outbound**: Os pacotes são primeiro encaminhados à interface de saída para apenas então serem processados pela lista de acesso.

Algumas regras devem ser seguidas na criação e implementação de listas de acesso em um router:

- Apenas uma lista de acesso pode ser aplicada por interface, protocolo ou direção. Isso significa que, se você estiver criando listas de acesso IP, **apenas uma lista entrante e uma sainte são permitidas por interface**;
- Organize suas listas de acesso para que os procedimentos mais específicos e críticos encontrem-se no início delas;
- Novas condições são **sempre** adicionadas ao final da lista existente;
- **Não se pode remover apenas uma linha de uma lista de acesso do tipo numerada**. Ao se tentar fazê-lo, toda a lista será deletada. É melhor copiar a lista de acesso inteira para um editor de textos e editá-la externamente. Após a edição ser completada, "copie e cole" a lista modificada para o IOS;

- A menos que sua lista de acesso termine com o comando *permit any*, **todos os pacotes que não sejam identificados com alguma condição da lista ativa serão descartados**. Por esse motivo, toda lista deve conter ao menos um comando *permit*, **do contrário você pode bloquear a interface onde ela for aplicada**;
- Primeiro crie listas de acesso para depois aplicá-las às interfaces. De nada adianta a aplicação de listas de acesso que não estejam presentes. Você pode ter uma série de listas de acesso criadas em seu router (**99 listas numeradas para cada tipo existente**). O que importa, na verdade, é qual lista você está, de fato, aplicando. Criar listas e não aplicá-las a uma determinada interface de nada adianta;
- Listas de acesso foram idealizadas e concebidas para filtrar o tráfego que atravessa um router. **Elas não filtrarão o tráfego originado pelo router onde se encontram aplicadas;**
- Listas de acesso padrão (*standard*) devem **sempre** ser aplicadas o mais próximo do destino possível;
- Listas de acesso estendidas (*extended*), dependendo do resultado que se deseja obter, podem ser aplicadas tanto próximas ao destino quanto da origem. Porém, para efeitos gerais - e do exame CCNA - adotemos a regra genérica de que **listas de acesso estendidas, na maioria dos casos, são aplicadas o mais próximo da origem possível**.

9.3.1 Listas de Acesso IP Padrão

Listas de acesso IP padrão (*standard IP access lists*) **filtram a rede utilizando o endereço IP de origem em um pacote IP**, ou seja, essencialmente, filtram a rede através da camada 3 (rede) do modelo OSI. Essas listas são identificadas por números compreendidos no intervalo 1-99 (veja tabela a seguir). É muito importante lembrar-se disso. 1-99: listas de acesso IP padrão, 100-199: listas de acesso IP estendidas. Memorize esses intervalos!

Tipo	Intervalo Numérico
IP Standard	1-99
IP Extended	100-199
IPX Standard	800-899
IPX Extended	900-999
IPX SAP	1000-1099

Eis o procedimento para se criar uma lista de acesso IP padrão:

```
RouterA(config)#access-list 10 ?
 deny    Specify packets to reject
 permit  Specify packets to forward
```

Após escolher o número desejado para a lista de acesso a ser criada (10, no nosso caso), deve-se definir se esta será uma lista do tipo *permit* ou *deny* (permitir/negar acesso). Suponhamos que seja uma lista de acesso *deny*:

```
RouterA(config)#access-list 10 deny ?
 Hostname or A.B.C.D Address to match
 any   Any source host
 host  A single host address
```

Deparamos-nos agora com três opções: pode-se utilizar o comando *any* para permitir ou negar o acesso a qualquer host ou rede, pode-se especificar o endereço IP para um host ou uma rede específica ou pode-se ainda utilizar o comando *host*, que tem exatamente o mesmo efeito de se especificar o endereço IP diretamente. Eis um exemplo de uma entrada que instrui a lista de acesso a negar qualquer pacote que tenha sido originado do host 172.16.30.2:

```
RouterA(config)# access-list 10 deny host 172.16.30.2
```

Host é o comando default, ou seja, se você simplesmente digitar *access-list 10 deny 172.16.30.2* o router entenderá como se o comando *host* tivesse sido digitado.

Existe ainda um outro modo de se especificar um host: **utilizando-se *wildcards***. Na verdade, para se especificar uma rede ou sub-rede, não há outro modo. Deve-se utilizar *wildcards* nas listas de acesso.

Wildcards são utilizados em listas de acesso para especificar um host, uma rede ou uma porção específica de uma rede. O primeiro passo no entendimento de *wildcards* é a compreensão da definição e do funcionamento dos *block sizes* (tamanhos de bloco).

Block sizes são utilizados para especificar um intervalo de endereços. A figura 9.4 apresenta alguns dos diferentes tamanhos de bloco existentes (note que basta iniciar em 4 e seguir multiplicando por 2).

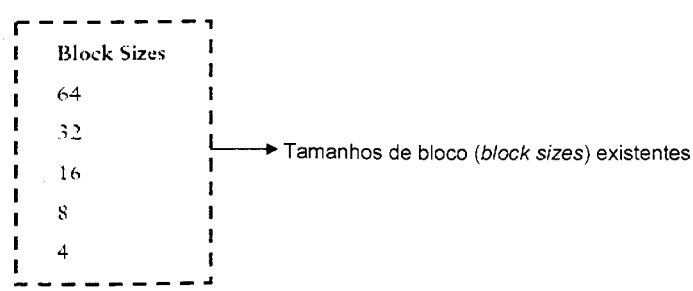


Figura 9.4: Block Sizes.

Quando você precisa especificar um intervalo de endereços, você deve escolher o tamanho de bloco (*block size*) que mais se aproxima de suas necessidades. Por exemplo: se você precisar especificar 34 redes, vai precisar de um *block size* tamanho 64. Por quê? Vamos analisar: o número de redes que queremos especificar (34) encontra-se entre os blocos 32 e 64, certo? Se escolhermos 32, não conseguiremos especificar as 34 redes que desejamos, mas um número inferior! Portanto, o número de bloco a ser escolhido deve **sempre ser o maior do intervalo**. Portanto, em nosso caso, 32 < 34 < 64.

Wildcards são usados em conjunto com o endereço do host ou da rede para informar ao router o intervalo de endereços desejado para filtragem. Para especificar apenas um host, o formato do endereço dever ser algo como:

```
172.16.30.5 0.0.0.0
```

Os **quatro zeros representam cada octeto do endereço**. Cada vez que um 0 aparece, significa que o octeto correspondente no endereço deve ser exatamente igual ao informado. **Para especificar que um determinado octeto pode ter qualquer valor, o número 255 é utilizado**. No exemplo a seguir, especificamos uma sub-rede inteira:

```
172.16.30.0 0.0.0.255
```

Isso informa ao router que os três primeiros octetos (172.16.30) devem ser idênticos aos informados; o quarto octeto (0), porém, pode conter qualquer valor.

Para especificar um intervalo específico de sub-redes, *block sizes* são utilizados. O intervalo de valores deve ser especificado com base em um *block size*. Em outras palavras, **não há como especificar 20 sub-redes**, por exemplo. Você pode apenas especificar exatamente a quantidade de redes que um block size permite. Por exemplo, **o intervalo será 16 ou 32, mas nunca 20.**

Vamos supor que você queira negar o acesso a uma parte da rede compreendida entre o intervalo 172.16.*8*.0 e 172.16.*15*.0. O tamanho de bloco a ser utilizado, nesse caso, é *8*. Eis o cálculo a ser efetuado: *15 - 8 = 7*. Lembre-se: *4 < 7 < 8*, portanto, o *block size* que devemos usar é o *8*. Logo, o endereço a ser informado seria *172.16.8.0* e o *wildcard* seria *0.0.7.255*. Sim, *7* e não *8*! O *wildcard* SEMPRE será o número do bloco (*block number*) menos 1 (*8 - 1 = 7*, no nosso caso). Se você definir um *block size* de *16*, seu *wildcard* trará o número *15*, e assim por diante. Eis um exemplo de aplicação:

```
RouterA(config)#access-list 10 deny 172.16.16.0 0.0.3.255
```

A configuração anterior informa ao router para iniciar no endereço de rede 172.16.16.0 e utilizar um *block size* de "4". Portanto, o intervalo seria de 172.16.16.0 até 172.16.19.0.

9.3.1.1 Listas de Acesso IP Padrão – Exemplo de Aplicação

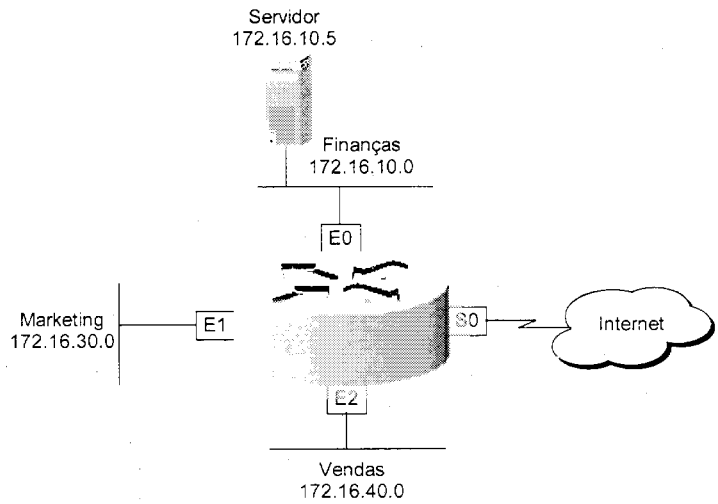


Figura 9.5: Exemplo prático de aplicação de uma lista de acesso IP padrão.

Vamos discutir agora como aplicar listas de acesso IP padrão para impedir o acesso de certos usuários a LAN do departamento de finanças. Na figura 9.5, um router tem três conexões LAN e uma conexão WAN para a Internet. Usuários do departamento de Vendas não devem ter acesso à LAN do departamento de Finanças, mas devem ter acesso à Internet e à LAN do departamento de Marketing. A LAN do departamento de Marketing precisa de acesso à LAN do departamento de Finanças.

No router em questão, a seguinte lista de acesso IP padrão é criada:

```
Acme#config t
Acme(config)#access-list 10 deny 172.16.40.0 0.0.0.255
Acme(config)#access-list 10 permit any
```

É de extrema importância o entendimento de que o comando *any*, usado, tem exatamente o mesmo efeito que a condição a seguir [1]:

```
Acme(config)#access-list 10 permit 0.0.0.0 255.255.255.255
```

Nessa altura, a lista de acesso está negando acesso à LAN de Vendas e permitindo o acesso de todas as outras LANs. A questão agora é: onde essa lista de acesso deve ser aplicada? Caso ela seja aplicada como uma lista entrante (*inbound*) na interface *E2*, por exemplo, você desativará essa interface, uma vez que toda a LAN de Vendas terá seu acesso negado

[1] Isso costuma ser cobrado no exame CCNA. Atenção!

às demais LANs conectadas ao router. Portanto, o melhor lugar para se aplicar a lista seria na interface *E0*, como uma lista sainte (*outbound*)[2]:

```
Acme(config)#int e0
Acme(config-if)#ip access-group 10 out
```

Isso impedirá completamente que os pacotes originados na rede 172.16.40.0 (Vendas) atravessem a interface *E0* (Finanças), porém, a LAN de Vendas ainda terá total acesso à LAN de Marketing e à Internet.

9.3.1.2 Listas de Acesso no Controle de Acessos via VTY (Telnet)

Impedir usuários de conectar-se a um router via Telnet pode ser um problema, já que qualquer porta ativa nele é passível de acesso VTY.

Entretanto, listas de acesso IP padrão podem ser usadas para controlar o acesso Telnet, através da aplicação delas diretamente às linhas VTY.

Para realizar essa operação:

1. Crie uma lista de acesso IP padrão que permita que apenas o host ou os hosts que você deseje possam conectar-se via Telnet ao router;
2. Aplique a lista de acesso criada diretamente às portas VTY, utilizando o comando *access-class*, como ilustrado a seguir.

```
RouterA#conf t
RouterA(config)#access-list 50 permit 172.16.10.3
RouterA(config)#line vty 0 4
RouterA(config-line)#access-class 50 in
```

No exemplo anterior, devido ao comando *deny any*, implícito no final da lista, a lista de acesso impede que qualquer host - exceto o host com endereço IP 172.16.10.3 - tenha acesso ao router via Telnet.

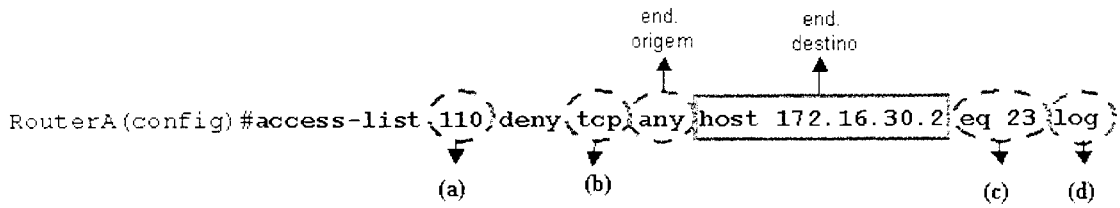
9.3.2 Listas de Acesso IP Estendidas

Listas de acesso IP estendidas permitem que se filtre a rede não apenas através do endereço IP de origem e destino, mas também através do protocolo e do **número de porta**.

Listas de acesso IP estendidas podem ser usadas para permitir que usuários acessem determinada LAN, porém, negando o acesso a serviços específicos. Isso não é possível com listas IP padrão.

---

[2] Lembre-se: Listas de acesso IP padrão devem ser aplicadas próximas ao destino, assim como o que foi feito neste exemplo.



No exemplo anterior, eis o que temos:

- **(a)110:** Informa ao comando *access-list* que se trata de uma lista IP estendida (100-199);
- **(b) tcp**: Informa o protocolo que será utilizado como filtro. No caso, utilizamos o protocolo TCP. Lembre-se de que, para filtragem através da camada de aplicação, o protocolo escolhido aqui deve permitir que você "suba" no modelo OSI até a camada 7 (*Application*). Por esse motivo, o TCP foi escolhido. Por exemplo, para filtragem da rede através de aplicações como Telnet ou FTP, TCP deve ser utilizado nesse campo;
- **(c) eq 23**: O atributo *eq* informa que pacotes serão verificados e comparados à lista apenas se originados na porta TCP especificada (23). No nosso caso, utilizamos a porta 23, que é o número de porta TCP utilizado pela aplicação Telnet. O nome da aplicação (*Telnet*) também poderia ter sido utilizado em lugar ao número da porta. Outras opções aqui poderiam ser: *eigrp, icmp, ip, udp*, entre outras. Para a prova CCNA, o protocolo TCP - e suas portas - é o mais importante. Memorize que a porta 23 = Telnet; 21 = FTP e 80 = WWW. Essas são as mais importantes e as únicas que o exame CCNA pede. Outras que valem a pena conhecer são: porta 25 = SMTP, 110 = POP, 53 = DNS;
- **(d) log**: Esse comando é utilizado para a geração de um arquivo (*log file*) que é enviado ao console toda vez que uma tentativa de acesso é efetuada. Esse recurso não é muito produtivo em um ambiente com tráfego intenso, mas é bastante útil em redes de pequeno porte.

Resumindo, a lista anteriormente criada, uma vez aplicada, bloqueia a porta Telnet (23) para o host 172.16.30.2. Caso esse host deseje acesso através de alguma outra aplicação, como FTP, por exemplo, obterá permissão.

9.3.2.1 Outro Exemplo de Lista IP Estendida

Eis um exemplo um pouco mais complexo de uma lista de acesso IP estendida:

```
Acme#config t
Acme(config)#access-list 110 deny tcp any host 172.16.10.5 eq 21
Acme(config)#access-list 110 deny tcp any host 172.16.10.5 eq 23
Acme(config)#access-list 110 permit ip any any
Acme(config)#int e0
Acme(config-if)#ip Access-group 110 out
```

Nesse exemplo, utilizando o mesmo diagrama presente na figura 9.5, negamos o acesso aos recursos de FTP (21) e Telnet (23) no servidor 172.16.10.5, presente na LAN Financeira. Todos os outros serviços encontram-se disponíveis para o acesso pelas LANs de Marketing e Vendas.

É importante entender por que as linhas *deny* foram configuradas primeiro na lista. O motivo é que, se você configurasse *permit* primeiro e *deny* depois, a LAN do departamento de finanças não seria capaz de se comunicar com nenhuma outra LAN, ou com a Internet, devido ao *deny* implícito no final de toda a lista de acesso. A configuração apresentada é o modo como deve ser feito. Qualquer outra maneira seria mais complicada e menos funcional.

Uma vez que as três outras LANs em nosso router precisam ser capazes de acessar a LAN do departamento Financeiro, a lista deve ser aplicada como sainte (*out*) na interface *E0*. Se a lista, entretanto, tivesse sido criada com o intuito de bloquear, por exemplo, o acesso ao departamento de Vendas somente, deveríamos aplicá-la próximo à origem, ou seja, na interface *E2*.

9.3.3 Listas IP Nomeadas (Named ACLs)

Listas de acesso são muito convenientes, porém, em grandes redes, podem tornar-se um problema no que diz respeito ao seu gerenciamento. Imagine que você seja um administrador de redes de uma grande corporação e que, de repente, lhe perguntem: Afinal, o que é essa lista de acesso 113? Pode ser difícil responder tal questão. Outro problema é com relação ao processo de edição de listas de acesso. Listas numeradas não permitem que apenas uma linha seja deletada ou que uma nova linha seja inserida entre duas existentes. Por esse motivo, a Cisco criou as listas de acesso nomeadas, ou seja, em vez de usar números, podemos nomeá-las para fácil identificação das suas funções. Por exemplo, em vez de usarmos uma lista de acesso número 113, poderíamos criar uma chamada *bloquear_vendas_out*! Muito mais intuitivo, não concorda? Listas de acesso nomeadas também permitem modos mais avançados de edição, como, por exemplo, remoção de apenas uma linha ou inserção de uma linha entre duas existentes.

Todas as regras que vimos anteriormente continuam válidas para listas nomeadas. Para criá-las no router, basta seguir os dois exemplos a seguir (um para cada tipo: *Standard* e *Extended*).

Exemplo de lista nomeada padrão:

```
Marco(config)#ip access-list standard Bloquear_Vendas
Marco(config-std-nacl)#deny 172.16.40.0 0.0.0.255
Marco(config-std-nacl)#permit any
Marco(config-std-nacl)#exit
```

E para aplicá-la a uma interface:

```
Marco(config)#int f0/0
Marco(config-if)#ip access-group Bloquear_Vendas out
Marco(config-if)#^Z
```

Simples, não? Vamos agora a um exemplo de lista nomeada estendida:

```
Marco(config)#ip access-list extended Bloquear_Telnet
Marco(config-ext-nacl)#deny tcp any any eq telnet
Marco(config-ext-nacl)#permit ip any any
```

E para aplicá-la:

```
Marco(config)#int f0/0
Marco(config-if)#ip access-group Bloquear_Telnet in
Marco(config-if)#^Z
```

Observe que na mesma interface (*FastEthernet0/0*) foram aplicadas duas listas de acesso. Isso não é um problema, já que cada lista encontra-se associada a uma direção diferente (a padrão está como *OUT* e a estendida, como *IN*). Observe também as instruções *permit*, no final de cada lista. Se elas não estivessem ali, a interface *F0/0* seria bloqueada para todos os pacotes no momento da aplicação das listas. Lembre-se desta e de outras regras referentes à lista de acesso.

9.3.4 Incluindo Descrições em ACLs

Muitas vezes é interessante registrar, no processo de configuração do router, para que determinada ACL está sendo implementada. Isso agiliza a identificação de problemas no futuro. Para configurar descrições em ACLs, utilize o comando *remark*, dentro do modo de configuração de ACLs. Exemplo:

```
Marco(config)#ip access-list extended Bloquear_Telnet
Marco(config-ext-nacl)#remark Bloqueia o acesso telnet para todos
Marco(config-ext-nacl)#deny tcp any any eq telnet
Marco(config-ext-nacl)#permit ip any any
```

9.3.5 Outros Tipos de ACLs

Existem outros tipos de ACL cujas configurações não fazem parte do escopo do exame CCNA. Apenas para efeito informativo, eis dois tipos bastante interessantes:

- **Lock and Key ACLs (ACLs Dinâmica):** Este tipo avançado de ACL depende da combinação de uma ACL estendida com um processo de autenticação Telnet. Antes de configurar uma ACL dinâmica, é preciso criar uma ACL estendida para bloquear todo o tráfego. O único modo de passar o bloqueio é se o usuário iniciar uma sessão Telnet ao router e conseguir autenticar-se. Assim que isso ocorre, a sessão Telnet é desfeita e a ACL estendida, que já existia, recebe uma regra adicional dinamicamente, permitindo, temporariamente, o tráfego originado pelo usuário e a ele destinado;
- **Time-based ACLs:** Este tipo de ACL funciona de forma análoga às ACLs estendidas, com a diferença que o gerenciamento de acesso é totalmente controlado por intervalos de tempo. Ou seja, você pode criar regras para que sejam aplicadas apenas em determinados intervalos de tempo de um dia, semana ou mês. Este tempo é controlado pelo relógio (clock) do router, portanto, ao utilizar este tipo de ACL, é interessante que o relógio do router esteja sincronizado com um servidor NTS (*Network Time Server*).

9.3.6 Monitorando Listas de Acesso IP

Eis uma lista dos comandos que podem ser utilizados com essa finalidade:

- **show access-list**: Apresenta todas as listas de acesso e seus parâmetros. Esse comando não informa em qual interface cada lista encontra-se aplicada;
- **show access-list 110**: Apresenta apenas os parâmetros configurados para a lista de acesso 110;
- **show access-list Bloquear_Telnet**: Mostra apenas os parâmetros configurados para a lista de acesso nomeada *Bloquear_Telnet*;
- **show ip access-list**: Apresenta apenas as listas de acesso IP configuradas no router;

- **show ip interface**: Exibe interfaces que possuem listas de acesso aplicadas;
- **show running-config**: Apresenta as listas de acesso e quais interfaces possuem listas de acesso aplicadas.

Questões de Revisão – Segurança de Redes

1. Como responsável pela segurança da rede de sua empresa, você está preocupado com vários tipos de ataques possíveis. Qual dos ataques listados abaixo é caracterizado pelo envio massivo de pacotes solicitando uma conexão TCP a um servidor?

a) Trojan Horse
b) Reconnaissance
c) Denial of Service
d) Brute Force
e) Virus
f) Worm

2. Um administrador de redes está preocupado em melhorar a segurança de sua rede. Quais procedimentos você recomendaria a ele para proteger os arquivos de configuração dos dispositivos de rede de forma a não serem acessados de fora da rede por pessoas não autorizadas (selecione 2 respostas)?

a) Utilizar um Firewall para restringir o acesso de pessoas não autorizadas aos elementos de rede.
b) Permitir o acesso irrestrito ao console e linhas VTY.
c) Prevenir o esquecimento de senhas desativando o serviço de criptografia.
d) Sempre utilizar o Telnet no acesso aos dispositivos, já que esta conexão é criptografada automaticamente.
e) Utilizar o SSH ou outro meio de transporte criptografado para acesso aos elementos de rede.
f) Utilizar sempre senhas simples, com o objetivo de evitar seu esquecimento acidental.

3. Você deseja aumentar a segurança de sua rede. Indique 2 elementos de segurança que podem ser instalados em sua rede para atingir este objetivo:

a) SDM
b) ATM
c) IDS
d) IOX
e) IPS
f) IOS
g) FR

4. Listas de acesso IP padrão utilizam qual das seguintes opções como base para permitir ou negar pacotes IP?

a) Endereço IP de origem
b) Endereço IP de destino
c) Protocolo
d) Porta TCP
e) Endereço MAC de origem

5. Listas de acesso IP estendidas utilizam quais das seguintes opções como base para permitir ou negar pacotes?

a) Endereço IP de origem
b) Endereço IP de destino
c) Protocolo
d) Porta
e) Todas as opções acima

6. Para especificar todos os hosts em uma rede IP *classful* 172.16.0.0, qual máscara "coringa" (wildcard) você usaria?

a) 255.255.0.0
b) 255.255.255.0
c) 0.0.255.255
d) 0.255.255.255
e) 0.0.0.255

7. Quais das seguintes sintaxes são válidas para especificar somente o host 172.16.30.55 em uma lista de acesso IP?

a) 172.16.30.55 0.0.0.255
b) 172.16.30.55 0.0.0.0
c) any 172.16.30.55
d) host 172.16.30.55
e) 0.0.0.0 172.16.30.55
f) ip any 172.16.30.55

8. Quais das seguintes listas de acesso permitem somente o tráfego HTTP através da rede 196.15.7.0?

a) access-list 100 permit tcp any 196.15.7.0 0.0.0.255 eq www
b) access-list 10 permit tcp any 196.15.7.0 0.0.0.255 eq www
c) access-list 100 permit 196.15.7.0 0.0.0.255 eq www
d) access-list 110 permit ip any 196.15.7.0 0.0.0.255 eq www
e) access-list 110 permit www 196.15.7.0 0.0.0.255
f) access-list 100 permit tcp any 196.15.7.0 0.0.0.255 eq 80

9. Quais dos seguintes comandos apresentam as interfaces que possuem listas de acesso IP aplicadas?

a) show ip port
b) show access-list
c) show ip interface

d) show access-list interface
e) show running-config

10. Qual wildcard você usaria para filtrar o intervalo de redes de 172.16.16.0 a 172.16.23.0?

a) 172.16.16.0 0.0.0.255
b) 172.16.255.255 255.255.0.0
c) 172.16.0.0 0.0.255.255
d) 172.16.16.0 0.0.8.255
e) 172.16.16.0 0.0.7.255
f) 172.16.16.0 0.0.15.255

11. Quais das seguintes opções representam opções válidas para uma lista de acesso IP nomeada?

a) ip access-list 10 standard Minha_Lista_Padrao
b) ip access-list 100 extended Minha_Lista_Estendida
c) ip access-list standard Minha_Lista_Padrao
d) ip access-list extended Minha_Lista_Estendida
e) ip access-list Minha_Lista

12. Qual wildcard você usaria para filtrar o intervalo de redes de 172.16.32.0 a 172.16.63.0?

a) 172.16.0.0 0.0.0.255
b) 172.16.255.255 0.0.0.0
c) 0.0.0.0 255.255.255.255
d) 172.16.32.0 0.0.0.255
e) 172.16.32.0 0.0.0.31
f) 172.16.32.0 0.0.31.255
g) 172.16.32.0 0.31.255.255
h) 172.16.32.0 0.0.63.255

13. Qual dos seguintes comandos aplicará a lista de acesso IP com o nome Lista1 para barrar o fluxo entrante de pacotes, assumindo que você já está no prompt da interface correta?

a) ip access-class Lista1 in
b) ip access-group in Lista1
c) ip access-class Lista1 out
d) ip access-group Lista1 out
e) ip access-group Lista1 in

14. Qual dos seguintes comandos apresenta o conteúdo da lista de acesso 187?

a) sh ip int
b) sh ip access-list
c) sh access-list 187
d) sh access-list 187 extended

15. Qual intervalo numérico define as listas de acesso IP estendidas?

a) 1-99
b) 200-299
c) 1000-1999
d) 100-199

16. Qual dos seguintes comandos é válido para a criação de uma lista de acesso IP estendida?

a) access-list 101 permit ip host 172.16.30.1 any eq 21
b) access-list 101 permit tcp host 172.16.30.1 any eq 21 log
c) access-list 101 permit icmp host 172.16.30.1 any ftp log
d) access-list 101 permit ip any eq 172.16.30.1 21 log

17. Qual intervalo numérico define listas de acesso IP padrão?

a) 100-199
b) 1-99
c) 1000-1999
d) 700-799

18. Qual a equivalência IP do *any* em uma lista de acesso IP?

a) 0.0.0.0 0.0.0.0
b) 255.255.255.255 255.255.255.255
c) any any
d) 0.0.0.0 255.255.255.255

19. Quais são os três comandos que podem ser usados para monitoramento de listas de acesso IP?

a) sh int
b) sh ip interface
c) sh run
d) sh access-list

20. Qual das seguintes linhas de comando deveria seguir a linha access-list 110 deny tfp any any eq ftp?

a) access-list 110 deny ip any any
b) access-list 110 permit tcp any any
c) access-list 110 permit ip any
d) access-list 110 permit ip any 0.0.0.0 255.255.255.255

21. Qual configuração de lista de acesso a seguir permite que apenas o tráfego destinado à rede classful 172.16.0.0 atravesse a interface S0?

a) access-list 10 permit 172.16.0.0 0.0.255.255 | int s0 | ip access-list 10 in

b) access-group 10 permit 172.16.0.0 0.0.255.255 | int s0 | ip access-list 10 out
c) access-list 10 permit 172.16.0.0 0.0.255.255 | int s0 | ip access-group 10 in
d) access-list 10 permit 172.16.0.0 0.0.255.255 | int s0 | ip access-group 10 out

22. Em que ponto as listas de acesso padrão devem ser aplicadas em uma rede?

a) No switch mais próximo.
b) Sempre o mais próximo da origem.
c) Sempre o mais próximo do destino.
d) No router com maior capacidade.

23. Em que ponto de uma rede as listas de acesso estendidas devem ser aplicadas, sempre que possível?

a) No switch mais próximo.
b) O mais próximo da origem.
c) O mais próximo do destino.
d) No router com maior capacidade.

24. Como você criaria uma ACL para bloquear o acesso Telnet apenas para hosts com ip ímpar, na rede local?

Respostas das Questões de Revisão – Segurança de Redes

01. C

02. A, E

03. C, E

4. A. Somente o endereço IP de origem é usado para filtrar a rede quando listas de acesso padrão são usadas.

5. E. Listas IP estendidas podem utilizar endereços IP de origem e destino, protocolos diversos, números de porta, entre outros parâmetros para filtragem de pacotes.

6. C. A máscara 0.0.255.255 informa ao router que os primeiros dois octetos devem ser iguais aos informados (172.16) e que os últimos dois podem ter qualquer valor.

7. B, D. O wildcard 0.0.0.0 informa ao router que os quatro octetos correspondentes no endereço devem ser iguais aos informados (172.16.30.55). O comando 0.0.0.0 pode ser substituído pelo comando host.

8. A, F. O primeiro item a ser verificado em uma questão como essa é o número da lista de acesso. Você verá que a resposta B está errada porque representa um número de lista IP padrão. O segundo item a ser verificado é o protocolo. Se a filtragem provém de um protocolo de camada superior, você deve utilizar UDP ou TCP. Isso elimina a resposta D. As respostas C e E possuem a sintaxe incorreta.

9. C, E. Apenas os comandos show ip interface e show run apresentarão as interfaces que possuem listas de acesso aplicadas.

10. E. As redes 172.16.16.0 a 172.16.23.0 possuem um block size de 8. O wildcard é sempre o valor do block size menos 1. Ex.: 8 - 1 = 7.

11. C, D. A sintaxe correta para criação de listas de acesso IP nomeadas segue o formato: ip access-list [standard/extended] [nome da lista].

12. F. As redes 172.16.32.0 a 172.16.63.0 possuem um block size de 32. O wildcard seria 0.0.31.255.

13. E. O comando ip access-group [nome da lista] [in/out] é a correta sintaxe para aplicação de listas de acesso nomeadas nas interfaces de um router.

14. B, C. Você pode visualizar listas de acesso através dos comandos show ip access-list ou show access-list [número da lista].

15. D. Listas IP estendidas são definidas no intervalo numérico de 100 a 199.

16. B. Lembre-se primeiro de checar o número da lista de acesso. Todas as listas nesse caso utilizam o número 101, o que as caracteriza como listas de acesso IP estendidas. A segunda coisa a ser checada é o protocolo. Somente uma lista está utilizando o TCP, necessário para acessar o protocolo (ou aplicação) FTP, através da porta lógica correspondente (21).

17. B. Listas IP padrão são definidas no intervalo numérico de 1 a 99.

18. D. 0.0.0.0 255.255.255.255 tem o mesmo efeito da palavra any em uma lista de acesso IP.

19. B, C, D. O comando show interface está errado porque não fornece nenhuma informação sobre listas de acesso. Os comandos show ip interface, show run e show access-lists fornecerão as informações para monitoramento de listas de acesso.

20. D. O comando access-list 110 permit ip any any é utilizado para especificar e permitir qualquer tipo de tráfego. O parâmetro 0.0.0.0 255.255.255.255 e o comando any possuem a mesma função.

21. C. Essa é uma lista de acesso IP padrão que realiza a filtragem baseada nos endereços IP de destino. O intervalo que identifica listas de acesso IP é 1-99. O comando para aplicar uma lista de acesso IP em uma interface é ip access-group. Como a questão especifica tráfego entrante, somente a resposta C é correta.

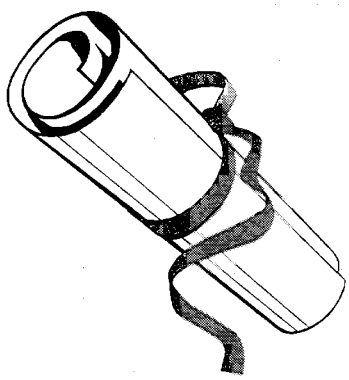
22. C. Listas padrão devem ser aplicadas o mais próximo possível do destino, sempre.

23. B. Sempre que possível, listas estendidas devem ser aplicadas o mais próximo possível da origem.

24. access-list 101 deny tcp 0.0.0.1 255.255.255.254 any eq telnet
access-list 101 permit ip any any

Relação dos Comandos Analisados

Comando	Descrição
0.0.0.0 255.255.255.255	*Wildcard*, o mesmo que o comando *any*
access-class	Aplica uma lista de acesso IP padrão a uma linha VTY
Access-list	Cria uma lista de acesso
Any	Especifica qualquer host e qualquer rede. O mesmo que 0.0.0.0 255.255.255.255
Host	Especifica o endereço de apenas um host
ip access-group	Aplica uma lista de acesso IP a uma interface
show access-lists	Apresenta todas as listas de acesso configuradas no router
show access-list 110	Apresenta apenas os parâmetros configurados para a lista 110
show ip access-list	Apresenta apenas listas de acesso IP
ip access-list extended Lista_Estendida	Cria a lista de acesso estendida chamada *Lista_Estendida* no router
sh access-list Lista_Estendida	Apresenta o conteúdo da lista chamada *Lista Estendida*
sh ip interface	Apresenta interfaces que possuem listas de acesso aplicadas, entre outras informações



10 Protocolos WAN

10.1 Tópicos Abordados

- Protocolos WAN:
  - O Protocolo HDLC;
  - Identificação de Operações PPP;
  - Configuração de Autenticação PPP;
  - Funcionamento do Frame-Relay;
  - Configuração de Frame-Relay LMIs, Maps e Subinterfaces
  - Monitoração de Operações Frame-Relay em um Router.

O sistema Cisco IOS é capaz de suportar diversos protocolos WAN (*Wide Area Protocol*) diferentes, que podem ajudá-lo a estender suas LANs para outras, remotamente localizadas. A interconexão de diversos sites dentro de uma corporação para troca de informações é imperativa na nova ordem econômica.

Entretanto, pense nos custos que isso traria se sua empresa precisasse implantar seus próprios cabos ou conexões para a interconexão de seus sites. Provedores de serviço permitem que conexões já instaladas por eles sejam arrendadas (*leased*) ou compartilhadas reduzindo enormemente os custos e o tempo de implantação.

É importante o entendimento dos diferentes tipos de protocolos e serviços WAN suportados pela Cisco. Não cobriremos aqui todos os protocolos suportados, apenas os abrangidos pelo exame CCNA. São eles: HDLC, PPP, Frame-Relay e ISDN. Outros exemplos populares seriam o ATM e o X.25.

10.2 Terminologia WAN

Para o entendimento das tecnologias WAN, é necessário o entendimento dos diferentes termos utilizados nesse tópico, assim como dos tipos de conexão que podem ser utilizados na interconexão de redes. Eis os termos mais comuns:

- **CPE (*Customer Premisses Equipment*)**: Define os equipamentos pertencentes ao assinante do serviço e localizados em suas instalações (normalmente um roteador ou um PABX);
- **Demarcation (*Demarc*)**: O último ponto sob a responsabilidade do provedor de serviço. Comumente, este ponto é um dispositivo localizado próximo ao CPE, responsável pela geração do clock de sincronismo para o CPE e pelo acesso físico à rede da operadora. Este elemento é conhecido como CSU/DSU (*Channel Service Unit / Data Service Unit*), no caso de conexões digitais. Quando a conexão contratada for analógica, o dispositivo que demarca o último ponto sob responsabilidade da operadora seria um MODEM;
- **Local loop**: Também conhecido como *Última Milha* (*last-mile*). Conecta o *demarc* à estação da operadora (*switching office*) mais próxima;
- **Central Office (CO)**: Conecta o assinante à rede do provedor (*provider's switching network*). O CO também é referido, às vezes, por POP (*Point of Presence*);
- **Toll Network**: Links de transporte (*trunk lines*) dentro da rede do provedor. Trata-se de uma coleção de estruturas e switches.

10.3 Tipos de Conexão WAN

- **Leased Lines**: Linhas privativas. Normalmente conhecidas como conexões ponto a ponto ou conexões dedicadas. Trata-se de um caminho WAN preestabelecido do CPE do site local, através de um switch DCE, até o CPE do site remoto, permitindo a comunicação ininterrupta entre redes DTE sem que procedimentos de ativação ou autenticação sejam necessários antes da transmissão de dados. São utilizadas linhas de transmissão seriais Síncronas de até 45Mbps (T3);
- **Circuit Switching**: Utiliza um procedimento de estabelecimento de link análogo a uma chamada telefônica.

Nenhum dado pode ser transmitido antes de uma conexão ponto a ponto ser estabelecida. Esse tipo de conexão é utilizado por modems comuns e ISDN. Utilizado em transmissões que requeiram baixa largura de banda;

- **Packet Switching**: Método de comutação WAN que permite o compartilhamento de largura de banda com outros usuários, resultando em grande redução de custos. Podemos comparar uma rede *packet switched* a uma linha telefônica comunitária. Uma vez que você não transmita dados constantemente, mas o faça esporadicamente, esse método pode reduzir seus custos drasticamente. Entretanto, se você transfere dados de forma constante, a melhor solução é o aluguel de uma linha privada (*leased line*). Frame-Relay, X.25 e ATM são exemplos de tecnologias que utilizam o método *packet switching*. As velocidades de transmissão variam de 56Kbps a 2Mbps.

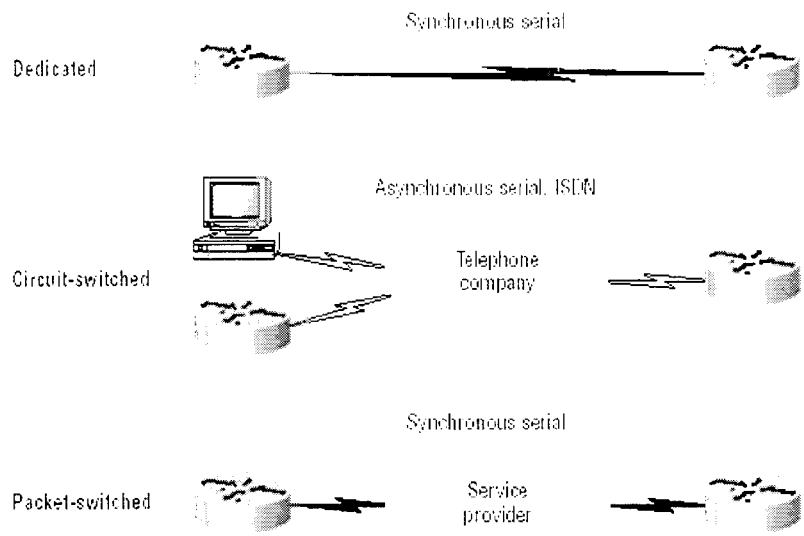


Figura 10.1: Tipos populares de conexão WAN.

10.4 Estudo dos Protocolos WAN

- **Frame-Relay**: Tecnologia de comutação de pacotes (*packet-switching*) que surgiu nos anos 90. O Frame-Relay é definido nas camadas física e de enlace (camadas 1 e 2), e é um protocolo de alta-performance. Ele assume que as estruturas utilizadas hoje são menos sujeitas a falhas do que quando o protocolo X.25 (do qual Frame-Relay é derivado) foi criado. Por esse motivo, o *overhead* foi reduzido, aumentando sua performance. O Frame-Relay possui uma relação custo-

benefício melhor que conexões ponto a ponto e suas velocidades variam de 64Kbps a 2048Kbps. Esse protocolo Frame-Relay disponibiliza recursos que possibilitam a alocação dinâmica de banda, assim como mecanismos eficientes para controle de congestionamento de dados;

- **ISDN (Integrated Services Digital Network)**: O ISDN, na verdade, não é um protocolo WAN, mas um padrão estabelecido pela indústria telefônica. Trata-se de uma série de serviços digitais que tornam possível a transmissão de voz e dados através de uma linha telefônica comum. O ISDN oferece uma solução de baixo custo para usuários remotos que necessitam de uma conexão relativamente rápida, se comparada à velocidade atingida via modems comuns. É também uma boa escolha para o estabelecimento de links de backup para outros tipos de conexões, como Frame-Relay ou conexões dedicadas;
- **LAPB (*Link Access Procedure, Balanced*)**: Esse protocolo orientado à conexão foi criado para ser utilizado na camada de enlace, juntamente com o protocolo X.25. O LAPB possui um *overhead* volumoso devido aos recursos de *windowing* e *time-out* que utiliza. Esse protocolo pode ser utilizado em lugar ao HDLC, se os links em questão forem extremamente sujeitos a falhas (*error-prone*). Como isso não é um problema real nos dias de hoje, o LAPB não é muito utilizado;
- **HDLC (*High-Level Data Link Control*)**: Protocolo orientado à conexão definido na camada de enlace. Possui um *overhead* bastante reduzido, se comparado ao protocolo LAPB. O HDLC não foi criado com a intenção de encapsular múltiplos protocolos de camada de rede através de um mesmo link. O **header HDLC não contém informações sobre o tipo de protocolo sendo transportado. Por esse motivo, cada fabricante que utiliza HDLC possui sua própria maneira de identificar o protocolo de camada de rede**, o que significa que o HDLC utilizado por cada fabricante é proprietário (exclusivo) aos equipamentos que fabricam;
- **SDLC (*Synchronous Data Link Control*)**: Protocolo de transmissão de dados mais utilizado em redes que obedecem ao padrão SNA (*Systems Network Architecture*) da IBM. O SDLC se assemelha ao protocolo HDLC (*High-level Data Link Control*), definido pela ISO (*International Organization for Standardization*);

- **PPP (*Point-to-Point Protocol*)**: Protocolo padrão da indústria. Uma vez que muitas versões do HDLC são proprietárias, o **PPP pode ser utilizado para criação de conexões ponto a ponto entre equipamentos de diferentes fabricantes.** Ele utiliza o campo *Network Control Protocol* (NCP) para identificação do protocolo de camada de rede. **Permite autenticação e conexões multilink e pode ser utilizado em links síncronos e assíncronos.**

10.4.1 O Protocolo HDLC

O HDLC é um popular protocolo de camada de enlace, padrão ISO, com orientação bit a bit, derivado do protocolo SDLC. Ele especifica um método de encapsulamento de dados em links seriais síncronos. O HDLC é um protocolo ponto a ponto utilizado em linhas privadas. Não é utilizado qualquer método de autenticação com esse protocolo.

Em protocolos com orientação byte a byte, informações de controle são codificadas usando-se bytes inteiros. Já em protocolos com orientação bit a bit (como é o caso do HDLC, SDLC, TCP, IP, entre outros), um bit pode representar uma informação de controle.

O HDLC é o **método de encapsulamento padrão utilizado em routers Cisco para conexões através de links seriais síncronos.** O HDLC utilizado pela Cisco, como comentamos, é proprietário ao fabricante, ou seja, apenas equipamentos Cisco são capazes de compreendê-lo.

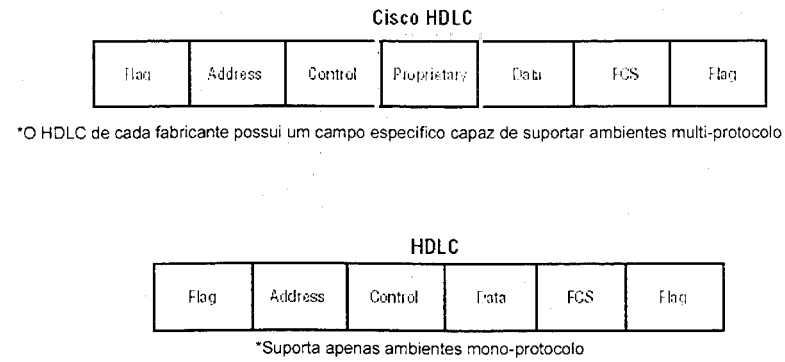


Figura 10.2: Frame HDLC proprietário Cisco e o frame HDLC padrão ISO.

Conforme a figura 10.2 mostra, a razão pela qual cada fabricante possui um método de encapsulamento HDLC único é que cada um adota uma metodologia diferente para fazer com que o protocolo HDLC se comunique com protocolos de camada de rede. Caso os fabricantes não implementassem uma solução para o HDLC se comunicar com os diferentes protocolos definidos na camada de rede, ele seria capaz de transportar apenas um protocolo. Esse cabeçalho proprietário é inserido no campo *data* do frame HDLC.

Caso você deseje conectar um router Cisco a um router de outro fabricante, o método de encapsulamento HDLC não poderia ser utilizado. Nesse caso, uma solução alternativa seria o uso do protocolo PPP, que é padronizado pela ISO.

10.4.2 O Protocolo PPP

O PPP é um protocolo de camada de enlace que pode ser usado através de links seriais síncronos (ex. ISDN) e assíncronos (*dial-up*) que utilizam LCP (*Link Control Protocol*) para estabelecer e gerenciar conexões na camada de enlace.

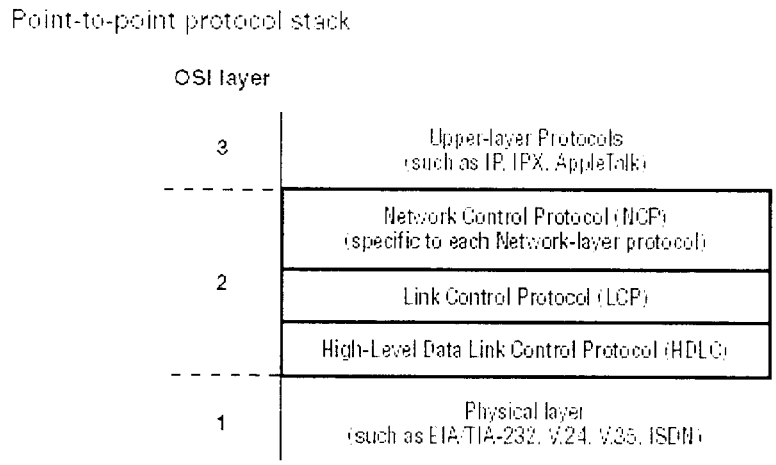


Figura 10.3: Pilha de protocolos que compõem o protocolo PPP e as camadas OSI.

A função básica do PPP é transportar pacotes de camada de rede através de um link ponto a ponto de camada de enlace. A figura 10.3 ilustra o conjunto (*stack*) de protocolos PPP mapeado ao modelo OSI.

O protocolo PPP é constituído de quatro componentes principais:

- **EIA/TIA-232-C**: Padrão internacional de camada física para comunicação serial;
- **HDLC**: Método de encapsulamento de datagramas através de links seriais;
- **LCP**: Protocolo utilizado no estabelecimento, configuração, manutenção e terminação de conexões ponto a ponto;
- **NCP**: Protocolo responsável pelo estabelecimento e configuração de diferentes protocolos de camada de rede. O protocolo PPP foi desenhado para permitir o uso simultâneo de múltiplos protocolos de camada de rede. Os protocolos usados aqui são específicos para cada protocolo de camada de rede. Alguns exemplos de protocolos usados: IPCP (IP Control Protocol) e IPXCP (IPX Control Protocol).

É importante entender que o conjunto de protocolos PPP é definidc nas camadas de enlace e física, somente. O NCP é utilizado para permitir a comunicação de múltiplos protocolos de camada de rede através dc seu encapsulamento através de um link PPP.

***Nota**: Repare que o protocolo PPP nada mais é que o HDLC ISO acrescido de funcionalidades extras, providas pelos outros protocolos da pilha.*

10.4.2.1 As Opções Disponíveis ao Protocolo LCP

O protocolo LCP (*Link Control Protocol*) disponibiliza ao encapsulamento PPP diferentes opções, incluindo as seguintes:

- **Autenticação**: Essa opção solicita, a partir do lado que está chamando, o envio de informações para identificação do usuário. Os dois métodos que iremos ver são PAP e CHAP;
- **Compactação**: Usada para maximizar o fluxo de dados (*throughput*) entre conexões PPP. O PPP descompacta o frame de dados na ponta receptora;
- **Detecção de Erros**: O PPP utiliza os recursos *Quality* e *Magic Number* para garantir o estabelecimento de uma conexão em fluxo de dados confiáveis;
- **Multilink**: A partir da versão 11.1 do sistema IOS, o recurso multilink é suportado em links PPP nos routers Cisco. Isso divide a carga PPP para dois ou mais circuitos paralelos, chamados *bundles*.

10.4.2.2 Estabelecimento de uma Sessão PPP

PPP pode ser utilizado com autenticação, ou seja, a comunicação entre dois routers deve prover informações que identifiquem o link como válido para comunicação. Quando conexões PPP são iniciadas, os links passam por três fases antes do estabelecimento da sessão:

1. **Link-establishment Phase**: Pacotes LCP são enviados por cada dispositivo PPP para configurar e testar o link. Os pacotes LCP contêm um campo chamado *Configuration Option*, que permite a cada dispositivo identificar o tamanho da compactação de dados e autenticação. Se não houver um campo *Configuration Option* presente, as configurações padrão são adotadas;

2. **Authentication Phase**: Se configurados, CHAP ou PAP podem ser utilizados para autenticar um link. O processo de autenticação acontece antes de as informações sobre protocolos de camada de rede serem processadas;
3. **Network-Layer Protocol Phase**: O PPP utiliza o protocolo NCP (*Network Control Protocol*) para permitir o encapsulamento e transmissão de múltiplos protocolos de camada de rede através de apenas um link PPP.

10.4.2.3 Os Métodos de Autenticação Utilizados pelo PPP

Existem dois métodos de autenticação que podem ser utilizados em links PPP:

- **Password Authentication Protocol (PAP)**: O PAP é o menos seguro dos dois métodos. Senhas (*passwords*) são enviadas como texto puro, sem que esquemas de criptografia sejam utilizados. Além disso, esse protocolo entra em ação apenas depois do estabelecimento inicial do link. Logo que um link PPP é estabelecido, o dispositivo remoto envia de volta ao router origem dados contendo o nome do usuário (*username*) e senha (*password*), até que eles sejam aceitos. Simplesmente isso;
- **Challenge Authentication Protocol (CHAP)**: O CHAP é ativado logo que um link PPP é estabelecido e, periodicamente, na sua checagem, para certificar-se de que o router ainda encontra-se em comunicação com o mesmo dispositivo.

Após o PPP ter concluído a fase inicial, o router local envia uma requisição challenge (*challenge request*) ao dispositivo remoto. Esse dispositivo envia ao router um valor calculado utilizando uma função especial chamada MD5. O router efetua, então, a comparação desse valor com o gerado por ele. Caso existam divergências, a conexão é imediatamente encerrada.

```
Router#conf t
Router(config)#int s0
Router(config-if)#encapsulation ppp
```

O processo de configuração PPP em uma interface é bastante simples. Para configurar PPP, basta seguir os passos ilustrados anteriormente. O encapsulamento PPP deverá estar configurado em ambas as interfaces conectadas através de um link serial para que o PPP funcione. Existem algumas outras configurações adicionais, que podem ser vistas ao se utilizar o comando *help*.

10.4.2.4 Configurando Autenticação PPP

Após configurar sua interface serial para suportar encapsulamento PPP, você pode então configurar o método de autenticação a ser utilizado por PPP entre dois routers. Primeiramente, **você deve configurar um *hostname* para o router,** caso isso já não tenha sido feito. Em seguida, defina um *username* e senha para o router localizado remotamente, que irá conectar-se ao seu router:

```
Router# config t
Router(config)# hostname RouterA
RouterA(config)# username net password cisco
```

Ao utilizar o comando *hostname*, lembre-se de que o *username* é o *hostname* do router localizado remotamente, que irá conectar-se ao seu router. No caso ilustrado, *net* é o *hostname* do router remoto. A senha definida para ambos os routers também deve ser a mesma. Trata-se de uma senha em formato texto, que pode ser visualizada ao se digitar o comando *sh run*. A senha pode ser criptografada com a utilização do comando *service password-encryption*, antes da definição do *username* e senha. Um *username* e uma senha devem ser configurados para cada dispositivo remoto a ser conectado, assim como para os routers remotos. Uma vez que o *hostname*, *usernames* e senhas tenham sido configurados, escolha o método de autenticação a ser utilizado - CHAP ou PAP:

```
RouterA# config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)# int s0
RouterA(config-if)# encap ppp
RouterA(config-if)# ppp authentication chap
RouterA(config-if)# ppp authentication pap
RouterA(config-if)# ^Z
RouterA#
```

Caso ambos os métodos sejam configurados, como ilustrado no exemplo anterior, **apenas o primeiro método será utilizado durante a "negociação" do link**. Caso ele venha a falhar, o segundo método é utilizado.

10.4.2.5 Verificação e Monitoramento PPP

Uma vez que o encapsulamento PPP esteja devidamente configurado, utilize o comando *sh int* para verificar se o PPP encontra-se, de fato, ativado:

```
RouterA#sh int s0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 10.0.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 239/255, txload 1/255, rxload 1/255
  Encapsulation PPP
  loopback not set
  Keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
[...]
```

Note o encapsulamento PPP no destaque.

Podemos ver também que o LCP está aberto (*LCP Open*) - lembre-se de que a função do LCP é estabelecer e manter conexões - e de que IPCP e CDPCP encontram-se ativos (*Open: IPCP, CDPCP*). Isso indica que os protocolos IP e CDP são suportados pela camada NCP.

Tanto a configuração como o monitoramento da autenticação PPP podem ser verificados através do comando *debug ppp authentication*.

10.4.3 O Protocolo Frame-Relay

O método de encapsulamento de alta performance conhecido como Frame-Relay é definido nas camadas física e de enlace do modelo OSI. Ele foi originalmente idealizado e desenvolvido para ser usado em interfaces ISDN e atualmente suporta uma grande variedade de interfaces.

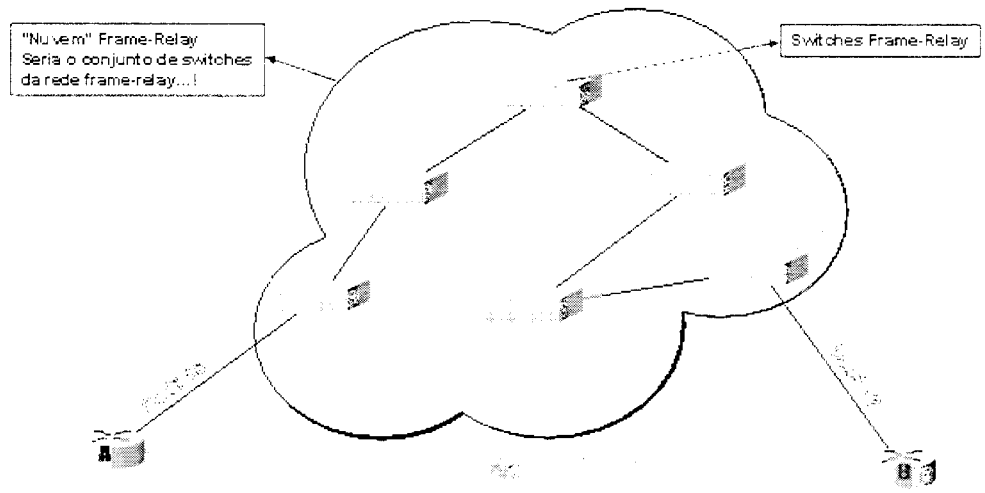
-Relay adotado pela Cisco suporta os seguintes protocolos:
, AppleTalk, XNS, IPX, CLNS, ISO, Banyan Vines, e
Bridging.

e-Relay provê uma interface de comunicação entre
s DTE e DCE. Como já estudamos, **DTEs englobam**
Cs, routers e bridges - equipamentos localizados no lado
s, geralmente, consistem de equipamentos de propriedade
a (*carrier*). O interessante sobre redes Frame-Relay (e outras,
é que elas operam na camada 2 do modelo OSI, ou seja,
quer informação de rede (camada 3) é completamente
para essas redes.

interfaces.

O Frame
IP, DECnet
Transparent

O Fram
dispositivo
terminais, P
cliente. DCE
da operadora
como ATM)
toda e qual
irrelevante p



Nesse exemplo, se o router A fizer um trace para o router B, tudo c que ele terá como resposta será a interface do próprio router B! Exato, não importa quantos switches Frame-Relay exista no caminho, o que os routers enxergarão será apenas um ao outro, como se estivessem diretamente conectados. E é exatamente isso o que é o PVC: Um circuitc virtual conectando os dois elementos diretamente de forma transparente.

O Frame-Relay é mais eficiente que o *X.25*, pois assume uma infra-estrutura menos sujeita a erros. Isso possibilita a redução do *overhead* utilizado. Ele provê comunicação orientada à conexão na camada de enlace, através do estabelecimento de circuitos virtuais (*Permanent Virtual Circuits - PVCs*). Esses circuitos são conexões lógicas criadas entre dois dispositivos DTE através de uma rede *packet-switched* e identificadas por um DLCI (*Data Link Connection Identifier*). Frame-Relay pode usar tanto circuitos virtuais permanentes (PVCs) como comutados (SVCs - *Switched Virtual Connections*), porém, **a grande maioria das redes Frame-Relay existentes utilizam apenas PVCs.** Esse tipo de circuito virtual estabelece o caminho completo até o destino antes de iniciar a transmissão de qualquer informação.

Para entender a terminologia utilizada é necessário, antes, que se entenda como o Frame-Relay funciona. A figura 10.4 contém vários termos utilizados na descrição das diferentes partes de uma rede Frame-Relay.

A idéia básica por trás do Frame-Relay é possibilitar a comunicação de usuários entre dois dispositivos DTE, através de dispositivos DCE. Para os usuários, a comunicação ocorre de forma transparente, como já mencionado.

A figura 10.4 ilustra tudo o que deve ocorrer para que dois dispositivos DTE possam se comunicar através de uma rede Frame-Relay.

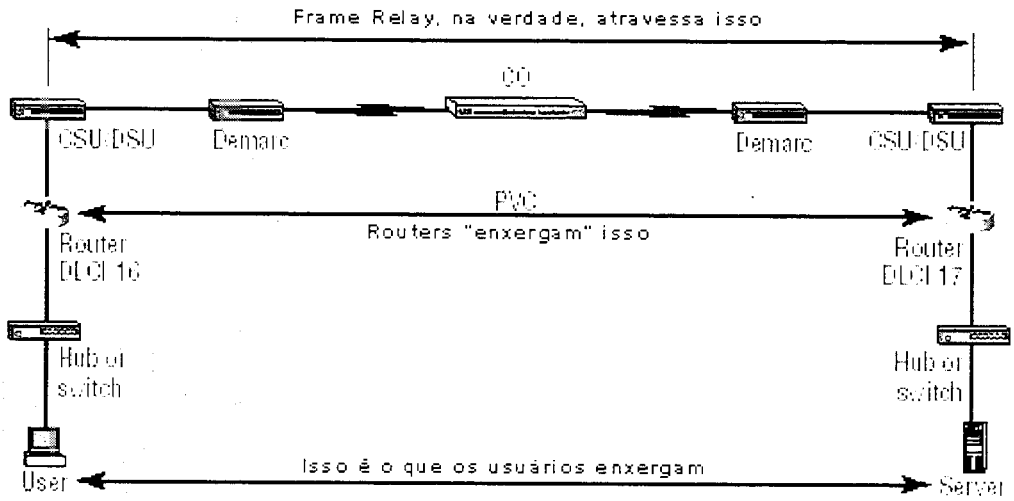


Figura 10.4: Operação de uma comunicação Frame-Relay.

A seguir, detalharemos o processo passo a passo.

1. O dispositivo de rede do usuário envia um frame através da rede local. O endereço de hardware (MAC) do router encontra-se no cabeçalho do frame enviado.
2. O router captura esse frame, extrai o pacote e descarta o frame. Em seguida, ele analisa o endereço IP de destino contido no pacote e confere - através de uma checagem na tabela de roteamento - se a rota até o referido endereço é conhecida.
3. O router, então, encaminha o pacote pela interface que, a princípio, pode alcançar a rede remota (se a rota até a rede remota não estiver na tabela de roteamento, o pacote será descartado). Uma vez que esta será uma interface serial com encapsulamento Frame-Relay, o router irá inserir o pacote na rede Frame-Relay encapsulado em um frame Frame-Relay. Será, então, adicionado a esse frame o número DLCI associado à interface serial em questão. Os DLCIs identificam o circuito virtual (PVC) para os routers e switches da operadora participantes da rede Frame-Relay.
4. O dispositivo CSU/DSU (*Channel Service Unit/Data Service Unit*) recebe o sinal digital e o codifica em um tipo de sinal que o switch localizado no *Packet Switch Exchange* (PSE) possa entender. O PSE recebe o sinal e extrai a seqüência de 1s e 0s da linha.
5. O CSU/DSU encontra-se conectado a um *demarc* instalado pelo provedor de serviço. O *demarc*, no caso de um circuito Frame-Relay, é uma "tomada" RJ-45 localizada próxima ao CSU/DSU.

6. O *demarc* consiste de um par de cabos trançados (*twisted pai cable*) que se conecta ao local loop. Este, por sua vez, se conect ao CO (*Central Office*). O modo como o local loop se conect ao CO engloba uma variedade de meios físicos. Os mai comuns sendo fibra óptica ou par trançado metálico.
7. O CO recebe o frame e o envia através da "nuvem" (rede Frame-Relay para o seu destino. Essa "nuvem" pode se composta por dezenas de *switching offices* ou mais. C endereço IP de destino e o número DLCI correspondent são analisados. Normalmente, o número DLCI da red remota é obtido através do *mapeamento IP-para-DLCI*. A bas de dados para esse mapeamento normalmente é criad manualmente pelo provedor do serviço, porém, pode se dinamicamente criada através do uso do protocolo IARI (*Inverse ARP*). Lembre-se de que, antes de dados seren enviados através da "nuvem", um circuito virtual ponto a ponto é estabelecido.
8. Uma vez que o frame alcance o *switching office* mais próxim do *destination office*, ele é enviado através do local loop. C frame é recebido no *demarc* destino e é então enviado ac dispositivo CSU/DSU local. Finalmente, o router destin extrai o pacote do frame e o insere na LAN, para que ele seja enviado ao dispositivo para o qual se destina.

10.4.3.1 Configuração do Frame-Relay em Routers Cisco

Ao configurar Frame-Relay em routers Cisco, você deve especificá-lo com um método de encapsulamento nas interfaces seriais. Existem apenas doi tipos de encapsulamento Frame-Relay: *Cisco* e *IETF*. A seguir ilustramo as duas opções ao se configurar Frame-Relay em um router Cisco.

```
Router#config t
Router(config)#int s0
Router(config-if)#encap frame-relay ?
 ietf  Use RFC1490 encapsulation
```

O método default é Cisco, a não ser que o IETF seja manualmente escolhido. O Cisco é o método que deve ser usado na conexão entre dois routers Cisco. Já **o IETF deve ser escolhido na conexão entre um router Cisco e um de outro fabricante.** Portanto, antes de optar por um método de encapsulamento, cheque com seu provedor qual equipamento eles utilizam.

10.4.3.2 DLCI – Data Link Connection Identifiers

Os circuitos virtuais criados pelo Frame-Relay são identificados pelo DLCI. Normalmente o provedor de serviço Frame-Relay, como uma operadora de telefonia, designa os números DLCI que são utilizados pelo Frame-Relay para distinguir entre os diferentes circuitos virtuais existentes em uma rede. No caso de muitos circuitos virtuais terminarem em apenas uma interface Frame-Relay multiponto, muitos DLCIs ficarão associados a ela.

Para que os dispositivos IPs em cada ponta do circuito virtual possam se comunicar, **seus endereços IPs devem ser mapeados para números DLCI**. Esse mapeamento pode ser realizado dinamicamente através do protocolo IARP (*Inverse Address Resolution Protocol*), ou manualmente, através do comando *Frame-Relay map*.

Cada número DLCI pode ter um significado local ou global em qualquer ponto da rede Frame-Relay. Algumas vezes, um provedor pode designar a um site um número DLCI que é propagado para todos os sites remotos que utilizam o mesmo PVC. Nesse caso, o PVC possui significância global (*global meaning*). Eis um exemplo: o escritório central de uma empresa pode ter o número DLCI 20 designado a ele. Todos os sites remotos deverão saber que o DLCI do escritório central é 20 e poderão usar esse PVC para se comunicar com ele.

Entretanto, o mais comum é dar ao DLCI um significado local (*local meaning*). Isso significa que os números DLCI apenas precisam ser únicos em uma mesma ponta de um link de acesso. **Dois números DLCI podem ser iguais em diferentes pontas de um mesmo circuito**, pois o Frame-Relay mapeia um número DLCI local para um circuito virtual em cada interface do switch. A figura 10.5 ilustra este princípio.

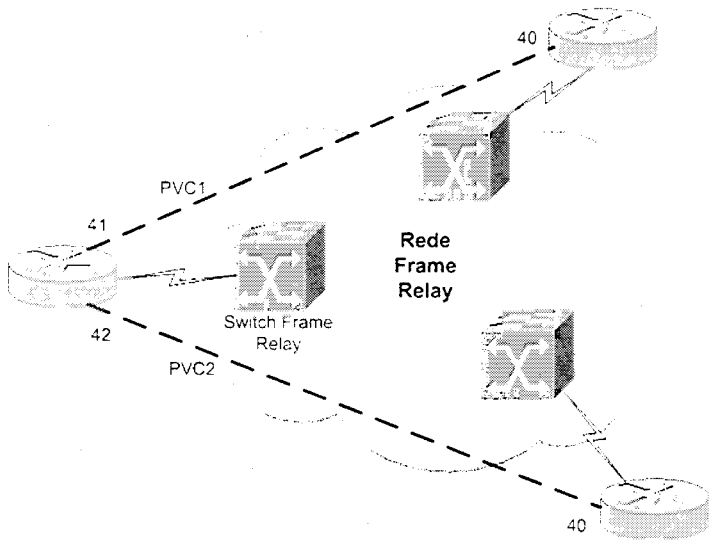


Figura 10.5: Funcionamento dos DLCIs em uma rede Frame-Relay.

Cada localidade remota pode, então, ter seu próprio número DLC e comunicar-se com a localidade central utilizando números DLC distintos. Números DLCI são tipicamente designados pelo provedor, e **começam no número 16.**

A seguir ilustramos como configurar o número DLCI para ser associado a uma interface.

```
Router(config-if)#frame-relay interface dlci ?
  <16-1007) Define a DLCI as part of the current subinterface
Router(config-if)#frame-relay interface dlci 16
```

10.4.3.3 Local Management Interface (LMI) e suas Mensagens

A interface de gerenciamento local (LMI) foi desenvolvida em 1990 pela Cisco, StrataCom, Northern Telecom e Digital Equipment Corporation (DEC), e ficou conhecida como *Gang-of-Four LMI* ou *Cisco LMI.*

Essa "gang" pegou o protocolo Frame-Relay básico, definido pelo CCITT, e adicionou a ele uma série de recursos que permitiram aos dispositivos de rede se comunicarem mais facilmente através de uma rede Frame-Relay.

O LMI é um padrão de sinalização entre um dispositivo CPE (como um router) e um frame switch e é responsável pelo gerenciamento e manutenção do status entre esses dispositivos. As mensagens LMI provêm informações sobre:

- **Keepalives**: Verifica quais dados estão fluindo;
- **Multicasting**: Provê um DLCI PVC local;
- **Endereçamento Multicasting**: Provê significância global;
- **Status dos Circuitos Virtuais**: Provê o status do DLCI.

A partir do sistema IOS 11.2, o tipo de LMI é automaticamente detectado (*auto-sensed*). Isso possibilita a uma interface determinar o tipo de LMI suportado pelo switch.

Se você não dispõe do recurso *auto-sense*, você deverá checar com o provedor qual o tipo de LMI a ser usado.

Os três diferentes tipos de LMI disponíveis são: Cisco, ANSI e Q933A. O tipo default é Cisco, mas você poderá ter que mudar para ANSI ou Q933A.

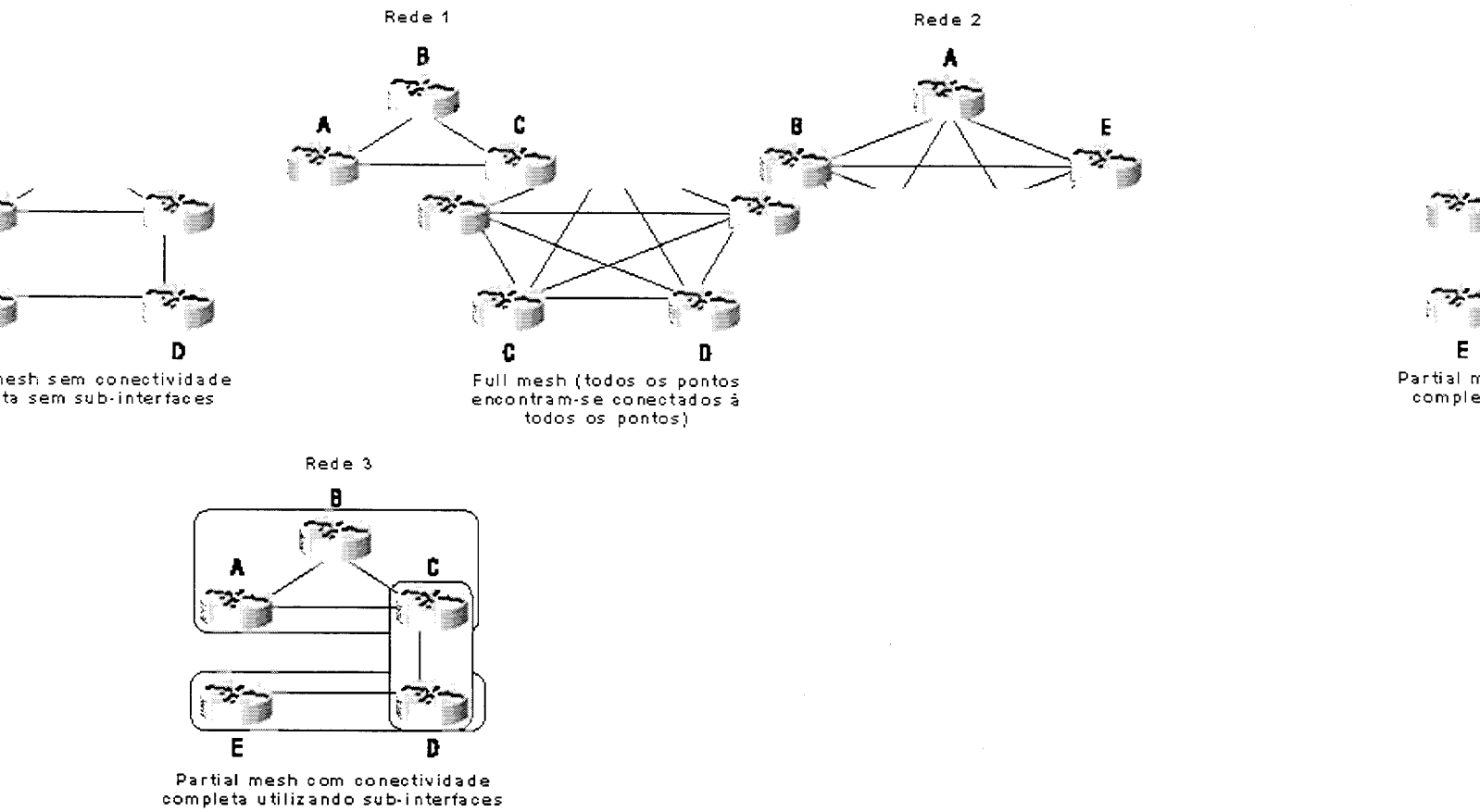
Routers recebem informações LMI em uma interface encapsulada Frame-Relay e atualizam o status dos circuitos virtuais para um dos três diferentes estados:

- **Ativo (*active state*)**: Tudo se encontra ativo e os routers podem trocar informações;
- **Inativo** (*inactive state*): A interface do router encontra-se ativa e conectada ao *switching office*, mas o router na outra ponta, não;
- **Deleted** (*deleted state*): Nenhuma informação LMI transmitida pelo switch está sendo recebida na interface do router. Isso pode ser devido a um problema de mapeamento ou do próprio link.

10.4.3.4 O Benefício Proporcionado por Subinterfaces

Você pode ter múltiplos circuitos virtuais em apenas uma interface serial e, ainda assim, tratar cada um como uma interface diferente. A isso chamamos subinterfaces. Pense em uma subinterface como uma interface física definida pelo IOS. Uma vantagem de se criar subinterfaces é a habilidade atingida de se designar diferentes características de camada de rede a cada subinterface e circuito virtual, como roteamento IP em uma e IPX em outra.

Você pode criar subinterfaces para amenizar os problemas causados por redes constituídas de forma parcialmente interconectadas (*partial meshed*), como na figura 10.6.



gura 10.6: Benefícios proporcionados pelo uso de subinterfaces. *Fi*

Por exemplo, digamos que você esteja adotando o protocolo IP em uma rede LAN. Se, em uma mesma rede física, o router A pode se comunicar com o router B e este com o router C, você normalmente assumiria que o router C pode se comunicar com o router A. Embora essa premissa seja verdadeira para uma LAN, não é necessariamente verdadeira para uma rede Frame-Relay, a não ser que o router A tenha um PVC definido até o C.

Na figura 10.6, a rede 1 encontra-se configurada com cinco sites. Para que essa rede funcione, uma rede totalmente interconectada (*fully meshed*), como a de número 2 na figura, teria de ser criada, a princípio. Entretanto, mesmo que o exemplo ilustrado na rede 2 seja totalmente funcional, sua implantação é extremamente cara. A solução apresentada na rede 3 - utilizando subinterfaces - é a de melhor custo-benefício.

Na rede 3, a configuração de subinterfaces é um modo de subdividir a rede Frame-Relay em sub-redes de menores proporções - cada uma com seu próprio endereço de rede. Portanto, os sites A, B e C encontram-se totalmente interconectados (*fully meshed network*), enquanto os sites C e D, e D e E encontram-se conectados através de conexões ponto a ponto.

A criação de subinterfaces também resolve o problema com protocolos de roteamento que utilizam o recurso *split horizon*. Como estudamos, esses protocolos não propagam atualizações pela mesma interface onde essas foram recebidas. Isso pode ser um problema em uma rede Frame-Relay totalmente interconectada. Entretanto, criando-se subinterfaces, protocolos de roteamento que recebem atualizações em uma subinterface podem propagar a mesma atualização por uma outra subinterface.

10.4.3.5 Criação de Subinterfaces

```
RouterA(config)#int s0
RouterA(config-if)#encapsulation frame-relay
RouterA(config-if)#int s0.?
 <0-4294967295> Serial interface number
RouterA(config-if)#int s0.16 ?
  multipoint       Treat as a multipoint link
  point-to-point   Treat as a point-to-point link
```

Subinterfaces são definidas através do comando *int s0.{número da subinterface}*, como ilustrado anteriormente.

Você pode definir um número virtualmente ilimitado de subinterfaces em uma determinada interface física (considerando a memória disponível do router). No exemplo anterior, escolhemos utilizar a subinterface 16, já que esse é o número que representa o DLCI designado àquela interface. Existem dois tipos de subinterface:

- **Point-to-point**: Usadas quando apenas um circuito virtual conecta um router a outro. Cada interface *point-to-point* requer sua própria sub-rede;
- **Multipoint**: Usadas quando o router é o centro de uma estrela de circuitos virtuais. Utiliza apenas uma sub-rede para todas as interfaces dos routers conectadas ao switch.

Ilustramos a seguir a saída do comando *sh run* em um router em ambiente de produção configurado com múltiplas subinterfaces. Note que cada uma tem seu número baseado no DLCI designado à interface. Isso ajuda na administração das interfaces. Note também que não há um tipo de LMI definido, o que significa que está sendo adotado o tipo padrão (Cisco) ou que o modo de detecção automática está ativo (no caso de o IOS ser versão 11.2 ou mais recente). Note ainda que cada subinterface é definida como uma sub-rede distinta, rede IPX distinta e alcance do cabo *AppleTalk* distinto.

Exemplo de saída do comando *sh run* em um router com múltiplas subinterfaces configuradas:

```
interface Serial0
no ip address
no ip directed-broadcast
encapsulation frame-relay
!
interface Serial0.102 point-to-point
ip address 10.1.12.1 255.255.255.0
no ip directed-broadcast
frame-relay interface-dlci 102
!
interface Serial0.103 point-to-point
ip address 10.1.13.1 255.255.255.0
no ip directed-broadcast
ted-broadcast                                                    no ip direct
 interface-dlci 103                                              frame-relay
                                                                 !
erial0.104 point-to-point                                        interface Se
0.1.14.1 255.255.255.0                                           ip address 1
ted-broadcast                                                    no ip direct
```

```
frame-relay interface-dlci 104
!
interface Serial0.105 point-to-point
ip address 10.1.15.1 255.255.255.0
no ip directed-broadcast
frame-relay interface-dlci 105
!
(...)
```

10.4.3.6 Mapeamento Frame-Relay

Conforme explicado anteriormente, para que dispositivos IPs possam se comunicar através de uma rede Frame-Relay, seus endereços IPs devem ser mapeados para números DLCI. Existem dois modos de se efetuar esse mapeamento: utilizando o comando *frame-relay map* ou usando o recurso *inverse-arp*.

```
RouterA(config)#int s0
RouterA(config-if)#encap frame
RouterA(config-if)#int s0.16 multipoint
RouterA(config-if)#no inverse-arp
RouterA(config-if)#ip address 172.16.30.1 255.255.255.0
RouterA(config-if)#frame-relay map ip 172.16.30.17 17 broadcast
RouterA(config-if)#frame-relay map ip 172.16.30.18 18 broadcast
RouterA(config-if)#frame-relay map ip 172.16.30.19 19 broadcast
RouterA(config-if)#^Z
```

Acima ilustramos um exemplo de uso do comando *map*. Eis um resumo do que foi feito:

Primeiro, configuramos a interface serial 0 para utilizar o encapsulamento Frame-Relay default (Cisco). Criamos, então, uma subinterface. Em seguida, desativamos o recurso *inverse-arp* e mapeamos três circuitos virtuais e seus números DLCI correspondentes. **Note que alteramos o tipo de encapsulamento (ietf) para a primeira subinterface.** O comando *frame-map* é a única maneira de se configurar múltiplos tipos de encapsulamento em uma mesma interface.

A palavra *broadcast* que aparece no final da linha de comando informa ao router para encaminhar mensagens broadcast destinadas à interface em questão para o circuito virtual especificado. Lembre-se que o Frame-Relay é um método de encapsulamento que não propaga *broadcasts* por default (ele é classificado como *non-broadcast multiaccess*), o que significa que ele não propagará algumas informações necessárias

otocolos de roteamento, afetando seu funcionamento. Para
e-Relay efetue a propagação de *broadcasts*, a palavra
tamente com o comando *frame-map* deve ser usada.

de aplicar o comando *map* a cada circuito virtual, você
r o recurso *inverse-arp* para que o mapeamento seja feito
nte. Nesse caso, a configuração anterior ficaria assim:

```
nfig)#int s0
nfig-if)#encap frame
nfig-if)#int s0.16 multipoint
nfig-if)#inverse-arp
nfig-if)#ip address 172.16.30.1 255.255.255.0
nfig-if)#^Z
```

e pode observar, esse método é muito mais fácil. Porém,
tável quanto o método manual.

squemas de Controle de Congestionamento mpregados pelo Frame-Relay

y utiliza três métodos para lidar com problemas de
mento:

DE (*Discard Eligibility*): Quando um router Frame-Relay
etecta congestionamento na rede Frame-Relay, ele ativa o
it DE no cabeçalho do pacote Frame-Relay (passará de 0
ara 1). Se o switch Frame-Relay estiver congestionado, ele
escartará primeiro os pacotes que tenham o bit DE ativado.

***a**: Se sua largura de banda estiver configurada com um CIR
nmited information Rate) de zero, o bit DE sempre se
ntrará ativado.*

ECN (*Forward-Explicit Congestion Notification*): Quando
rede Frame-Relay identifica um congestionamento na
nuvem", o switch ativa o bit FECN no cabeçalho do pacote
rame-Relay. Isso informará ao DCE destino que a rota
ecém-atravessada pelo pacote em questão encontra-se
ongestionada;

BECN (*Backward-Explicit Congestion Notification*):
Quando o switch detecta um congestionamento na rede
rame-Relay, ele ativa o bit BECN no cabeçalho do pacote
rame-Relay e o envia de volta ao router origem,
nformando-o que reduza o fluxo de pacotes.

a alguns pro
que o Fram
broadcast jun

Em vez
pode utiliza
dinamicame

```
RouterA(co
RouterA(co
RouterA(co
RouterA(co
RouterA(co
RouterA(co
```

Como se
não é tão es

10.4.3.7 Es Er

Frame-Rela
congestiona

- D
  d
  b
  p
  d

---

*Not
(Co
enco*

- F
  a
  "
  F
  r
  c
- B
  Q
  F
  F
  i

10.4.3.8 Commited Information Rate (CIR)

O Frame-Relay permite que múltiplos usuários compartilhem uma mesma rede de pacotes (*packet-switched network*) simultaneamente. Isso é positivo, uma vez que divide o custo da utilização dos switches entre os usuários. Entretanto, o conceito Frame-Relay se baseia na premissa de os usuários da rede não enviarão dados de forma constante simultaneamente. **O Frame-Relay funciona melhor com tráfego em rajadas (*burst traffic*).**

Ele funciona provendo uma largura de banda dedicada para cada usuário, que fica comprometido com aquela largura todo o tempo. Provedores de serviço, normalmente, permitem que usuários adquiram uma quantidade de largura de banda menor do que aquela de que realmente necessitam. A isso chamamos CIR. O que isso implica é que um usuário pode adquirir uma largura de banda em uma rede Frame-Relay de, por exemplo, 256Kbps, sendo possível que ele atinja velocidades em rajada muito superiores. O CIR especifica que, enquanto a transmissão de dados feita por dispositivo em uma rede Frame-Relay não exceda o CIR, a rede continuará a encaminhar os pacotes ao PVC. Entretanto, **se o fluxo de dados exceder o CIR, não há garantias.**

O valor do CIR a ser contratado junto à operadora deve ser escolhido com base em projeções realísticas. Alguns provedores permitem a aquisição de um CIR de zero. Isso pode ser uma opção quando custo é um problema e o reenvio constante de pacotes é aceitável. Entretanto, deve-se entender que **o bit DE, nesse caso, estará sempre ativado.**

10.4.3.9 Monitorando Frame-Relay em Routers Cisco

Os seguintes comandos podem ser utilizados para o gerenciamento das configurações Frame-Relay em um router Cisco:

- **Show frame-relay lmi**: Apresenta estatísticas sobre o tráfego LMI ocorrido entre um router local e um switch Frame-Relay;
- **Show frame-relay pvc**: Relaciona todos os circuitos virtuais (PVCs) configurados (interfaces) e respectivos números DLCI. Apresenta o status de cada conexão PVC e estatísticas de tráfego. Também informa o número de pacotes BECN e FECN recebidos pelo router;
- **Show interface**: O comando *sh interface* pode ser usado para checagem de tráfego LMI. Apresenta informações sobre o encapsulamento utilizado, assim como informações sobre

camadas 2 (data-link) e 3 (rede). A informação sobre o tipo de LMI sendo usado é **apresentada como LMI DLCI 1023 (Cisco) ou LMI DLCI 0 (ANSI);**

- **Show frame map**: Apresenta o mapeamento IP/IPX-para-DLCI;
- **Debug frame lmi**: A informação originada desse comando permite que você verifique e identifique problemas em conexões Frame-Relay, ajudando-o a determinar se a comunicação *router-switch* Frame-Relay está ocorrendo sem problemas. A saída desse comando é apresentada no console do router, por default.

Questões de Revisão – Protocolos Wan

1. Quais dos seguintes protocolos fazem parte do conjunto de protocolos usado pelo PPP?

a) HDLC
b) LCP
c) SDLC
d) NCP
e) LAPB

2. Quantos tipos de encapsulamento Frame-Relay os routers Cisco suportam?

a) 2
b) 3
c) 4
d) 5

3. Quantos tipos de LMI encontram-se disponíveis?

a) 2
b) 3
c) 4
d) 5

4. Com relação ao protocolo Frame-Relay, qual das seguintes afirmações é correta?

a) O encapsulamento Cisco deve ser usado se a conexão envolver um equipamento de outro fabricante.
b) O encapsulamento ANSI deve ser adotado se a conexão envolver um equipamento de outro fabricante.
c) O encapsulamento IETF deve ser usado se a conexão envolver um equipamento de outro fabricante.
d) O encapsulamento Q.933a deve ser usado se a conexão envolver um equipamento de outro fabricante.

5. Qual é o tipo de LMI default em roteadores Cisco?

a) Q.933A
b) ANSI
c) IETF
d) Cisco

6. Qual das seguintes tecnologias WAN estabelece um PVC na camada 2?

a) X.25 c) Frame-Relay
b) ISDN d) HDLC

7. Se você desejasse visualizar os DLCIs configurados em sua rede Frame-Relay, quais comandos você usaria?

a) sh frame-relay d) sh frame-relay dlci
b) show running e) sh frame-relay pvc
c) sh int s0

8. Qual a função do protocolo IARP?

a) Mapear endereços X.21 para X.25.
b) Mapear DLCIs para endereços de rede.
c) Prover endereçamento SMDS.
d) Mapear endereços ATM para circuitos virtuais (VCs).

9. Qual das opções abaixo seria a melhor colocação com relação ao DLCI?

a) Seu uso é facultativo em redes Frame-Relay.
b) Representa apenas um circuito físico.
c) É usado na identificação de conexões lógicas entre dispositivos DTE.
d) É usado para identificar o início de um frame durante o processo de comutação em uma LAN.

10. Qual comando lista todos os PVCs e DLCIs configurados?

a) sh frame pvc c) sh frame lmi
b) sh frame d) sh pvc

11. Qual é o encapsulamento default para links seriais ponto a ponto entre dois routers Cisco?

a) SDLC b) HDLC c) Cisco d) ANSI

12. Quais informações a Interface de Gerenciamento Local (LMI) fornece?

a) O status dos circuitos virtuais (PVCs).
b) Os valores dos DLCIs.
c) Informação sobre significância (global ou local) dos DLCIs.
d) O tipo de encapsulamento LMI em uso.

13. Qual protocolo do conjunto PPP viabiliza a utilização de múltiplos protocolos de camada de rede durante uma conexão?

a) LCP b) NCP c) HDLC d) X.25

14. Qual protocolo do conjunto PPP é usado no estabelecimento, configuração e autenticação de uma conexão na camada de enlace?

a) LCP
b) NCP
c) HDLC
d) X.25

15. Em redes Frame-Relay, o que identifica o PVC?

a) NCP b) LMI c) IARP d) DLCI

16. Qual das afirmações abaixo é verdadeira com relação aos LMIs?

a) Mapeiam os valores dos DLCIs para circuitos virtuais.
b) Mapeiam endereços X.21 para circuitos virtuais.
c) Informam o status dos circuitos virtuais.
d) Provêm informações sobre os valores DLCI em uso.

17. Qual dos seguintes é usado para controle de congestionamento em redes Frame-Relay?

a) DLCI
b) IARP
c) LMI
d) BECN

Respostas das Questões de Revisão – Protocolos WAN

1. **A, B, D**. Os protocolos que pertencem à pilha de protocolos PPP são o HDLC e o LCP, localizados na subcamada MAC da camada de enlace e o NCP, localizado na subcamada LLC da camada de enlace.

2. **A**. Routers Cisco suportam dois tipos de encapsulamento Frame-Relay: Cisco e IETF, sendo Cisco o tipo de encapsulamento Frame-Relay default.

3. **B**. Routers Cisco suportam três tipos de LMI: Cisco, ANSI e Q.933A, sendo Cisco o tipo default.

4. **C**. IETF é o método de encapsulamento que deve ser utilizado em conexões Frame-Relay entre routers não-Cisco.

5. **D**. O tipo de LMI default em routers Cisco é *Cisco*.

6. **C**. O protocolo Frame-Relay estabelece PVC na camada de enlace.

7. **B, E**. Os comandos show running-config e show frame-relay *pvc* podem ser utilizados para visualização dos DLCIs configurados em um router.

8. **B**. IARP é utilizado para mapear endereços de rede para valores DLCI.

9. **C**. O uso dos DLCIs é necessário para cada circuito Frame-Relay. O número do DLCI identifica os PVCs em cada circuito. Os PVCs são conexões lógicas entre dois dispositivos DTE.

10. **A**. O comando *show frame-relay pvc* apresenta informações sobre os PVCs e os respectivos DLCIs associados.

11. **B**. A Cisco define uma versão proprietária do protocolo HDLC como encapsulamento default em todas as conexões seriais ponto a ponto.

12. **A, B, C**. A mensagem fornecida pelo LMI fornece o status dos PVCs, os valores DLCI associados a cada PVC e a significância global ou local dos valores DLCI.

13. **B**. O NCP atua na subcamada LLC da camada de enlace e possibilita que múltiplos protocolos de rede sejam usados com PPP.

14. **A**. O LCP atua na subcamada MAC da camada de enlace e gerencia o estabelecimento, configuração e autenticação de uma conexão nessa camada.

15. **D**. DLCIs são responsáveis pela identificação dos PVCs em uma rede Frame-Relay.

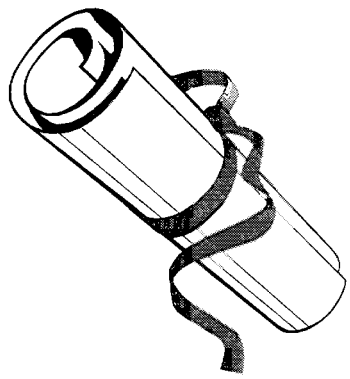
16. **C, D**. A mensagem fornecida pelo LMI fornece o status dos PVCs, os valores DLCI associados a cada PVC e a significância global ou local dos valores DLCI.

17. **D**. Backward-Explicit Congestion Notification (BECN) é utilizado para amenizar problemas de congestionamento em redes Frame-Relay.

Relação dos Comandos Analisados

Comando	Descrição
debug frame-relay lmi	Apresenta o fluxo lmi entre um router e um switch Frame-relay
encapsulation frame-relay	Muda o encapsulamento para Frame-Relay em uma interface serial
encapsulation frame-relay ietf	Muda o encapsulamento para ietf, permitindo a interconexão entre routers Cisco e de outros fabricantes
encapsulation hdlc	Restabelece o encapsulamento default (HDLC) em um link serial
encapsulation ppp	Altera o encapsulamento em um link serial para PPP
frame-relay interface-dlci	Configura o endereço PVC em uma interface ou subinterface serial
frame-relay lmi-type	Configura o tipo do LMI em um link serial
frame-relay map	Cria mapas PVC-para-IP estáticos

Comando	Descrição
interface s0.16 multipoint	Cria uma interface multiponto em um link serial
interface s0.16 point-to-point	Cria uma interface ponto a ponto em um link serial
no inverse-arp	Desativa o recurso IARP para a configuração estática de mapas Frame-relay
ppp authentication chap	Informa PPP para usar o método de autenticação CHAP
ppp authentication pap	Informa PPP para usar o método de autenticação PAP
show frame-relay lmi	Define o tipo do LMI em uma interface serial
show frame-relay map	Apresenta o mapeamento IP/IPX-para-PVC estático e dinâmico
show frame-relay pvc	Apresenta os PVCs configurados e respectivos DLCIs
show ip route	Apresenta a tabela de roteamento IP
username {nome} password {pwd}	Cria *usernames* e senhas para autenticação em um router Cisco



11 Configuração de Switches

11.1 Configuração de Switches Catalyst 2900

- Configurações Básicas;
- Gerenciamento da Tabela de Endereçamento MAC;
- Definição de Endereços MAC Permanentes e Estáticos;
- Configuração de Segurança em Portas;
- Configuração de VLANs;
- Configurações VTP.

O exame 640-802 cobra conhecimentos em switches da linha 2900. Neste livro, veremos como configurar o modelo 2950. Na verdade, todas as configurações que veremos aqui, aplicadas ao modelo 2950, podem ser realizadas exatamente da mesma forma em outras linhas de switches Cisco (ex. 3560, 3750, etc).

O switch Catalyst 2950 é um dos modelos básicos dentro da família Catalyst da Cisco. Existem 6 modelos distintos ainda comercializados, dentro desta família: 2950G-12 (12 portas FastEthernet e 2 slots GBIC para uplinks), 2950G-24 (24 portas FastEthernet e 2 slots GBIC para uplinks), 2950G-48 (48 portas FastEthernet e 2 slots GBIC para uplinks), 2950G-48DC (semelhante ao 2950G-48, mas com alimentação DC), 2950C-24 (24 portas FastEthernet e 2 portas 100Base-FX para uplink), e 2950T-24 (24 portas FastEthernet e 2 portas 10/100/1000BaseT para uplink). Todos os modelos disponíveis possuem ao menos portas 10/100 e, portanto, aceitam configurações de *trunking* em todas as portas.

É interessante mencionar, entretanto, que nenhum switch da linha 2950 suporta *ISL trunking*. Esta linha suporta apenas **trunking IEEE 802.1q** (*dot1q*). Ao que parece, a Cisco já vem adotando o encapsulamento 802.1q como padrão em seus switches já há algum tempo, o que me leva a concluir que o protocolo proprietário ISL, criado pela empresa, deixará em breve de ser suportado.

Neste capítulo, analisaremos como inicializar e configurar os switches Catalyst 2950 via linhas de comando (CLI). Começaremos com a conexão do cabo console e com o que acontece assim que um switch é inicializado. Após passarmos pelos comandos básicos, ilustraremos como configurar VLANs, roteamento inter-VLAN e VTP em um switch Cisco.

11.2 Recursos do Switch 2950

A linha 2950, assim como os roteadores vistos anteriormente, permite sua configuração via CLI. Ainda hoje, existem dois tipos de sistemas operacionais que podem rodar em switches Cisco Catalyst:

- **IOS**: Nesse caso, o processo de configuração do switch é muito similar ao de um router. Switches Catalyst 29x0, 35xx, 36xx, 37xx, dentre outros, podem rodar o sistema IOS;
- **CatOS**: Esse sistema usa uma série de comandos CLI mais antigos (*set-based*). Os switches que são configurados via *CLI set-based* são os mais antigos, como o 2926, o 2948G e a linha 5000, porém, switches mais recentes como os das linhas 45xx e 65xx também podem rodar este sistema. Na verdade, switches das linhas 45xx e 65xx podem rodar tanto CatOS quanto IOS. A tendência é a migração do CatOS para o IOS, já que a Cisco tende a não suportar mais o CatOS em breve. Nesta parte, iremos nos concentrar na linha 2900, pois esta é a única linha cobrada no novo exame CCNA (640-802).

O IOS que roda na linha Catalyst adota uma interface de configuração muito similar ao IOS que roda em roteadores que já vimos. Aliás, tanto switches quanto routers (nem todos, mas a grande maioria que ainda é suportada pela Cisco) também podem ser configurados por meio de uma ferramenta gráfica chamada *Cisco Network Assistant* <http://www.cisco.com/en/US/products/ps5931/>. Eu vou comentar sobre esta ferramenta mais adiante. Para a configuração via

Telnet, lembre-se de que **o switch precisa ter um endereço IP configurado.**

11.2.1 Slots GBIC (Gigabit Interface Converter)

A linha 2950, assim como as linhas superiores (35xx, 37xx, etc), disponibiliza slots GBIC para a conexão de uplinks. GBICs (*Gigabit Interface Converter*) são módulos normalmente utilizados para a interconexão de switches e, também, para a conexão de switches a routers ou servidores. No geral, qualquer tipo de conexão que necessite de uma banda mais elevada (GigabitEthernet) pode usar um dos slots GBIC existentes. O slot vem vazio de fábrica. É necessário adquirir um módulo que atenda às suas necessidades. Dentre os módulos existentes, eis alguns que podem ser utilizados na linha 2950:

- 1000BASE-T (Gigabit UTP);
- 1000BASE-SX (Gigabit Fibra);
- 1000BASE-LX/LH (Gigabit Fibra);
- 1000BASE-ZX (Gigabit Fibra).

Além disso, existe a possibilidade de utilizar um módulo especialmente desenvolvido para conexão entre switches chamado Cisco Gigastack, formando uma topologia em anel e, portanto, provendo contingência em caso de rompimento de uma fibra.

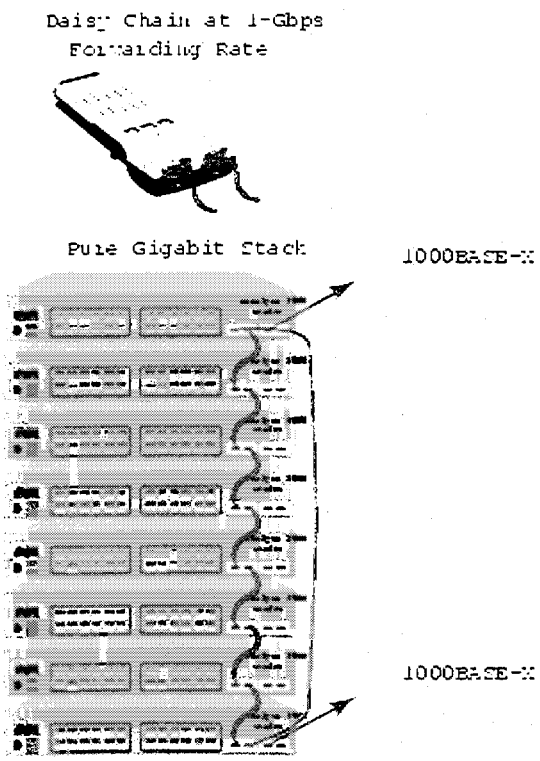


Figura 11.1: Topologia criada utilizando a tecnologia Gigastack da Cisco.

A principal vantagem em utilizar a tecnologia Gigastack para empilhamento de switches Cisco é que, utilizando estes módulos, o tráfego que passa de um switch para o outro não utiliza o *backplane* (capacidade física de processamento de quadros) dos switches intermediários, economizando recursos preciosos como CPU e memória.

11.2.2 Conexão à Porta Console

A linha 2900, assim como os routers que já vimos, possui uma porta console em sua parte traseira. Trata-se de uma porta RJ-45 para conexão ao terminal. Uma vez conectado o cabo ao switch e ao terminal, é necessário inicializar um programa emulador de terminal, como o *HyperTerm*, do Windows. As configurações para esse programa devem ser as mesmas utilizadas para os routers:

- 9600bps;
- 8 Data Bits;
- Parity None;
- Stop Bits 1;
- Flow Control None.

Nota: *Nunca conecte cabos ethernet, ISDN e telefônico à porta console de um switch. Isso poderá danificá-lo.*

11.2.3 Inicialização do Switch

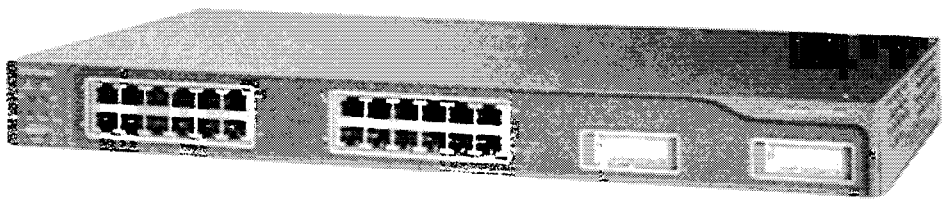
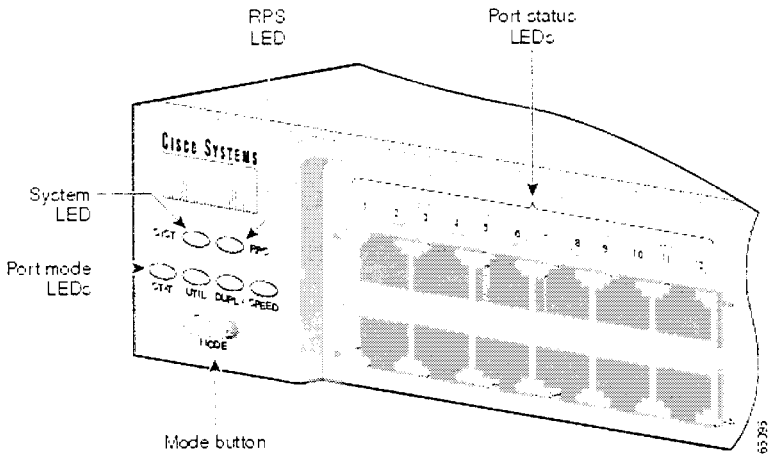


Figura 11.2: Switch Catalyst 2950G-24.

Antes de inicializar um switch, certifique-se do seguinte:

- Todos os cabos de rede encontram-se firmemente conectados;
- O terminal encontra-se conectado à porta console;
- O software emulador de terminal encontra-se corretamente configurado.

Uma vez que tudo esteja checado e ok, ligue o switch e observe a seqüência dos leds.



Uma luz verde aparece ao lado da palavra *SYSTEM* assim que o sistema estiver operando. Caso algum problema ocorra, a cor será âmbar (alaranjado). O *LED RPS* apenas ficará ativo na existência de uma fonte de alimentação redundante (chamada RPS - *Redundant Power Supply*) O único botão existente é o *MODE*. Ao pressioná-lo você pode ver os quatro diferentes status dos LEDs do switch *(port mode LEDs)*:

- **STAT**: Indica o status das portas:
  - Verde - dispositivo conectado ao switch;
  - Verde Piscante - atividade na porta;
  - Âmbar - falha de comunicação na porta.
- **UTIL**: Indica a largura de banda em uso no switch, em escala logarítmica.

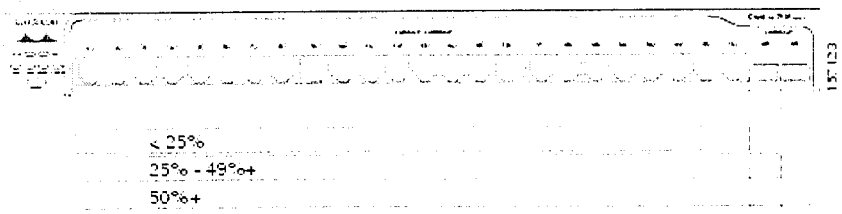


Figura 11.3: Utilização medida em um switch 2950-24.

- **DUPLX**: Apresenta as portas do switch configuradas em *full-duplex*. Se o LED da porta estiver verde, a porta encontra-se operando em *Full-Duplex*. Se estiver apagado encontra-se em *Half-Duplex*.
- **SPEED**: Apresenta a banda configurada nas portas. Se o LED da porta se encontrar apagado, a porta está operando em 10 Mbps. Se estiver verde, está operando em 100 Mbps Se estiver verde piscante, a porta encontra-se operando em 1000 Mbps (apenas em portas 10/100/1000)do switch configuradas em *full-duplex*.

11.2.3.1 Rotina de Inicialização

Assim que um switch 2950 é inicializado, da mesma forma que um router, ele entra em modo de teste (*POST*). No início, todos os LEDs encontram-se verdes. Esses LEDs se apagam após o final do modo *POST*.

Caso seja identificada uma falha em alguma porta durante o *POST*, ambos - os LEDs SYSTEM e o da porta em questão - mudam a cor para âmbar. Caso nenhuma falha seja identificada, todos os LEDS piscam e, em seguida, se apagam. Caso você tenha um terminal conectado ao switch, é possível verificar o status do POST na tela do terminal:

```
POST: System Board Test : Passed
POST: Ethernet Controller Test : Passed
ASIC Initialization Passed

POST: FRONT-END LOOPBACK TEST : Passed
cisco WS-C2950C-24 (RC32300) processor (revision Q0) with
20713K bytes of memory.
Processor board ID FOC0835Y342
Last reset from system-reset
Running Enhanced Image
26 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:12:00:D9:67:00
Motherboard assembly number: 73-5750-13
Power supply part number: 34-0965-01
Motherboard serial number: FOC08351CL9
Power supply serial number: DAB0833EKMA
Model revision number: Q0
Motherboard revision number: A0
Model number: WS-C2950C-24
System serial number: FOC0835Y342

        - System Configuration Dialog -

Would you like to enter the initial configuration dialog? [yes/no]:
```

Notem que o diálogo inicial é idêntico ao apresentado pelos routers. Digitamos *No* seguido de *Enter*, ou simplesmente, digitamos *Ctrl+C*:

```
Press RETURN to get started!

Switch>
```

A linha 2950, dependendo do modelo, possui apenas **portas do tipo fixas**, ou seja, não há como alterar suas características através de módulos. Existem modelos que possuem 2 slots GBIC, possibilitando a inserção de módulos compatíveis. A linha 2950 possui todas as suas portas de acesso 100BaseT para conexão com usuários finais e, dependendo do modelo, duas portas 100BaseFX (fibra) fixas ou dois slots GBIC para uplinks (conexão com outros switches/criação de links de transporte).

Assim que um dispositivo é conectado a uma porta do switch, o LED correspondente se ativa e assim permanece. **Caso o LED não se ative, pode ter havido um problema com o dispositivo, com a porta do switch, ou com o cabo utilizado.** Caso o LED se ative e desative pode haver um problema de *auto-speed* e *duplex*.

11.2.4 Definindo Senhas de Modo Privilegiado e Usuário

Senhas em um Catalyst 2950 são configuradas do mesmo modo que em um router. Você utiliza o comando *enable secret* para definir a senha de modo privilegiado.

Eis um exemplo de como se configurar senhas de modo privilegiado em um switch:

```
Switch(config)#enable secret cisco
Switch(config)#exit
```

Para configurar uma senha de modo usuário, o processo é idêntico ao utilizado em um router:

```
Switch(config)#line console 0
Switch(config-line)#pass cisco
Switch(config-line)#login

Switch(config)#line vty 0 15
Switch(config-line)#pass cisco
```

11.2.5 Configuração do Hostname

Para configuração do hostname em um switch, o procedimento idêntico ao visto para um roteador, conforme exemplificado abaixo:

```
Switch#config t
Enter configuration commands, one per line. End with
CNTL/Z
Switch#(config)#hostname CAT2950
CAT2950(config)#
```

11.2.6 Configuração do Endereço IP

Não é obrigatória a configuração de um endereço IP para o switch, porém, se você deseja dispor do recurso de configurá-lo remotamente por meio de um *web-browser* ou via Telnet, um IP precisa ser configurado. A seguir, as configurações default de um switch Catalyst 2950:

- **IP do default gateway**: *0.0.0.0;*
- **CDP**: *Enabled;*
- **Switching Mode**: *Store and Forward* (nenhum outro modo é suportado);
- **Portas 100BaseT**: *Auto-negotiate duplex mode;*
- **Spanning Tree**: *Enabled;*
- **Senha de Console**: Nenhuma.

Para configurar um endereço IP e o endereço do default gateway em um switch 2950, utilize os comandos ilustrados a seguir:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan1
Switch(config-if)#ip add 1.1.1.100 255.255.255.0
Switch(config-if)#ip default-gateway 1.1.1.1
Switch(config)#^Z
```

Note que o endereço IP é configurado na interface VLAN1. A VLAN1 é a VLAN nativa do switch, ou seja, mesmo que você não a tenha configurado, ela já está lá. Ao configurar um endereço IP nesta VLAN, você está, na verdade, designando um endereço IP ao seu switch.

11.2.7 Configuração de Interfaces (Portas)

É importante saber como acessar as portas de um switch. O switch 2950 usa a sintaxe {tipo de interface}{slot}/{porta}, ou seja, *FastEthernet 0/1* referencia a primeira porta do switch (a contagem começa em 1). A linha 2900, por não ser modular, possui apenas um slot (*0*).

Para configurar uma interface em um switch 2950, basta ir ao modo de configuração global e utilizar o comando *interface*. Descrevemos o processo a seguir:

```
Switch(config)#int fastEthernet ?
  <0-1>  FastEthernet interface number

Switch(config)#int fastEthernet 0/?
```

```
  <0-26>  FastEthernet interface number

Switch(config)#int fastEthernet 0/1
Switch(config-if)#
```

No exemplo anterior, o comando help (?) nos mostra 27 porta disponíveis (0-26), no entanto, a porta "0" não existe. Ao tenta configurá-la, o switch acusa um erro:

```
Switch(config)#interface fastEthernet 0/0
                         ^

% Invalid input detected at '^' marker.
```

Um pequeno "deslize" da Cisco! Bom, uma vez que você s encontre no modo de configuração de interface (config-if), você pod utilizar o comando help (?) para verificar uma lista dos comando disponíveis. Entre eles, temos: *cdp, description, duplex, exit, help shutdown* e *spanning-tree.*

11.2.7.1 Configuração de Descrições nas Interfaces

Mais uma vez, o modo de efetuar esse procedimento é idêntico a realizado em routers:

```
Switch(config)#int f0/1
Switch(config-if)#description Finance_VLAN
Switch(config-if)#int f0/2
Switch(config-if)#description trunk para o switch SW4
Switch(config-if)#
```

Para visualizar as descrições, utilize o comando *sh int* (ex.: *sh int f0/1*

11.2.7.2 Configuração da Velocidade e do Modo Duplex da Porta

```
Switch(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation
Switch(config-if)#duplex full
Duplex can not be set until speed is set to non-auto value
```

Note que o switch exige que, antes do duplex ser configurado, velocidade da porta seja fixada, já que a porta vem pré-configurad como *auto.*

```
Switch(config-if)#speed 100
Switch(config-if)#duplex full
```

A próxima tabela apresenta as diferentes opções duplex disponíveis em switches da série 2950. As portas FastEthernet são *auto-duplex*, por default, o que significa que tentarão detectar o tipo de duplex configurado na outra ponta. **Isso pode ou não funcionar.** Uma boa regra é configurar portas FastEthernet como *full-duplex*.

Parâmetro	Definição
Auto	Modo de autoconfiguração. Default para todas as portas 100baseTX.
Full	Força as portas para operação FULL DUPLEX.
Half	Força as portas para operação HALF DUPLEX.

Uma vez que o modo duplex esteja definido, você pode usar o comando *show int* para verificar sua configuração:

```
Switch(config-if)#do sh int f0/1
FastEthernet0/1 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 0012.00d9.6701 (bia
0012.00d9.6701)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is unsupported output flow-control is
unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
[...]
```

11.2.8 Verificação da Conectividade IP

É importante sempre testar a configuração IP de qualquer dispositivo em uma rede. Switches não fogem à regra. Ping, *Traceroute* e Telnet, como sempre, são as melhores ferramentas para se utilizar nesse caso.

11.2.9 Apagando a Configuração de um Switch

A configuração de um switch, assim como a de um router, encontra-se armazenada na NVRAM e, assim como um router, o comando para apagar as configurações da memória é o mesmo.:

```
Switch#erase start
Erasing the nvram filesystem will remove all configuration
```

```
files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
01:16:33: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram
Switch#
```

11.2.10 Gerenciamento da Tabela de Endereços MAC

Switches efetuam a filtragem da rede através dos endereços de hardwar (MAC) dos dispositivos. Eles criam tabelas MAC que incluem endereço dinâmicos, permanentes e estáticos. A tabela-filtro é gerada conform hosts enviam frames com dados sobre seus endereços de hardware. O switches, então, armazenam esses dados em suas tabela-filtrc relacionando-os com o segmento e porta onde foram recebidos.

Os switches estão continuamente adicionando novos endereço MAC às suas tabelas-filtro. Conforme hosts são adicionados o removidos da rede, os switches dinamicamente atualizam essas tabela Caso um dispositivo seja removido da rede ou perca o contato com switch por muito tempo, os dados correspondentes na tabela-filtro irã expirar após um período predeterminado de tempo. A tabela-filtro d um switch pode ser visualizada através do comando *show mac-addres table*, conforme é ilustrado a seguir:

```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
[...]
   1    0000.21c9.a79b    DYNAMIC     Fa0/23
   1    0002.b977.da80    DYNAMIC     Fa0/23
   1    0002.b977.da97    DYNAMIC     Fa0/23
   1    000f.b578.5f04    DYNAMIC     Fa0/23
   1    0013.ce5d.6ed6    DYNAMIC     Fa0/23
Total Mac Addresses for this criterion: 5
```

Os endereços na tabela são de cinco dispositivos conectados a switch. Todos foram dinamicamente inseridos, o que significa que switch verificou o endereço de origem do frame assim que ele atravessc a interface e o inseriu em sua tabela MAC. Caso a tabela MAC

sobrecarregue e atinja sua capacidade de armazenamento, o switch irá propagar todos os novos endereços recebidos até que um dos armazenados em sua tabela expire. A tabela MAC de um switch pode ser apagada completamente através do comando *clear mac-address-table*:

```
Switch#clear mac-address-table ?
  dynamic       dynamic entry type
  notification  Clear MAC notification Global Counters<cr>
```

11.2.10.1 Configuração de Endereços MAC Estáticos

Endereços MAC estáticos podem ser configurados em uma porta de switch através do comando *mac-address-table static [endereço MAC][vlan] [interface]*. Veja o exemplo que segue:

```
Switch(config)#mac-address-table static aaaa.aaaa.aaaa vlan 1
interface FastEthernet 0/1

Switch(config)#do sh mac-add
          Mac Address Table
-------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
[...]
   1    aaaa.aaaa.aaaa    STATIC      Fa0/1
Total Mac Addresses for this criterion: 5
```

11.2.10.2 Configuração de Segurança em Portas

Nota: *Para facilitar nossas vidas, muitas configurações nos switches 2950 podem ser realizadas simultaneamente em várias interfaces por meio do comando "interface range", como o exemplo abaixo:*

```
Switch(config)#interface range fastEthernet 0/1 - 10 ,
fastEthernet 0/12
Switch(config-if-range)# no shut
```

Neste exemplo, as portas de 1 a 10 e a porta 12 serão ativadas pelo comando no shut.

Segurança em portas (*switchport security*) é um modo de se evita que usuários conectem um dispositivo ao switch sem que administrador tenha conhecimento. **Por default, 132 endereços d hardware são permitidos em apenas uma interface (porta) de ur switch.** Eis uma forma de limitar isso usando os recursos de *port-securit* do IOS:

```
Switch(config-if)#switchport port-security mac-address ?
  H.H.H   48 bit mac address
  sticky  Configure dynamic secure addresses as sticky

Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
  <cr>

Switch(config-if)#switchport port-security violation shutdown
```

Note que o comando deve ser digitado no modo de configuraçã de interface. Para começar a utilizar os recursos do *port-security*, preciso tirar a interface do modo dinâmico e passá-la para o mod estático. É isso o que o comando *switchport port-security mac-addre* faz.

Existem dois modos de fixar o endereço MAC na interface. U deles é o manual e o outro é o automático (*sticky*). Neste último, switch aprende o endereço MAC e o adiciona à tabela-filtro pelo tem que for determinado pelo parâmetro *aging*. Veja que limitamos o núme máximo de MACs associados à porta em "2" (*switchport port-securi maximum 2*) e, na sequência, colocamos uma ação para ser tomac caso esta condição (máximo 2) seja violada.

No caso, a ação é *shutdown*, ou seja, caso alguém tente conect mais de dois dispositivos à interface configurada ou conectar apen 1 dispositivo que não tenha o endereço MAC autorizado (registrac na tabela pelo parâmetro *sticky*), a porta será desativada e apen poderá ser ativada novamente manualmente, por meio do comanc *no shut*.

Para verificar as configurações de segurança em uma determinac porta, utilize o comando *show port-security address*:

```
Switch#show port-security address
          Secure Mac Address Table
------------------------------------
Vlan    Mac Address       Type            Ports   Remaining Age
                                                    (mins)
----    -----------       ----            -----   -------------
   1    0004.00d5.285d    SecureDynamic   Fa0/18        -
------------------------------------

Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024

Switch#show port-security interface fa0/18
Port Security                          : Enabled
Port Status                            : Secure-up
Violation Mode                         : Shutdown
Aging Time                             : 0 mins
Aging Type                             : Absolute
SecureStatic Address Aging             : Disabled
Maximum MAC Addresses                  : 2
Total MAC Addresses                    : 1
Configured MAC Addresses               : 0
Sticky MAC Addresses                   : 0
Last Source Address                    : 0004.00d5.285d
Security Violation Count               : 0
```

NOTA: Se apenas digitarmos o comando switchport port-security em uma interface do switch, o modo de segurança é automaticamente habilitado utilizando seus parâmetros default: Maximum MAC Add: 1, violation Shutdown, MAC Add sticky.

11.2.11 Utilizando o Comando Show Version

O comando *show version* pode ser utilizado na visualização de informações básicas sobre o switch. Essas informações incluem o **tempo de utilização do switch, a versão do IOS e o endereço MAC do switch em si.**

```
Switch#sh ver
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(20)EA1a,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Mon 19-Apr-04 20:58 by yenanh
Image text-base: 0x80010000, data-base: 0x805A8000
```

```
ROM: Bootstrap program is C2950 boot loader

Switch uptime is 2 hours, 14 minutes
System returned to ROM by power-on
System image file is "flash:/c2950-i6q4l2-mz.121-20.EA1a.bin"

cisco WS-C2950C-24 (RC32300) processor (revision Q0) with
20713K bytes of memory.
Processor board ID FOC0835Y342
Last reset from system-reset
Running Enhanced Image
26 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:12:00:D9:67:00
Motherboard assembly number: 73-5750-13
Power supply part number: 34-0965-01
Motherboard serial number: FOC08351CL9
Power supply serial number: DAB0833EKMA
Model revision number: Q0
Motherboard revision number: A0
Model number: WS-C2950C-24
System serial number: FOC0835Y342
Configuration register is 0xF
```

11.2.12 Configuração de VLANs

A configuração de VLANs, ao contrário do que se possa imaginar, é direta e descomplicada. O difícil é entender quais usuários devem ser alocados em cada VLAN. Uma vez definido o número de VLANs a serem criadas e os usuários participantes em cada uma delas, as VLANs podem ser criadas sem problemas. Em um switch da linha 2950, podem ser criadas **até 250 VLANs** . Uma diferente instância de *spanning tree* pode ser configurada para cada VLAN criada.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Teste10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Teste20
Switch(config-vlan)#
Switch#
```

Para configurar VLAN em um switch via IOS, use o comando *vlan [número da VLAN]*. Uma vez no modo de configuração de VLANs (*config-vlan*), utilize o comando *name* [nome da VLAN] para associar um nome à VLAN criada. Anteriormente ilustramos um exemplo da criação de 2 VLANs com 2 diferentes nomes (*Teste10 e Teste20*). Uma vez criadas as VLANs desejadas, elas podem ser verificadas através do comando *show vlan*. Por default, **todas as portas do switch encontram-se associadas à VLAN 1**, conhecida como VLAN administrativa. Para alterar a VLAN associada a uma determinada porta, você deve acessá-la e informar qual a nova VLAN a ser associada.

Você pode configurar cada porta do switch para participar de uma determinada VLAN através dos comandos *switchport mode access | switchport access vlan [número]*. A configuração pode ser feita porta a porta, ou em várias portas simultaneamente por meio do comando *interface range*. A seguir ilustramos a associação das interface 2 a 6 à VLAN 10, e da interface 10 à VLAN 20:

```
Switch(config)#interface range fastEthernet 0/2 - 6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#interface 0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

Para verificar sua configuração, utilize o comando *sh vlan*. Outro comando que pode ser usado para verificação de VLANs é o *sh vlan name [nome da VLAN]*. Esse comando apresenta uma série de estatísticas sobre a VLAN desejada.

11.2.12.1 Configuração de Portas de Transporte (Trunk Links)

Para que uma porta do switch se comporte como um link de transporte, ou um *trunk*, utilize o comando *switchport mode trunk* na interface desejada. A seguir ilustramos um exemplo de utilização desse comando:

```
Switch(config)#int f0/1
Switch(config-if)#switchport mode trunk
```

Lembre-se que todas as VLANs encontram-se na porta de transporte configurada, por default. Para permitir que apenas determinadas VLANs trafeguem por um link de transporte, **as VLANs indesejadas devem ser manualmente deletadas (*cleared*).**

***Nota**: Lembre-se disso para o exame CCNA!*

Utilize o comando *switchport trunk allowed vlan* [VLAN ou intervalo de VLANs] para definir exatamente quais VLANs poderão atravessar o link de transporte. As razões para se excluir VLANs do link de transporte incluem:

1. Você não desejar que *broadcasts* de uma determinada VLAN atravessem o link de transporte;
2. Você desejar evitar que informações sobre alterações na topologia sejam propagadas através de um link onde a VLAN em questão não é suportada.

Exemplo:

```
Switch(config-if)#switchport trunk allowed vlan 10,20-30,40
```

O comando anterior fará com que o link de transporte propague informações sobre as VLANs 10, 20 a 30 e 40.

Quando habilitamos o trunk em uma determinada interface, por default, a VLAN1 é a VLAN nativa da porta, ou seja, informações originadas na VLAN1 passam pelo link de transporte sem *tag* (*untagged*). Você pode alterar a VLAN nativa usando o comando *switchport trunk native vlan [VLAN]*:

```
Switch(config-if)#switchport trunk native vlan 10
```

O comando anterior faz com que a VLAN 10 passe a ser a VLAN nativa da porta e, portanto, informações originadas nesta VLAN passarão sem marcação (*untagged*) pelo link de transporte.

11.2.12.2 Verificação de Links de Transporte

Para verificar suas portas de transporte, utilize o comando *show interface trunk*.

```
Switch#sh interfaces f0/23 trunk

Port        Mode         Encapsulation  Status       Native vlan
Fa0/23      on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/23      10,20-30,40

Port        Vlans allowed and active in management domain
Fa0/23      10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/23      10,20
Switch#
```

11.2.12.3 Configuração dos Modos STP

Para alterar o modo STP para Rapid STP, ou para ativar os modos backbonefast e outros, utilize o comando spanning tree [parâmetro]:

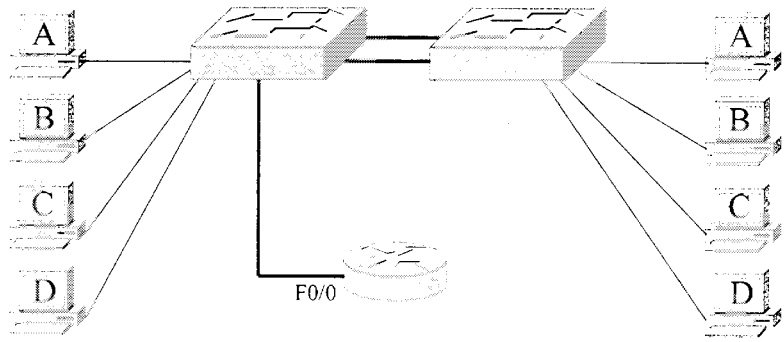
```
Switch(config)#spanning-tree ?
  backbonefast  Enable BackboneFast Feature
  etherchannel  Spanning tree etherchannel specific
configuration
  extend        Spanning Tree 802.1t extensions
  loopguard     Spanning tree loopguard options
  mode          Spanning tree operating mode
  mst           Multiple spanning tree configuration
  pathcost      Spanning tree pathcost options
  portfast      Spanning tree portfast options
  uplinkfast    Enable UplinkFast Feature
  vlan          VLAN Switch Spanning Tree

Switch(config)#spanning-tree mode ?
  mst         Multiple spanning tree mode
  pvst        Per-Vlan spanning tree mode
  rapid-pvst  Per-Vlan rapid spanning tree mode

Switch(config)#spanning-tree mode rapid-pvst
```

11.2.12.4 Configuração Etherchannel

A configuração do Etherchannel é bastante direta. Basta criar o grupo Etherchannel (interface virtual que agregará as demais) e associar as interfaces físicas ao grupo criado:

```
Switch(config-if)#interface port-channel 1

Switch(config-if)#interface fast0/1

Switch(config-if)#channel-group 1 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected

Switch(config-if)#channel-group 1 mode on
Switch(config-if)#interface fast0/2
Switch(config-if)#channel-group 1 mode on
```

11.2.12.5 Configuração de Roteamento dot1q



Para ser capaz de suportar roteamento dot1q em uma interface FastEthernet de um router, essa interface deve ser dividida em uma série de interfaces lógicas, uma para cada VLAN. Estas são conhecidas como subinterfaces. Na rede ilustrada anteriormente, temos quatro VLANs (A, B, C, D), logo devemos criar quatro subinterfaces. Cada VLAN encontra-se em uma sub-rede diferente, portanto, eis o endereçamento que adotaremos:

VLAN 10	(A) default	172.16.10.0 /24
VLAN 20	(B) Vendas	172.16.20.0 /24
VLAN 30	(C) Marketing	172.16.30.0 /24
VLAN 40	(D) Finanças	172.16.40.0 /24

Cada host pertencente a cada uma destas VLANs deve usar o mesmo endereçamento de sub-rede. Para configurar o router para roteamento inter-VLAN, os três passos a seguir devem ser completados:

1. Ative *dot1q trunking* na porta do switch conectada ao router;
2. Ative encapsulamento *dot1q* para cada subinterface definida no router;
3. Configure um endereço IP em cada subinterface

A criação de subinterfaces já foi discutida anteriormente, portanto, não iremos repetir o procedimento aqui. Para configurar o roteamento dot1q em uma subinterface, utilize o comando *dot 1q [número da VLAN]*. Você pode, então, configurar um endereço IP na subinterface. Lembre-se que todos os hosts em uma mesma VLAN devem fazer parte da mesma sub-rede. A seguir ilustramos como proceder na configuração de router 2621 para que ele suporte roteamento dot1q para as quatro VLANs que definimos. Por que um 2621A e não um 2501? Lembre-se (mais uma vez): o encapsulamento dot1q (ou mesmo o ISL) **não** pode ser ativado em portas que operem a menos de 100Mbps. Routers da

série 2500 não possuem portas FastEthernet (apenas Ethernet), portanto, não suportam encapsulamento dot1q ou ISL.

```
2621#config t
2621(config)#int f0/0
2621(config-if)#no shut
2621(config-if)#int f0/0.10
2621(config-subif)#encap dot1q 10
2621(config-subif)#ip add 172.16.10.1 255.255.255.0
2621(config-subif)#int f0/0.20
2621(config-subif)#encap dot1q 20
2621(config-subif)#ip add 172.16.20.1 255.255.255.0
2621(config-subif)#int f0/0.30
2621(config-subif)#encap dot1q 30
2621(config-subif)#ip add 172.16.30.1 255.255.255.0
2621(config-subif)#int f0/0.40
2621(config-subif)#encap dot1q 40
2621(config-subif)#ip add 172.16.40.1 255.255.255.0
```

Eis o que foi feito, passo a passo:

1. Configuramos a subinterface com o mesmo número da VLAN que desejamos rotear. Esse número possui significância local somente, ou seja, os números das subinterfaces não importam para a rede;
2. Em seguida habilitamos o método de encapsulamento (dot1q);
3. Finalmente, informamos o endereço IP e máscara de rede para cada uma das subinterfaces. Note que o endereço IP definido para a subinterface deve pertencer ao intervalo válido da sub-rede em questão. No caso, a VLAN 10 possui endereço de rede 172.16.10.0, portanto, a subinterface 0/0.10 foi configurada com o endereço IP 172.16.10.1. Este endereço IP será o default gateway para os hosts presentes nesta subrede.

O mesmo é feito para as três VLANs restantes. Veja, no entanto, que **cada subinterface se encontra em uma sub-rede diferente.**

11.2.12.6 Configuração do Modo VTP na Linha 2900

```
Switch>en
Switch#conf t
Switch(config)#vtp mode client
```

```
Setting device to VTP CLIENT mode.
Switch(config)#vtp mode server
Setting device to VTP SERVER mode.

Switch(config)#vtp domain ccna

Switch(config)#vtp pruning
Pruning switched on

Switch#sh vtp status
VTP Version                     : 2
Configuration Revision          : 9
Maximum VLANs supported locally : 250
Number of existing VLANs        : 12
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE6 0x50 0xCC 0xB7 0x7D 0x89
0x19 0x45
Configuration last modified by 1.1.1.1 at 3-1-93 02:55:55
Local updater ID is 1.1.1.1 on interface Vl1 (lowest numbered
VLAN interface found)
```

Acima, estão exemplificados os comandos que configuram o switch para os modos VTP client e VTP server (default), e os comandos para habilitar o *pruning* e verificar o status do VTP.

***Atenção**: Saber configurar VTP em switches 2950 é de extrema importância para o novo exame Cisco CCNA.*

11.3 Recuperação de Senhas com Switches 2950

***Nota**: Este tópico não será cobrado no exame.*

O processo de recuperação de senhas para switches da linha 2950 tem um início similar ao dos switches 1900, porém, daí para frente, a coisa muda de figura:

1. Desligue seu cabo de força, aguarde alguns segundos, pressione o botão *MODE* na parte dianteira do switch e religue-o (mantendo o botão *MODE* pressionado até que o led *STAT* se apague);

2. Digite o comando *flash_init*:

```
switch: flash_init
Initializing Flash...
flashfs[0]: 143 files, 4 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 3612672
flashfs[0]: Bytes used: 2729472
flashfs[0]: Bytes available: 883200
flashfs[0]: flashfs fsck took 86 seconds
....done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
switch:
```

3. Digite o comando *load_helper;*
4. Digite o comando *dir flash*:

```
switch: dir flash:
Directory of flash:/
2    -rwx  1803357   <date>              c2950-c3h2s-mz.120-
5.WC7.bin
4    -rwx  1131      <date>              config.text
5    -rwx  109       <date>              info
6    -rwx  389       <date>              env_vars
7    drwx  640       <date>              html
18   -rwx  109       <date>              info.ver
403968 bytes available (3208704 bytes used)
switch:
```

Observe que o arquivo 4 é o arquivo de configuração.

5. Renomeie o arquivo de configuração (4) usando o comando *rename flash:config.text flash:config.old;*
6. Digite *boot* para recarregar o router (dar um *reload*);
7. Nesse ponto, após recarga do switch, o menu inicial de configuração (modo *setup*) lhe será apresentado. Digite *Ctrl+C* ou *n* para sair dele e ir para o modo de configuração via linha de comando (CLI). Acesse o modo privilegiado digitando *em;*
8. Renomeie a configuração presente na flash novamente usando o comando *flash:config.old flash:config.text;*

9. Copie a configuração para a memória RAM usando o comando *copy flash:config.text system:running-config;*
10. Altere a senha (ex. *enable secret [nova senha]*);
11. Salve a configuração (*copy run start* ou *wr*). Pronto!

Para o exame CCNA, isso é tudo o que é necessário saber sobre configuração de switches.

Questões de Revisão – Configuração de Switches

1. O que é verdadeiro sobre o led de status na interface de um switch?
   a) É usado para verificar se houve um *loop* na rede.
   b) É usado para identificar sinalização RTS.
   c) Quando um dispositivo é conectado a uma porta, o LED de status é ativado e assim permanece.
   d) Quando um dispositivo é conectado a uma porta, o LED de status é ativado e, em seguida, se apaga.

2. Qual tipo de cabo Ethernet deve ser utilizado na conexão entre duas portas de um switch?
   a) Straight-through
   b) Rolled
   c) Crossover
   d) Fibra-óptica

3. Quais alternativas apresentam os comandos válidos para configuração do endereço IP e default gateway em um switch 2900?
   a) ip address 172.16.10.16 255.255.255.0
   b) ip default-gateway 172.16.10.1
   c) ip address 172.16.10.16 mask 255.255.255.0
   d) default-gateway 172.16.10.1

4. Qual comando apresenta a tabela de filtragem MAC em um switch 2900?
   a) 2900#sh mac-filter-table
   b) 2900#sh mac-address-table
   c) 2900(config)#sh mac-address-table
   d) 2900#sh filter-address-table

5. Qual dos comandos abaixo configura corretamente um endereço IP de gerenciamento e o default gateway em um switch 2950?

a) 2950(config)#ip address 192.168.10.10 255.255.255.0 | ip default-gateway 192.168.10.1
b) 2950(config)#int vlan 1 | ip address 192.168.10.10 255.255.255.0 | ip default-gateway 192.168.10.1
c) 2950(config)#int f0/1 | ip address 192.168.10.10 255.255.255.0 | ip default-gateway 192.168.10.1
d) 2950(config)#int f0/0 | ip address 192.168.10.10 255.255.255.0 | ip default-gateway 192.168.10.1

6. Qual dos comandos abaixo configura uma VLAN 2 chamada VENDAS em um switch 2950?

a) 2950(config)#vlan 2 name VENDAS
b) 2950(config)#vlan 2 | name VENDAS
c) 2950(config)#int f0/0 | vlan 2 name VENDAS
d) 2950(config)#vlan-data 2 | name VENDAS

7. Qual dos comandos abaixo configura um switch 2950 para o modo VTP transparente?

a) 2950(config)#vtp mode transp
b) 2950(config-vtp)#vtp mode trans
c) 2950(config)#vtp transpar mode
d) 2950(config)#vtp-data transp

8. Qual dos comandos abaixo pode ser usado para associar um switch 2950 ao domínio VTP chamado "CCNA"?

a) 2950#vtp domain CCNA
b) 2950(config)#vtp server CCNA
c) 2950(config)#vtp domain-name CCNA
d) 2950(config)#vtp domain CCNA

9. Qual o modo de comutação em um switch 2950?

a) Store-and-forward
b) FragmentFree
c) Modified Cut-through
d) Cut-through

10. O processo de configuração de senhas de modo usuário e privilegiado, assim como muitas outras configurações em um switch 2950 é idêntico ao que foi visto para roteadores.

a) Verdadeiro
b) Falso

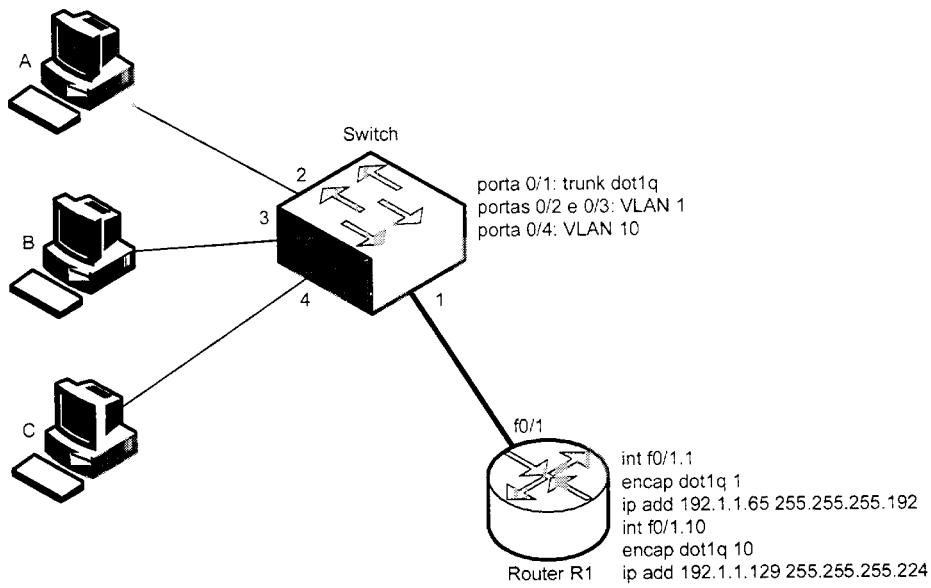
11. O comando usado para associar a VLAN 2 chamada VENDAS à interface F0/3 em um switch 2950 é:

a) 2950(config)#int f0/2 | vlan 2
b) 2950(config)#int f0/2 | port mode access vlan 2
c) 2950(config)#int f0/2 | switchport access vlan 2
d) 2950(config)#int f0/2 | switchport mode access vlan 2

12. O comando usado para configurar uma porta em um switch 2950 para operar em modo de transporte (trunk) é:

a) 2950(config)#int f0/2 | switchport trunk
b) 2950(config)#int f0/2 | port trunk
c) 2950(config)#int f0/2 | switchport mode trunk
d) 2950(config)#int f0/2 | mode trunk

13. Observe o diagrama:

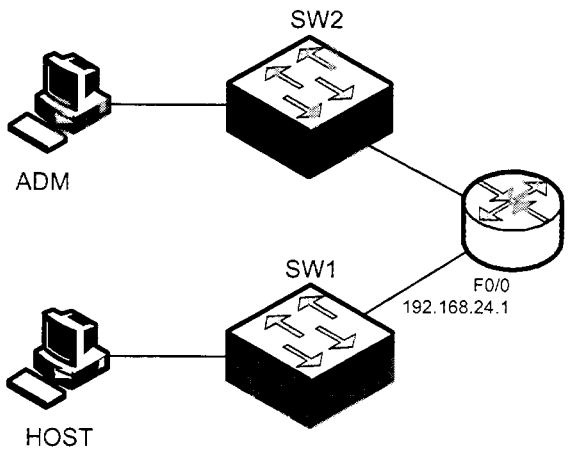


Baseado na topologia e configurações ilustradas, quais comandos você deve configurar no switch para que a porta f0/1 do router se comunique com a porta 1 do switch (selecione 3 respostas)?

a) Switch(config)# interface fastethernet 0/1
b) Switch(config-if)# switchport mode access
c) Switch(config-if)# switchport mode trunk
d) Switch(config-if)# switchport access vlan 1
e) Switch(config-if)# switchport trunk encapsulation isl
f) Switch(config-if)# switchport trunk encapsulation dot1q

14. O administrador da rede ilustrada não consegue estabelecer uma sessão Telnet com o switch SW1, entretanto, os hosts conectados a este switch conseguem pingar a interface f0/0 do router. Baseando-se nas informações apresentadas a seguir, e assumindo que tanto o router

quanto o switch SW2 estão devidamente configurados, qual dos seguintes comandos poderia resolver o problema apresentado?




```
Configs no SW1:
============
inte vlan 1
 ip add 192.168.24.2 255.255.255.0
!
line con 0
line vty 0 4
 pass cisco
 login
!
end
```

a) SW1(config)# ip default-gateway 192.168.24.1

b) SW1(config)# interface fa0/1
SW1(config-if)# ip address 192.168.24.3 255.255.255.0

c) SW1(config)# line con0
SW1(config-line)# password cisco
SW1(config-line)#login

d) SW1(config)# interface fa0/1
SW1(config-if)# duplex full
SW1(config-if)# speed 100

e) SW1(config)# interface fa0/1
SW1(config-if)# switchport mode trunk

f) Nenhuma das anteriores

15. Um determinado switch teve uma de suas portas configurada com o comando *switchport trunk native vlan 998*. O que este comando faz?

a) Torna a VLAN 998 a VLAN nativa (naquela porta) para tráfego sem marcação.
b) Bloqueia a VLAN998 para passagem de tráfego não marcado.
c) Cria a interface VLAN998.
d) Nenhuma das anteriores.

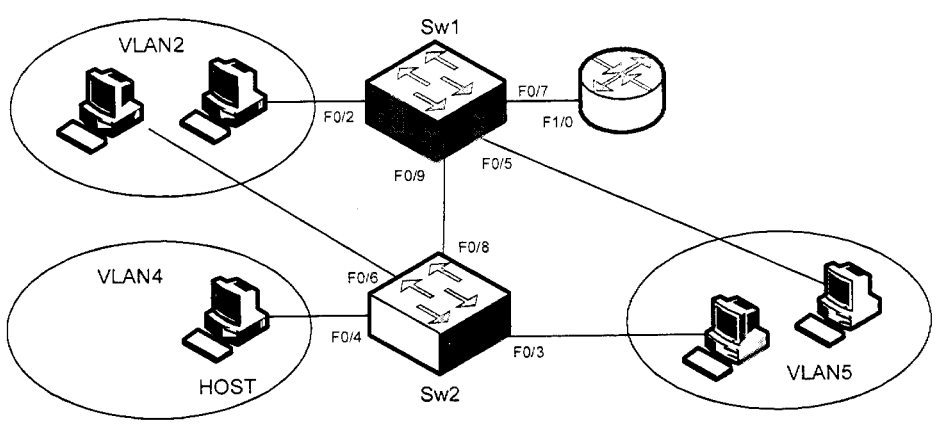
16. Você deseja configurar um trunk IEEE 802.1q em um switch. Quais comandos podem ser usados para isso (selecione 2)?

a) Switch(vlan)# mode trunk
b) Switch(config)# switchport access mode trunk
c) Switch(config-if)# switchport mode trunk
d) Switch(config-if)# switchport trunk encapsulation dot1q
e) Switch(config)# switchport access mode 1
f) Switch(vlan)# trunk encapsulation dot1q

17. Em uma determinada LAN, 2 switches encontram-se interconectados. As portas 1, 2 e 3 estão associadas à VLAN 1 e as portas 4, 5 e 6 estão associadas à VLAN 2, em ambos os switches. Estes 2 switches encontram-se conectados por um link de transporte. Quais das condições abaixo podem verificar a operação das VLANs e do trunk (selecione todas as corretas)?

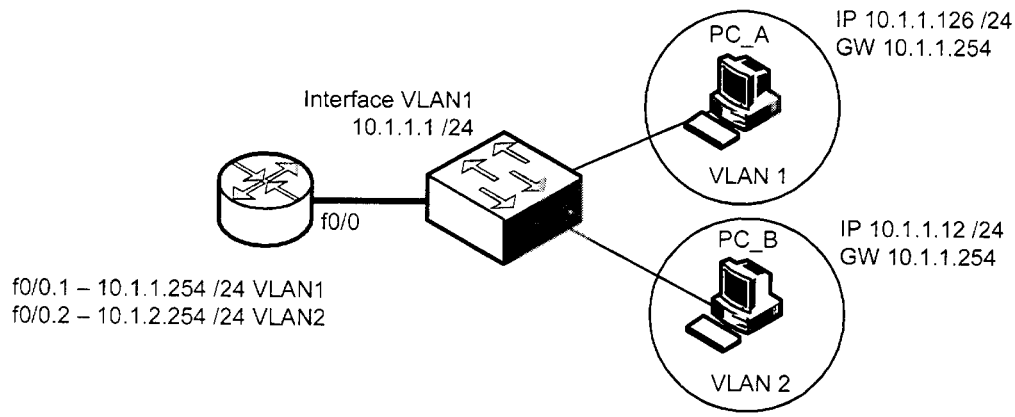
a) Host 1 na VLAN 1 consegue pingar o Host 2 na VLAN 1.
b) Host 1 na VLAN 1 consegue pingar o Host 4 na VLAN 2.
c) Host 1 na VLAN 1 não consegue pingar o Host 2 na VLAN 1.
d) Host 4 na VLAN 2 não consegue pingar o Host 1 na VLAN 1.
e) Host 4 na VLAN 2 consegue pingar o Host 2 na VLAN 2.

18. Observe atentamente o diagrama apresentado. A configuração de ambos os switches está completa. Durante testes, foi percebido que usuários conectados ao switch 1 não conseguem conectar-se a usuários na mesma VLAN no switch 2. O que deve ser feito para sanar este problema?



a) Assegurar que o endereço IP do switch 1 encontra-se na mesma rede IP do switch 2.
b) Certificar que o mesmo número de interface é utilizado para conectar os 2 switches.
c) Certificar que as portas que conectam os 2 switches está em modo trunk.
d) Assegurar que os switches 1 e 2 encontram-se interconectados via cabo straight-through.

19. Observe o diagrama:



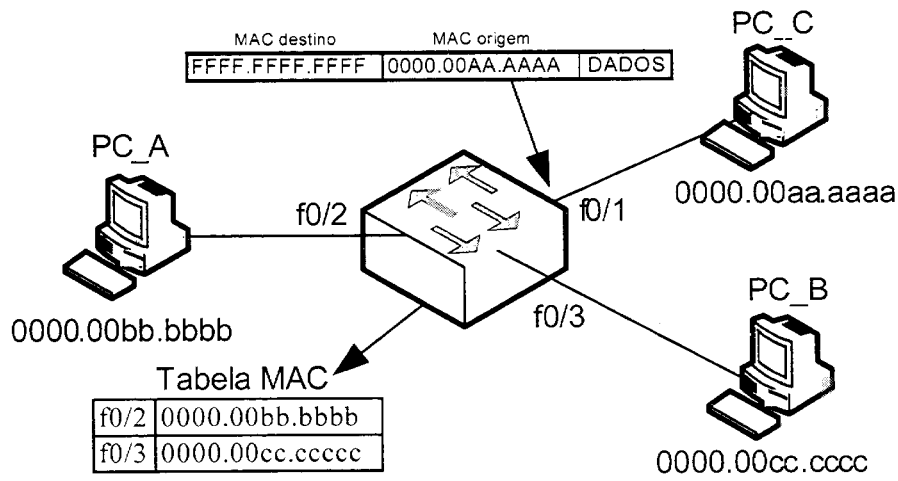
A rede anteriormente ilustrada está com problemas de conectividade. Quais das seguintes configurações podem solucionar o problema (selecione 2)?

a) Configurar o gateway 10.1.1.1 no PC_A
b) Configurar o endereço IP 10.1.2.2 no PC_B
c) Configurar o endereço IP 10.1.2.2 no PC_A
d) Configurar o gateway 10.1.2.254 no PC_B

20. A política de segurança de uma determinada empresa estabelece que apenas 1 host pode ser conectado fisicamente a uma interface de um dado switch. Se esta regra for violada, a interface deve ser automaticamente desativada. Quais 2 comandos devem ser configurados em um switch 2950 para alcançar este objetivo?

a) SW1(config-if)# switchport port-security maximum 1
b) SW1(config)# mac-address-table secure
c) SW1(config)# access-list 10 permit ip host
d) SW1(config-if)# switchport port-security violation shutdown
e) SW1(config-if)# ip access-group 10

21. Considere o seguinte diagrama:



A porta f0/1 do switch apresentado é configurada conforme abaixo:

SW3(config-if)# switchport port-security
SW3(config-if)# switchport port-security mac-address sticky
SW3(config-if)# switchport port-security maximum 1

O host C acaba de se conectar à rede. O frame enviado por ele é apresentado no diagrama. Baseado nas informações apresentadas, quais 2 ações serão tomadas (selecione 2)?

a) Todos os frames com endereço MAC de destino 0000.00aa.aaaa serão encaminhados pela fa0/1.
b) Os hosts B e C podem encaminhar frames pela interface f0/1, porém, frames originados de outros switches não serão encaminhados pela porta f0/1.
c) Apenas frames com endereço MAC de origem 0000.00bb.bbbb, o primeiro MAC aprendido pelo switch, serão encaminhados pela porta fa0/1.
d) O frame apresentado será descartado quando chegar ao switch.
e) Apenas o host C será autorizado a conectar-se a porta f0/1.
f) A tabela MAC do switch terá agora uma entrada adicional, com o endereço MAC FFFF.FFFF.FFFF associado à porta f0/1.

22. Um switch é configurado conforme apresentado abaixo:

SW3(config-if)# switchport port-security
SW3(config-if)# switchport port-security mac-address sticky

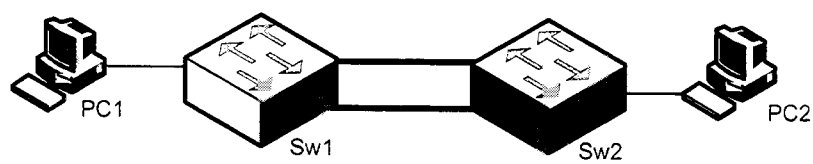
Selecione a alternativa que melhor descreve o resultado desta configuração.

a) Um endereço MAC dinamicamente aprendido é salvo na base de dados VLAN (VLAN database).
b) Um endereço MAC dinamicamente aprendido é salvo na NVRAM.
c) Um endereço MAC estaticamente configurado é salvo na NVRAM apenas se frames originados por este MAC forem recebidos.
d) Um endereço MAC dinamicamente aprendido é salvo na running-config.
e) Um endereço MAC estaticamente configurado é salvo na running-config apenas se frames originados por este MAC forem recebidos.
f) Nenhuma das anteriores.

23. Um administrador de uma rede deseja controlar o acesso de usuários à rede baseado nos endereços MAC. Qual destes recursos previne que hosts não-autorizados se conectem a um switch e tenham acesso à rede?

a) BPDU
b) Port security
c) RSTP
d) STP
e) VTP
f) Blocking mode

24. Observe o diagrama:



Quando o PC1 envia uma solicitação ARP ao PC2, a performance da rede cai dramaticamente e os switches envolvidos detectam uma quantidade muito grande de frames broadcast. O que pode estar causando isso?

a) O recurso portfast não se encontra habilitado em todas as portas dos switches.
b) Os PCs encontram-se em 2 VLANs distintas.
c) O protocolo Spanning Tree não está ativado nos switches.
d) O PC2 está com problemas e não responde às solicitações ARP.
e) A versão do VTP em uso em um switch é diferente da em uso no outro.
f) Nenhuma das anteriores.

Respostas das Questões de Revisão – Configuração de Switches

1. **C**. Assim que um dispositivo é conectado a uma porta de um switch, o LED na porta correspondente se ativa e assim permanece. Se não houver nenhum dispositivo conectado a uma determinada porta assim que o switch é ligado, o LED se acende e, em seguida, se apaga.

2. **C**. Cabos Ethernet *crossover* devem ser usados na conexão entre dois switches.

3. **A, B**. Os comandos *ip address* e *ip default-gateway* configuram endereços IPs e o default gateway em um switch

4. **B**. O comando *sh mac-address-table* apresenta todos os endereços existentes na tabela de filtragem.

5. **B**. No switch 2950, o endereço IP de gerenciamento deve ser associado à VLAN administrativa (VLAN 1).

6. **B**. No switch 2950, o modo para configurar uma VLAN é através do comando vlan [número]/name [nome].

7. **A**. No switch 2950, o comando para mudar o modo VTP é vtp mode [modo VTP].

8. **D**. No switch 2950, o comando usado para associação a um domínio VTP é vtp domain [domínio VTP].

9. **A**. Apenas o modo store & forward de comutação é suportado nos switches mais recentes, dentre eles, o 2950.

10. **A**. Os comandos IOS do modelo 2950 se assemelham aos usados em routers. Exemplos: configuração de senhas, do hostname, banners etc.

11. **C**. Para associação de VLANs a interfaces no switch 2950, o comando switchport access vlan [número] pode ser usado.

12. **C**. Para configuração do modo trunk em uma interface do switch 2950, o comando switchport mode trunk pode ser usado.

13. **A, C, F**

14. **A**

15. **A**

16. **C, D**

17. **A, D, E**

18. **C**

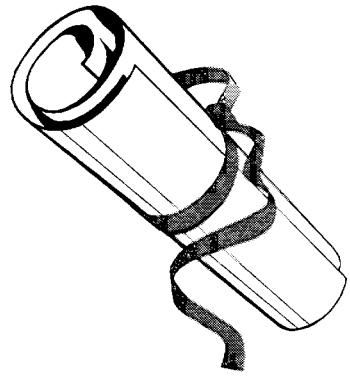
19. **B, D**

20. **A, D**

21. **A, E**
22. **A**
23. **B**
24. **C**

Relação dos Comandos Analisados

Comando	Descrição
config t	Coloca o switch em modo de configuração global
enable secret	Configura a senha *enable secret*
show run	Apresenta a configuração ativa
hostname	Define um hostname para o switch
ip default-gateway	Define o default gateway do switch
interface fastethernet 0/1	Configura interface f0/1
interface fastethernet 0/26	Configura interface f0/26
show inter f0/1	Apresenta estatísticas da interface f0/1
show int f0/26	Apresenta estatísticas da interface f0/26
description	Configura uma descrição para uma interface
duplex	Define o modo duplex de uma interface
ping	Testa a configuração IP
show mac-address-table	Apresenta a tabela MAC gerada dinamicamente
clear mac-address-table	Limpa a tabela MAC gerada dinamicamente
switchport port secure	Modo de configuração de segurança para portas de switches
show version	Fornece informação sobre o IOS, assim como o tempo de atividade do switch e seu endereço MAC
show vlan	Apresenta todas as VLANs configuradas
vlan 2 | name vendas	Cria a VLAN 2 chamada vendas
switchport access vlan 2	Associa uma VLAN 2 a uma porta, estaticamente
switchport mode trunk	Coloca uma porta em modo trunk
vtp domain	Define o nome do domínio VTP
vtp server	Configura o switch para agir como servidor VTP
vtp client	Configura o switch para agir como cliente VTP
vtp password	Define uma senha para o domínio VTP
show vtp status	Apresenta a configuração VTP em um switch
vtp pruning	Ativa VTP pruning em um switch
delete vtp	Deleta configurações VTP de um switch
int f0/0.1	Cria uma subinterface
encapsulation isl 2	Define roteamento ISL para a VLAN 2



Referências

BOYLES, Tim. et al. *Cisco CCNP Certification Library.* [s. l.]: Cisco Press, [s. d.].

CERF, Vinton. How the Internet Came to Be. Disponível em: <http://www.virtualschool.edu/mon/Internet/CerfHowInternetCame2B.html>. Acesso em: 20 out. 2005.

COMER, Douglas E. *Computer Networks and Internets.* [s. l.]: Prentice Hall, [s. d.].

COMPUTER HISTORY MUSEUM. Disponível em: <http://www.computerhistory.org/exhibits/internet_history>. Acesso em: 13 mai. 2008.

DODGE, Martin. *An Atlas of Cyberspace.* Disponível em: <http://www.cybergeography.org/atlas/historical.html>. Acesso em: 13 out. 2007.

DOWNER, Kevin. et al. *InternetWorking: Manual de Tecnologias.* [s. l.]: Cisco Press, [s. d.].

GIBSON, Steve. *What is the Internet?* Disponível em: <http://grc.com/dos/theinternet.htm>. Acesso em: 10 set. 2005.

LAMMLE, Todd. *Cisco CCNA Study Guide.* [s. l.]: Sybex, [s. d.].

MINOLI, Daniel; SCHMIDT, Andrew. *Internet Architectures.* [s. l.]: Wiley, [s. d.].

ODOM, Wendell. *CCNA ICND1 - Official Exam Certification Guide.* Cisco Press, 2007.

SEARCHNETWORKING.COM. *Definitions.* OSI. Disponível em: <http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212725,00.html>. Acesso em: 11 mai. 2008.

SCHAFER, John. *Wireless Data Options.* Disponível em: <www.itcom.itd.umich.edu/wirelessl>. Acesso em: 20 ago. 2007.

STALLINGS, William. *The Origins Of OSI*. Disponível em: <http://williamstallings.com/Extras/OSI.html>. Acesso em: 19 jun. 2008.

TEARE, Diane. *Cisco Internetworking Technologies Handbook*. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.pdf>. Acesso em: 12 jun. 2008.

CISCO SYSTEMS. Disponível em: <http: //www.cisco.com>. Acesso em: jan. 2008.

Grupos de Discussão/Comunidades On-line:

Blog sobre Certificações Cisco

<http://blog.ccna.com.br>

CCNA Brasil

<http://br.groups.yahoo.com/group/ccna_brasil>

Cisco Certified

<http://br.groups.yahoo.com/group/ciscocertified>

Grupo Cer T.I. fique-se!

<http://br.groups.yahoo.com/group/certifique-se>

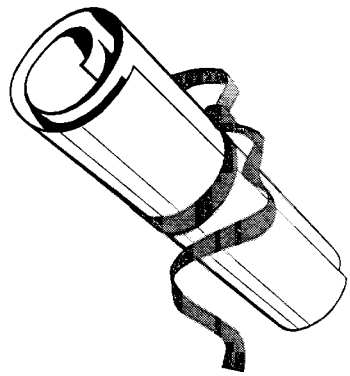
Redes WAN

<http://br.groups.yahoo.com/group/redewan>

Sistema Rau-tu – Redes Wan - UNICAMP

<http://www.rau-tu.unicamp.br/redeswan>

Nota: O autor não mantém nenhum tipo de relação comercial com as empresas citada nesta obra. Todos os nomes comerciais que aparecem nela pertencem aos seus respectivos donos (Cisco Systems, Cisco Career Certifications, as siglas CCNA, CCNP e CCIE, o logo e o modelo piramidal são copyright ©Cisco Systems).



Glossário

Agente: Um programa de computador ou processo que opera sobre uma aplicação cliente ou servidor e realiza uma função específica, como uma troca de informações.

Alias: Segundo nome ou apelido. Pode referenciar um endereço eletrônico alternativo de uma pessoa ou grupo de pessoas ou o segundo nome de uma máquina. É também um dos comandos básicos do UNIX.

ANSI: Acrônimo de *American National Standards Institute*, uma organização afiliada à ISSO, que é a principal organização norte-americana envolvida na definição de padrões (normas técnicas) básicos como o ASCII.

Aplicação: Programa que faz uso de serviços de rede, tais como transferência de arquivos, login remoto e correio eletrônico.

Archie: Um serviço de busca de arquivos armazenados em FTP anônimo. Pouco disseminado no Brasil.

ARPANET: *Advanced Research Projects Agency Network*. Rede de longa distância criada em 1969 pela *Advanced Research Projects Agency* (ARPA, atualmente *Defense Advanced Projects Research Agency* ou DARPA) em consórcio com as principais universidades e centros de pesquisa dos EUA, com o objetivo específico de investigar a utilidade da comunicação de dados em alta velocidade para fins militares. É conhecida como a rede-mãe da Internet de hoje e foi colocada fora de operação em 1990, posto que estruturas alternativas de redes já cumpriam seu papel nos EUA.

ASCII: *American Standard Code for Information Interchange*. Trata-se de um esquema de codificação que atribui valores numéricos às letras do alfabeto, números, sinais de pontuação e alguns símbolos especiais para ser usado em computadores e dispositivos de armazenamento eletrônico de dados.

Assinatura: 1. Um arquivo (tipicamente de três ou quatro linhas) que as pessoas inserem no fim de suas mensagens; 2. Ato de subscrever uma lista de discussão ou newsgroup; 3. Informação que autentica uma mensagem.

Backbone: A interconexão central de uma rede Internet. Pode ser entendido como uma espinha dorsal de conexões que interliga pontos distribuídos de uma rede, formando uma grande via por onde trafegam informações.

Baud rate: Medida de taxa de transmissão elétrica de dados em uma linha de comunicação. Mede o número de sinais elétricos transmitidos por unidade de tempo.

BBS: *Bulletin Board System* é um sistema que, tipicamente, oferece serviços de correio eletrônico, repositório de arquivos (de programas, dados ou imagens) e outros serviços, tais como conversação on-line. Seus assinantes, usualmente, obtêm acesso através de linhas telefônicas (isto é, de voz) utilizadas via computador pessoal e modem.

BITNET: *Because It's Time Network*. Rede de computadores formada em maio de 1981 para interconectar instituições educacionais e de pesquisa, fazendo uso de um protocolo chamado RSCS (*Remote Spooling Communication System*). Teve seu tráfego encerrado em 1996.

Bps: Uma medida da taxa de transferência real de dados de uma linha de comunicação. É dada em bits por segundo. Variantes ou derivativos importantes incluem Kbps (= 1.000 bps) e Mbps (= 1.000.000 bps).

Bridge: Um dispositivo que conecta duas ou mais redes de computadores transferindo, seletivamente, dados entre ambas.

Browser: O browser é um cliente para extração de informação em um servidor Web ou gopher. Tipicamente, um browser será um programa em um computador pessoal que acessará, através de uma linha telefônica, um servidor (isto é, um programa que atende a demanda de clientes remotos) contendo informações de interesse amplo.

CCITT: Acrônimo de *Comité Consultatif Internationale de Telegraphie et Telephonie*, um órgão da *International Telecommunications Union* (ITU) das Nações Unidas que define padrões de telecomunicações (em 1993, foi extinto e suas atribuições passaram para o ITU-TSS, *Telecommunications Standards Section* da ITU).

CERN: Trata-se do *European Laboratory for Particle Physics*, possivelmente o mais importante centro para pesquisas avançadas em física nuclear e de partículas, localizado em Genebra, Suíça. O nome CERN relaciona-se ao seu nome anterior, *Conseil Europeen pour la Recherche Nucleaire*. Para os usuários Internet, o CERN é conhecido como o local onde foi desenvolvida a Web.

Ciberespaço: Conjunto de computadores e serviços que constitui a rede Internet. Termo cunhado em analogia com o espaço sideral explorado pelos astronautas.

Cliente: É um processo ou programa que requisita serviços a um servidor.

Correio eletrônico: Um meio de comunicação baseado no envio e recepção de textos, chamados de mensagens, através de uma rede de computadores.

Domínio: É uma parte da hierarquia de nomes da Internet - DNS -, que permite identificar as instituições ou conjunto de instituições na rede. Sintaticamente, um nome de domínio da Internet consiste de uma seqüência de nomes separados por pontos (.). Por exemplo, ci.rnp.br. Nesse caso, dentro do domínio ci.rnp.br, o administrador do sistema pode criar diferentes grupos como info.ci.rnp.br ou staff.ci.rnp.br, conforme a necessidade.

Domínio público, software de: Programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso. Em geral, o software pode ser utilizado sem custos para fins estritamente

educacionais e não tem garantia de manutenção ou atualização. Um dos grandes trunfos da Internet é a quantidade praticamente inesgotável de softwares de domínio público, de excelente qualidade, que circulam pela rede.

DNS: O *Domain Name System* (DNS) é um serviço e protocolo da família TCP/IP para armazenamento e consulta a informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes Internet em seus números IPs correspondentes.

Download: Transferência de uma cópia de um arquivo presente em um computador remoto para outro computador através da rede. O arquivo recebido é gravado em disco no computador local. O computador de onde os dados são copiados é subentendido como "maior" ou "superior" segundo algum critério hierárquico, enquanto o computador para o qual os dados são copiados é subentendido "menor" ou "inferior" na hierarquia. O sentido literal é, portanto, "puxar para baixo".

Ethernet: Um padrão muito usado para a conexão física de redes locais, originalmente desenvolvido pelo *Palo Alto Research Center* (PARC) da Xerox nos EUA. Descreve protocolo, cabeamento, topologia e mecanismos de transmissão.

E-mail (correio eletrônico): 1. Correio eletrônico; 2. Endereço de correio eletrônico.

FAQ: Acrônimo de *Frequently Asked Questions*; documento com perguntas e respostas sobre determinado assunto, em geral voltado para leigos ou neófitos.

FDDI: Acrônimo de *Fiber Distributed Data Interface*, um padrão para o uso de cabos de fibras óticas em redes locais (LANs) e metropolitanas (MANs). A FDDI fornece especificações para a velocidade de transmissão de dados (alta, 100 Mbps) em redes em anel, podendo, por exemplo, conectar mil estações de trabalho a distâncias de até 200 Km.

FidoNet: Rede mundial de BBS, baseada no uso do protocolo Fido, interligando computadores pessoais via linhas telefônicas.

Finger: Um serviço Internet que permite obter informações sobre usuários de uma máquina.

Firewall: Um sistema de segurança de rede, cujo principal objetivo é filtrar o acesso a uma rede determinada.

Foo: Uma palavra comumente usada para exemplificar qualquer coisa em literatura técnica na área de informática. Por exemplo, ela freqüentemente aparece em exemplos de nomes de domínios como ana@foo.bar.com (a utilização de foo com bar significa o acrônimo).

FUBAR: *Fucked Up Beyond All Recognition*. Comumente usado por militares norte-americanos.

Freenet: Uma máquina na Internet que é dedicada a acesso pela comunidade sem cobrança de nenhuma taxa. O acesso é fornecido através de bibliotecas públicas ou acesso dial-up. Oferece serviços de BBSs, correio eletrônico e acesso (restrito, em geral) à Internet.

FTP: *File Transfer Protocol*. Protocolo padrão da Internet, usado para transferência de arquivos entre computadores.

FTP anônimo: Serviço que possibilita o acesso a repositórios públicos de arquivos via FTP.

FYI: Acrônimo de *For Your Information* (FYI): uma série de artigos sobre a Internet; são similares às RFCs, mas possuem conteúdo consideravelmente menos técnico e não definem novos padrões.

Gateway: 1. Sistema que possibilita o intercâmbio de serviços entre redes com tecnologias completamente distintas, como FidoNet e Internet; 2. Sistema e convenções de interconexão entre duas redes de mesmo nível e idêntica tecnologia, mas sob administrações distintas; 3. Roteador (terminologia TCP/IP).

Gopher: Um sistema distribuído para busca e recuperação de documentos, que combina recursos de navegação através de coleções de documentos e bases de dados indexadas, por meio de menus hierárquicos. O protocolo de comunicação e o software seguem o modelo cliente-servidor, permitindo que usuários em sistemas heterogêneos naveguem, pesquisem e recuperem documentos armazenados em diferentes sistemas, de maneira simples e intuitiva.

Host: Computador ligado a uma rede.

HTML: Acrônimo de *Hypertext Markup Language*, é a linguagem padrão para escrever páginas de documentos Web (WWW). É uma variante da SGML (*Standard Generalized Markup Language*), bem mais fácil de aprender e usar, que possibilita preparar documentos com gráficos e links para outros documentos para visualização em sistemas que utilizam Web.

HTTP: O protocolo HTTP (*HyperText Transfer Protocol*) permite que os autores de hipertextos incluam comandos que possibilitam saltos para recursos e outros documentos disponíveis em sistemas remotos, de forma transparente para o usuário.

Internet: Significa a "rede das redes". Originalmente criada nos EUA, ela se tornou uma associação mundial de redes interligadas, que utilizam protocolos da família TCP/IP. A Internet provê transferência de arquivos, login remoto, correio eletrônico, news e outros serviços.

IP: O Internet Protocol é o protocolo responsável pelo roteamento de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP, desenvolvida e usada na Internet. É considerado o mais importante dos protocolos em que a Internet é baseada.

IRC: Acrônimo de *Internet Relay Chat*; serviço que possibilita a comunicação escrita on-line entre vários usuários pela Internet. É a forma mais próxima do que seria uma "conversa escrita" na rede.

ISO: *International Organization for Standardization* (ISO), uma organização internacional formada por órgãos de diversos países que discute, especifica e propõe padrões para protocolos de redes. Muito conhecida por ter estabelecido um modelo de sete camadas que descreve a organização conceitual de protocolos, o OSI.

ISDN [RDSI]: Uma rede digital que integra serviços de diversas naturezas como voz, dados, imagens etc., que deve substituir gradualmente a infra-estrutura física atual de comunicações, em que cada serviço tende a trafegar por segmentos independentes.

ITU: *International Telecommunications Union*. Órgão da ONU responsável pelo estabelecimento de normas e padrões em telecomunicações.

LAN [Rede Local]: Acrônimo de *Local Area Network*, rede de computadores limitada, em geral, limitada a um prédio ou conjunto de prédios de uma instituição.

Listserv: Servidor de listas de discussões.

Login remoto: Acesso a um computador via rede para execução de comandos. Para todos os efeitos, o computador local, usado pelo usuário para "logar" no computador remoto, passa a operar como se fosse um terminal desse último.

MAN [Rede metropolitana]: Acrônimo de *Metropolitan Area Network*, uma rede com tecnologia que opera a alta velocidade (de centenas de megabits por segundo a alguns gigabits por segundo) e que tem abrangência metropolitana.

Mosaic: Um programa cliente de fácil utilização projetado para procura de informações na Web. Distribuído como freeware, o Mosaic foi criado pelo *National Center for Supercomputing Applications* (NCSA) dos EUA e tem capacidade multimídia.

Multicast: Um endereço para uma coleção específica de nós numa rede ou uma mensagem enviada a uma coleção específica de nós. É útil para aplicações como teleconferência.

Navegação: Ato de conectar-se a diferentes computadores da rede distribuídos pelo mundo, usando as facilidades providas por ferramentas como browsers Web. O navegante da rede realiza uma "viagem" virtual explorando o ciberespaço, da mesma forma que o astronauta explora o espaço sideral. Cunhado por analogia ao termo usado em astronáutica.

Net: The Net ou Internet, a rede.

Netiqueta: Um conjunto de regras de etiqueta para o uso socialmente responsável da Internet, ou seja, o modo como os usuários devem proceder na rede, especialmente na utilização de correio eletrônico.

Netnews: Usenet News, Usenet ou News. Serviço de discussão eletrônica sobre vasta gama de assuntos, cada qual ancorado por um grupo de discussão.

Newsgroup: Grupo temático de discussão do netnews.

NFS: O *Network File System*, desenvolvido pela *Sun Microsystems Inc.*, é um protocolo que usa IP para permitir o compartilhamento de arquivos entre computadores.

NIC [CI]: *Network Informations Center*, centro de informação e assistência ao usuário da Internet que disponibiliza documentos, como RFCs, FAQs e FYIs, realiza treinamentos etc.

NIS: Acrônimo para *Network Information System* (NIS), é um sistema distribuído de bases de dados que troca cópias de arquivos de configuração unindo a conveniência da replicação à facilidade da gerência centralizada. Servidores NIS gerenciam as cópias de arquivos de bases de dados e clientes NIS requerem informação dos servidores em vez de usar suas cópias locais desses arquivos. É muito usado por administradores UNIX para gerenciar bases de dados distribuídas através de uma rede.

NIS+: Versão atualizada do NIS de propriedade da *Sun Microsystems Inc.* que provê mais recursos ao serviço e uma maior segurança.

Nó: Qualquer dispositivo, inclusive servidores e estações de trabalho, ligado a uma rede.

NOC [CO]: *Network Operations Center*. Um centro administrativo e técnico responsável por gerenciar os aspectos operacionais da rede, como o controle de acesso, roteamento etc.

OSI: O *Open Systems Interconnection* (OSI) é um modelo conceitual de protocolo com sete camadas definido pela ISO, para a compreensão e o desenvolvimento de redes de computadores. Trata-se de uma padronização internacional para facilitar a comunicação entre computadores de diferentes fabricantes.

Pacote: 1. Dado encapsulado para transmissão na rede; 2. Um conjunto de bits compreendendo informação de controle, endereço fonte e destino dos nós envolvidos na transmissão.

Ping: O ping (*Packet Internet Groper*) é um programa usado para testar o alcance de uma rede, enviando a nós remotos uma requisição e esperando por uma resposta.

PIR [Ponto de Interconexão de Redes]: Locais previstos para a interconexão de redes de mesmo nível (*peer networks*), visando assegurar que o roteamento entre redes seja eficiente e organizado. No Brasil, os três principais PIRs estão previstos em Brasília, Rio de Janeiro e São Paulo.

PoP: Ponto de Presença de uma espinha dorsal de rede. Local onde uma rede permite acesso a sub-redes e a provedores de serviços. Uma rede madura cobre sua região de atuação através de pontos de presença nas principais cidades/distritos dela, interligados por um conjunto de linhas dedicadas, compondo um backbone.

POP: *Post Office Protocol*. Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

Porta: Uma abstração usada pelo protocolo TCP/IP para distinguir entre conexões simultâneas para apenas um host destino. O termo também é usado para denominar um canal físico de entrada ou de um dispositivo.

Postmaster: E-mail do responsável pelo correio eletrônico de uma instituição.

PPP: Um dos protocolos mais conhecidos para acesso via interface serial, permite que um computador faça uso do TCP/IP através de uma linha telefônica convencional e um modem de alta velocidade. É considerado o sucessor do SLIP por ser mais confiável e eficiente.

Protocolo: Uma descrição formal de formatos de mensagem e das regras que dois computadores devem obedecer ao trocar mensagens. Um conjunto de regras padronizadas que especificam o formato, a sincronização, o seqüenciamento e a verificação de erros em comunicação de dados. O protocolo básico utilizado na Internet é o TCP/IP.

Provedor de Acesso: Instituição que se liga à Internet, via um ponto de presença ou outro provedor, para obter conectividade IP e repassá-la a outros indivíduos e instituições, em caráter comercial ou não.

Provedor de Informação: Instituição cuja finalidade principal é coletar, manter e/ou organizar informações on-line para acesso através da Internet, por parte de assinantes da rede. Essas informações podem ser de acesso público

incondicional, caracterizando assim um provedor não-comercial ou, no outro extremo, constituir um serviço comercial onde existem tarifas ou assinaturas cobradas pelo provedor.

Provedor de Serviço: Pode ser tanto o provedor de acesso quanto o de informação.

Repetidor: Um dispositivo que propaga (regenera e amplifica) sinais elétricos em uma conexão de dados, para estender o alcance da transmissão sem fazer decisões de roteamento ou de seleção de pacotes.

RFC: Acrônimo para *Request For Comments*. RFCs constituem uma série de documentos editados desde 1969 e que descrevem aspectos relacionados com a Internet, como padrões, protocolos, serviços, recomendações operacionais etc. Uma RFC é, em geral, muito densa do ponto de vista técnico.

Roteador/Router: Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes. Tipicamente, uma instituição, ao se conectar à Internet, deverá adquirir um roteador para conectar sua Rede Local (LAN) ao ponto de presença mais próximo.

Servidor: 1. No modelo cliente-servidor, é o programa responsável pelo atendimento a determinado serviço solicitado por um cliente. Serviços como Archie, Gopher, WAIS e WWW são providos por servidores; 2. Referindo-se a equipamento, o servidor é um sistema que provê recursos tais como armazenamento de dados, impressão e acesso dial-up para usuários de uma rede de computadores.

Site [instalação]: 1. Uma instituição onde computadores são instalados e operados; 2. Um nó Internet.

Shareware: Programa disponível publicamente para avaliação e uso experimental, mas cujo uso em regime pressupõe que o usuário pagará uma licença ao autor. Note-se que shareware é distinto de freeware, no sentido de que um software em shareware é comercial, embora em termos e preços diferenciados em relação a um produto comercial "ortodoxo".

SLIP: *Serial Line IP* é um protocolo Internet bastante popular usado via interfaces seriais.

Smiley: Uma "carinha" construída com caracteres ASCII e muito usada em mensagens eletrônicas para dar idéia de sentimentos ou emoções. Por exemplo, a mais comum é :-), que significa humor e ironia. Você deve girar o smiley 90 graus para a direita para entendê-lo.

SMTP: O *Simple Mail Transfer Protocol* é o protocolo TCP/IP usado para troca de mensagens via correio eletrônico na Internet.

SNMP: O *Simple Network Management Protocol* é um protocolo usado para monitorar e controlar serviços e dispositivos de uma rede TCP/IP. É o padrão adotado pela RNP para a gerência de sua rede.

Sysop: A pessoa que opera e mantém um BBS. Abreviatura de *system operator*.

Talk: Serviço que permite a comunicação escrita on-line entre dois usuários da Internet.

TCP/IP: Acrônimo de *Transmission Control Protocol/Internet Protocol*, é a família de protocolos para a comunicação de dados inter-redes, originalmente proposta

para a *Advanced Research Products Agency Network* (ARPANet). Hoje é um padrão de fato para inter-redes abertas e seu uso é amplamente difundido dentro e fora dos EUA.

Telnet: Serviço que permite login remoto segundo o jargão e a vertente técnica Internet.

Transceiver: Dispositivo utilizado na conexão física de um nó a uma rede local. Efetua a transferência e cópia de arquivos entre duas máquinas via rede. Na Internet, implantada e conhecida por FTP.

UDP: Acrônimo para *User Datagram Protocol*, é o protocolo de transporte sem conexão da família TCP/IP, usado com aplicações como de gerenciamento de redes (SNMP) e de serviço de nomes (DNS).

URL: Acrônimo para *Uniform Resource Locator*, é um localizador que permite identificar e acessar um serviço na rede Web. Por exemplo, a URL a seguir aponta para o WWW do HPG: <http://www.hpg.com.br/>.

UUCP: *UNIX-to-UNIX CoPy* é uma coleção de programas para intercomunicação de sistemas UNIX. Possibilita a transferência de arquivos, execução de comandos e correio eletrônico.

Veronica: Acrônimo para *Very Easy Rodent-Oriented Net-wide Index to Computerized Archives*. Ferramenta para pesquisa no *GopherSpace*, o conjunto de servidores *Gopher* disponíveis na Internet.

Waffle: Um programa que possibilita a um BBS tornar-se um site Usenet.

WAIS: Acrônimo para *Wide Area Information Server*, é um serviço de bases de dados distribuídas acessíveis via Internet, cuja principal peculiaridade é a conversão automática de formatos para visualização remota de documentos e dados.

WAN [Rede de longa distância]: Acrônimo de *Wide Area Network*, uma rede que interliga computadores distribuídos em áreas geograficamente separadas.

WHOIS: Banco de dados de informações sobre domínios, redes, hosts e pessoas, fornecendo um serviço de diretório de usuários da Internet.

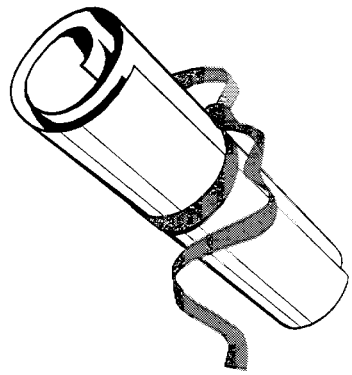
WORM: Acrônimo de *Write Once Read Many*. 1. Ferramenta de busca na rede Web; 2. Verme, programa que, explorando deficiências de segurança de hosts, logrou propagar-se de forma autônoma na Internet na década de 80.

WWW: *World Wide Web* ou Web. Meta-rede, baseada em hipertextos, que integra diversos serviços Internet, através de uma interface que possibilita o acesso a informações multimídia.

X.25: Protocolo de roteamento muito utilizado em redes públicas de pacotes.

X.400: Um protocolo que especifica serviços do tipo *store-and-forward*, sendo o serviço de correio eletrônico *Message Handle System* (MHS) o mais conhecido deles, como parte das recomendações OSI/ISO.

X.500: É um padrão ITU-TSS/ISO para serviços de diretório eletrônico.



Apêndice A

Laboratórios

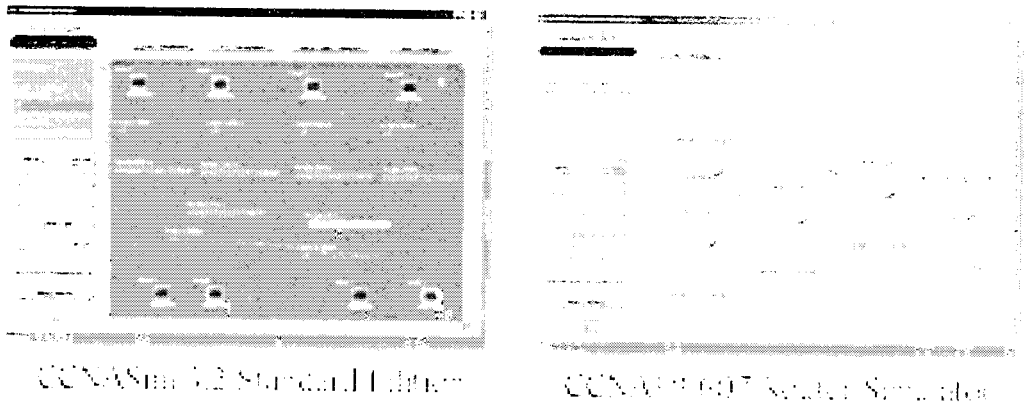
O exame Cisco CCNA em sua nova versão (640-802) ainda foca na porção teórica dos assuntos abordados. No entanto, como o exame utiliza simuladores do IOS em algumas questões, é aconselhável que você procure ter acesso a algum equipamento Cisco ou, ao menos, a um bom simulador ou emulador (software) do sistema IOS. Existem vários disponíveis, porém, em sua maioria, apenas em versões comerciais. A seguir comento os dois mais populares e onde podem ser obtidos:

- **Boson Router Simulator <http://www.routeru.com/>**

Este simulador do sistema IOS é um dos mais completos existentes. A Boson permite que se obtenha o aplicativo de seu site, porém, a versão disponibilizada de graça é bastante limitada. Para ter acesso a todos os recursos, deve-se desembolsar algo em torno de US$90 (preço médio dos programas simuladores). Entre as vantagens deste aplicativo encontra-se a possibilidade de se criar diversos cenários virtuais e a variedade de comandos suportados.

- **RouterSim 3.2 <http://www.routersim.com/>**

Na minha opinião é o melhor simulador IOS existente hoje no mercado. O software é tão completo que algumas empresas efetivamente o utilizam como ferramenta no planejamento de redes WAN. A configuração criada pode ser copiada para um router verdadeiro e vice-versa. Disponibiliza uma série de equipamentos (routers, switches, hubs e PCs) para a montagem dos mais diversos cenários e também aceita uma grande variedade de comandos. Pode ser obtido no site da empresa. Este simulador não é gratuito!



Os softwares citados permitem que você pratique para o exame CCNA (em alguns casos, até para o CCNP!). Contudo, é desnecessário dizer que o contato com o equipamento real sempre é recomendado. É importante lembrar que simuladores não conseguem reproduzir todas as características dos roteadores reais e, por isso, alguns comandos podem não funcionar com estes softwares.

Uma alternativa, nesse caso, é a utilização de um software que emula um (ou mais) roteador Cisco em seu PC. Trata-se do *Dynamips*, um software relativamente novo que reproduz via software as características físicas de um roteador real, tornando um PC comum capaz de rodar o software IOS como se fosse um roteador real. A melhor parte do *Dynamips* é que ele é - pasmem - totalmente gratuito.

Tutorial para uso do Dynamips

Baseado no tutorial oficial disponível no site: <http://dynagen.org/tutorial.htm>.

Introdução

Dynamips é um emulador de roteadores Cisco desenvolvido por Christophe Fillot. Atualmente, ele é capaz de emular as plataformas 1700, 2600, 3600, 3700, e 7200, rodando imagens do sistema IOS tradicionais (as mesmas que rodam nos roteadores reais). Obviamente, um roteador emulado não pode substituir um router real, em uma rede. Isso porque um router emulado pelo *Dynamips* não consegue chegar nem perto da performance oferecida por um router Cisco real (o que é lógico, já que o emulador faz em software tudo o que um roteador Cisco real faz em hardware dedicado).

O interessante do *Dynamips* é que ele permite que um único PC seja capaz de emular mais de 1 roteador simultaneamente. O número de instâncias (routers emulados) possíveis é basicamente limitado pela velocidade e a quantidade de memória que sua máquina dispõe, assim

como a versão do sistema operacional que roda na mesma. O *Dynamips* tende a rodar de forma mais eficiente em ambientes Linux do que em ambientes Windows, apesar de ser compatível com ambos.

Para rodar o *Dynamips*, é preciso instalar também a biblioteca PCAP (*WinPCap*, no Windows e a *LibPCap* no Linux). Esta biblioteca permite o acesso direto à camada física da(s) placa(s) de rede do PC onde o *Dynamips* será instalado, permitindo que interfaces FastEthernet de routers emulados sejam associadas à interfaces físicas reais do PC. Por que isso é particularmente interessante? Porque permite que você conecte seu roteador emulado a uma rede real! Isso mesmo. É possível a conexão de roteadores e switches reais (de qualquer fabricante) a um roteador emulado pelo *Dynamips*. Isso é ótimo se você precisa montar um ambiente de laboratório, por exemplo. Aliás, esta é a principal finalidade do *Dynamips*: Arquitetar laboratórios para estudos dirigidos de redes de computadores. E ele cumpre este papel muito bem!

O *Dynamips* em sua forma *stand alone*, ou seja, sozinho, é bastante complicado de ser utilizado. Pensando nisso, foi criado o *Dynagen*, basicamente uma interface de configuração para o *Dynamips*. O *Dynagen* provê um modo descomplicado de se criar ambientes utilizando o *Dynamips*.

Instalação

Seguem os pré-requisitos para se instalar o *Dynamips / Dynagen* em sua máquina (vou listar o mínimo necessário para rodar os cenários que apresentarei mais adiante, mas a aplicação pode rodar em máquinas menos robustas):

- Pentium IV;
- 1 GB de memória RAM;
- Ideal ter ao menos uma placa de rede;
- Imagem do IOS para a plataforma que pretende utilizar;
- Windows XP ou Linux com suporte à linguagem Python.

A instalação para Windows é extremamente simples. Basta baixar o executável no site oficial <http://dynagen.org/> e instalá-lo como se fosse qualquer outra aplicação. No caso de Linux, é necessário antes certificar-se que sua distribuição possui a biblioteca *LibPCap* instalada. Depois, basta baixar os executáveis em <http://dynagen.org/> e pronto!

Iniciando a Emulação

Assim que o *Dynamips* é instalado (Windows), alguns atalhos já aparecem em seu desktop: *Dynamips Server, Network Device List* e *Dynagen Sample Labs*. Vamos começar pelo atalho *Dynagen Sample Labs*. Clicando nele, você abre uma pasta contendo alguns arquivos com a extensão *.net*, que são os arquivos de configuração do *Dynamips*. Os arquivos são em modo texto e tem uma sintaxe muito parecida com os arquivos *.ini* do Windows (ou do DOS). Vamos pegar como exemplo o arquivo *Simple1.net*. Se abrirmos este arquivo utilizando um editor de textos comum, eis o que teremos:

```
# Simple lab

[localhost]

  [[7200]]
  image = \Program Files\Dynamips\images\c7200-adventerprisek9-
mz.124-4.T1.bin
  # On Linux / Unix use forward slashes:
  # image = /opt/7200-images/c7200-adventerprisek9-mz.124-4.T1.bin
  npe = npe-400
  ram = 160

  [[ROUTER R1]]
  s1/0 = R2 s1/0

  [[router R2]]
  # No need to specify an adapter here, it is taken care of
  # by the interface specification under Router R1
```

Note que, por default, o *Dynamips* emula um roteador Cisco 7200. Isto é interessante se você pensa em montar um cenário altamente complexo, mas por outro lado, a emulação de um roteador deste porte consome muita memória e CPU. Minha sugestão é que você comece alterando o tipo de router a ser emulado. Vamos seguindo linha a linha a configuração. Antes de mais nada, tenha em mente que o símbolo # denota um comentário, ou seja, a linha precedida por este símbolo não será considerada na execução:

```
# Simple lab
```

Comentário. Trata-se do nome do cenário, somente.

```
[localhost]
```

O *Dynamips* é um software servidor, ou seja, assim que ele é iniciado ele fica aguardando uma conexão TCP em uma determinada porta. Por default, esta porta é a TCP7200. Este modo do *Dynamips* é chamado de *Hypervisor*. O *Dynagen* é o software cliente que irá acessar este servidor. O *Dynamips* pode rodar em diversos PCs simultaneamente, ou seja, você pode iniciar uma sessão de emulação de 2 routers em um PC, outra sessão de 2 routers em outro PC, e pode controlar ambas de uma única máquina, via *Dynagen*, com um único arquivo *.net*.

```
[[7200]]
```

Aqui você define qual a plataforma a ser emulada. No caso, 7200.

```
image = \Program Files\Dynamips\images\c7200-adventerprisek9-
mz.124-4.T1.bin
```

O próximo passo é informar, no arquivo *.net*, onde se encontra a imagem do IOS que será utilizada. Pode ser qualquer pasta em seu PC.

```
# On Linux / Unix use forward slashes:
# image = /opt/7200-images/c7200-adventerprisek9-mz.124-4.T1.bin
```

Comentários sobre como proceder se o Dynamips estiver rodando em Linux.

```
npe = npe-400
```

Definição de qual o tipo de NPE deve ser emulado (apenas para plataforma 7200).

```
ram = 160
```

Definição da quantidade de memória RAM a ser alocada para cada instância emulada

```
[[ROUTER R1]]
```

Definição da primeira instância (o nome R1 foi escolhido ao acaso. Poderia ser qualquer outro nome)

```
s1/0 = R2 s1/0
```

Indicação de como o roteador definido na primeira instância (R1) encontra-se conectado ao roteador definido na segunda instância (R2, logo abaixo). No caso, a interface serial S1/0 do R1 conecta-se à interface serial s1/0 do R2. Poderíamos ter uma série de outras combinações.

```
[[router R2]]
```

Definição da segunda instância.

```
# No need to specify an adapter here, it is taken care of
# by the interface specification under Router R1
```

Comentário informando que não é preciso configurar nada nesta instância, pois a conexão com o R1 foi definida na primeira instância.

O arquivo *.net* comentado anteriormente produz um cenário conforme o ilustrado na figura 1.

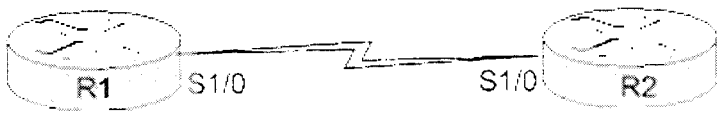
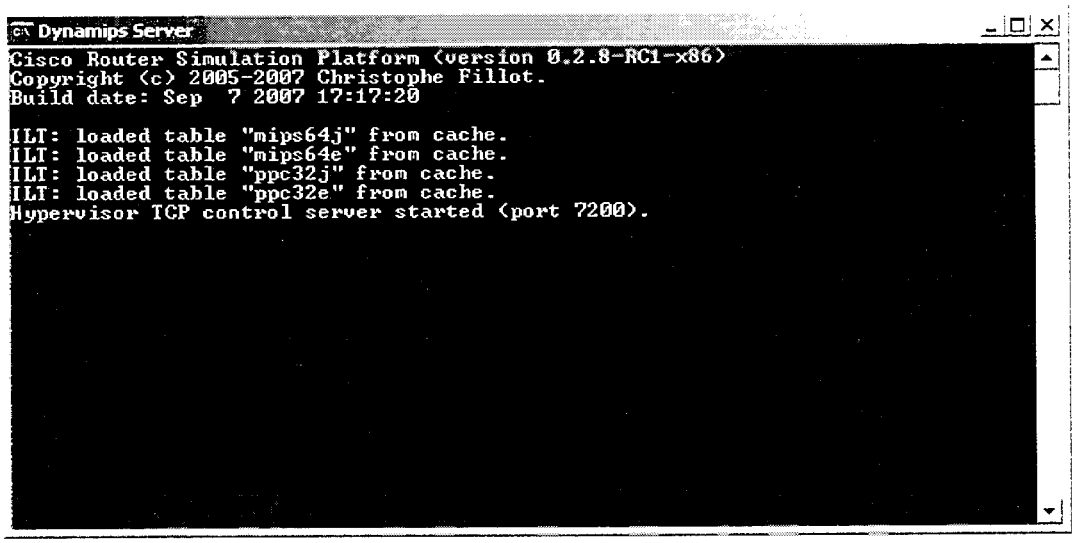
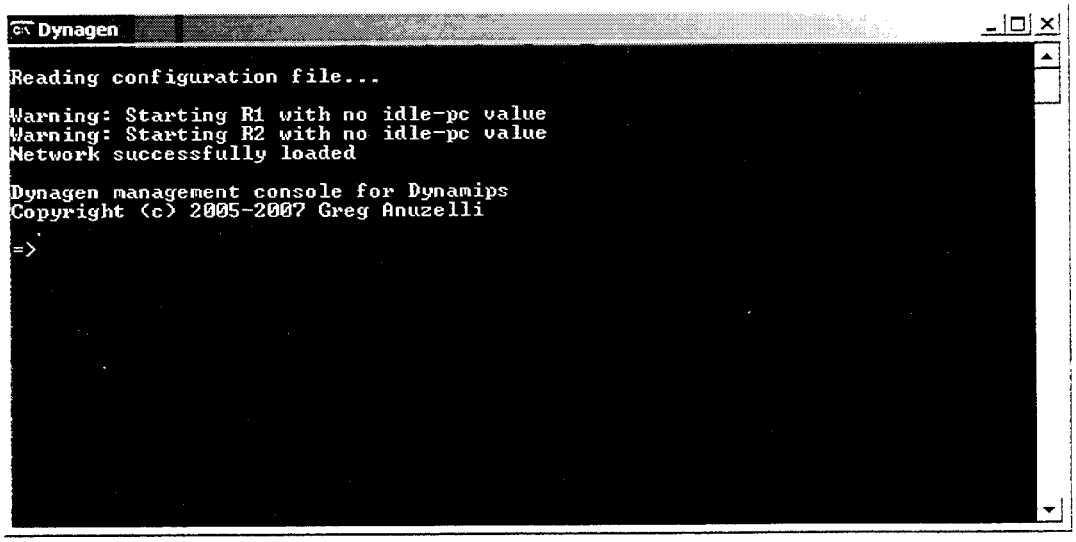


Figura 1: Exemplo de cenário do Dynamips.

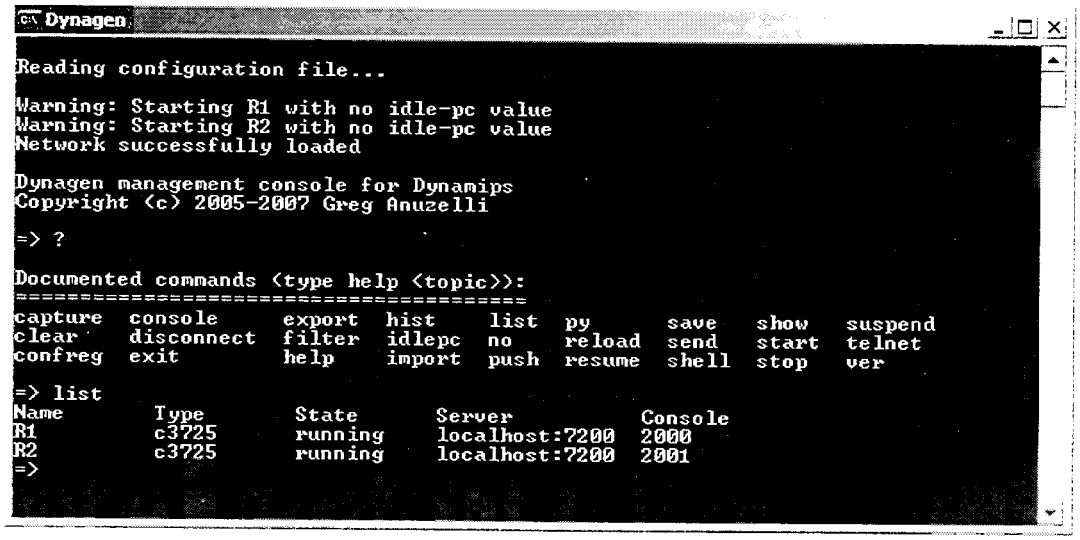
Bom, uma vez definidos os parâmetros no arquivo *.net*, podemos iniciar a emulação. Para isso, clique duas vezes no ícone em seu desktop chamado *Dynamips Server*:



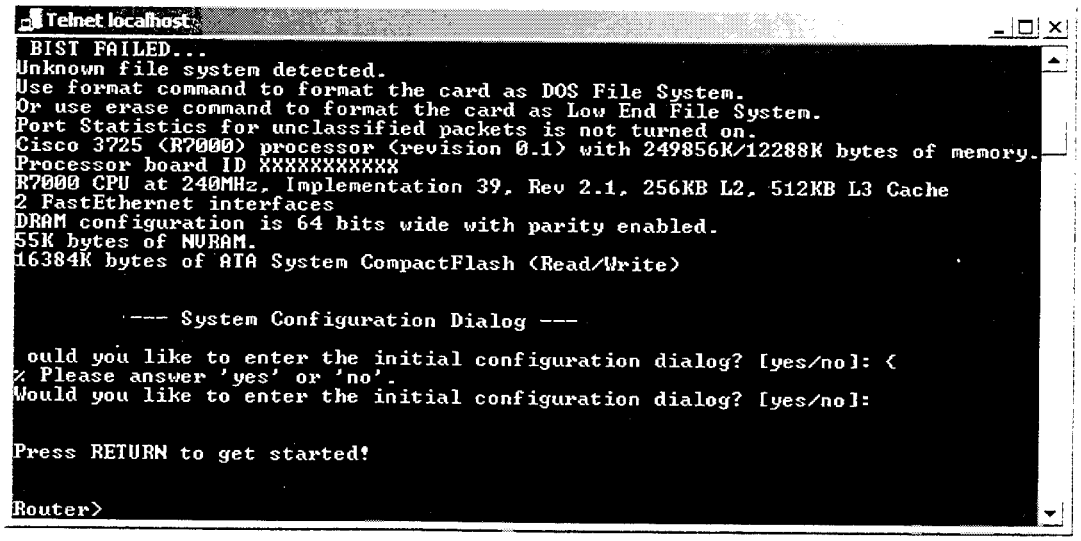
Na sequência, localize o arquivo *.net* que você deseja usar, e clique duas vezes sobre ele:



Esta tela aparece logo que você executa o arquivo *.net*, e é chamada de *Console Dynagen*. É uma espécie de central de controle. Para saber quais comandos você tem a disposição, basta digitar ?. Por exemplo:

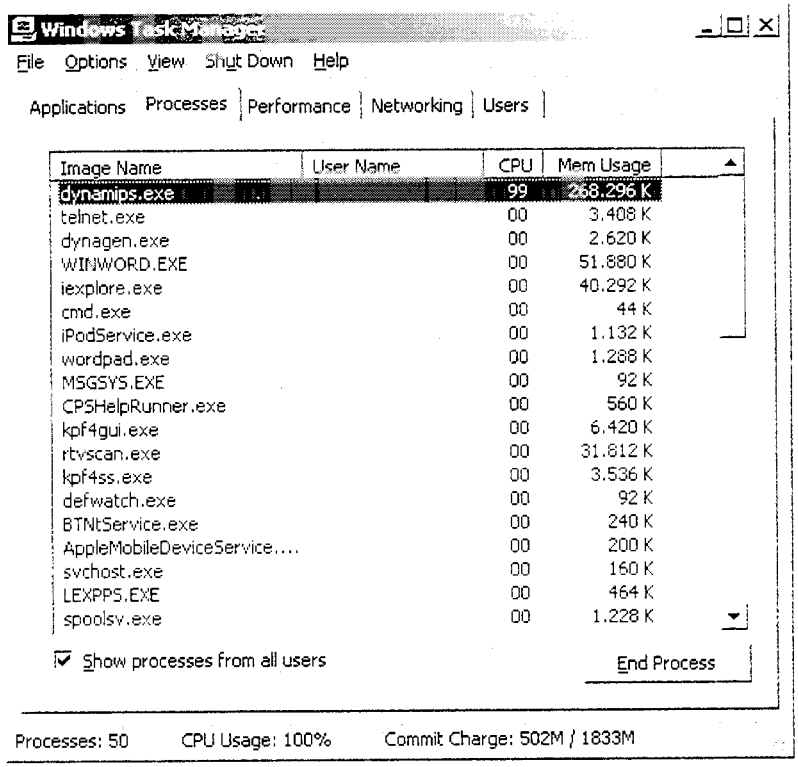


Usando o comando *list*, eu obtenho uma lista dos dispositivos emulados. No caso, tenho 2 roteadores da linha 3725 (depois mostro como alterar os tipos de roteadores). Para acessar o roteador é preciso que eu digite no *Console Dynagen* a opção *telnet R1*, por exemplo. Assim que eu fizer isso, uma janela se abre com uma sessão console ao router R1. Isso mesmo, uma sessão console! Lembre-se que eu não tenho nada configurado no roteador. Assim sendo, apenas posso acessá-lo via porta console. Apesar do comando no *Console Dynagen* ser *telnet [instância]*, o que ele faz, na verdade, é conectar-se à porta console (virtual) da instância desejada, por meio de um artifício chamado *Telnet Reverso*. Eis a tela de conexão ao console do router R1:

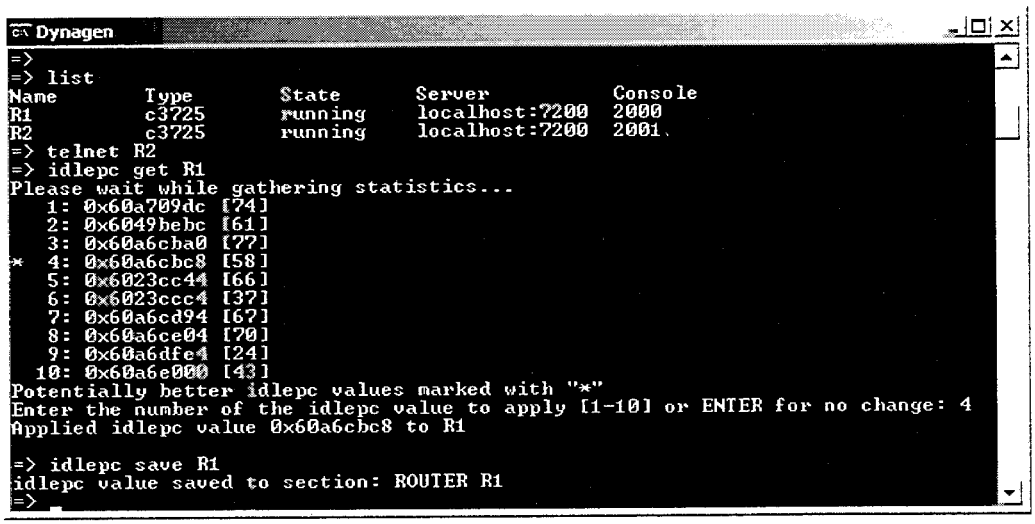


Utilização de Recursos

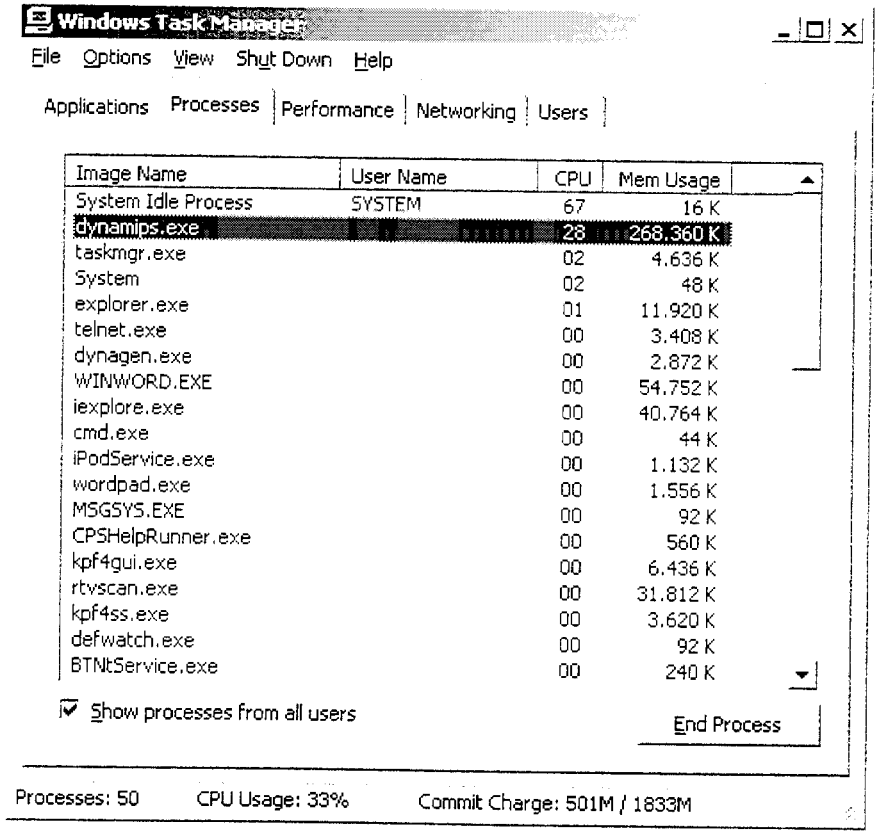
O *Dynamips* é sedento por CPU e memória. Assim que você inicia a emulação, notará que a CPU de seu PC vai a quase 100%:



Para amenizar o problema, existe um parâmetro que deve ser configurado chamado *idlepc*. Como o valor deste parâmetro é praticamente impossível de ser definido manualmente, o *Console Dynagen* incorporou esta funcionalidade e, convenientemente, consegue não apenas definir qual o valor, mas também salva-o em seu arquivo *.net* para que, na próxima execução de seu cenário, sua CPU não seja tão solicitada. Basta digitar o comando *idlepc get [nome da instância]* e aguardar:



Veja que 10 valores são apresentados, sendo que o que o *Dynagen* considera o mais apropriado é marcado com *. Basta você fazer a sua escolha (escolhi a sugestão do *Dynagen*, no exemplo) e posteriormente usar o comando *idlepc save [nome da instância]* para que o valor fique permanentemente registrado no arquivo *.net*. Note como o consumo da CPU cai assim que eu faço o mesmo para o router R2:



Este passo, portanto, é de suma importância, especialmente se você for utilizar um cenário com mais de 2 routers. Lembre-se que é necessário ter muita memória (cada instância utiliza a quantidade de memória definida no arquivo *.net*) e muita CPU para agüentar um cenário mais complexo.

Emulação de Outras Plataformas

Como foi mencionado, o *Dynamips* suporta a emulação de diversas plataformas: 1700, 2600, 3600, 3700, e 7200. Tenha em mente, entretanto, que quanto mais avançada for a plataforma escolhida, mais recursos do seu PC ela tende a utilizar. Eu adoto a linha 3600, por exemplo, é uma boa plataforma para laboratórios, permite que se rode as versões mais recentes do IOS (12.4) com as features mais atualizadas, e não consome muita memória e CPU. Como fazer para alterar a plataforma no arquivo *.net*?

Eis como proceder:

```
# Simple lab
[localhost]
    [[3620]] -> Alteração da plataforma
        image = \Program Files\Dynamips\images\c3620-is-mz.123-
14.T7.bin  -> Alteração da imagem do IOS
        ram = 64 -> Alteração da quantidade de memória (cheque
os requerimentos da imagem de IOS que você escolheu)
    [[ROUTER R1]]
        model = 3620 -> Esta nova linha é necessária
        S1/0 = R2 S1/0
    [[ROUTER R2]]
```

Como pode ser observado, é bastante simples alterar a plataforma a ser emulada. Outros parâmetros interessantes de se conhecer que podem fazer parte dos arquivos *.net* são:

slot0 = NM-16ESW - Insere um módulo NM-16ESW em um dos routers emulados (basta escolher qual).

Por exemplo:

```
[[ROUTER R1]]
    model = 3620 -> Esta nova linha é necessária
    S1/0 = R2 S1/0
    slot0 = NM-16ESW
```

Este módulo é um switch com 16 portas, e pode ser usado em cenários que tenham switches, por exemplo.

Outros módulos suportados são:

- NM-1E (Ethernet, 1 port);
- NM-4E (Ethernet, 4 ports);
- NM-1FE-TX (FastEthernet, 1 port);
- NM-4T (Serial, 4 ports).

E para a plataforma 7200, temos somente os *Port Adapters*:

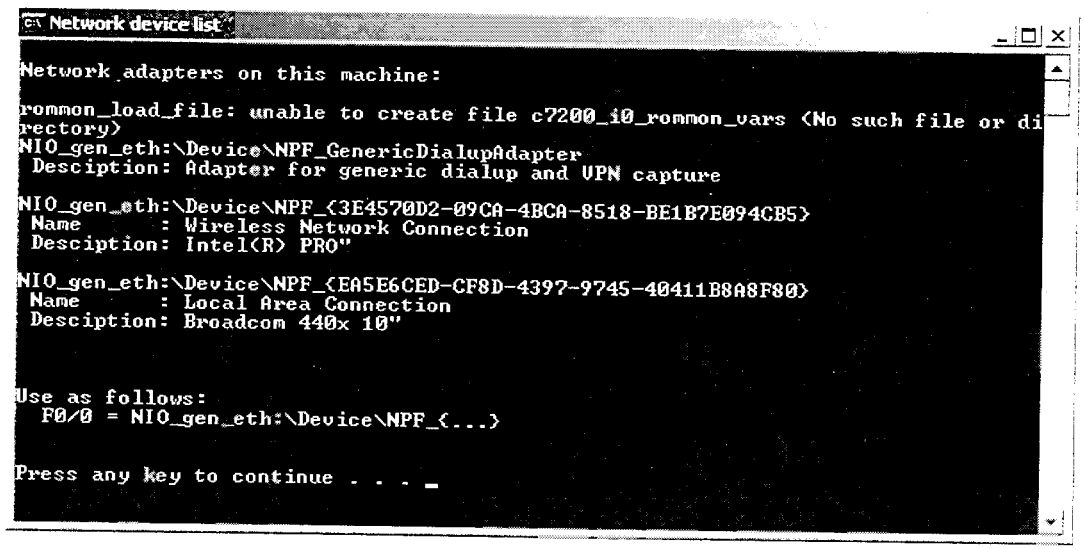
- PA-FE-TX (FastEthernet);
- PA-2FE-TX (FastEthernet, 2 ports);
- PA-4E (Ethernet, 4 ports);
- PA-8E (Ethernet, 8 ports);
- PA-4T+ (Serial, 4 ports);
- PA-8T (Serial, 8 ports);
- PA-A1 (ATM);
- PA-POS-OC3 (POS);
- PA-GE (GigabitEthernet).

Ou seja, basta ter imaginação e é possível fazer com o *Dynamips* praticamente tudo o que se faz com um router real.

Conexão com Redes Reais

É possível associar uma interface FastEthernet de um router virtual (emulado) à uma interface física real no seu PC. Desta forma, pode-se conectar seu cenário, montado com o *Dynamips*, à uma rede real. Para isso, basta seguir os passos:

Determine o atributo da interface física (real) desejada. Para isso, clique 2 vezes no ícone *Network Device List* em seu desktop:



Neste exemplo, aparecem 3 interfaces. Uma VPN, uma Wireless e uma Ethernet UTP (tradicional). Vamos supor que eu queira associar a interface UTP do meu laptop à interface FastEthernet do meu roteador virtual R1. Basta eu adicionar a seguinte linha no arquivo *.net*:

```
F0/0 = NIO_gen_eth:\Device\NPF_{EA5E6CED-CF8D-4397-9745-
40411B8A8F80}
```

Fazendo isso, assim que eu iniciar a simulação, meu router emulado R1 poderá se comunicar com o mundo externo (mundo real) por intermédio da interface Ethernet do meu laptop. Para todos os efeitos, é como se meu laptop fosse um roteador. Se eu conectá-lo a um switch Cisco real, por exemplo, e o CDP estiver rodando, o switch mostrará meu laptop como sendo um roteador Cisco da plataforma informada no arquivo .net.

O *Dynamips* é muito mais do que eu apresentei aqui, neste breve tutorial. Há muito mais sobre ele que eu não vou mencionar, do contrário, teria que escrever um livro apenas sobre este assunto (para

mostrar que não estou exagerando, eu baseei minha dissertação de mestrado no *Dynamips*). Mas vou deixar alguns links de referência, caso você se interesse:

- Tutorial oficial do Dynamips / Dynagen (em inglês): <http://dynagen.org/tutorial.htm>.
- Fórum oficial de discussão sobre o Dynamips / Dynagen: <http://7200emu.hacki.at/>.
- Vídeo-tutoriais sobre o Dynagen (português): <http://blog.ccna.com.br/?p=78>; <http://blog.ccna.com.br/?p=104>; <http://blog.ccna.com.br/?p=165>.

Nota: *Dúvidas sobre Dynamips / Dynagen, mesmo que saiam do escopo do CCNA, podem ser apresentadas no blog que eu mantenho <http://blog.ccna.com.br> ou no grupo de discussão do Yahoo: <http://www.yahoogrupos.com.br/groups/certifique-se>.*

Cenários para serem Implementados no Dynamips / Dynagen

Os labs sugeridos a seguir foram idealizados para utilização com routers emulados, utilizando-se o software *Dynamips / Dynagen*.

Os cenários ilustrados utilizam roteadores virtuais para exercer a função de hosts, entretanto, existe uma opção bem mais "leve" para simular hosts, que se integra perfeitamente com o Dynamips, chamada VPCS <http://wiki.freecode.com.cn/doku.php?id=wiki:vpcs&s=vpc>. Um tutorial de como utilizar este software juntamente com o Dynamips encontra-se disponível no fórum do blog que mantenho <http://blog.ccna.com.br/forum/comments.php?DiscussionID=31>.

Cenário 1: VLANs e Roteamento dot1q

Um dos melhores cenários é a configuração de roteamento inter-VLANs, utilizando a interface FastEthernet 0/0 de um roteador como o 3620 e o protocolo IEEE 802.1q. A seguir temos uma sugestão de como proceder para implementar esse cenário.

O diagrama a ser implementado é apresentado na figura 2.

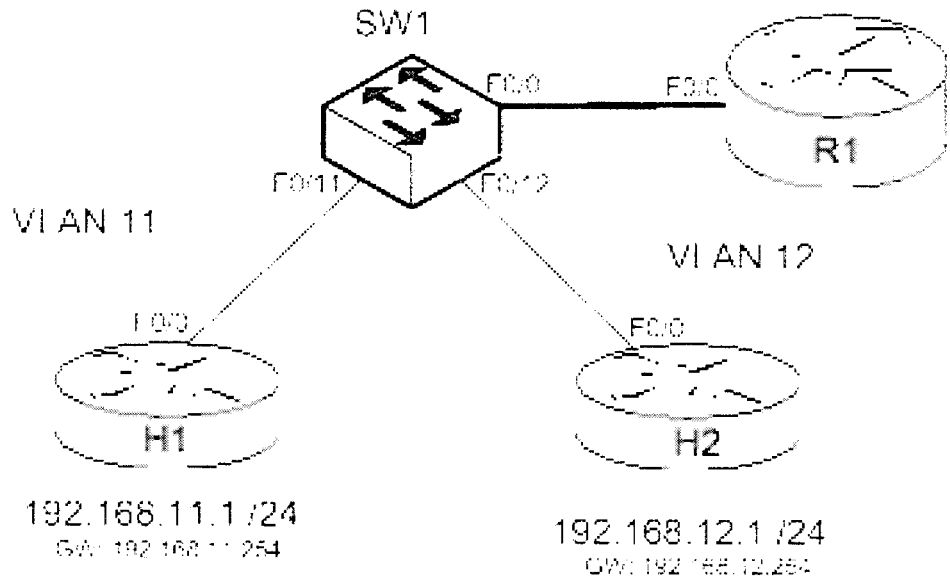


Figura 2: Diagrama do cenário 1, proposto.

Objetivo: Criar duas VLANs no Switch SW1, associar cada roteador (H1 e H2) a uma VLAN e rede, conforme ilustrado, e configurar o roteamento entre as VLANs criadas utilizando apenas a interface F0/0 do router R1 e o protocolo IEEE 802.1q. Note que os routers H1 e H2, neste cenário, têm a mera função de hosts (PCs) comuns. Por esse motivo, a função de roteamento IP neles será desativada, para que eles passem a operar como PCs comuns conectados a uma rede. Para testar o cenário após implementá-lo, utilize as ferramentas PING e TRACE.

As configurações do arquivo *.net* para o *Dynagen* seguem:

```
# Lab 01 - Roteamento dot1q
[localhost]
    [[3620]]
     image = \Program Files\Dynamips\images\c3620-is-mz.123-21.bin
        ram = 64
    [[ROUTER SW1]]
        model  = 3620
        slot0  = NM-16ESW
        idlepc = 0x60535eb4
        F0/0   = R1 F0/0
        F0/11  = H1 F0/0
        F0/12  = H2 F0/0
    [[ROUTER R1]]
        model = 3620
        idlepc = 0x60535eb4
```

```
[[ROUTER H1]]
    model = 3620
    idlepc = 0x60535eb4
[[ROUTER H2]]
    model = 3620
    idlepc = 0x60535eb4
```

Nota: Este cenário exige bastante do PC em termos de emulação. Se você não tiver um PC que atenda aos requisitos colocados no início deste capítulo, dificilmente este cenário irá funcionar. Os cenários apresentados aqui foram testados em um notebook Centrino 1.7 com 768MB de memória, e rodaram de forma satisfatória. ***Lembre-se que os valores de idlepc aqui são apenas sugeridos.*** *Talvez seja interessante redefinir estes valores em seu PC.*

Solução Sugerida

Configuração do Switch SW1

A configuração de VLANs no switch emulado pelo *Dynamips* é ligeiramente diferente do que vimos anteriormente no livro. Isso porque o switch emulado adota o modo antigo de configuração, que utiliza o modo *VLAN DATABASE*. Apenas neste modo, VLANs podem ser adicionadas ou deletadas, e os parâmetros VTP configurados. Abaixo, a solução sugerida:

```
conf t
hostname SW1
exit
!
vlan database
 vlan 11 name VLAN11
 vlan 12 name VLAN12
apply
exit
!
conf t
interface FastEthernet0/0
 switchport mode trunk
 no ip address
!
```

```
interface FastEthernet0/11
 switchport access vlan 11
 no ip address
!
interface FastEthernet0/12
 switchport access vlan 12
 no ip address
!
end
```

Configuração do Router R1 para Roteamento dot1q

```
conf t
!
 int f0/0
 no ip address
 no shut
!
 int f0/0.11
 encap dot1q 11
 ip add 192.168.11.254 255.255.255.0
!
 int f0/0.12
 encap dot1q 12
 ip add 192.168.12.254 255.255.255.0
!
end
```

Configuração do Router H1 (Função de Host)

```
conf t
 int f0/0
 ip add 192.168.11.1 255.255.255.0
 no shut
 exit
!
 no ip routing
!
 ip default-gateway 192.168.11.254
!
end
```

Verifique as configurações realizadas por meio de PINGs e TRACEs entre os elementos H1 e H2. Verifique o resultado.

Configuração do Router H2 (Função de Host)

```
conf t
int f0/0
 ip add 192.168.12.1 255.255.255.0
 no shut
 exit
!
 no ip routing
!
 ip default-gateway 192.168.12.254
!
end
```

Cenário 2: Configuração de Roteamento EIGRP e Listas de Acesso

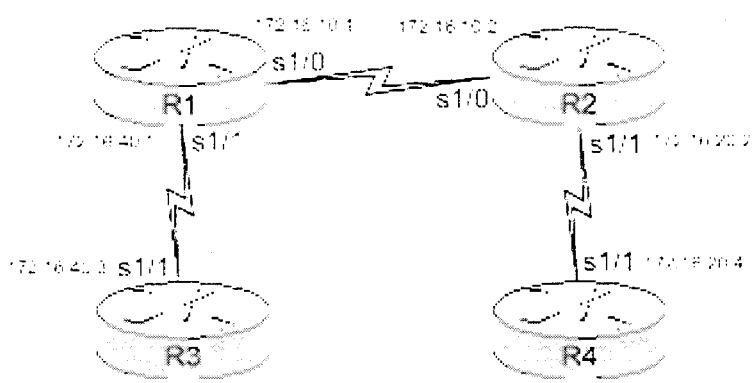


Figura 3 – Diagrama do laboratório de ACL.

Objetivo: Configure a rede ilustrada utilizando EIGRP no ASN 65000, crie uma lista de acesso que negue requisições ICMP (Ping, por exemplo) originadas do router R3 com destino ao router R4 e aplique-a na(s) interface(s) e sentido(s) mais conveniente(s). OBS: Suponha máscara de rede /24 para todas as redes ilustradas.

Arquivo *.net* para este lab:

```
# Lab 02 - ACLs
[localhost]
    [[3620]]
      image = \Program Files\Dynamips\images\c3620-is-mz.123-21.bin
        ram = 64
```

```
[[ROUTER R1]]
    model  = 3620
    idlepc = 0x60535eb4
    s1/0 = R2 s1/0
    s1/1 = R3 s1/1
[[ROUTER R2]]
    model  = 3620
    idlepc = 0x60535eb4
    s1/1 = R4 s1/1
[[ROUTER R3]]
    model  = 3620
    idlepc = 0x60535eb4
[[ROUTER R4]]
    model  = 3620
    idlepc = 0x60535eb4
```

Solução Sugerida

Configurações Iniciais e de Roteamento:

Router R1

```
config t
 hostname R1
 interface Serial1/0
 ip address 172.16.10.1 255.255.255.0
 interface Serial1/1
 ip address 172.16.40.1 255.255.255.0
!
router eigrp 65000
 no auto-sum
 netw 172.16.0.0
!
end
```

Router R2

```
config t
 hostname R2
 interface Serial1/0
 ip address 172.16.10.2 255.255.255.0
 interface Serial1/1
 ip address 172.16.20.2 255.255.255.0
```

```
!
router eigrp 65000
 no auto-sum
 netw 172.16.0.0
!
end
```

Router R3

```
config t
 hostname R3
 interface Serial1/1
 ip address 172.16.40.3 255.255.255.0
!
router eigrp 65000
 no auto-sum
 netw 172.16.0.0
!
end
```

Router R4

```
config t
 hostname R4
 interface Serial1/1
 ip address 172.16.20.4 255.255.255.0
!
router eigrp 65000
 no auto-sum
 netw 172.16.0.0
!
end
```

Verifique se as configurações foram bem sucedidas por meio do comando *sh ip route* ou testando a camada de rede via PINGS, TRACES, etc.

Configuração e Aplicação da ACL:

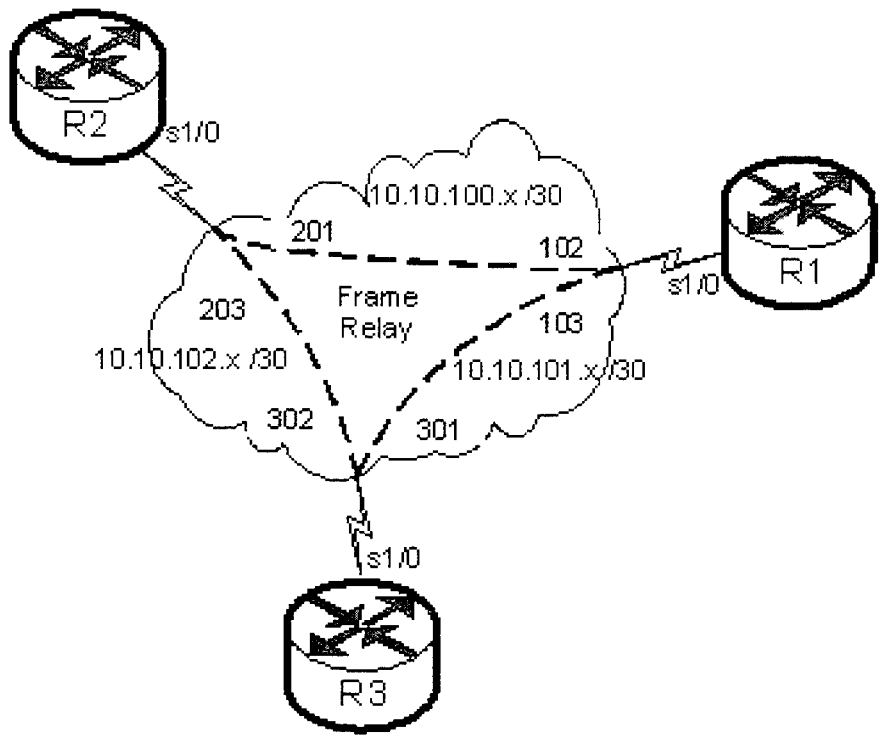
A ACL deve ser aplicada no router R1, no sentido IN. Por que? Simples... Você deve lembrar-se que uma ACL é totalmente alheia aos pacotes originados pelo próprio router. Portanto, se aplicarmos a ACL em R3, ela não terá efeito algum, já que o router não analisa os pacotes gerados

por ele mesmo. Assim sendo, seguindo as melhores práticas, o local mais próximo da origem seria a interface S1/1 do router R1, no sentido IN, para que os pacotes gerados pelo router R3 sejam analisados e os pacotes ICMP com destino ao R4 sejam barrados.

```
config t
 access-list 101 deny icmp host 172.16.40.3 host 172.16.20.4
 access-list 101 permit ip any any
 int s1/1
 ip access-group 101 in
!
end
```

Teste a configuração tentando um ping de R3 para a interface s1/1 de R4. Você verá que não vai surtir efeito. Aproveite para testar comandos de debug ou modifique as configs e verifique os resultados!

Cenário 3: Configuração Frame-Relay



Objetivo: Configurar a rede Frame-Relay para interconectividade dos routers, conforme ilustrado. Ative também o protocolo de roteamento EIGRP no ASN 65000 para divulgação de todas as subredes envolvidas no cenário.

Arquivo *.net* para este lab:

```
# Lab 03: Frame Relay

[localhost]

 [[3725]]
   image = C:\Program Files\Dynamips\images\c3725-ipvoicek9-mz.124-9.T
    ram = 256

 [[ROUTER R1]]
    model = 3725
    idlepc = 0x60bb55d0
    s1/0 = F1 1
 [[ROUTER R2]]
    model = 3725
    idlepc = 0x60bb55d0
    s1/0 = F1 2
 [[ROUTER R3]]
    model = 3725
    idlepc = 0x60bb55d0
    s1/0 = F1 3

 [[FRSW F1]]
    1:102 = 2:201
    1:103 = 3:301
    2:203 = 3:302
```

Solução Sugerida

Router R1:

```
conf t
!
hostname R1
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
!
interface Serial1/0.102 point-to-point
 ip address 10.10.100.1 255.255.255.252
```

```
 frame-relay interface-dlci 102
!
interface Serial1/0.103 point-to-point
 ip address 10.10.101.1 255.255.255.252
 frame-relay interface-dlci 103
!
router eigrp 65000
 network 10.0.0.0
 no auto-summary
!
end
```

Router R2:

```
conf t
!
hostname R2
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
!
interface Serial1/0.201 point-to-point
 ip address 10.10.100.2 255.255.255.252
 frame-relay interface-dlci 201
!
interface Serial1/0.203 point-to-point
 ip address 10.10.102.2 255.255.255.252
 frame-relay interface-dlci 203
!
router eigrp 65000
 network 10.0.0.0
 no auto-summary
!
end
```

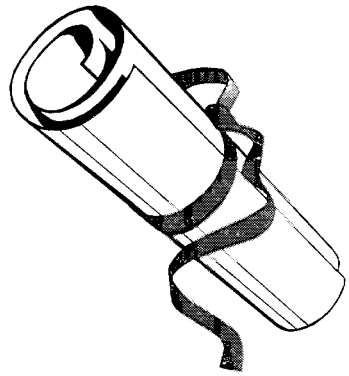
Router R3:

```
conf t
!
hostname R3
```

```
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
!
interface Serial1/0.301 point-to-point
 ip address 10.10.101.2 255.255.255.252
 frame-relay interface-dlci 301
!
interface Serial1/0.302 point-to-point
 ip address 10.10.102.2 255.255.255.252
 frame-relay interface-dlci 302
!
router eigrp 65000
 network 10.0.0.0
 no auto-summary
!
end
```

Repare que o *Dynagen* consegue simular uma nuvem Frame-Relay sem problemas! Para testar este cenário, realize os testes de conectividade padrão (ping, etc), examine a tabela de roteamento e utilize os comandos de verificação Frame-Relay para compreendê-los melhor.

Dica: Os 3 cenários sugeridos neste apêndice são apenas SUGESTÕES! Você pode adicionar mais elementos aos cenários apresentados, elaborar seus próprios cenários, rodar outros protocolos, testar NAT, etc! Sua imaginação é o limite. Espero que estes labs tenham sido de alguma utilidade.



Apêndice B

Comandos para Prática

Básicos	
Entrar em modo privilegiado	**enable**
Sair do modo privilegiado	**disable**
Encerrar uma sessão console ou Telnet	**exit**
Encerrar uma sessão console ou Telnet	**logout**
Entrar em modo *setup*	**setup**
Apresentar a configuração da RAM	**show running-config**
Apresentar a configuração da NVRAM	**show startup-config**
Apresentar informações sobre o IOS, hardware e *configuration register*	**show version**
Apresentar os arquivos armazenados na FLASH	**show flash**
Salvar configuração na NVRAM	**copy running-config startup-config**
Ativar configuração salva na NVRAM	**copy startup-config running-config**
Copiar configuração salva em um servidor TFTP para a NVRAM	**copy tftp running-config**
Upgrade do IOS armazenado na FLASH de uma imagem armazenada em um servidor TFTP	**copy tftp flash**
Efetuar backup da imagem armazenada na FLASH para um servidor TFTP	**copy flash tftp**
Instruir o router para inicializar de uma determinada imagem armazenada na FLASH	**boot system flash [filename]**
Instruir o router para inicializar de uma determinada imagem armazenada em um servidor TFTP	**boot system tftp [filename]**

Básicos	
Entrar em modo de configuração global	**config terminal**
Definir um banner MOTD (*Message Of The Day*)	**banner motd # message #**
Definir um banner LOGIN	**banner login # message #**
Definir um banner EXEC	**banner exec # message #**
Definir um banner INCOMING	**banner incoming # message #**
Nomear um router	**hostname [name]**
Desabilitar DNS lookups	**no ip domain-lookup**
Especificar um servidor DNS	**ip name-server server-ip1 [server-ip2...server-ip6]**
Desabilitar o recurso HTTP Server	**no ip http server**
Alterar o tamanho do *history buffer*	**terminal history size 20**

Senhas	
Definir uma senha para modo privilegiado	**enable password | [password]**
Definir uma senha criptografada para modo privilegiado	**enable secret | [password]**
Definir uma senha para sessões Telnet	**line vty 0 4 | login | password [passwords]**
Definir uma senha para a porta console	**line console 0 | login | password [passwords]**

Configuração de Interfaces	
Configurar a interface Ethernet 0	**interface e 0**
Configurar a primeira interface serial	**interface s 0**
Configurar a segunda interface Token Ring	**interface t 1**
Ativar uma interface	**no shutdown**
Desativar uma interface	**shutdown**
Definir o *clock rate* em uma interface DCE	**clock rate 56000**
Definir a largura de banda (*bandwidth*)	**bandwidth 64**
Apresentar o status da interface	**show interface serial 1**
Apresentar tipo de sinalização (DTE ou DCE)	**show controllers serial 1**
Definir intervalo *keepalive*	**keepalive 10**

IP	
Desativar roteamento IP (ativado por default)	**no ip routing**
Apresentar a tabela de roteamento IP	**show ip route**
Configurar um endereço IP em uma interface	**ip address 192.168.1.12 255.255.255.0**
Habilitar roteamento RIP	**router rip | network [network-address1] | network [network-address2...]**

IP	
Desabilitar *Split-Horizon* em uma interface	**no ip split-horizon**
Habilitar *RIP triggered updates*	**ip rip triggered**
Desabilitar sumarização automática de rotas	**no auto-summary**
Habilitar roteamento IGRP	**router igrp [as-number] | network [network-address1] | network [network-address2...]**
Habilitar roteamento RIPv2	**router rip | version 2 | network [network-address1] | network [network-address2...]**
Habilitar roteamento OSPF	**router ospf [process number] | network [network address] | wildcard [wildcard mask] | area [area number]**
Habilitar roteamento EIGRP	**router eigrp [as-number] | network [network-address1] | network [network-address2...]**

PPP	
Habilitar PPP em uma interface	**encapsulation ppp**
Definir modo de autenticação PPP como PAP	**ppp authentication PAP**
Definir modo de autenticação PPP como CHAP	**ppp authentication CHAP**
Define o primeiro método de autenticação PPP como PAP e o segundo como CHAP	**ppp authentication PAP CHAP**
O inverso do comando acima	**ppp authentication CHAP PAP**
Define *CHAP username*	**ppp chap hostname [username]**
Define *CHAP password*	**ppp chap password [password]**
Define *PAP username*	**ppp pap sent-username [username] [password]**
Define um *username* e senha para routers que queiram se comunicar via PPP	**username [username] password [password]**
Habilita compressão PPP em uma interface	**ppp compress [predictor | stac]**
Habilita multilink PPP em uma interface	**ppp multilink**
Apresenta informações sobre PPP multilink	**show ppp multilink**

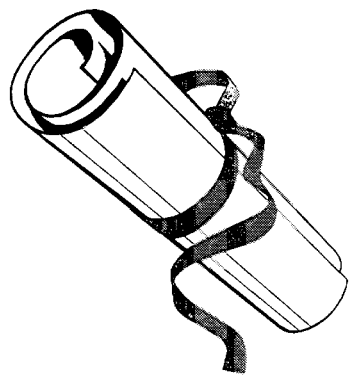
Frame-Relay	
Habilita encapsulamento Frame-Relay em uma interface e define o tipo de encapsulamento a ser utilizado	**encapsulation frame-relay [cisco | ietf]**
Especifica manualmente o tipo de LMI	**frame-relay lmi type [ansi | cisco | q9331]**
Define a largura de banda de um link	**bandwidth 64**
Mapeamento manual de endereço para DLCI	**frame-relay map protocol protocol-address dlci [broadcast] [ietf | cisco]**
Definição manual da DLCI	**frame-relay local-dlci [number]**
Apresenta estatísticas sobre os circuitos PVC	**show Frame-Relay pvc**
Apresenta estatísticas sobre LMIs	**show Frame-Relay lmi**
Apresenta tabela de mapeamento em atividade	**show Frame-Relay map**

CDP	
Apresenta dispositivos diretamente conectados	**show cdp neighbor**
Apresenta informações detalhadas sobre dispositivos diretamente conectados	**show cdp neighbor detail**
Desabilita CDP no router	**no cdp run**
Desabilita CDP para uma determinada interface	**no cdp enable**
Define o intervalo para transmissão de pacotes CDP	**cdp timer 90**
Define o tempo que um dispositivo deve reter um pacote CDP	**cdp holdtime 180**
Limpa informações sobre dispositivos vizinhos na tabela CDP	**clear cdp table**

Comandos de Edição	
Relembrar o último comando digitado no *history buffer*	**CTRL-P ou seta p/ cima**
Relembrar o próximo comando no *history buffer*	**CTRL-N ou seta p/ baixo**
Autocompletar comandos	**TAB**
Encerrar modo de configuração	**CTRL-Z**
Mover o cursor para trás um caractere	**Ctrl-B ou seta p/ a esquerda**
Mover o cursor para frente um caractere	**Ctrl-F ou seta p/ a direita**
Mover o cursor para o início da linha de comando	**Ctrl-A**
Mover o cursor para o final da linha de comando	**Ctrl-E**

Access Control Lists (Listas de Acesso)	
IP Standard Access Lists (intervalo de 1 a 99)	
Objetivo: Configure a interface ethernet 0 para negar pacotes entrantes originados da sub-rede 192.168.1.0 / 24	
1. Negar a sub-rede	**access-list 1 deny 192.168.1.0 0.0.0.255**
2. Permitir todas as outras (lembre-se de que existe um comando *deny any* implícito!)	**access-list 1 permit any**
3. Aplicar a lista criada à interface ethernet 0	**interface ethernet 0 | ip access-group 1 in**
IP Extended Access Lists (intervalo de 100 a 199)	
Objetivo: Configure a interface ethernet 0 para negar a sub-rede 192.168.1.0 o acesso à Web	
1. Negar a sub-rede	**access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 80**
2. Permitir o acesso das outras sub-redes	**access-list 100 permit ip any any**
3. Aplicar a lista criada à interface ethernet 0	**interface ethernet 0 | ip access-group 100 out**
Objetivo: Configure a interface serial 1 para negar o host 192.168.1.222 de estabelecer uma sessão Telnet para qualquer host pertencente à sub-rede 172.16.8.1 / 16	
1. Negar a sub-rede	**access-list 101 deny tcp host 192.168.1.222 172.16.8.1 0.0.255.255 eq 23**
2. Permitir todas as outras	**access-list 101 permit ip any any**
3. Aplicar a lista criada à interface serial 1	**interface serial 1 | ip access-group 101 out**

***Nota**: Procure praticar todos os comandos aqui listados. É de vital importância para o sucesso no exame que você se habitue à terminologia, principalmente dos comandos destacados (que são os que devem ser cobrados nas questões que envolvem o simulador IOS).*



Apêndice C

Estudo de Casos

Vamos ver alguns cenários/estudos de caso, para sedimentar bem toda a teoria que vimos no decorrer deste livro. Apresentarei dois cenários com nível de dificuldade alto, se comparados ao exame CCNA. Se você for capaz de compreendê-los, certamente estará mais perto do título CCNA.

Cenário 1: Empresa NETCOM

Tópicos analisados: Sub-redes, configuração de switches e de roteamento inter-VLANS, listas de acesso, VLANs, VTP e o modelo Cisco de 3 camadas.

A NETCOM é uma empresa de consultoria localizada em São Paulo/Capital. A empresa hoje aluga cinco andares de um prédio comercial no centro da cidade. O CIO da empresa, grande colega seu, lhe confidenciou que está com um problema lógico em sua rede. A empresa possui uma rede plana e isso está gerando problemas de segurança e de performance. O CIO demonstrou um interesse em adotar VLANs como forma de segmentar a rede, contudo, não sabe muito bem quais as vantagens dessa tecnologia, nem como implementá-la. Disse também que possui um router 1721 sobrando e que o endereço de rede atual (192.168.100.0 /24) **não** deve ser alterado neste momento por razões corporativas. O modelo de todos os switches é Catalyst 2950.

Eis o seu desafio: A rede original e a rede que você irá propor ao CIO encontram-se ilustradas a seguir. Você agora precisa:

1. Detalhar ao CIO os problemas existentes na rede como ela se encontra hoje;
2. Convencê-lo de que ao adotar a sua proposta ele estará, de fato, resolvendo os problemas levantados;
3. Configurar o router e os switches existentes, sendo que, para os switches, o central deve operar em modo VTP servidor e os periféricos, no modo VTP clientes. Configure o domínio VTP "ccna";
4. Apresentar as configurações do router e do switch central da rede, assim como configurar os três switches periféricos para o modo VTP Cliente e mesmo domínio VTP do switch central;
5. Mapear a rede proposta ao modelo Cisco de 3 camadas, se aplicável.

Boa sorte!

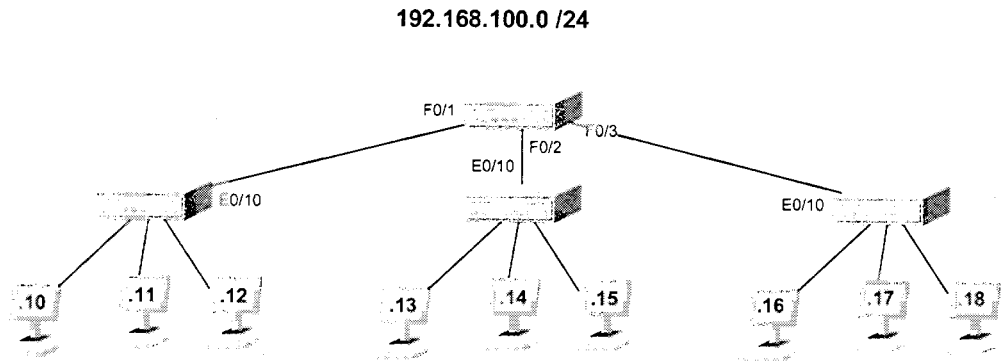


Diagrama 1: Rede atual – empresa NETCOM.

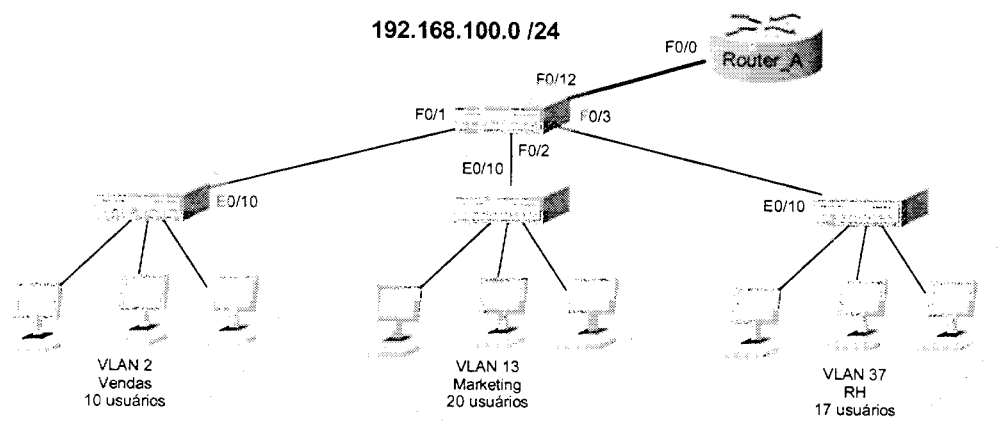


Diagrama 2: Rede proposta – empresa NETCOM.

Solução Sugerida:

Como você pode observar, o problema não é simples. Vamos por partes, então. Observando o Diagrama 1, onde a rede em seu estado atual é apresentada, os principais problemas que podemos identificar são:

- Existe apenas um domínio de *broadcast*, ou seja, pacotes de *broadcast* enviados pelo PC com endereço 192.168.100.10, por exemplo, serão recebidos por **todas** as máquinas da rede. Isso nos leva ao segundo ponto, a seguir;
- A segurança da rede é precária, em parte devido ao problema mencionado anteriormente. Note que temos três departamentos críticos aqui e não seria interessante ter o tráfego do departamento de RH, por exemplo, sendo recebido por máquinas não-autorizadas;
- A performance da rede tende a piorar à medida que o número de usuários simultaneamente conectados a ela aumenta, exatamente pelo fato de haver apenas um domínio de *broadcast*;
- A rede não apresenta escalabilidade, ou seja, não prevê o crescimento futuro, o que pode ser um complicador mais adiante.

Se você foi capaz de identificar mais problemas além dos mencionados anteriormente, parabéns! Esse era exatamente o seu trabalho. Pensar como um verdadeiro consultor de redes.

Partindo para o diagrama sugerido (2), temos que aprontar as coisas para a apresentação ao CIO. Antes de mais nada, repare que a rede atual usa uma rede classe C (192.168.100.0 /24), e como foi mencionado, a troca de endereço de rede não é uma alternativa. Vamos adotar a criação de VLANs; portanto, teremos que segmentar essa rede classe C em três redes menores - isso mesmo: sub-redes! Essa seria então nossa primeira tarefa: criar o plano de endereçamento IP dessa nova rede. Observe a ilustração 2 e mãos a obra (tente fazer isso sozinho, **antes** de olhar a solução, do contrário, este exercício é inútil)!

Plano de Endereçamento IP

Temos a necessidade de criar três sub-redes, partindo de uma rede classe C. Para isso, usaremos o cálculo a seguir:

$2^x - 2 >= 3 \quad 2^3 - 2 = 6 \quad 6 >= 3$

Repare que nosso "x" é igual a 3, e que teremos seis sub-redes válidas no total. Bom, sabendo-se que x = 3, podemos concluir que 3 bits "0"

da máscara padrão foram convertidos para "1", para a criação de sub-redes. Se a máscara padrão de redes classe "C" é /24, nossa "nova" máscara será /27 (24+3) ou 255.255.255.224. Cada uma dessas seis sub-redes pode conter até 30 hosts (2^5 -2 = 30, onde "5" é o número de "0s" que sobraram na máscara).

Bom, uma vez que temos nossa máscara, descobrir quais as redes que ela nos proporciona é fácil (lembra-se?). O cálculo é 256 - 224 = 32. Portanto, nossas sub-redes ocorrem em intervalos de 32. São elas:

192.168.100.32	192.168.100.64	192.168.100.96
192.168.100.128	192.168.100.160	192.168.100.192

Como apenas necessitamos de três, vamos escolher as três primeiras:

192.168.100.32	192.168.100.64	192.168.100.96

Logo, nosso plano de endereçamento ficaria assim:

Rede 1 (VLAN 2):	192.168.100.32
Broadcast:	192.168.100.63
Gateway (router):	192.168.100.33
Intervalo de hosts:	192.168.100.34 - 192.168.100.62
Rede 2 (VLAN 13):	192.168.100.64
Broadcast:	192.168.100.95
Gateway (router):	192.168.100.65
Intervalo de hosts:	192.168.100.66 - 192.168.100.94
Rede 3 (VLAN 37):	192.168.100.96
Broadcast:	192.168.100.127
Gateway (router):	192.168.100.97
Intervalo de hosts:	192.168.100.98 - 192.168.100.126

Seguindo o cronograma, uma vez que já montamos nosso plano de endereçamento e nossa rede proposta encontra-se pronta (Diagrama 2), temos agora que explicar ao CIO da empresa como solucionaria os quatro pontos anteriormente levantados.

Basicamente, criar VLANs significa criar domínios de *broadcast*, ou seja, cada VLAN é seu próprio domínio de *broadcast*. Em nosso caso, estaríamos isolando os *broadcasts* dos departamentos de RH, Marketing e Vendas ao associarmos cada um deles a uma VLAN diferente. Dessa forma, a performance da rede melhoraria, assim como a sua segurança. Quanto ao problema de escalabilidade, basta VLANs adicionais serem

criadas conforme a necessidade (lembrando que temos três sub-redes "sobrando"). A segurança da rede poderia ser adicionalmente reforçada com o uso de listas de acesso no router 1721, que fará o roteamento inter-VLANs (usando dot1q, no caso, já que switches 2950 não suportam ISL).

Configurações Propostas

Switch Central

```
Switch_C#config t
Switch_C(config)#vtp domain ccna
Switch_C(config)#vlan 2
Switch_C(config-vlan)#name Vendas
Switch_C(config-vlan)#vlan 13
Switch_C(config-vlan)#name Marketing
Switch_C(config-vlan)#vlan 37
Switch_C(config-vlan)#name RH
Switch_C(config-vlan)#exit
Switch_C(config)#int f0/1
Switch_C(config-if)#switchport access vlan 2
Switch_C(config-if)#int f0/2
Switch_C(config-if)#switchport access vlan 13
Switch_C(config-if)#int f0/3
Switch_C(config-if)#switchport access vlan 37
Switch_C(config-if)#int f0/12
Switch_C(config-if)#switchport mode trunk
Switch_C(config-if)#^Z
```

Switches Periféricos (todos usam a mesma configuração apresentada a seguir)

```
Switch#config t
Switch(config)#vtp mode client
Switch(config)#vtp domain ccna
```

Router (1721)

Seguindo nosso plano de endereçamento:

```
1721#config t
1721(config)#int f0/0.2
1721(config-subif)#encap dot1q 2
1721(config-subif)#ip add 192.168.100.33 255.255.255.224
1721(config-subif)#int f0/0.13
1721(config-subif)#encap dot1q 13
1721(config-subif)#ip add 192.168.100.65 255.255.255.224
```

```
1721(config-subif)#int f0/0.37
1721(config-subif)#encap dot1q 37
1721(config-subif)#ip add 192.168.100.97 255.255.255.224
1721(config-subif)#int f0/0
1721(config-if)#no shut
```

Note que não é necessário configurar rotas nesse router, uma vez que todas as redes já se encontram diretamente conectadas à interface Fa0/0. Basta agora que a configuração IP dos PCs de cada VLAN obedeça ao plano de endereçamento estabelecido e que usem o endereço do default gateway presente nele (que nada mais é do que o endereço de cada subinterface *dot1q* no router).

Com relação ao mapeamento da nova rede ao modelo Cisco de 3 camadas. A resposta é **sim**, é possível. Temos, neste exemplo, muito bem definidas ao menos duas camadas do modelo: Acesso e Distribuição. Na camada de Distribuição estaria o nosso router 1721 e apenas ele, enquanto na camada de Acesso estariam os switches.

Apenas para encerrar em grande estilo, vamos supor que nosso CIO nos faça uma última solicitação (antes de nos pagar, claro): ele deseja que o servidor presente na VLAN de RH com o IP 192.168.100.100 seja acessado apenas internamente, ou seja, nenhum usuário que não pertença à VLAN de RH deve ter acesso a ele. Como implementaríamos isso? Pense um pouco antes de ir à solução.

A solução para esse problema é a adoção de listas de acesso em nosso router, claro. Como o objetivo é negar todo e qualquer acesso que não seja interno ao servidor presente na VLAN de RH, podemos criar uma regra permitindo RH e negando todo o resto:

```
1721(config)#access-list 111 deny ip any host 192.168.100.100
1721(config)#access-list 111 permit ip any any
```

Você deve estar se perguntando onde está o comando que permite que usuários da VLAN RH tenham acesso ao servidor 192.168.100.100. Basta pensarmos um pouco: o servidor encontra-se na mesma LAN dos usuários que poderão acessá-lo, portanto, eles não precisam chegar ao router para acessar o servidor em questão - o acesso se dá via rede local. Por esse motivo, não é necessário uma linha na lista de acesso permitindo a rede local.

Bom, nossa lista está criada. Note que ela **deve** terminar com um *permit any*, do contrário, o *deny any* implícito irá bloquear todo o tráfego onde essa lista for aplicada. Agora, a pergunta: **onde** aplicar essa lista e em que direção?

Lembre-se de que listas de acesso estendidas são normalmente melhor acomodadas o mais próximo possível da origem. No nosso caso,

não existe apenas uma origem, mas múltiplas. Por esse motivo, o ideal - neste caso específico - seria aplicar essa lista o mais próximo possível do destino, no caso, a subinterface f0/0.37, onde a VLAN de RH encontra-se conectada. Quanto à sua direção, ela deve analisar o tráfego que sai por essa interface, ou seja, *out*.

```
1721(config)#interface f0/0.37
1721(config-if)#ip access-group 111 out
```

Cenário 2 – Empresa ACME

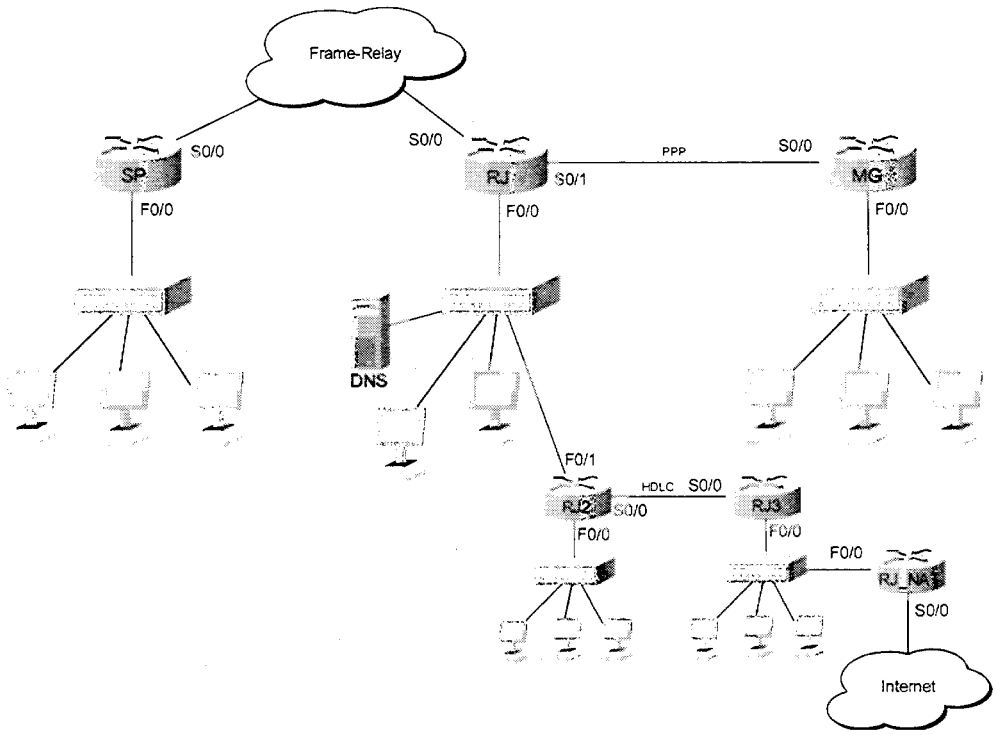


Diagrama 3: Rede da empresa ACME.

Tópicos analisados: Roteamento EIGRP, roteamento estático default, sub-redes, VLSM, sumarização de rotas, *ip-helper*, listas de acesso, configuração Frame-Relay, PPP, NAT e configuração de senhas.

Neste cenário, você deverá configurar os routers da rede apresentada no diagrama 3, baseando-se nas seguintes premissas:

O número de usuários nas localidades SP, RJ e MG não ultrapassa 20. As localidades RJ2 e RJ3 têm cinco usuários cada. O router RJ_NAT não possui usuários conectados, encontrando-se diretamente conectado ao router RJ3, via LAN. Sua função é meramente agir como um dispositivo NAT para acesso à Internet. A rede apresentada opera sob a rede *classful* 192.168.200.0 /24 e não existe a possibilidade de se usar outra rede que não essa. Na localidade RJ, temos o servidor DNS central da rede da empresa, ou seja, você precisa ter isso em mente ao configurar os routers das outras localidades (lembrando que DNS opera usando

broadcasts). O acesso à Internet é centralizado e ocorre através do router RJ_NAT. Isso significa que todas as outras localidades devem passar por RJ_NAT para chegar à Net (observe que você precisará configurar NAT neste router). A conexão entre SP e RJ é feita via Frame-Relay *point-to-point*, já a conexão entre RJ e MG via PPP serial e a conexão entre RJ2 e RJ3, via HDLC serial. O protocolo de roteamento adotado pela empresa é o EIGRP e o número de sistema autônomo é 65001.

Eis o que deve ser feito:

1. Elabore um plano de endereçamento IP que suporte todas as redes presentes no diagrama e, ao mesmo tempo, permita a sumarização das redes de RJ2 e RJ3 para RJ. Procure pensar em algo que permita a escalabilidade dessa rede no futuro - na medida do possível, claro;
2. Crie e aplique uma lista de acesso que proíba somente à rede local conectada ao router RJ3 o acesso à Internet;
3. Apresente as configurações de cada um dos routers, incluindo senhas de modo privilegiado e usuário (VTY) para todos eles (use *ccna[nome do router]* como senha *enable* para cada um deles e *vty[nome do router]* para senhas de acesso Telnet).

A tabela a seguir ilustra alguns dados relevantes:

IP da interface Serial0/0 do router RJ_NAT (saída para Internet)	200.204.103.65 /30 (512k)
IP do servidor DNS	Deve ser o último IP válido da sub-rede
Conexão serial SP x RJ	Frame-Relay ponto a ponto (1024k)
DLCI interface S0/0 Router SP	101
DLCI interface S0/0 Router RJ	102
Conexão serial RJ x MG	Serial PPP (2048k)
Conexão serial RJ2 x RJ3	HDLC PPP (2048k)
Usuários conectados a SP	20
Usuários conectados a RJ	20
Usuários conectados a MG	20
Usuários conectados a RJ2	5
Usuários conectados a RJ3	5
Protocolo de roteamento adotado	EIGRP
Sistema autônomo (para uso com EIGRP)	65001

Solução Sugerida (antes de olhar a solução, procure resolver o desafio sozinho!)

Vamos começar pelo plano de endereçamento IP. Temos a necessidade de endereçar cinco redes locais (SP, RJ, MG, RJ2 e RJ3) e três redes

seriais WAN (SP-RJ, RJ-MG, RJ2-RJ3). Portanto, temos de nos preocupar com oito redes, no total.

Fazendo o cálculo:

$2^x - 2 >= 8 \quad 2^4 - 2 = 14 \quad 14 >= 8$

Supostamente estaríamos usando uma máscara /28 (255.255.255.240), já que "x" é igual a 4 (4 bits de hosts sendo usados para criação de sub-redes). O problema aqui é que, se fizermos isso, estaremos criando 14 sub-redes (seis a mais do que necessitamos), e cada uma suportaria um máximo de 14 hosts (sobram quatro "0s" na máscara /28, logo, portanto, $2^4 - 2 = 14$ hosts). Isso não atende aos pré-requisitos impostos. As redes de SP, RJ e MG possuem 20 hosts cada. Essa máscara não abrangeria todos eles. Em contrapartida, temos cinco redes que possuem um número bastante reduzido de hosts. As sub-redes seriais, por exemplo, precisam de apenas dois hosts cada. Vamos, então, usar a técnica de VLSM para repensar esse plano de endereçamento.

Vamos focar nas redes mais "populosas" (LANs de SP, RJ e MG). Se em vez de usarmos um "x" igual a 4, como fizemos antes, usarmos um "x" igual a 3, o que teríamos?

$2^3 - 2 = 6$

Teríamos, portanto, uma máscara /27 nos entregando seis sub-redes válidas, cada uma comportando até 30 hosts! Como temos apenas três redes que efetivamente possuem um número maior de hosts, podemos reservar três dessas seis sub-redes para endereçar as LANs de SP, RJ e MG. Com as três sub-redes restantes, vamos pegar uma e subdividi-la ainda mais, para que comporte todos os links seriais. Finalmente, pegamos uma das duas sub-redes que sobraram e a subdivimos para acomodar as LANs de RJ2 e RJ3. Fazendo isso, teríamos ainda um saldo de uma sub-rede, capaz de endereçar até 30 hosts - que pode ser usado para necessidades futuras.

As seis sub-redes que obtemos com nossa máscara (/27) são:

192.168.200.32	192.168.200.64	192.168.200.96
192.168.200.128	192.168.200.160	192.168.200.192

Usaremos a rede "128" para a criação de sub-redes para as conexões seriais e a sub-rede "160" para a criação de duas sub-redes para endereçamento das LANs de RJ2 e RJ3.

Nosso plano de endereçamento ficaria assim:

Site	Rede LAN	Máscara	Rede WAN		Máscara
SP	192.168.200.32	/27	SP-RJ	192.168.200.128	/30
RJ			RJ-SP	192.168.200.128	/30
RJ	192.168.200.64	/27	RJ-MG	192.168.200.132	/30
MG	192.168.200.96	/27	MG-RJ	192.168.200.132	/30
RJ2	192.168.200.160	/28	RJ2-RJ3	192.168.200.136	/30
RJ3	192.168.200.176	/28	RJ3-RJ2	192.168.200.136	/30

Nota: A conexão entre os routers RJ3 e RJ_NAT é realizada via LAN, ou seja, o endereço de rede para essa conexão também será 192.168.200.176.

O esquema a seguir foi montado para ajudá-lo a entender o que foi feito.

Criação das sub-redes /30 (para uso nas conexões seriais)

Sub-rede Original	192.168.200.128	11100000	/27
Sub-rede VLSM	192.168.200.128	11111100	/30
Novas sub-redes	192.168.200.132	11111100	/30
	192.168.200.136	11111100	/30
	192.168.200.140	11111100	/30
	192.168.200.144	11111100	/30
	192.168.200.148	11111100	/30
	192.168.200.152	11111100	/30
	192.168.200.156	11111100	/30

Criação das sub-redes /28 (para uso nas LANs de RJ2 e RJ3)

Sub-rede Original	192.168.200.160	11100000	/27
Sub-rede VLSM	192.168.200.160	11110000	/28
Novas sub-redes	192.168.200.176	11110000	/28

Uma vez que temos em mãos nosso plano de endereçamento e as informações necessárias, podemos partir para a montagem das configurações dos routers. Vamos fazê-lo por partes.

Antes de mais nada, vamos configurar as interfaces de cada router e ativar o roteamento EIGRP neles.

Router SP:

```
Router>en
Router#config t
Router(config)#hostname SP
SP(config)#enable secret ccnaSP
SP(config)#line vty 0 4
SP(config-line)#passw telnetSP
SP(config-line)#exit
SP(config)#int f0/0
```

```
SP(config-if)#ip add 192.168.200.33 255.255.255.224
SP(config-if)#no shut
SP(config-if)#int s0/0
SP(config-if)#description Conexao Frame 512k para RJ
SP(config-if)#band 512
SP(config-if)#ip add 192.168.200.129 255.255.255.252
SP(config-if)#encap frame-relay
SP(config-if)#frame-relay interface-dlci 101
SP(config-if)#no shut
SP(config-if)#ip classless
SP(config)#ip subnet-zero
SP(config)#ip route 0.0.0.0 0.0.0.0 s0/0
SP(config-if)#router eigrp 65001
SP(config-router)#no auto-summary
SP(config-router)#network 192.168.200.32 255.255.255.224
SP(config-router)#network 192.168.200.128 255.255.255.252
SP(config-router)#^Z
SP#
```

Router RJ:

```
Router>en
Router#config t
Router(config)#hostname RJ
RJ(config)#enable secret ccnaRJ
RJ(config)#line vty 0 4
RJ(config-line)#passw telnetRJ
RJ(config-line)#exit
RJ(config)#int f0/0
RJ(config-if)#ip add 192.168.200.65 255.255.255.224
RJ(config-if)#no shut
RJ(config-if)#int s0/0
RJ(config-if)#description Conexao Frame 512k para SP
RJ(config-if)#band 512
RJ(config-if)#ip add 192.168.200.130 255.255.255.252
RJ(config-if)#encap frame-relay
RJ(config-if)#frame-relay interface-dlci 102
RJ(config-if)#no shut
RJ(config-if)#int s0/1
RJ(config-if)#description Conexao PPP com MG
RJ(config-if)#band 2048
RJ(config-if)#ip add 192.168.200.133 255.255.255.252
RJ(config-if)#encap ppp
RJ(config-if)#no shut
```

```
RJ(config-if)#ip classless
RJ(config)#ip subnet-zero
RJ(config)#ip route 0.0.0.0 0.0.0.0 f0/0
RJ(config)#router eigrp 65001
RJ(config-router)#no auto-summary
RJ(config-router)#network 192.168.200.64 255.255.255.224
RJ(config-router)#network 192.168.200.132 255.255.255.252
RJ(config-router)#network 192.168.200.128 255.255.255.252
RJ(config-router)#^Z
RJ#
```

Router MG:

```
Router>en
Router#config t
Router(config)#hostname MG
MG(config)#enable secret ccnaMG
MG(config)#line vty 0 4
MG(config-line)#passw telnetMG
MG(config-line)#exit
MG(config)#int f0/0
MG(config-if)#ip add 192.168.200.97 255.255.255.224
MG(config-if)#no shut
MG(config-if)#int s0/0
MG(config-if)#description Conexao PPP com RJ
MG(config-if)#band 2048
MG(config-if)#ip add 192.168.200.134 255.255.255.252
MG(config-if)#encap ppp
MG(config-if)#no shut
MG(config-if)#ip classless
MG(config)#ip subnet-zero
MG(config)#ip route 0.0.0.0 0.0.0.0 s0/0
MG(config)#router eigrp 65001
MG(config-router)#no auto-summary
MG(config-router)#network 192.168.200.96 255.255.255.224
MG(config-router)#network 192.168.200.132 255.255.255.252
MG(config-router)#^Z
MG#
```

Router RJ2:

```
Router>en
Router#config t
Router(config)#hostname RJ2
RJ2(config)#enable secret ccnaRJ2
```

```
RJ2(config)#line vty 0 4
RJ2(config-line)#passw telnetRJ2
RJ2(config-line)#exit
RJ2(config)#int f0/0
RJ2(config-if)#ip add 192.168.200.161 255.255.255.240
RJ2(config-if)#no shut
RJ2(config)#int f0/1
RJ2(config-if)#ip add 192.168.200.66 255.255.255.224
RJ2(config-if)#no shut
RJ2(config-if)#int s0/0
RJ2(config-if)#description Conexao HDLC com RJ3
RJ2(config-if)#band 2048
RJ2(config-if)#ip add 192.168.200.137 255.255.255.252
RJ2(config-if)#no shut
RJ2(config-if)#ip classless
RJ2(config)#ip subnet-zero
RJ2(config)#ip route 0.0.0.0 0.0.0.0 s0/0
RJ2(config)#router eigrp 65001
RJ2(config-router)#no auto-summary
RJ2(config-router)#network 192.168.200.160 255.255.255.240
RJ2(config-router)#network 192.168.200.64 255.255.255.224
RJ2(config-router)#network 192.168.200.136 255.255.255.252
RJ2(config-router)#^Z
RJ2#
```

Router RJ3:

```
Router>en
Router#config t
Router(config)#hostname RJ3
RJ3(config)#enable secret ccnaRJ3
RJ3(config)#line vty 0 4
RJ3(config-line)#passw telnetRJ3
RJ3(config-line)#exit
RJ3(config)#int f0/0
RJ3(config-if)#ip add 192.168.200.177 255.255.255.240
RJ3(config-if)#no shut
RJ3(config-if)#int s0/0
RJ3(config-if)#description Conexao HDLC com RJ2
RJ3(config-if)#band 2048
RJ3(config-if)#ip add 192.168.200.138 255.255.255.252
RJ3(config-if)#no shut
RJ3(config-if)#ip classless
RJ3(config)#ip subnet-zero
```

```
RJ3(config)#ip route 0.0.0.0 0.0.0.0 f0/0
RJ3(config)#router eigrp 65001
RJ3(config-router)#no auto-summary
RJ3(config-router)#network 192.168.200.176 255.255.255.240
RJ3(config-router)#network 192.168.200.136 255.255.255.252
RJ3(config-router)#^Z
RJ3#
```

Router RJ_NAT:

```
Router>en
Router#config t
Router(config)#hostname RJ_NAT
RJ_NAT(config)#enable secret ccnaRJ4
RJ_NAT(config)#line vty 0 4
RJ_NAT(config-line)#passw telnetRJ4
RJ_NAT(config-line)#exit
RJ_NAT(config)#int f0/0
RJ_NAT(config-if)#ip add 192.168.200.178 255.255.255.240
RJ_NAT(config-if)#no shut
RJ_NAT(config-if)#int s0/0
RJ_NAT(config-if)#description Conexao para a Internet
RJ_NAT(config-if)#band 512
RJ_NAT(config-if)#ip add 200.204.103.65 255.255.255.252
RJ_NAT(config-if)#no shut
RJ_NAT(config-if)#ip classless
RJ_NAT(config)#ip subnet-zero
RJ_NAT(config)#ip route 192.168.200.0 255.255.255.0 f0/0
RJ_NAT(config)#ip route 0.0.0.0 0.0.0.0 s0/0
RJ_NAT(config)#^Z
RJ_NAT#
```

Nossos routers encontram-se agora com as configurações básicas e roteamento ativados. Nesse momento, todas as LANs podem ser alcançadas, pois as rotas para elas são descobertas por intermédio do protocolo EIGRP. Note que apenas divulgamos as sub-redes das LANs no protocolo, já que não é necessário divulgar as sub-redes de WAN (para os usuários, a comunicação é transparente e fim a fim). Note também que rotas default foram configuradas em todos os routers. Isso significa que, se um pacote com endereço destino que não pertença à tabela de roteamento chegar ao router, ele não será descartado, mas encaminhado à interface definida como default gateway.

Nota: *Para uso de rotas default, os comandos ip subnet-zero e ip classless devem estar configurados.*

O próximo passo é informar aos routers como proceder no que se refere ao tratamento de *broadcasts* em busca de um servidor DNS. Antes de mais nada, precisamos definir o endereço do servidor DNS. A regra foi clara: devemos usar o último IP válido da sub-rede onde ele se encontra (RJ), logo, 192.168.200.94. Usaremos o comando *ip helper-address* para informar aos routers sobre ele:

Router SP:

```
SP(config)#int f0/0
SP(config-if)#ip helper-address 192.168.200.94
```

Router RJ:

Nesse router, a configuração não é necessária, já que o servidor DNS encontra-se diretamente conectado via LAN.

Router MG:

```
MG(config)#int f0/0
MG(config-if)#ip helper-address 192.168.200.94
```

Router RJ2:

```
RJ2(config)#int f0/0
RJ2(config-if)#ip helper-address 192.168.200.94
```

Router RJ3:

```
RJ3(config)#int f0/0
RJ3(config-if)#ip helper-address 192.168.200.94
```

Router RJ_NAT:

A configuração não é necessária nesse router, pois sua função é meramente a conexão com a Internet.

***Nota**: O comando ip helper-address apenas precisa ser configurado nas interfaces LAN, já que os broadcasts serão originados nelas.*

Continuando, o próximo requerimento é que seja feita a sumarização das redes locais em RJ2 e RJ3. Isso basicamente significa dizer que a interface F0/1 do router RJ2 informará para o restante da rede que, atrás dela, encontram-se as duas redes locais (192.168.200.160 /28 e 192.168.200.176 /28), porém, fará isso divulgando apenas uma rota sumarizada. Do modo como as duas sub-redes foram criadas, fica fácil fazer essa sumarização. Basta analisar o padrão dos bits mais significativos (bits à esquerda) de cada uma delas, no 4º octeto:

```
160 = 10100000
176 = 10110000
```

Portanto, podemos ver que a sumarização é possível e que nossa rede sumarizada seria:

192.168.200.160 (primeira rede);

255.255.255.224 ou /27 (24 bits dos três primeiros octetos + três bits usados no último octeto, assim como o padrão de bits acima nos mostro

Agora, vamos à configuração da sumarização no router RJ2:

Router RJ2:

```
RJ2(config)#interface f0/1
RJ2(config-if)#ip summary-address eigrp 65001 192.168.200.160
255.255.255.224
RJ2(config-if)#^Z
RJ2#
```

Próximo requerimento em nossa lista: configuração de NAT no router RJ_NAT. A seguir, a configuração sugerida para atingir esse objetivo:

```
RJ_NAT(config)#int f0/0
RJ_NAT(config-if)#ip nat inside
RJ_NAT(config-if)#int S0/0
RJ_NAT(config-if)#ip nat outside
RJ_NAT(config-if)#exit
RJ_NAT(config)#access-list 11 permit 192.168.200.0 0.0.0.255
RJ_NAT(config)#ip nat pool internet 200.204.103.65
200.204.103.65 prefix 24
RJ_NAT(config)#ip nat inside source list 11 pool internet
overload
```

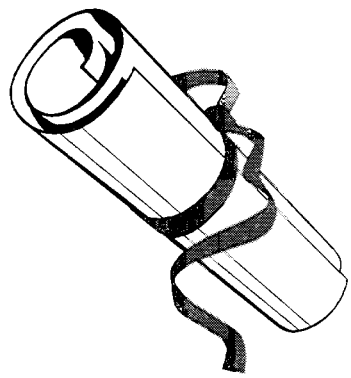
Finalmente, a última solicitação foi com relação à criação de uma lista de acesso que evitasse que qualquer máquina conectada à rede local de RJ3 pudesse acessar a Internet. Essa lista seria algo como:

```
access-list 10 deny 192.168.200.176 0.0.0.15
access-list 10 permit any
```

Observe que sequer foi necessária a criação de uma lista estendida. Uma lista padrão já dá conta do recado. Com relação à sua aplicação, devemos lembrar que listas de acesso padrão **sempre** devem ser aplicadas o mais próximo possível do destino. No nosso caso, o destino é a Internet e o local em nossa rede mais próximo dele é a interface serial0/0 do router RJ_NAT. Portanto:

```
RJ_NAT(config)#access-list 10 deny 192.168.200.176 0.0.0.15
RJ_NAT(config)#access-list 10 permit any
RJ_NAT(config)#interface s0/0
RJ_NAT(config-if)#ip access-group 10 out
```

Com isso, concluímos este estudo de caso. Observe que os dois estudos apresentados cobrem muitos dos conceitos que vimos no decorrer do livro. Procure compreender o que foi feito em ambos.

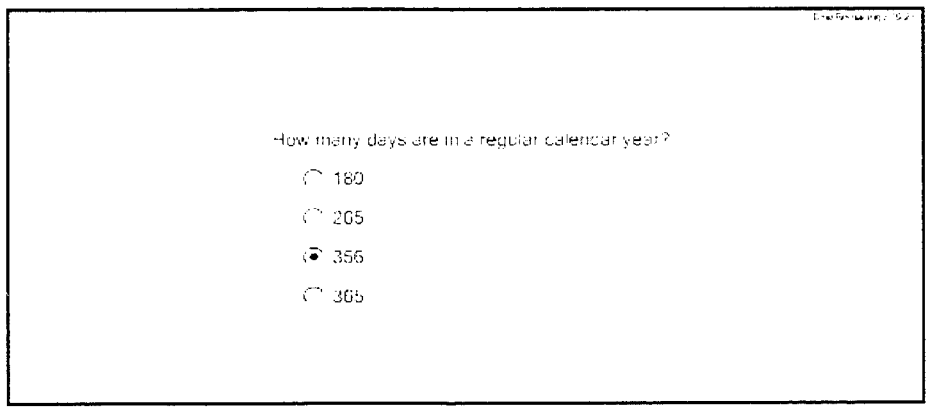


Apêndice D

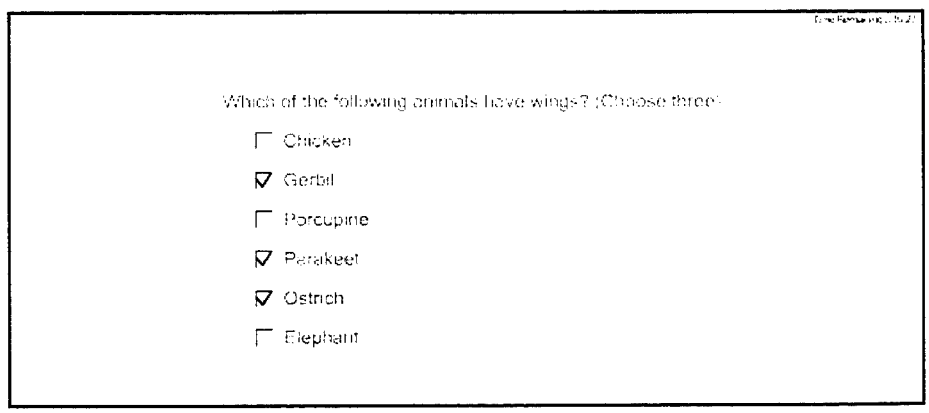
A Interface do Exame 640-802

Neste apêndice ilustrarei alguns exemplos de interfaces com o usuário que podem ser esperadas na nova versão do exame CCNA.

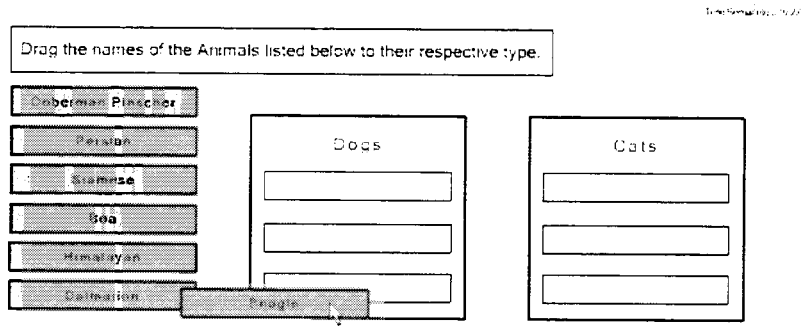
Exemplo 1: Questões de múltipla escolha (com apenas uma alternativa correta):



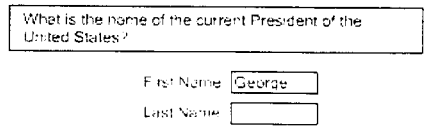
Exemplo 2: Questões de múltipla escolha (com mais de uma alternativa correta):



Exemplo 3: Questões do tipo "arraste e solte" (muito comuns quando o tópico é o modelo de camadas OSI!):



Exemplo 4: Questões do tipo "preencha o espaço em branco" (comuns quando o tópico é o sistema IOS e seus comandos):

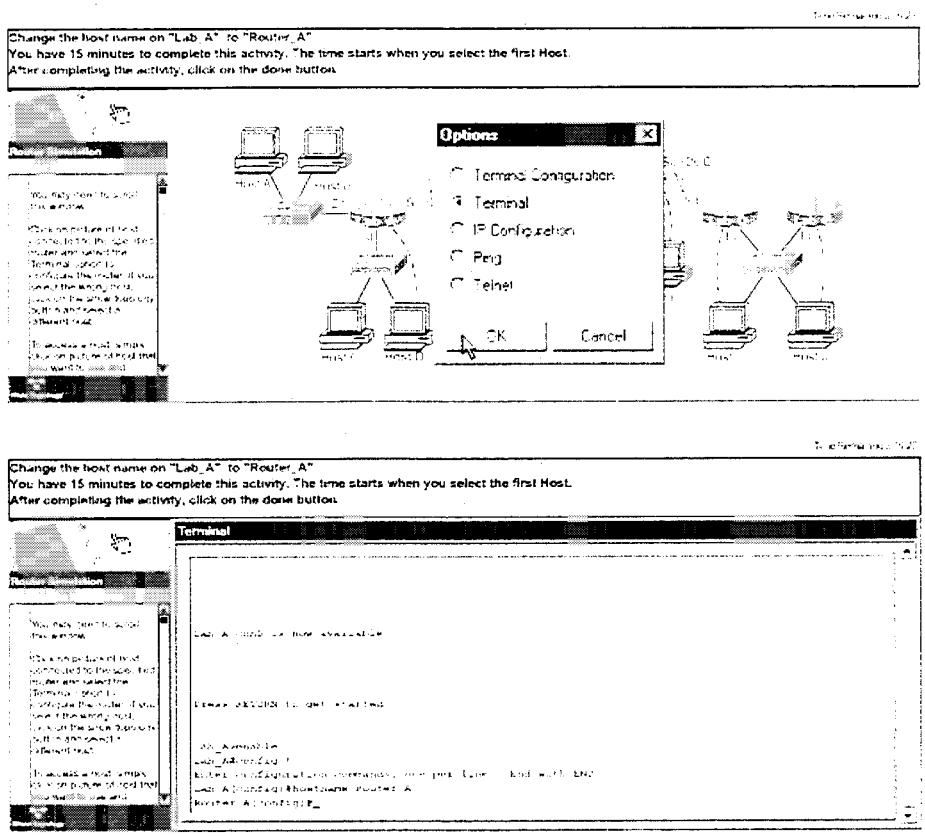


Apesar de presentes no novo formato do exame, esses quatro exemplos já faziam parte do exame em seu formato antigo (640-801). Note que **sempre** que uma questão apresentar mais de uma alternativa correta (exemplo 2), o método de escolha se dá através de *check boxes*, enquanto no exemplo 1, onde apenas uma alternativa é verdadeira, o método de seleção é o *radio-button*.

Exemplo 5: Questões que fazem uso do simulador IOS:

Seguindo o que já vinha sendo cobrado no exame anterior (801), os simuladores estão também presentes no exame 802. Esse tipo de questão apresenta uma interface que simula uma sessão (console ou Telnet) com um roteador ou switch Cisco (bem nos moldes dos programas simuladores, como o NetSim), exigindo um conhecimento mais apurado no que se refere à configuração de um dispositivo de rede. Note no exemplo a seguir que uma pequena rede é apresentada ao examinado. Do seu lado esquerdo, encontram-se as perguntas ou solicitações (ex.: configure o protocolo OSPF na rede apresentada). A partir desse ponto, o examinado deve clicar no dispositivo desejado. Ao selecionar um dispositivo, uma janela pop-up será apresentada e você deverá fazer a escolha entre os diversos modos de operação disponíveis:

- **Terminal Configuration**: Permite que o examinado configure o programa emulador console (essa opção deve ser utilizada somente se necessário. Lembre-se das configurações default: 9600/8 Data Bits/*Parity None*/Stop Bits 1/ *Flow Control none*);
- **Telnet**: Permite que se inicie uma sessão Telnet partindo do host selecionado;
- **Ping**: Transmite um pacote ICMP Ping para o endereço especificado (use para testar conectividade);
- **IP Configuration**: Permite que um endereço IP e uma máscara sejam designados ao host em questão;
- **Terminal**: Permite que uma sessão console seja iniciada com um dispositivo diretamente conectado à porta serial do host (note a presença de linhas tracejadas no diagrama. Elas indicam quais dispositivos encontram-se diretamente conectados via porta console a quais hosts).



A figura anterior ilustra a tela apresentada após selecionarmos o host na tela anterior e optarmos por *Terminal*. Note na imagem, à esquerda, a presença da ação solicitada. No exemplo, o examinado deve digitar os comandos que permitam a troca do nome do router em questão de *Lab_A* para *Router_A*. As questões que envolvem o simulador no exame real são relativamente simples.

***Atenção**: Entre as questões práticas, três das mais comuns são: ativar o protocolo de roteamento (ex.: RIP ou OSPF) em uma rede apresentada, configuração de senhas (usuário, privilegiado e telnet) e configuração básica de um switch 2950 (saiba configurar modos VTP e endereço IP de gerenciamento nele). Configuração de listas de acesso e NAT também podem ser cobradas em questões práticas. Em alguns casos, a rede já se encontra pré-configurada, porém, com problemas de comunicação. O candidato deve identificar os problemas e corrigi-los.*

***Lembre-se: Sempre salve sua configuração** através do comando copy running-config start-config! Esquecer esse detalhe pode lhe custar pontos ou mesmo invalidar **completamente** as questões de simulação.*

Dicas:

- Não espere por mais de três questões com simuladores em todo o exame;
- Uma das questões desse tipo pode lhe apresentar uma rede como a sugerida há pouco e lhe pedir que configure um determinado host para que ele seja capaz de pingar um determinado dispositivo (ou outro host). Outra questão típica: habilitar um protocolo de roteamento na rede apresentada (provavelmente EIGRP ou OSPF) que permita que todos os hosts ilustrados tenham conectividade;
- Outra questão corriqueira que utiliza o simulador é a configuração de senhas de modo usuário e modo privilegiado, assim como senhas Telnet. Saiba como realizar essas tarefas!
- Um terceiro exemplo pode ser a configuração de uma lista de acesso, simples, porém normalmente envolvendo as linhas VTY (Telnet);
- Pode ser apresentada uma rede pré-configurada no simulador e o enunciado dizer que algo não está funcionando a contento. Você poderá ter que fazer um *troubleshooting* da rede para identificar o problema. Normalmente, o problema é óbvio e rápido de ser corrigido;
- Não desperdice seu tempo fazendo algo que não lhe foi explicitamente pedido (exemplo: não configure o host *C* se a questão pede que você mude o nome do roteador *E*).

Marco Aurélio Filippetti

CCNA 4.1 Guia Completo de Estudo

Visual Books

Recentemente, o CCNA deixou de ser a base da pirâmide de certificações da Cisco, posição agora ocupada pela certificação CCENT.

Com isso, o exame de certificação Cisco CCNA teve novos tópicos incorporados e seu nível de dificuldade aumentado, tornando-se mais complexo, e ainda mais difícil de ser obtido. Tais mudanças são extremamente positivas, pois o mercado tende a valorizar cada vez mais profissionais que possuam o título CCNA.

Profissionais que satisfazem os requisitos mínimos exigidos pela Cisco e obtêm a certificação CCNA têm a certeza de que serão valorizados, pois esse certificado é muito requisitado pelo mercado atual. Um CCNA, na teoria, é capaz de implementar, configurar, gerenciar e prestar suporte a redes de pequeno e médio porte (LANs, MANs ou WANs).

O livro CCNA 4.1 – Guia Completo de Estudo é a ferramenta ideal para preparar o candidato rumo ao exame Cisco 640-802, abrangendo 100% dos tópicos abordados por ele e complementando a parte teórica com cenários que podem ser facilmente implementados em laboratório ou no simulador Dynamips.

Esta edição contém dois cenários avançados, que reproduzem alguns problemas do mundo real encarados por um administrador de redes, acompanhados de sua devida resolução.

Esta obra é totalmente focada para o exame Cisco CCNA 640-802 e vai ajudar o leitor a superar todos os obstáculos para obter essa tão respeitada certificação.

Um simulado do exame está disponível para download no site da editora.

Visual Books
www.visualbooks.com.br

ISBN: 978-857502-238-2
9 788575 022382