

SÉRIE TECNOLOGIA DA INFORMAÇÃO - *HARDWARE*

ARQUITETURA DE REDES





*Iniciativa da CNI - Confederação
Nacional da Indústria*

SÉRIE TECNOLOGIA DA INFORMAÇÃO - HARDWARE

ARQUITETURA DE REDES



CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI

Robson Braga de Andrade
Presidente

DIRETORIA DE EDUCAÇÃO E TECNOLOGIA

Rafael Esmeraldo Lucchesi Ramacciotti
Diretor de Educação e Tecnologia

SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI

Conselho Nacional

Robson Braga de Andrade
Presidente

SENAI – Departamento Nacional

Rafael Esmeraldo Lucchesi Ramacciotti
Diretor-Geral

Gustavo Leal Sales Filho
Diretor de Operações



*Iniciativa da CNI - Confederação
Nacional da Indústria*

SÉRIE TECNOLOGIA DA INFORMAÇÃO - HARDWARE

ARQUITETURA DE REDES



© 2012. SENAI – Departamento Nacional

© 2012. SENAI – Departamento Regional de Santa Catarina

A reprodução total ou parcial desta publicação por quaisquer meios, seja eletrônico, mecânico, fotocópia, de gravação ou outros, somente será permitida com prévia autorização, por escrito, do SENAI.

Esta publicação foi elaborada pela equipe do Núcleo de Educação a Distância do SENAI de Santa Catarina, com a coordenação do SENAI Departamento Nacional, para ser utilizada por todos os Departamentos Regionais do SENAI nos cursos presenciais e a distância.

SENAI Departamento Nacional

Unidade de Educação Profissional e Tecnológica – UNIEP

SENAI Departamento Regional de Santa Catarina

Núcleo de Educação – NED

FICHA CATALOGRÁFICA

S491a

Serviço Nacional de Aprendizagem Industrial. Departamento Nacional.
Arquitetura de redes / Serviço Nacional de Aprendizagem
Industrial. Departamento Nacional, Serviço Nacional de Aprendizagem
Industrial. Departamento Regional de Santa Catarina. Brasília :
SENAI/DN, 2012.

186 p. il. (Série Tecnologia da informação - Hardware).

ISBN

1. Rede de computadores. 2. Arquitetura de computadores. 3.
OSI (Padrão de redes de computação). 4. TCP/IP (Protocolo de rede
de computação). I. Serviço Nacional de Aprendizagem Industrial.
Departamento Regional de Santa Catarina. II. Título. III. Série.

CDU: 004.7

SENAI

Serviço Nacional de
Aprendizagem Industrial
Departamento Nacional

Sede

Setor Bancário Norte • Quadra 1 • Bloco C • Edifício Roberto
Simonsen • 70040-903 • Brasília – DF • Tel.: (0xx61) 3317-
9001 Fax: (0xx61) 3317-9190 • <http://www.senai.br>

Lista de ilustrações

Figura 1 - Rede BBS.....	18
Figura 2 - Dispositivos finais e intermediários.....	20
Figura 3 - Meios físicos de rede.....	21
Figura 4 - Mensagem <i>Unicast</i>	22
Figura 5 - Mensagem <i>Multicast</i>	23
Figura 6 - Mensagem <i>Broadcast</i>	23
Figura 7 - Rede Local.....	24
Figura 8 - Rede de longa distância.....	25
Figura 9 - Rede cliente/servidor.....	26
Figura 10 - Rede ponto a ponto.....	27
Figura 11 - Modelo de Refêrencia OSI	29
Figura 12 - Modelo de Referência TCP/IP	30
Figura 13 - Processo de Encapsulamento dos Dados	32
Figura 14 - A Camada de Aplicação do modelo OSI.....	36
Figura 15 - Acessando um Servidor WEB.....	37
Figura 16 - Uso dos protocolos SMTP, POP e IMAP	39
Figura 17 - Configuração de conta de e-mail.....	40
Figura 18 - Exemplo de configuração DNS em um dispositivo final	41
Figura 19 - Troca de mensagens DHCP	41
Figura 20 - Estrutura de uma rede SNMP	42
Figura 21 - Camada de apresentação	44
Figura 22 - A Camada de Sessão.....	45
Figura 23 - A Camada de Transporte.....	48
Figura 24 - Sincronização do handshake triplo.....	50
Figura 25 - Finalização da conexão.....	50
Figura 26 - Ordenando os segmentos	51
Figura 27 - Confirmação positiva	52
Figura 28 - Controle de fluxo	53
Figura 29 - Número de Portas.....	53
Figura 30 - A Camada de Rede	62
Figura 31 - Componentes básicos do datagrama	64
Figura 32 - Campos do pacote IP.....	65
Figura 33 - Estrutura hierárquica	67
Figura 34 - Endereço IPv4.....	68
Figura 35 - Pacote IPv6.....	73
Figura 36 - Fluxo de solicitações ARP.....	80
Figura 37 - Domínios de broadcast separados por roteador	81
Figura 38 - Visão da camada de enlace no modelo de referênciia OSI	86
Figura 39 - Navegação na Internet	88
Figura 40 - <i>Layout</i> de quadro.....	88

Figura 41 - Layout detalhado do quadro.....	89
Figura 42 - Rede ponto-a-ponto.....	92
Figura 43 - Rede multiacesso	92
Figura 44 - Rede em anel.....	93
Figura 45 - Primeiro diagrama de rede.....	94
Figura 46 - Domínio de colisão em barramento	97
Figura 47 - Domínio de colisão com hub e switch.....	97
Figura 48 - Visão da camada física no modelo de referência OSI	102
Figura 49 - Meios físicos de cobre	105
Figura 50 - Meios físicos de fibra	107
Figura 51 - Topologias Físicas de Rede	109
Figura 52 - Pilha TCP/IP com suas quatro camadas	114
Figura 53 - Relação entre os modelos de referência OSI e TCP/IP	117
Figura 54 - Cada classe com sua máscara padrão em binário, decimal e prefixo de rede.....	122
Figura 55 - Porções do endereço IP para classfull e com a divisão em sub-redes	124
Figura 56 - Identificação da porção de rede e host e dos bits mais significativos.....	125
Figura 57 - Bits emprestados para criar a sub-rede e a nova máscara de sub-rede.....	125
Figura 58 - Primeira sub-rede	125
Figura 59 - Bits da porção de rede e as demais redes para a divisão realizada	126
Figura 60 - Alocação de bits para os dois casos: escolha pelo número de redes ou pelo número de hosts.....	128
Figura 61 - Bits disponíveis para empréstimo em cada classe.....	129
Figura 62 - Bits emprestados para obter quatrocentas sub-redes.....	130
Figura 63 - Endereço de broadcast da primeira rede	130
Figura 64 - Máscara padrão e máscara de sub-rede	130
Figura 65 - Endereço de rede e broadcast da segunda rede	131
Figura 66 - Porções de um endereço IPv4 depois de dividido	132
Figura 67 - Endereço de broadcast da primeira rede	133
Figura 68 - Bits emprestados para obter dez sub-redes	134
Figura 69 - Endereço de broadcast da primeira rede	135
Figura 70 - Endereço de rede e broadcast da segunda rede	135
Figura 71 - Porções do endereço IPv4 antes e depois da divisão em sub-redes.....	137
Figura 72 - Endereço de broadcast da primeira rede	137
Figura 73 - Bits emprestados para obter dez sub-redes	138
Figura 74 - Endereço de broadcast da primeira rede	139
Figura 75 - Endereço de rede e broadcast da segunda rede	139
Figura 76 - Porções de um endereço IPv4 depois de dividido	141
Figura 77 - Endereço de rede da segunda sub-rede	141
Figura 78 - Repetidor interligando dois segmentos de rede	148
Figura 79 - Utilização de HUBs respeitando a regra 5-4-3-2-1	150
Figura 80 - Domínios de Colisão e Broadcast.....	151
Figura 81 - Ponto de Acesso sem fio conectado a uma rede cabeada	154
Figura 82 - Placa de rede no modo normal e em modo promíscuo	162
Figura 83 - Análise de protocolos utilizando hubs e switches.....	163

Figura 84 - Tela Inicial do Wireshark	165
Figura 85 - Seleção de interface de captura no Wireshark.....	165
Figura 86 - Interfaces disponíveis na estação de análise de protocolos	166
Figura 87 - Captura de tráfego com o Wireshark.....	166
Figura 88 - Informações do Frame	167
Figura 89 - Informações do quadro Ethernet.....	167
Figura 90 - Detalhes do protocolo IP	168
Figura 91 - Detalhes do segmento TCP	168
Figura 92 - Informações do protocolo utilizado na camada de aplicação	168
Figura 93 - Uso de filtros no Wireshark.....	169
Figura 94 - Opções de filtragem de protocolos.....	169
Figura 95 - Resumo da captura de tráfego	170
Figura 96 - Acesso a funcionalidade de seguir um fluxo TCP.....	170
Figura 97 - Acompanhamento de um fluxo TCP	171
Figura 98 - Toda a troca de informações do fluxo selecionado.....	171
Figura 99 - Tela inicial do analisador de protocolos da Microsoft	172
Figura 100 - Aba de captura do Microsoft Network Monitor	172
Figura 101 - Captura de tráfego.....	173
Figura 102 - Tela inicial do netStumbler	174
Figura 103 - NetStumbler listando as redes sem fio detectadas	174
Figura 104 - Gráfico de ruído e sinal gerado pelo NetStumbler	175
 Quadro 1 - Matriz curricular.....	14
Quadro 2 - Vantagens e desvantagens das redes cliente/servidor e ponto a ponto.....	28
Quadro 3 - Observando uma URL	37
Quadro 4 - Os campos do segmento TCP	55
Quadro 5 - Exemplo de um segmento UDP	56
Quadro 6 - Tipos e Códigos das mensagens ICMP	78
Quadro 7 - Organizações e protocolos	90
 Tabela 1 - Principais aplicações	54
Tabela 2 - Classes de endereçamento IP	69
Tabela 3 - Detalhes das classes de endereçamento IP	71
Tabela 4 - Endereços Privados	72
Tabela 5 - Padrões Ethernet	96
Tabela 6 - Métodos e vantagens	104
Tabela 7 - Número de redes e <i>hosts</i> por rede em cada classe	123
Tabela 8 - Endereços de sub-rede para a divisão do exemplo 1	132
Tabela 9 - Endereço de sub-rede para a divisão do exemplo 2	134
Tabela 10 - Endereços de sub-rede para a divisão do exemplo 3.....	136
Tabela 11 - Endereço de sub-rede para a divisão do exemplo 4.....	138
Tabela 12 - Endereços de sub-rede para a divisão do exemplo 5.....	140
Tabela 13 - Divisão de sub-redes para o exemplo 6	142

Sumário

1 Introdução	13
2 Fundamentos de Redes de Computadores.....	17
2.1 Evolução e aplicabilidade.....	18
2.2 Elementos de uma rede	19
2.3 Tipos de comunicação (<i>Unicast, Multicast e Broadcast</i>)	21
2.4 Classificação de redes	24
2.4.1 LAN.....	24
2.4.2 WAN	25
2.4.3 Redes cliente/servidor	26
2.4.4 Rede Ponto a Ponto.....	26
2.5 Arquitetura de camadas	29
2.5.1 Modelo de Referência OSI.....	29
2.5.2 Modelo de Referência TCP/IP.....	30
2.6 O processo de encapsulamento dos dados.....	31
3 Modelo OSI – As Camadas Superiores	35
3.1 Camada de aplicação.....	36
3.1.1 HTTP e HTTPS.....	37
3.1.2 FTP e TFTP	38
3.1.3 SMTP, POP e IMAP	39
3.1.4 DNS	40
3.1.5 DHCP	41
3.1.6 SNMP	42
3.2 Camada de apresentação.....	43
3.3 Camada de sessão.....	44
4 A Camada de Transporte.....	47
4.1 Conceitos da camada de transporte	48
4.1.1 Serviço orientado à conexão	49
4.1.2 Entrega ordenada	51
4.1.3 Entrega confiável	51
4.1.4 Controle de fluxo.....	52
4.1.5 Identificar diferentes aplicações.....	53
4.2 Protocolos orientados à conexão	55
4.3 Protocolos não-orientados à conexão.....	56
4.4 Comparando o TCP e o UDP	57
5 A Camada de Rede	61
5.1 Conceitos da camada de rede	62
5.2 IPv4.....	63
5.2.1 Pacote IP	64
5.2.2 Endereçamento IPv4.....	66

5.3 Classes de Endereços IP	69
5.4 Endereços públicos e endereços privados.....	72
5.5 IPv6	73
5.5.1 O Pacote IPv6.....	73
5.5.1 Endereçamento IPv6.....	74
5.6 <i>Internet Control Message Protocol</i> (ICMP).....	77
5.7 <i>Address Resolution Protocol</i> (ARP)	79
5.8 Domínios de <i>broadcast</i>	81
 6 A Camada Enlace	85
6.1 Conceitos da camada de enlace	86
6.1.1 Tecnologias de Rede Local.....	90
6.1.2 Acesso ao meio	91
6.2 Ethernet (IEEE 802.3) e suas variantes.....	94
6.3 Domínios de colisões	96
 7 A Camada Física.....	101
7.1 Conceitos da camada física.....	102
7.1.1 Métodos de sinalização	104
7.1.2 Métodos de codificação	104
7.2 Meios físicos de transmissão	105
7.2.1 Cabo de cobre	105
7.2.2 Fibra	106
7.2.3 Sem fio	108
7.3 Topologias.....	109
 8 O Modelo TCP/IP	113
8.1 A Pilha de protocolos TCP/IP	114
8.1.1 Camada de Aplicação.....	115
8.1.2 Camada de Transporte.....	115
8.1.3 Camada de Internet	116
8.1.4 Camada de Acesso à Rede	116
8.2 Comparando o Modelo TCP/IP e OSI.....	116
 9 Sub-redes.....	121
9.1 O que são sub-redes.....	122
9.2 Realizando o cálculo de sub-redes	126
 10 Ativos de Rede.....	145
10.1 Tipos de ativos de rede	146
10.2 Funcionamento e características	148
10.2.1 Repetidor.....	148
10.2.2 Hub	149
10.2.3 Pontes	150
10.2.4 Switches	151

10.2.5 Pontos de acesso a rede sem fio	153
10.2.6 Roteadores.....	154
11 Analisadores de Protocolos	159
11.1 O que é um analisador de protocolo?	160
11.2 Tipos de analisadores de protocolos	164
11.2.1 Wireshark.....	165
11.2.2 Microsoft Network Monitor	172
11.2.3 Netstumbler	173
Referências.....	179
Minicurrículo dos Autores.....	181
Índice	183

Introdução

1



Seja bem vindo à unidade curricular Arquitetura de Redes do primeiro módulo específico do Curso Técnico em Redes de Computadores!

Nesta unidade curricular vamos estudar os principais conceitos de arquitetura de redes, padrões e tecnologias, bem como, observar a documentação da rede para aplicar estes conceitos em projetos de redes.

Lembre-se: é importante estar sempre preparado tanto nas competências técnicas quanto nas relacionais para poder atuar pró-ativamente e ser um bom profissional.

A seguir, confira na matriz curricular os módulos e unidades curriculares previstos, com as respectivas cargas horárias.

Técnico em Redes de Computadores

MÓDULOS	DENOMINAÇÃO	UNIDADES CURRICULARES	CARGA HORÁRIA	CARGA HORÁRIA DO MÓDULO
Básico	Básico	<ul style="list-style-type: none"> • Eletroeletrônica Aplicada • Montagem e Manutenção de Computadores • Ferramentas para Documentação Técnica 	60h 160h 120h	340h
Específico I	Ativos de Rede	<ul style="list-style-type: none"> • Cabeamento Estruturado • Arquitetura de Redes • Comutação de Rede Local • Interconexão de Redes PR • Gerenciamento e Monitamento de Rede 	108h 80h 120h 96h 60h	464h
Específico II	Servidores de Rede	<ul style="list-style-type: none"> • Servidores de Rede • Serviços de Rede • Serviços de Convergência • Segurança de Redes 	120h 120h 60h 96h	396h

Quadro 1 - Matriz curricular
Fonte: SENAI DN

Agora você é convidado a trilhar os caminhos do conhecimento. Faça deste processo um momento de construção de novos saberes, onde teoria e prática devem estar alinhadas para o seu desenvolvimento profissional. Bons estudos!

Anotações:

Fundamentos de Redes de Computadores

2



Para iniciar os estudos dos fundamentos de redes de computadores, vamos começar pela evolução e aplicabilidade das redes desde a década de 1940 até os dias atuais. Depois, estudaremos os elementos que compõem uma rede e como elas são classificadas. Por último, vamos entender como uma rede estruturada em camadas ajuda no aprendizado e na padronização das tecnologias e como as informações podem ser transmitidas entre uma origem e um destino.

Ao final deste capítulo você terá subsídios para:

- a) compreender os fundamentos de redes de computadores no processo de comunicação entre dispositivos de redes.

A partir de agora você entrará no campo das redes de computadores e todos os assuntos aqui abordados serão de fundamental importância para as suas práticas. Por isso, dedique-se ao estudo, pois motivação e comprometimento são fundamentais para um bom aprendizado.

2.1 EVOLUÇÃO E APLICABILIDADE

A história das redes de computadores não é muito simples, e contou com o envolvimento de pessoas de diversas partes do mundo nos últimos 40 anos. Os processos de invenção e comercialização são um tanto complexos, mas, para começar a entender sobre o assunto, acompanhe uma visão simplificada da evolução da Internet.

Tudo começou na década de 1940, quando os computadores eram enormes dispositivos e as falhas eram comuns. Com a invenção do transistor, ficou disponível a fabricação de computadores menores e mais confiáveis. No final dos anos 50, com a invenção do circuito integrado, começava uma nova era na fabricação de computadores. Já nos anos 60, o uso de mainframes com terminais era muito comum, assim como os circuitos integrados eram utilizados em grande escala.

Os computadores menores, chamados de minicomputadores, começaram a surgir no final das décadas de 1960 e 1970, mesmo assim, eles ainda eram muito grandes se comparados aos computadores modernos. Foi então que, no final da década de 1970, a Apple apresentou o primeiro microcomputador, e, no começo da década de 1980, a IBM apresentou o seu primeiro computador pessoal.

Foi somente na metade da década de 1980 que os computadores standalone começaram a trocar dados em redes ponto a ponto por meio de modems com acesso discado utilizando linhas telefônicas. Estas redes eram chamadas de BBS (*Bulletin Boards Systems*).

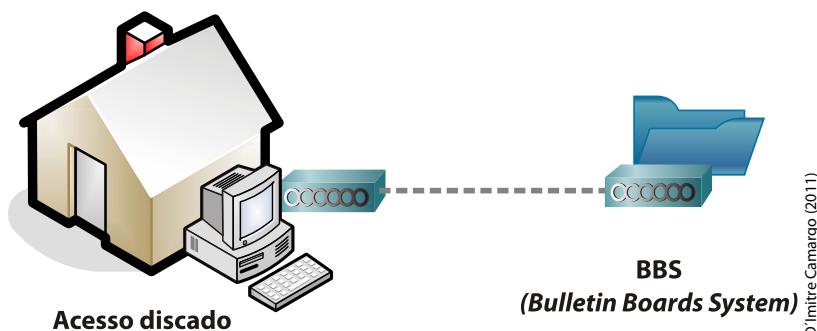


Figura 1 - Rede BBS

Paralelo a esta evolução, o Departamento de Defesa dos EUA (DoD) trabalhava em uma rede com diversas comunicações de longa distância para fins militares e científicos, e que mais tarde veio a se tornar a Internet que conhecemos hoje.

Ainda nos anos 80, as empresas observaram os ganhos em produtividade e em economia de recursos com o compartilhamento dos mesmos. Assim, novas redes eram criadas e expandidas numa velocidade impressionante, juntamente com novos produtos e tecnologias de redes. Com este rápido crescimento, as re-

des criadas não eram padronizadas e não tinham uma compatibilidade entre os diversos desenvolvedores e fabricantes, com isso, as tecnologias eram incompatíveis umas com as outras.

Foi então que, ainda no início da década de 1980, a ISO (*International Organization of Standardization*) cria o modelo de referência OSI (*Open Systems Interconnection*) para padronizar esta rede e tornar possível a comunicação entre diversos fabricantes, e, em 1984, é fundada a Cisco System, que hoje é um dos maiores fabricantes de roteadores do mundo.

Você conferiu como foi a evolução e como é a aplicabilidade das redes de computadores. A seguir, você estudará os elementos de uma rede de computadores. Continue atento!

2.2 ELEMENTOS DE UMA REDE

Você já sabe como as redes de computadores foram criadas, porém, para entender melhor como ocorre a comunicação nessas redes é preciso conhecer os requisitos necessários para que ocorra a transmissão de informações entre origem e destino, que são:

- a) regras;
- b) dispositivos;
- c) meio físico;
- d) mensagem.

A seguir, confira mais detalhadamente cada um desses requisitos.

a) Regras

As regras são os protocolos de comunicações necessários para organizar a comunicação propriamente dita. Imagine uma situação onde uma pessoa que só fala o idioma português se apresenta para uma pessoa que só fala o idioma alemão. Provavelmente eles não vão conseguir se comunicar por utilizarem idiomas diferentes, ou seja, protocolos diferentes.

São exemplos de protocolos: TCP, IP, IPX, SPX, UDP, SCP.

Segundo a *Cisco Networking Academy* (2011), os protocolos fornecem:

- a) o formato ou estrutura da mensagem;
- b) o método pelo qual os dispositivos de rede compartilham informações sobre rotas com outras redes;
- c) como e quando mensagens de erro e de sistema são passadas entre dispositivos;
- d) a configuração e término das sessões de transferência de dados.

b) Dispositivos

Os dispositivos são os equipamentos que se conectam na rede de computador para transmitir as informações. São classificados em dispositivos finais e dispositivos intermediários. Os dispositivos finais são aqueles que originam e recebem as informações, ou seja, fazem a interface entre os usuários e a rede de comunicação. Computadores e servidores são exemplos de dispositivos finais. Os dispositivos intermediários são aqueles que realizam a comunicação entre os dispositivos finais assegurando a troca de informações por meio da rede. Exemplos de dispositivos intermediários são os hubs, switches e roteadores.

Confira, a seguir, a representação gráfica desses dispositivos.

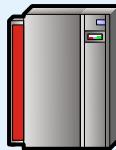
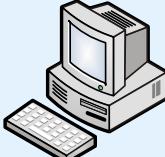
DISPOSITIVOS FINAIS	DISPOSITIVOS INTERMEDIÁRIOS
 Servidor	 Roteador
 Computador Pessoal	 LAN Switch
 Laptop	 LAN Hub

Figura 2 - Dispositivos finais e intermediários
Fonte: Cisco Networking Academy (2011)

D1mitre Camargo (2011)

c) Meio Físico

Para que a informação seja transmitida entre os dispositivos finais, um meio físico de rede precisa estar disponível. É por meio deste meio físico que a mensagem será transmitida.

Como exemplos de meios físicos temos: os cabos de cobre, cabos de fibra óptica e o ar, para redes sem fio. Na figura a seguir você pode visualizar esses exemplos de meios físicos. Confira!



Figura 3 - Meios físicos de rede
Fonte: Cisco Networking Academy (2011)

d) Mensagem

A mensagem é a informação que precisa ser transmitida entre origem e destino. Qualquer informação que precisa ser transportada entre dispositivos finais é um exemplo de mensagem, como um e-mail, página de web, mensagens instantâneas e até mesmo jogos on-line.

Não se preocupe, pois, nos próximos capítulos, você estudará mais detalhadamente os protocolos, dispositivos e meios físicos.

Como você pôde perceber, fazem parte dos elementos de uma rede de computadores: regras, dispositivos, o meio físico e a própria mensagem que é transmitida por ela. E, falando em mensagem, existem alguns tipos de comunicação. É importante que você os conheça.

2.3 TIPOS DE COMUNICAÇÃO (UNICAST, MULTICAST E BROADCAST)

É importante você conhecer os tipos de mensagens que podem ser transmitidas entre *hosts* com base no endereçamento. Uma mensagem pode ser transmitida para três tipos de destinos diferentes: *Unicast*, *Multicast* *Broadcast*.

Uma mensagem transmitida contendo um endereço de destino ***Unicast*** é aquela mensagem tradicional, enviada de origem a destino conforme você viu anteriormente, ou seja, um único dispositivo de origem envia uma mensagem para outro dispositivo de destino único. Veja a representação do envio de uma mensagem *Unicast* entre o dispositivo A e o dispositivo B.

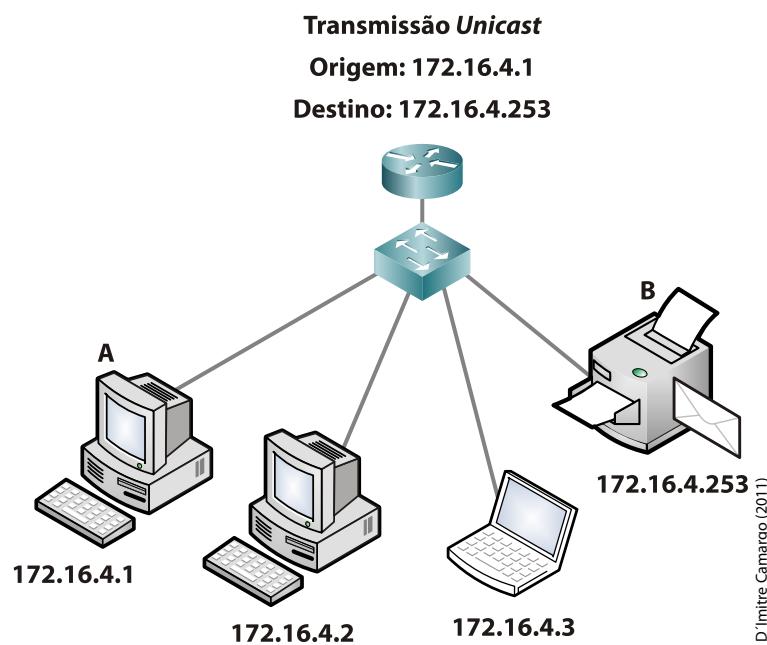


Figura 4 - Mensagem *Unicast*
Fonte: Cisco Networking Academy (2011)

Uma mensagem em ***Multicast*** é utilizada quando uma mensagem precisa ser transmitida para um determinado grupo de dispositivos de destino dentro de uma rede, ou seja, a mensagem não será recebida por um único dispositivo ou todos os dispositivos naquela rede e sim, para um grupo específico.

Veja um exemplo de uma mensagem *Multicast* onde o dispositivo A envia uma mensagem em *Multicast* para o grupo a que pertencem os dispositivos C e D.

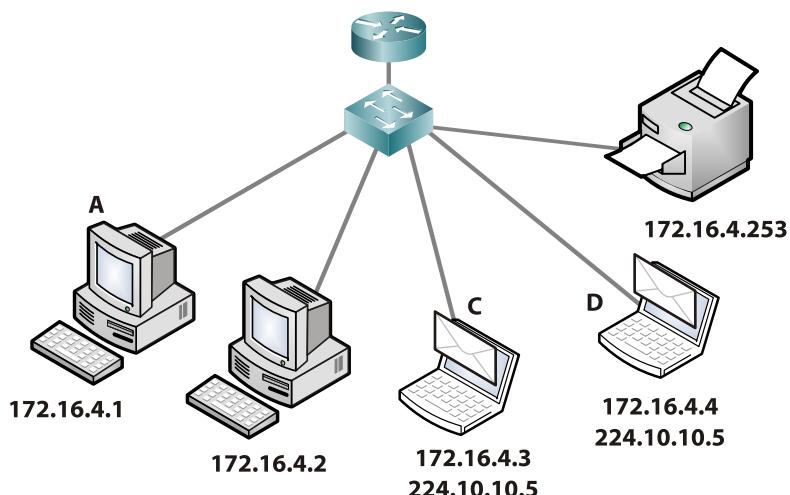


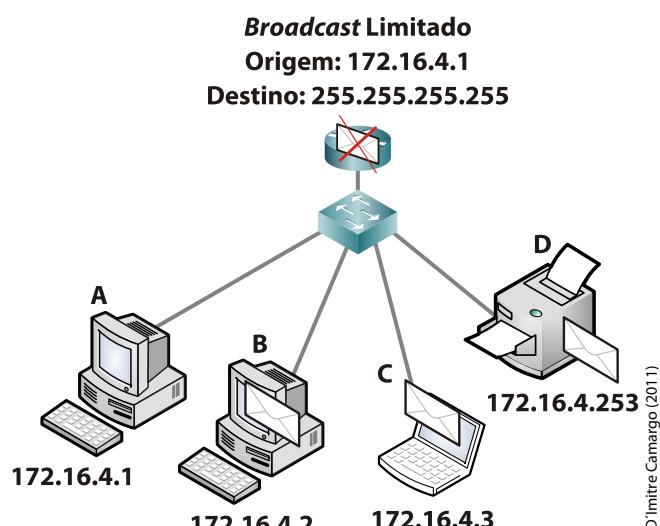
Figura 5 - Mensagem Multicast
Fonte: Cisco Networking Academy (2011)

D'lmitre Camargo (2011)



Quando você for estudar os protocolos de roteamento dinâmico, mais adiante no curso, aprenderá que os protocolos RIPv2 e EIGRP¹ utilizam respectivamente os endereços de Multicast 224.0.0.9 e 224.0.0.10.

Uma mensagem em **Broadcast** é utilizada quando uma informação precisa ser transmitida para todos os dispositivos dentro de uma determinada rede ou sub-rede. Por exemplo, você verá mais adiante no curso que, quando um dispositivo de origem não conhece o endereço MAC do dispositivo de destino, ele emite um *Broadcast* de camada 2 chamado de solicitação ARP ou *ARP Request*. Veja, na figura a seguir, a demonstração de uma mensagem em *Broadcast* sendo enviada do dispositivo A.



Broadcast Limitado
Origem: 172.16.4.1
Destino: 255.255.255.255
Figura 6 - Mensagem Broadcast
Fonte: Cisco Networking Academy (2011)

D'lmitre Camargo (2011)

² ACRÔNIMO

Conjunto de letras, pronunciado como uma palavra normal, formado a partir das letras iniciais (ou de sílabas) de palavras sucessivas que constituem uma denominação.

³ BLUETOOTH

Protocolo utilizado em redes sem fio para realizar conexões de curtas distâncias entre dispositivos. Tais como: impressoras, celulares, PDA, câmeras digitais, etc.

Como você pôde observar, os tipos de comunicação podem ser por *Unicast*, *Multicast* e *Broadcast*. E você sabe qual é a classificação das redes? Não? Então confira a seguir.

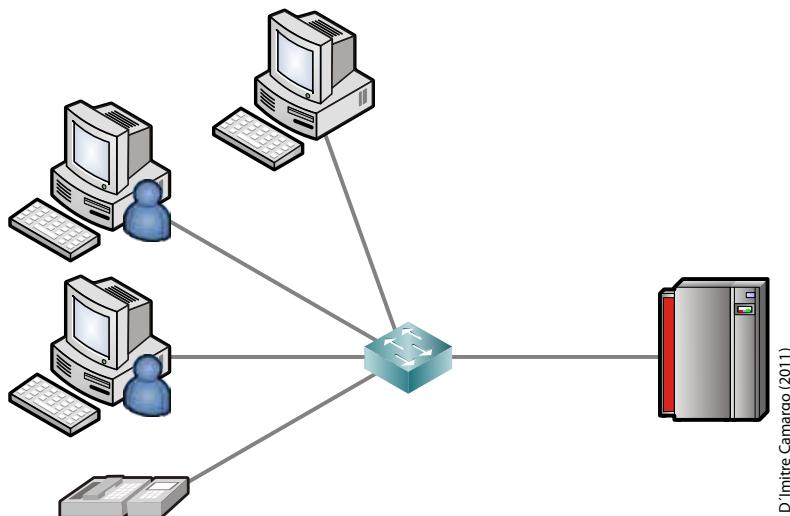
2.4 CLASSIFICAÇÃO DE REDES

Uma rede de computador pode ser classificada de diversas formas, dependendo do enfoque dado ao assunto. Vamos ver, agora, dois tipos de classificação de redes: uma classificação com base no tamanho de uma determinada rede e outra classificação relacionada com a função do dispositivo final em uma rede.

Analisando uma rede com base no tamanho e abrangência, iremos nos depa-rar com os seguintes conceitos:

2.4.1 LAN

Uma LAN é o acrônimo² de Rede de Área Local (*Local Area Network*), onde os computadores que fazem parte desta rede estão fisicamente localizados em um mesmo espaço físico, geralmente limitado por uma sala, um andar de um prédio ou, até mesmo, todo o prédio ou escritório. A LAN também pode ser chamada de rede local. Como estes dispositivos estão diretamente conectados no mesmo es-paço físico por meio de cabos de cobre, fibra ou sem fio, a velocidade de transmis-são em uma LAN é consideravelmente alta, geralmente em 10/100/1000 Mbps, de forma ininterrupta. Veja um exemplo de LAN.



D'Imitre Camargo (2011)

Figura 7 - Rede Local
Fonte: Cisco Networking Academy (2011)

Nessa figura, você pode observar dispositivos finais interligados com um dispositivo intermediário, no caso um *switch*, em uma LAN.

2.4.2 WAN

Uma WAN é o acrônimo de Rede de Área Distribuída (*Wide Area Network*). Pode ser chamada também de Rede de Longa Distância. Uma WAN se caracteriza pela união ou interligação de diversas LANs. Para que estas LANs possam ser interligadas, serviços de provedores de telecomunicações geralmente são utilizados. Veja, a seguir, uma figura que demonstra uma WAN.

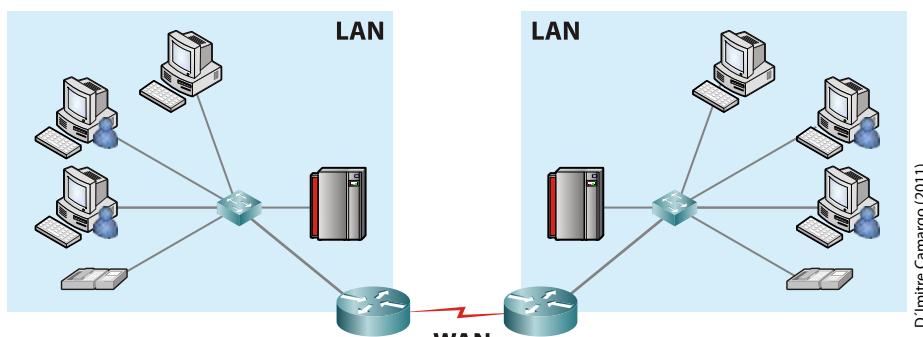


Figura 8 - Rede de longa distância
Fonte: Cisco Networking Academy (2011)

D'Inácio Camargo (2011)

Nessa figura, você pode observar duas redes locais interligadas por um link serial, formando uma WAN.

Conheça agora outros tipos de redes.

MAN: Rede de Área Metropolitana que interliga LANs em uma distância não tão maior do que uma WAN. São, geralmente, disponibilizadas por operadoras de TV a cabo.

PAN: Rede de Área Pessoal que interliga dispositivos bem próximos uns dos outros, geralmente utilizando tecnologias de *bluetooth*³.

SAN: Rede de Área de Armazenamento usada na interligação de servidores e recursos de armazenamento.

WLAN: Muito próxima de uma LAN, mas, utiliza redes sem fio

WMAN: Muito próxima de uma MAN, mas, utiliza redes sem fio.

WWAN: Muito próxima de uma WAN, mas, utiliza redes sem fio.

Agora vamos analisar uma rede com base na importância e função do dispositivo final:

2.4.3 REDES CLIENTE/SERVIDOR

Em uma rede cliente/servidor as funções de ambos são bem definidas. O servidor tem a função de fornecer algum serviço ou recurso para os seus clientes da rede, enquanto que o cliente tem a única função de utilizar os serviços e recursos oferecidos pelo servidor. Um servidor sempre vai se comportar como um servidor e o cliente, sempre como um cliente. Veja, na figura a seguir, a demonstração de uma rede cliente/servidor.

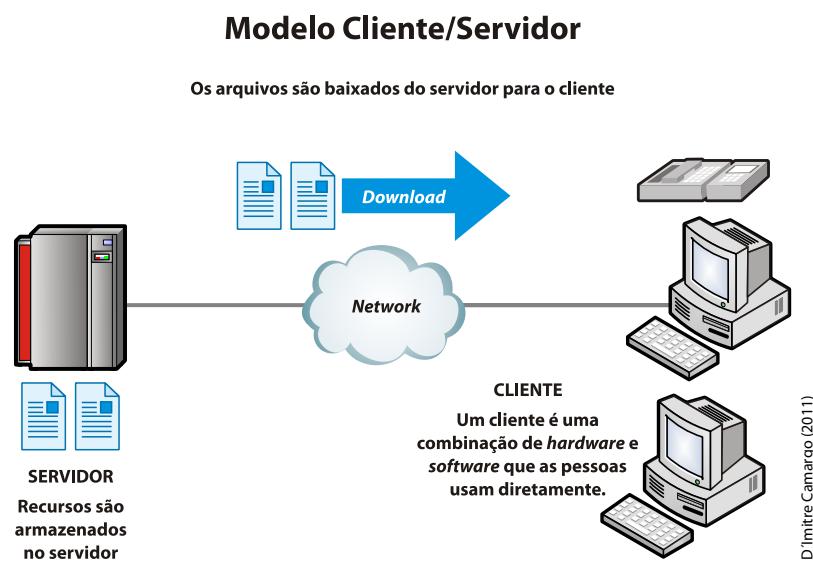


Figura 9 - Rede cliente/servidor
Fonte: Cisco Networking Academy (2011)

2.4.4 REDE PONTO A PONTO

Em uma rede ponto a ponto, as funções de cliente e servidor não são bem definidas, ou seja, em um momento um dispositivo poderá fazer o papel de servidor e, logo após, poderá fazer o papel de um cliente.

Vejamos um exemplo dessa situação, no “Casos e Relatos” a seguir.



CASOS E RELATOS

Comportamento de redes cliente/servidor e ponto a ponto

Lucas precisa instalar um programa por meio de um CD de instalação, mas o seu computador não possui um aparelho de leitura de CD. Ele procura um computador que tenha o aparelho de leitura na sua rede local, insere o CD neste aparelho e executa a instalação do programa por meio da rede. Desta forma, o seu computador está agindo como um cliente, enquanto que o computador onde Lucas inseriu o CD está agindo como um servidor. Imagine agora que este mesmo computador que Lucas inseriu o CD para instalação precise imprimir um arquivo de texto, mas, ele não possui impressora. No caso, o PC de Lucas tem uma impressora instalada, sendo assim, por meio do compartilhamento da sua impressora, o outro computador poderá fazer a impressão pela rede. Agora, o seu computador estará agindo como um servidor, e o outro computador da rede estará agindo como um cliente, ou seja, os papéis se inverteram.

Observe, na figura a seguir, a demonstração de uma rede ponto a ponto.

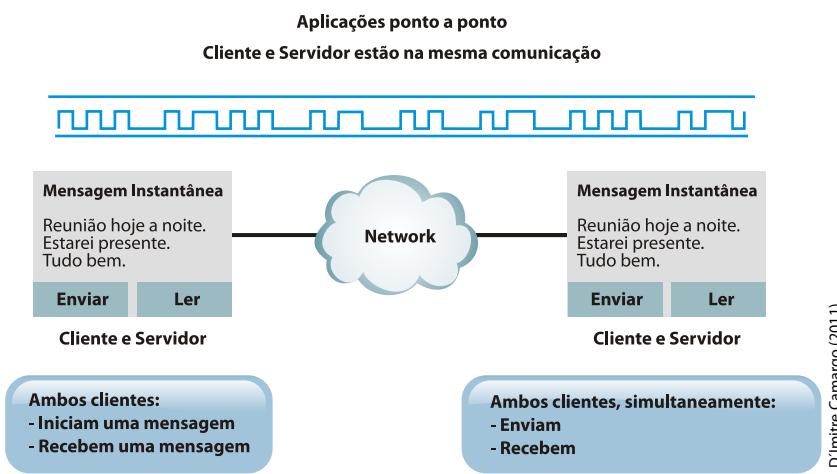


Figura 10 - Rede ponto a ponto
Fonte: Cisco Networking Academy (2011)

No quadro a seguir, você pode observar as vantagens e desvantagens das redes cliente/servidor e ponto a ponto.

	REDE PONTO A PONTO	REDE CLIENTE/SERVIDOR
VANTAGENS	Mais econômica para implementar. Não exige software adicional especializado de administração de redes. Não exige um administrador dedicado de redes.	Oferece melhor segurança. É mais fácil de se administrar quando a rede é grande, pois a administração é centralizada. Pode-se fazer backup dos dados em um local central.
DESVANTAGENS	Não se adapta bem ao crescimento de grandes redes e a administração se torna mais difícil de ser gerenciada. Cada usuário precisa ser treinado para realizar tarefas administrativas. Menos segura. Todas as máquinas que compartilham os recursos têm o desempenho afetado de maneira negativa.	Exige software especializado muito caro para a operação e a administração de redes. Exige hardware mais caro e muito mais potente para a máquina do servidor. Requer um administrador profissional. Possui um único ponto de falha: se o servidor estiver inativo, os dados do usuário não estarão disponíveis.

Quadro 2 - Vantagens e desvantagens das redes cliente/servidor e ponto a ponto

Fonte: Cisco Networking Academy (2011)



VOCÊ SABIA?

Geralmente, uma rede ponto a ponto possui um máximo de 10 computadores enquanto que uma rede cliente/servidor possui mais do que 10 computadores. Não necessariamente esta regra deverá ser seguida, dependendo do uso da rede em questão, esta quantidade pode ser diferente.

No capítulo 6 você verá outro tipo de classificação de redes com base no layout dos cabos de rede que chamamos de Topologia Física.

Nessa etapa, você acompanhou as classificações de redes utilizadas hoje em dia, que são: a rede do tipo LAN, a WAN, a cliente/servidor e a ponto a ponto e agora já sabe como e onde utilizar cada tipo. A seguir, você encontrará mais informações importantes para o seu dia a dia nessa área.

2.5 ARQUITETURA DE CAMADAS

Até o momento você pôde observar o quanto o mundo de redes de computadores é complexo com todos estes dispositivos comunicando-se entre si. Para facilitar o entendimento de todo esse processo de comunicação em redes, uma abordagem em camadas foi desenvolvida e foi chamada de Arquitetura de Camadas, ou também, Arquitetura de Protocolos.

Além de ajudar no processo de ensino e aprendizagem das redes de computadores, esta abordagem em camadas foi desenvolvida por questões de padronização de hardware, software e protocolos de comunicação. Desta forma, os diversos fabricantes podiam se basear em um modelo para desenvolver seus equipamentos e aplicações.

Vamos estudar neste curso dois modelos de camadas: um modelo usado como referência e outro modelo usado como aplicação. Estes modelos são o Modelo de Referência OSI e o Modelo de Referência TCP/IP.

2.5.1 MODELO DE REFERÊNCIA OSI

O Modelo de Referência OSI (*Open Systems Interconnection*) foi criado pela ISO⁴ (*International Organization for Standardization*) em 1984 para manter uma maior interoperabilidade e compatibilidade entre as diversas tecnologias de rede existentes.

O modelo OSI é composto de sete camadas conforme descritas na figura a seguir.



Figura 11 - Modelo de Referência OSI
Fonte: Cisco Networking Academy (2011)

Cada camada do modelo OSI possui funções e características distintas. Veja, a seguir, uma função resumida de cada camada:

- a) **Aplicação:** fornece serviços de redes para as aplicações;
- b) **Apresentação:** fornece uma estrutura de formatação dos dados;
- c) **Sessão:** estabelece, gerencia e termina sessões entre aplicações;
- d) **Transporte:** estabelece, mantém e termina circuitos virtuais entre dispositivos finais;
- e) **Rede:** endereçamento de rede e determinação do melhor caminho;
- f) **Enlace de dados:** controle de acesso ao meio de rede;
- g) **Física:** transmissão binária através dos meios físicos de redes.

Mais adiante, nesta unidade curricular, você estudará os detalhes de cada camada do modelo OSI.

2.5.2 MODELO DE REFERÊNCIA TCP/IP

O O Modelo de Referência TCP/IP, como seu próprio nome já diz, é um modelo utilizado na aplicação de toda a Internet e redes de computadores, ou seja, o modelo OSI é usado como uma referência, enquanto que o modelo TCP/IP é o modelo ao qual a Internet se desenvolveu e funciona até hoje.

O modelo TCP/IP foi desenvolvido pelo DoD (Departamento de Defesa dos EUA) com o objetivo de criar uma rede tolerante a falhas, onde, caso uma bomba caísse em um quartel general, a comunicação não seria interrompida. Este modelo foi desenvolvido como um padrão aberto onde atualmente toda a Internet tem o seu funcionamento.

O modelo TCP/IP é composto de quatro camadas, conforme descrito na figura a seguir.

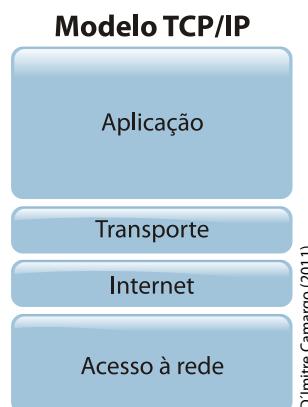


Figura 12 - Modelo de Referência TCP/IP
Fonte: Cisco Networking Academy (2011)

No capítulo 8 você estudará os detalhes de cada camada do modelo TCP/IP. Agora, confira como é o processo de encapsulamento dos dados. Como você acabou de ver, considerando a arquitetura de camadas, existem dois modelos usados como referência na análise e estudo de redes. Acompanhe, em seguida, como é o processo de encapsulamento dos dados.

2.6 O PROCESSO DE ENCAPSULAMENTO DOS DADOS

Agora que você já tem um conhecimento inicial sobre as camadas do modelo OSI você vai aprender o que ocorre quando um dispositivo de origem envia uma mensagem para um dispositivo de destino. Em cada camada do modelo OSI, uma PDU (*Protocol Data Unit*) é utilizada. O processo que esta mensagem sofre por meio de todas as camadas do modelo OSI é chamado de encapsulamento dos dados.



VOÇÊ SABIA?

PDU é o acrônimo dado à Unidade de Dados de Protocolo. Cada camada do modelo OSI utiliza uma PDU para encapsular os dados a serem transmitidos entre origem e destino.

Vamos imaginar a seguinte situação:

Cecília envia uma mensagem de texto para Vicente. Conforme visto anteriormente, o usuário se comunica com a rede através de um aplicativo, e este aplicativo se comunica com a rede através da camada de aplicação. Na camada de aplicação, o texto enviado por Cecília é encapsulado numa PDU que chamamos de PDU DADOS. Esta PDU DADOS será processada pelas três camadas superiores do modelo OSI (Aplicação, Apresentação e Sessão).

Na camada de transporte esta PDU DADOS será encapsulada em outra (ou outras) PDU que chamamos de SEGMENTO. Não necessariamente toda PDU DADOS será transformada em uma única PDU SEGMENTO, ou seja, dependendo do tamanho dos dados transferidos vários SEGMENTOS poderão ser criados e encapsulados. Nesta camada, o segmento receberá um endereçamento chamado de “porta” para identificar a comunicação.

Na camada de rede, a PDU SEGMENTO será encapsulada numa PDU chamada PACOTE. O pacote também possui um endereçamento, no caso, o endereçamento IP. Será por meio deste endereçamento que o pacote será roteado da origem até o destino pelas redes.

Agora, na camada de enlace de dados, o PACOTE será encapsulado numa PDU chamada QUADRO. O QUADRO também receberá um endereçamento para comunicação dentro da rede física, ou seja, receberá um endereço MAC para identificação dentro da rede local. Além deste endereçamento, o QUADRO também receberá um *trailer* com informações de um FCS (*Frame Check Sequence*), que tem a função de identificar possíveis erros na transmissão do QUADRO.

Finalizando o processo de encapsulamento dos dados, o QUADRO da camada de enlace será transformado numa sequência de *bits* para transmissão pelo meio físico da rede, sendo assim, a PDU da camada física é chamada de BITS. Os *bits* então serão transmitidos pelo meio físico de rede até chegar ao destino correto. Ao chegar ao destino, ocorrerá o processo inverso, que é chamado de processo de desencapsulamento dos dados, onde Vicente receberá a mensagem enviada por Cecília.

Devemos imaginar que estes bits encontrarão dispositivos intermediários pelo caminho, nos quais, o processo de desencapsulamento e encapsulamento ocorrerá até a camada em que o dispositivo intermediário reside. Veja a demonstração do processo completo na figura a seguir.

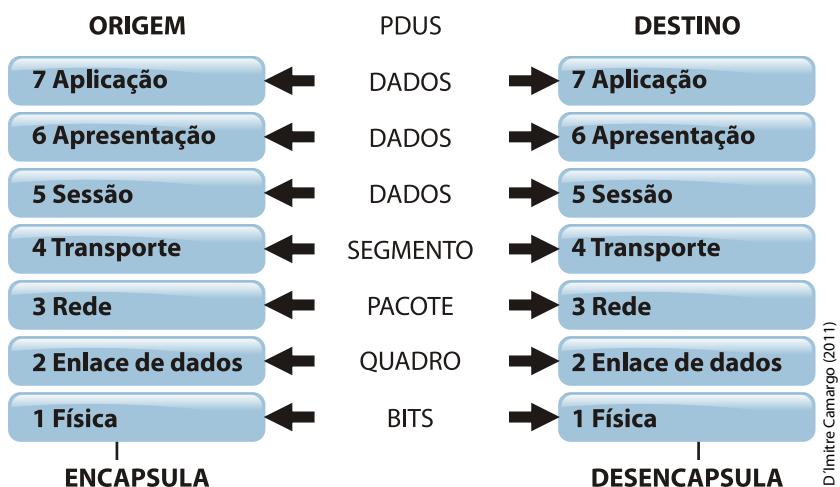


Figura 13 - Processo de Encapsulamento dos Dados
Fonte: Adaptado de Cisco Networking Academy (2011)



FIQUE ALERTA

O conhecimento do processo de encapsulamento e desencapsulamento dos dados é de extrema importância para entendermos o funcionamento das redes de computadores.

**SAIBA
MAIS**

Para saber mais sobre o assunto consulte o livro Guia de Certificação Oficial para o Exame.

ODOM, Wendell. **CCENT/CCNA ICND 1: Guia Oficial de Certificação do Exame.** Rio de Janeiro: Alta Books, 2008. 458 p.

Para entender melhor o processo e encapsulamento, você conferiu um exemplo e a demonstração do processo completo. No próximo capítulo você conhecerá as características e funções das camadas superiores do modelo OSI. Confira!

**RECAPITULANDO**

Neste capítulo você conheceu vários conceitos de redes de computadores, desde o início das redes, passando pelo processo de evolução e sua aplicabilidade. Depois estudou os elementos necessários na comunicação em rede. Logo em seguida, viu os tipos de comunicação que existem entre origem e destino. Depois, estudou algumas das classificações das redes de computadores e os detalhes de uma arquitetura de camadas, e, por último, pôde verificar o processo de encapsulamento dos dados e como ocorre uma comunicação entre origem e destino. Estes conceitos ajudarão a entender com mais facilidade o mundo das redes de computadores. Nos próximos capítulos você estudará, mais detalhadamente, o que ocorre em cada camada do modelo OSI.

Modelo OSI – As Camadas Superiores

3



Neste capítulo você estudará as características e funções das camadas superiores do modelo OSI, começando pela camada de aplicação com suas características, funções e os protocolos que funcionam nesta camada. Logo após, verá a camada de apresentação, onde você estudará as principais funções desta camada. Por último, a função da camada de sessão.

Ao final deste capítulo você terá subsídios para:

- a) conhecer os principais conceitos das camadas superiores do modelo OSI.

3.1 CAMADA DE APLICAÇÃO

A camada de aplicação do modelo OSI (camada 7) é a camada que tem a função de fornecer uma interface de comunicação entre o usuário e a rede, ou seja, esta camada está mais próxima do usuário, fornecendo o seu acesso à rede. O acesso destes usuários se dará por meio de aplicações de redes, e entre os mais populares, pode-se destacar:

- a) navegação de Internet (WEB);
- b) correio eletrônico;
- c) mensagens instantâneas;
- d) compartilhamento de arquivos;
- e) jogos on-line;
- f) transferência de arquivos.

Estas aplicações de redes vão necessitar de protocolos de comunicação para realizar a interface para a rede. Alguns exemplos de protocolos de comunicação da camada de aplicação são:

- a) HTTP e HTTPS;
- b) FTP e TFTP;
- c) SMTP, POP e IMAP;
- d) DNS;
- e) DHCP;
- f) SNMP.

A figura a seguir apresenta uma visão das sete camadas do modelo OSI, com destaque para a camada de aplicação, função básica, e alguns protocolos que trabalham nesta camada. Confira.

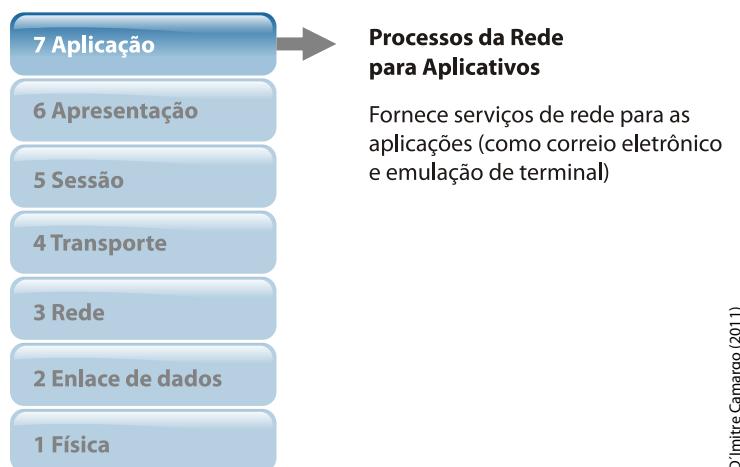


Figura 14 - A Camada de Aplicação do modelo OSI
Fonte: Cisco Networking Academy (2011)

Conheça, agora, as principais características dos protocolos da camada de aplicação mais comuns em redes de computadores.

3.1.1 HTTP E HTTPS

Quando um usuário navega na Internet, ele utiliza um navegador WEB para solicitar uma página a um servidor WEB, para isso, ele digita o endereço da página que quer navegar. Esse endereço é chamado de URL (*Uniform Resource Locator*). O protocolo de comunicação usado para transferir estas páginas é chamado de HTTP (*Hyper Text Transfer Protocol*). Veja um exemplo:

HTTP://	WWW.	CISCO.COM	/EDU/
Identifica para o navegador o protocolo que deve ser usado.	Identifica o nome do host ou o nome de uma máquina específica.	Representa a entidade de domínio do site web.	Identifica a pasta onde as páginas web estão localizadas no servidor. Como nenhum nome é especificado, o navegador carregará a página padrão identificada pelo servidor.

Quadro 3 - Observando uma URL
Fonte: Cisco Networking Academy (2011)

A WEB utiliza uma arquitetura do tipo cliente/servidor, na qual uma aplicação “cliente utilizando um browser¹” solicita uma informação a um servidor de WEB. Este servidor possui um serviço WEB pronto para atender a solicitação do cliente. Observando o endereço URL o servidor sabe qual página o cliente está solicitando. Veja!

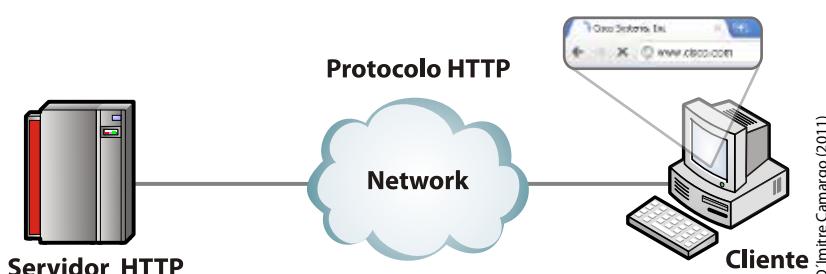


Figura 15 - Acessando um Servidor WEB
Fonte: Cisco Networking Academy (2011)

Apesar de cumprir perfeitamente com sua função, o protocolo HTTP não é um protocolo seguro, ou seja, as informações trafegadas por este protocolo são transmitidas em texto claro e, caso a informação seja interceptada durante a comunicação, os dados poderão ser comprometidos. Para resolver este problema, o protocolo HTTP Seguro (HTTPS) poderá ser utilizado. O HTTPS utiliza autenticação e criptografia na transferência de arquivos entre cliente e servidor, garantindo assim, uma maior segurança das informações trafegadas.



FIQUE ALERTA

Os temas “autenticação e segurança” serão estudados mais adiante neste curso.

3.1.2 FTP E TFTP

O protocolo FTP (*File Transfer Protocol*) é um protocolo que tem como finalidade principal transferir arquivos de um computador para outro, copiando e movendo arquivos dos servidores para os clientes e vice-versa. O FTP é um protocolo confiável e orientado à conexão, ou seja, existe uma garantia de que as informações serão entregues ao destino.

O protocolo TFTP (*Trivial File Transfer Protocol*) é um protocolo que tem a mesma finalidade do FTP, ou seja, transferir arquivos. A grande diferença entre estes protocolos é que o TFTP não é confiável e também não é orientado à conexão, ou seja, não existe garantia na entrega da informação. Por este motivo o TFTP é mais rápido do que o FTP, justamente por não usar recursos que garantam a entrega dos dados. Por outro lado, o FTP é muito mais seguro e confiável.



VOCÊ SABIA?

O FTP é utilizado para transferências de arquivos onde a comunicação possa não ser confiável, como a Internet, por exemplo.

No capítulo seguinte você estudará os conceitos de protocolos confiáveis e orientados à conexão. Aguarde!

Para entender melhor sobre FTP e TFTP, acompanhe, no “Casos e Relatos”, um exemplo de como salvar informações na rede.



CASOS E RELATOS

Pedro é o administrador de redes de uma instituição de ensino e precisa salvar as configurações de um roteador em dois servidores diferentes. Um servidor fica na rede local de Pedro, enquanto o outro servidor está hospedado na Internet. Sabendo que a Internet pode conter links instáveis entre o seu roteador na rede local e o servidor na Internet, Pedro resolve utilizar o protocolo FTP para transferir o arquivo de configuração até este servidor. Para salvar as configurações do roteador na rede local, Pedro utiliza o protocolo TFTP, justamente por saber que a rede local possui uma comunicação mais confiável e estável.

3.1.3 SMTP, POP E IMAP

Estes protocolos são utilizados para a transferência de e-mails. O SMTP (*Simple Mail Transfer Protocol*) é o protocolo usado para transferir e-mails entre servidores de e-mail, e também pela aplicação do cliente para enviar e-mails. Os protocolos POP (*Post Office Protocol*) e IMAP (*Internet Message Access Protocol*) são usados pela aplicação do cliente para baixar um e-mail do servidor de e-mail local.

Veja a figura a seguir. Ela mostra um exemplo de uso destes protocolos.

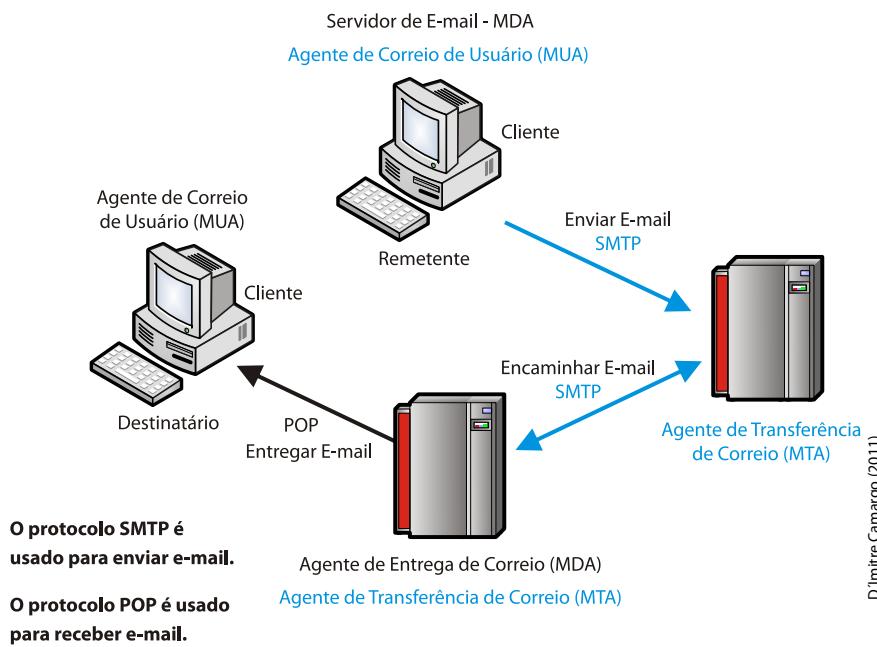


Figura 16 - Uso dos protocolos SMTP, POP e IMAP
Fonte: Cisco Networking Academy (2011)

Na próxima figura você pode conferir um exemplo de configuração de uma conta de e-mail com os endereços dos servidores SMTP e POP.

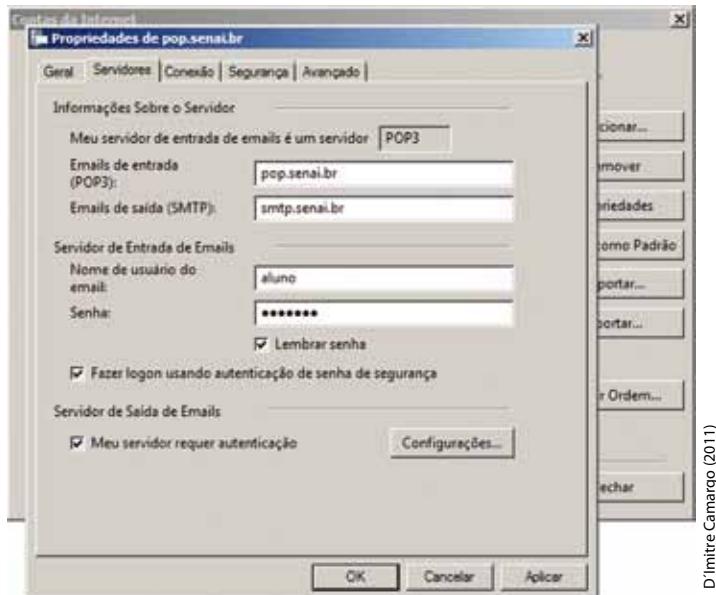


Figura 17 - Configuração de conta de e-mail

3.1.4 DNS

Para que a comunicação ocorra em uma rede de dados, os dispositivos necessitam de uma numeração de rede (IP) para estabelecer a comunicação entre origem e destino. Com o rápido crescimento da Internet ficou impossível para as pessoas lembrarem-se dos endereços IPs de todos os sites a serem navegados.

O protocolo DNS (*Domain Name System*) tem a função de traduzir nomes de domínio em endereços e IPs e vice-versa. Quando digitamos uma URL em um *browser*, esta URL precisa ser traduzida em um endereço de camada de rede (IP) para que a comunicação ocorra. Desta forma, os usuários não precisam decorar endereços IPs para navegar na Internet, eles precisam somente saber a URL do site a ser visitado.

Para um dispositivo final navegar na Internet, ele precisa ser configurado com um endereço de um servidor DNS. Desta forma, basta o usuário digitar o domínio do site a ser visitado que o serviço de DNS fará a tradução deste domínio para um endereço IP. Veja um exemplo de um dispositivo final com o DNS configurado.

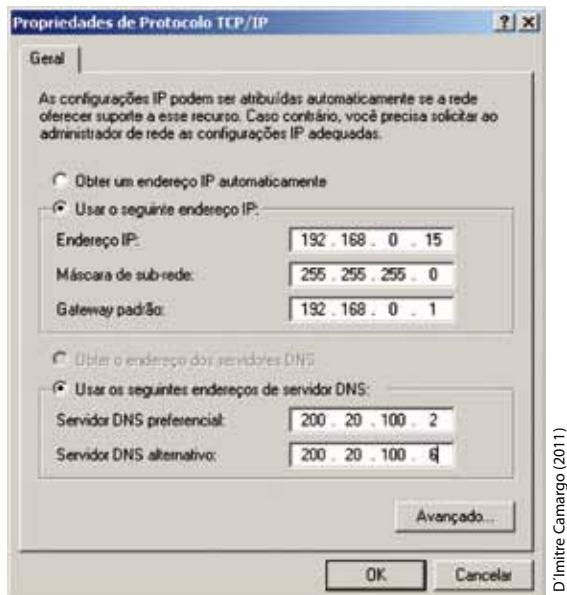


Figura 18 - Exemplo de configuração DNS em um dispositivo final

3.1.5 DHCP

Um dispositivo final necessita de um endereço IP para comunicar-se na rede. Este endereço IP poderá ser fornecido de duas formas. A primeira forma é por meio de um endereço estático, onde o administrador da rede atribui o endereçamento para cada dispositivo manualmente. A segunda forma é por meio de um serviço dinâmico, onde um protocolo fornece o endereçamento automaticamente para cada dispositivo na rede.

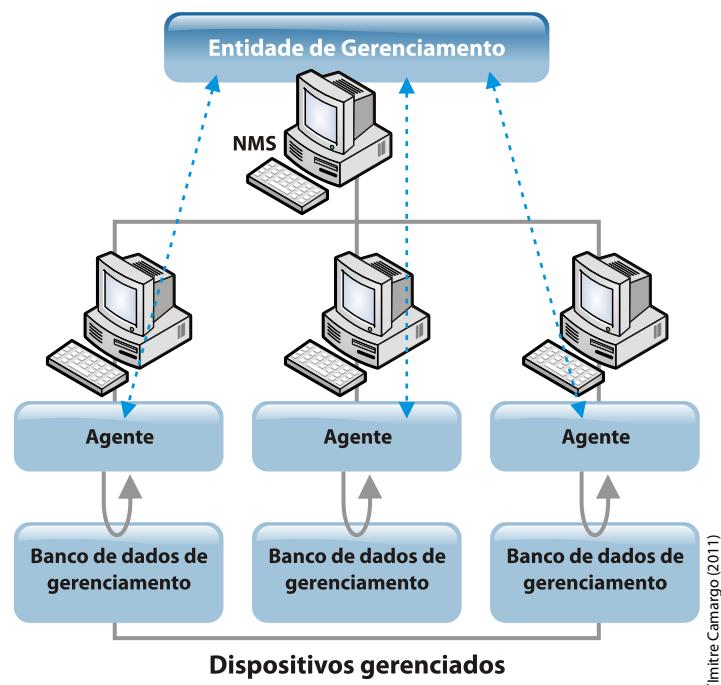
O DHCP (*Dynamic Host Configuration Protocol*) é o protocolo que fornece dinamicamente as informações de configuração necessárias para os dispositivos finais poderem se comunicar. Dentre as informações de configuração, as mais comuns são: IP, máscara, *gateway* e DNS. As redes que possuem uma grande quantidade de dispositivos finais utilizam o DHCP para facilitar o gerenciamento e a manutenção de todo o endereçamento IP desta rede. Veja na figura a seguir a demonstração da troca de mensagens DHCP entre cliente e servidor.

Figura 19 - Troca de mensagens DHCP
Fonte: Cisco Networking Academy (2011)

Os dispositivos finais que devem ser configurados com o serviço DHCP são os *hosts* dos usuários, enquanto que servidores e impressoras devem ter seu endereçamento IP configurados manualmente. Isso porque estes dispositivos devem manter sempre o mesmo endereçamento IP.

3.1.6 SNMP

O SNMP (*Simple Network Management Protocol*) é um protocolo que tem a função de trocar informações de gerenciamento entre os dispositivos de uma determinada rede. O SNMP ajuda os administradores de rede a gerenciar a rede de forma otimizada, onde mensagens de alerta são enviadas para o computador que gerencia a rede. Veja a estrutura de uma rede de gerenciamento SNMP.



D'ImitreCamargo (2011)

Figura 20 - Estrutura de uma rede SNMP
Fonte: Cisco Networking Academy (2011)

Confira, a seguir, os componentes de uma rede SNMP, segundo Cisco Networking Academy (2011).

- Entidade de gerenciamento:** também chamado de NMS (*Network Management Systems*) é o responsável pela aplicação principal, ou seja, é quem gerencia a rede. Geralmente instalado em um servidor dedicado.

- b) **Dispositivos gerenciados:** são os dispositivos que estão sendo gerenciados pelo protocolo SNMP. Exemplos de dispositivos gerenciados são os roteadores, switches, servidores, etc.
- c) **Agentes:** são módulos de software de gerenciamento de rede que residem em dispositivos gerenciados. Um agente tem conhecimento local de informações de gerenciamento e as converte para uma forma compatível com o SNMP.



**SAIBA
MAIS**

Você encontra mais informações sobre os protocolos das camadas de aplicação no livro:
KUROSE, James F.; ROSS, Keith W. Redes de computadores e a Internet: uma abordagem top-down. 3. ed. São Paulo: Pearson Education do Brasil, 2006. 634 p.

Você já sabe que o modelo OSI é composto por sete camadas, sendo que a primeira delas (falando das camadas superiores) é a camada de aplicação. As demais camadas você estudará a partir de agora. Continue atento aos estudos.

3.2 CAMADA DE APRESENTAÇÃO

Sua principal função é representar os dados para que os mesmos estejam legíveis para a camada de apresentação do dispositivo de destino. Vejamos as funções da camada de apresentação:

- a) representação dos dados;
- b) formatação de dados;
- c) estruturação dos dados;
- d) negociação e sintaxe entre as camadas de aplicação e sessão.

Além destas funções de representação de dados, a camada de apresentação também é responsável por realizar a compactação e criptografia. A figura seguinte apresenta uma visão das sete camadas do modelo OSI, com destaque para a camada de apresentação.

² MPEG

Grupo definido pela ISO para padronizar compressão e transmissão de áudio e vídeo.

³ JPEG

Também usado para comprimir dados, geralmente imagens fotográficas.

⁴ GIF

É usado na formatação de imagens de baixa resolução, como ícones.

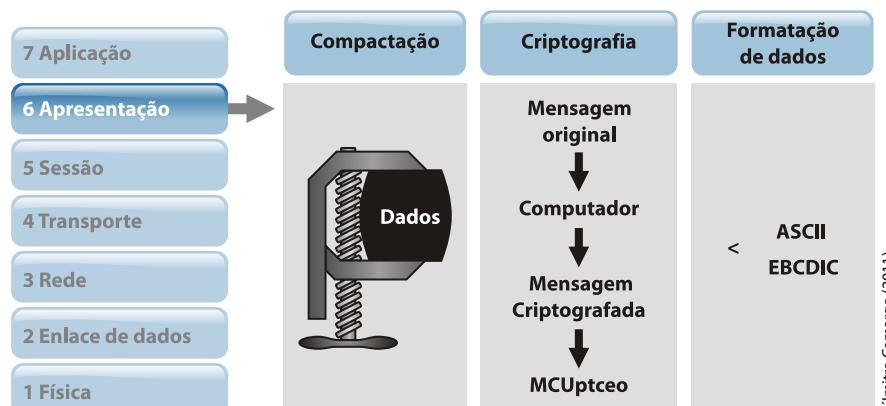


Figura 21 - Camada de apresentação
Fonte: Cisco Networking Academy (2011)

D'Imitre Camargo (2011)

São exemplos de padrões de formatação definidos na camada de apresentação: **MPEG²**, **JPEG³** e **GIF⁴**.

Nesse item você conferiu os exemplos de padrões de formatação que são definidos na camada de apresentação, que é a camada responsável por representar os dados de maneira legível. A próxima camada que você estudará é a camada de sessão.

3.3 CAMADA DE SESSÃO

A camada 5 do modelo de referência OSI tem como principais funções: estabelecer, gerenciar e terminar sessões entre aplicativos. Além disso, é a camada de sessão que entrega os dados para a camada de transporte, fazendo a conexão das camadas de mais alto nível com a camada de transporte.

A figura a seguir apresenta uma visão das sete camadas do modelo OSI com destaque para a camada de sessão.



D'Imitre Camargo (2011)

Figura 22 - A Camada de Sessão
Fonte: Cisco Networking Academy (2011)



FIQUE ALERTA

No capítulo 8 você verá que as três camadas superiores do modelo OSI serão somadas em apenas uma camada do modelo TCP/IP. Aguarde!



RECAPITULANDO

Neste capítulo você aprendeu os vários conceitos das camadas superiores do modelo de referência OSI. Primeiramente, estudou as características da camada de aplicação, bem como, os principais protocolos que residem nesta camada. Depois, estudou, também, as características da camada de apresentação. Por último, viu a função da camada de sessão. No próximo capítulo, você estudará com mais detalhes o que ocorre na camada de transporte do modelo OSI.

A Camada de Transporte

4



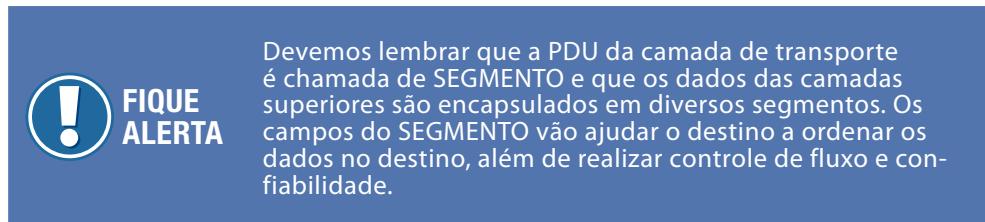
Neste capítulo, você verá as principais funções da camada de transporte do modelo de referência OSI, como por exemplo, controle de conexão, número de sequência, confiabilidade, controle de fluxo e número de portas. Depois, verá os dois principais protocolos da camada de transporte (TCP e UDP), suas funcionalidades e características. Por último, verá as diferenças e semelhanças entre o TCP e UDP.

Ao final desse capítulo você terá subsídios para:

- a) conhecer os principais conceitos da camada de transporte do modelo OSI, entender e diferenciar os protocolos TCP e UDP.

4.1 CONCEITOS DA CAMADA DE TRANSPORTE

A camada de transporte do modelo OSI (camada 4) é a camada que tem como função transportar e controlar o fluxo de dados entre origem e destino, de forma confiável e precisa. Para fazer esta tarefa, a camada 4 terá que garantir que os segmentos cheguem com sucesso até o destino; caso algum segmento não chegue ao destino, a camada de transporte terá que pedir uma retransmissão. Além disso, a camada de transporte precisa ordenar todos os segmentos no dispositivo de destino. Por último, a camada de transporte precisa prevenir e controlar os congestionamentos na rede.



A camada 4 fornece serviços de transporte do dispositivo de origem ao dispositivo de destino. Esta camada precisa estabelecer uma comunicação lógica entre estes dispositivos. Os principais protocolos na camada de transporte precisam segmentar e remontar os dados enviados pelas diversas aplicações das camadas superiores. Sendo assim, a camada de transporte vai fornecer um serviço de comunicação lógica entre dispositivos finais.

A figura a seguir apresenta uma visão das sete camadas do modelo OSI com destaque para a camada de transporte.

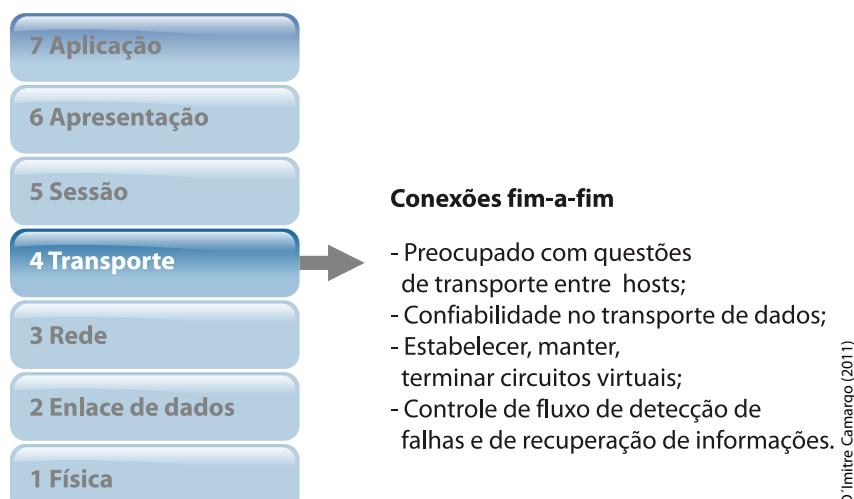


Figura 23 - A Camada de Transporte
Fonte: Cisco Networking Academy (2011)

Para realizar todas estas funções, a camada de transporte precisa utilizar várias funcionalidades, como as que você pode ver a seguir:

- a) serviço orientado à conexão;
- b) entrega ordenada;
- c) entrega confiável;
- d) controle de fluxo;
- e) identificar diferentes aplicações.

4.1.1 SERVIÇO ORIENTADO À CONEXÃO

A camada de transporte utiliza um serviço orientado à conexão para garantir confiabilidade. Ser um protocolo orientado à conexão significa que uma sessão precisa ser estabelecida entre origem e destino antes da transmissão dos dados propriamente ditos. Após esta sessão ser estabelecida, os dados poderão ser transmitidos e, após o término de transmissão das informações, a sessão será encerrada.

A camada de transporte realiza este estabelecimento de comunicação por meio do *handshake triplo*. O *handshake triplo* consiste em uma sincronização iniciada pelo cliente ao servidor. Vejamos a seguir como ocorre esta sincronização entre os dispositivos finais. Acompanhe o processo de sincronização.

O dispositivo que está iniciando a comunicação envia um segmento contendo um número de sequência inicial indicando um início de comunicação. Este é o SYN inicial.

O dispositivo receptor responde com um SYN/ACK confirmindo a comunicação.

O dispositivo que iniciou a comunicação responde a confirmação, completando o estabelecimento e sincronização da comunicação.

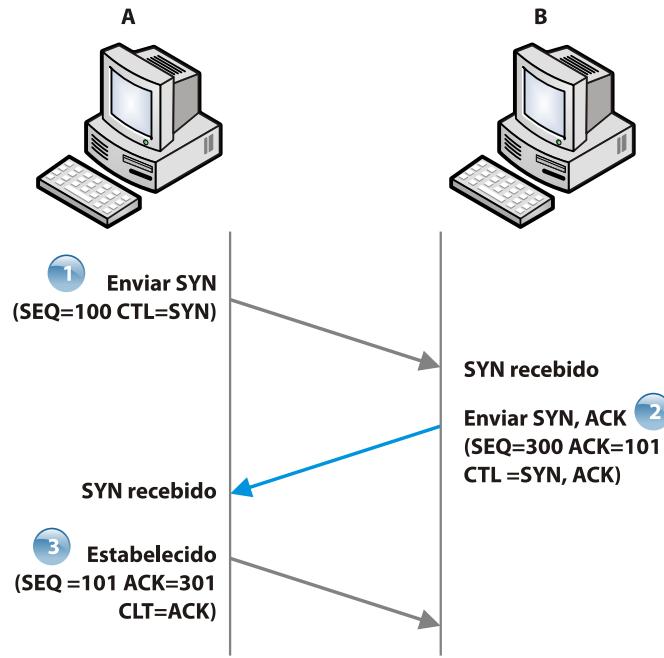


Figura 24 - Sincronização do handshake triplo
Fonte: Cisco Networking Academy (2011)

D'Imitre Camargo (2011)

Agora que o estabelecimento da comunicação já foi concluído, os dados poderão ser transmitidos, ou seja, somente depois do *handshake* triplo, os dados serão enviados pelo dispositivo de origem. Após os dados serem transmitidos, a sessão precisa ser encerrada, conforme demonstra a figura a seguir.

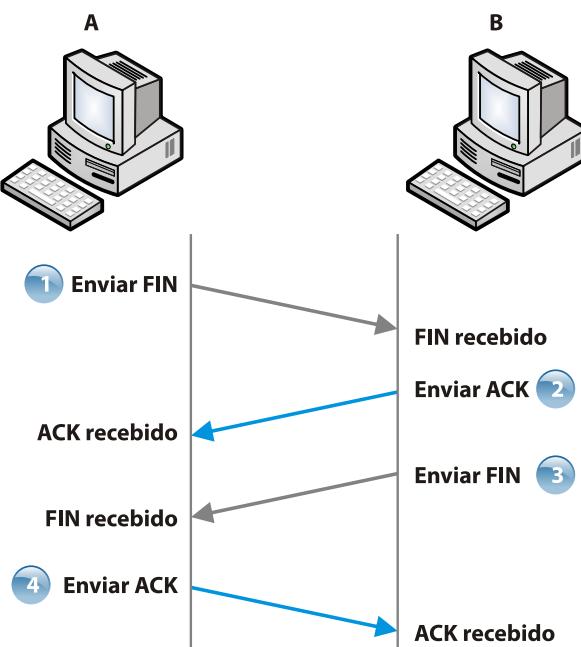


Figura 25 - Finalização da conexão
Fonte: Cisco Networking Academy (2011)

D'Imitre Camargo (2011)

4.1.2 ENTREGA ORDENADA

Quando os diversos segmentos são enviados entre dispositivos de origem e destino numa comunicação, a chegada ao destino pode ser de forma desordenada, justamente pelas diversas rotas disponíveis na comunicação em rede. Para que os segmentos possam ser ordenados no destino, cada segmento recebe um número de sequência. Quando estes segmentos chegam fora de ordem, eles são colocados em *buffer* para, depois de ordenados, serem entregues à camada superior. Vamos observar a ordenação dos segmentos na figura a seguir.

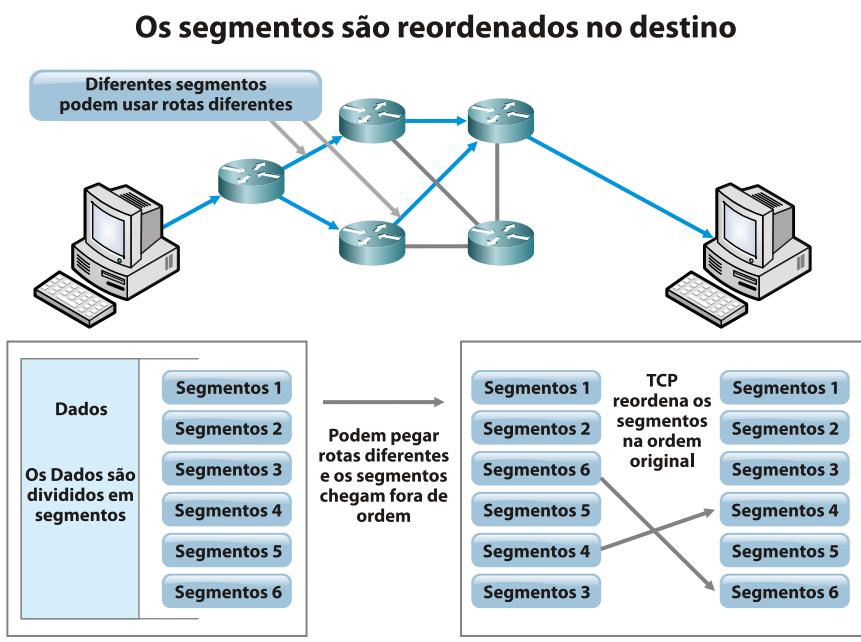
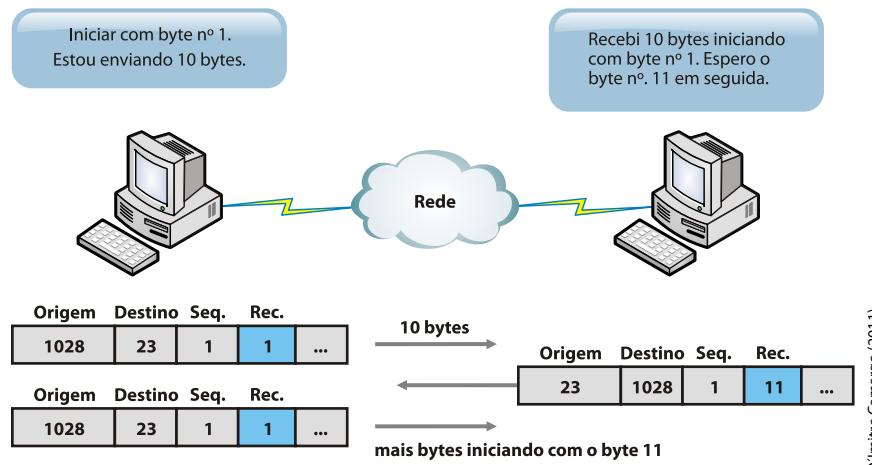


Figura 26 - Ordenando os segmentos
Fonte: Cisco Networking Academy (2011)

Nesta forma de ordenar os segmentos à camada de transporte, é possível garantir que segmentos faltantes sejam reenviados.

4.1.3 ENTREGA CONFIÁVEL

Outro recurso usado pela camada de transporte para garantir confiabilidade na comunicação são as confirmações positivas. Também chamado de confirmações esperadas. Para isso, são usados os números de sequência juntamente com os números de confirmações (ACK). Ao receber os segmentos enviados pela origem, o destino confirma o recebimento destes segmentos pedindo o próximo segmento, ou seja, o próximo segmento é solicitado e com isso, o dispositivo de origem entende que o destino recebeu todos os segmentos anteriores. Vejamos a figura a seguir.



D'Imitre Camargo (2011)

Figura 27 - Confirmação positiva
Fonte: Cisco Networking Academy (2011)

4.1.4 CONTROLE DE FLUXO

A camada de transporte controla e gerencia o fluxo das informações, indicando a quantidade de informação que poderá ser transmitida antes de aguardar uma confirmação de recebimento do destino. A camada de transporte realiza esta função por meio do janelamento. Por exemplo, caso o tamanho da janela seja 3, o dispositivo de origem vai enviar 3 segmentos para o dispositivo de destino e, depois disso, a origem aguarda uma confirmação de recebimento por parte do destino. Após o destino confirmar o recebimento dos 3 segmentos, a origem poderá enviar mais 3 segmentos.

Essa janela é uma janela móvel, também chamada de janela deslizante, ou seja, o valor do tamanho da janela não é fixo. Os valores da janela vão sendo alterados durante a transmissão e, dessa forma, o fluxo de informações vai sendo gerenciado, ocorrendo o controle de fluxo.

Acompanhe um exemplo do controle de fluxo com o janelamento.

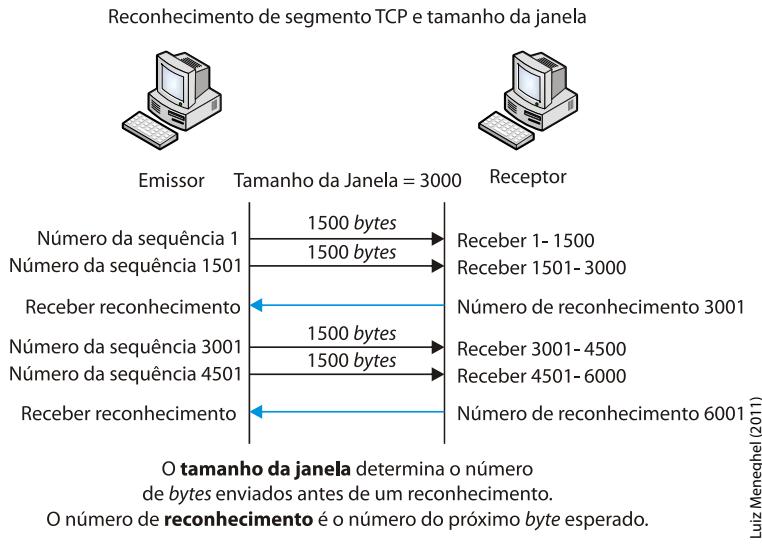


Figura 28 - Controle de fluxo
 Fonte: Cisco Networking Academy (2011)

4.1.5 IDENTIFICAR DIFERENTES APLICAÇÕES

A camada de transporte precisa utilizar uma forma de identificar as diversas comunicações simultâneas que ocorrem entre dispositivos de origem e destino, iguais ou diferentes. Imagine um dispositivo recebendo ao mesmo tempo um e-mail, uma mensagem no MSN e uma página WEB. Como o dispositivo vai saber identificar qual aplicação precisa receber a informação?

Os números de portas são usados para identificar essas comunicações entre diversas aplicações. Quando um dispositivo inicia uma comunicação, ele escolhe um número de porta de origem e outro número de porta de destino. A porta de origem identifica a comunicação na origem, enquanto que a porta de destino vai identificar a aplicação que vai receber a informação no destino. No retorno da comunicação, estes números são trocados. Veja a figura a seguir, identificando os números de portas.

Faixa de números de portas	Grupo de portas
0 a 1023	Portas conhecidas (contato)
1024 a 49151	Portas registradas
49152 a 65535	Portas privadas e/ou dinâmicas

Portas TCP registradas:
 1863 MSN Messenger
 8008 Alternar HTTP
 8080 Alternar HTTP

Portas TCP Conhecidas:
 21 FTP
 23 Telnet
 25 SMTP
 80 HTTP
 110 POP3
 194 Internet Relay Chat (IRC)
 443 HTTP Seguro (HTTPS)

Luiz Meneghel (2011)

Figura 29 - Número de Portas
 Fonte: Cisco Networking Academy (2011)

Conforme você pôde ver na figura, existem três faixas de números de portas. A primeira faixa de 0 a 1023 identifica as portas conhecidas, ou seja, números de portas para aplicações previamente estabelecidas. Veja as principais aplicações e seus números de portas:

Tabela 1 - Principais aplicações

NÚMERO DA PORTA	PROTOCOLO
20 e 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
69	TFTP
80	HTTP
110	POP
143	IMAP
443	HTTPS

A segunda faixa de números de portas, de 1024 a 49151, identifica as portas registradas. Estas identificam processos ou aplicações do usuário, ou seja, aplicações individuais do usuário final. As portas registradas também podem ser usadas dinamicamente, como uma porta de origem do dispositivo que inicia a comunicação. Um exemplo clássico de uma porta registrada é a porta 1863 do MSN.

A terceira faixa de números de portas, de 49152 até 65535, identifica as portas privadas ou dinâmicas. Estes números de portas são geralmente usados dinamicamente por aplicações do dispositivo que inicia a transmissão, apesar de que geralmente estes dispositivos possam usar portas registradas.



**SAIBA
MAIS**

Para saber mais sobre as portas, acesse o site a seguir. Disponível em: <<http://www.iana.org/assignments/port-numbers>> e confira uma lista completa.

Você acabou de conhecer as várias funcionalidades que a camada de transporte utiliza. Viu só como o número da porta é importante para que o dispositivo saiba identificar qual aplicação receberá a informação? Confira, a seguir, os protocolos orientados à conexão e entenda que tipo de serviço é esse.

4.2 PROTOCOLOS ORIENTADOS À CONEXÃO

Como já foi visto neste capítulo, a camada de transporte fornece um serviço orientado à conexão, e o protocolo de camada de transporte que fornece um serviço orientado à conexão é o TCP (*Transmission Control Protocol*). Sendo assim, o TCP aplica todas as funcionalidades de entrega ordenada, confiável e com controle de fluxo vistas anteriormente.

Para utilizar estes recursos de entrega ordenada, confiável e com controle de fluxo, o TCP precisa utilizar uma estrutura de segmento que comporte todas estas funções. Veja no quadro a seguir os campos de um segmento TCP.

Segmento TCP			
Bit (0)	Bit (15)	Bit (16)	Bit (31)
Porta de origem (16)		Porta de destino (16)	
Número de sequência (32)			
Número de reconhecimento (32)			
Comprimento do cabeçalho (4) Reservado (6) Bits de código (6)	Janela (16)		
Checksum (16)	Urgente (16)		
Opções (0 ou 32, se houver)			
DADOS DA CAMADA DE APLICATIVOS (tamanho varia)			



Quadro 4 - Os campos do segmento TCP
Fonte: Cisco Networking Academy (2011)

Confira, a seguir, uma análise dos principais campos do segmento TCP.

- Porta de origem:** campo de 16 bits que contém o número da porta origem.
- Porta de destino:** campo de 16 bits que contém o número da porta de destino.
- Número de Sequência:** campo de 32 bits utilizado para ordenar os segmentos.
- Número de reconhecimento:** campo de 32 bits com o número de confirmação que indica o próximo segmento TCP esperado.
- Comprimento do cabeçalho:** campo de 4 bits que indica o tamanho do cabeçalho do segmento.
- Janela:** campo de 16 bits com o número de segmentos que poderão ser transmitidos antes de aguardar uma confirmação.
- Checksum¹:** campo de 16 bits para o cálculo de verificação de erros.
- Dados:** campo com os dados das camadas superiores.

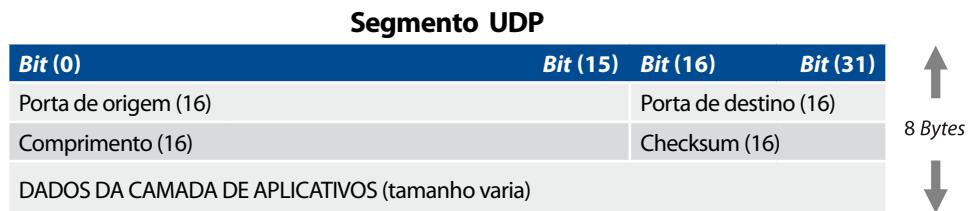
Agora você já sabe o que é um serviço de protocolo orientado à conexão, e conhece os principais campos do segmento TCP. Confira, a seguir, os protocolos não-orientados à conexão e entenda por que é importante estabelecer uma comunicação entre origem e destino de dados.

4.3 PROTOCOLOS NÃO-ORIENTADOS À CONEXÃO

Nem sempre a camada de transporte precisa oferecer um serviço confiável, onde é necessário estabelecer uma comunicação entre origem e destino antes de enviar os dados, bem como, oferecer uma entrega ordenada e com controle de fluxo. Nestes casos, onde a confiabilidade não é necessária, um protocolo não-orientado à conexão poderá ser utilizado.

O protocolo da camada de transporte que oferece serviço não-orientado à conexão é o UDP (User Datagram Protocol) e um exemplo de seu formato pode ser visto no quadro a seguir.

Segmento UDP			
Bit (0)	Bit (15)	Bit (16)	Bit (31)
Porta de origem (16)		Porta de destino (16)	
Comprimento (16)		Checksum (16)	
DADOS DA CAMADA DE APLICATIVOS (tamanho varia)			



Quadro 5 - Exemplo de um segmento UDP
Fonte: Cisco Networking Academy (2011)

Vamos analisar os principais campos do segmento UDP:

- Porta de origem:** campo de 16 bits que contém o número da porta origem.
- Porta de destino:** Campo de 16 bits que contém o número da porta de destino.
- Comprimento:** Campo de 16 bits que indica o tamanho do datagrama, incluindo os dados.
- Checksum:** Campo de 16 bits para o cálculo de verificação de erros.
- Dados:** Campo com os dados das camadas superiores.

Muito interessante esse assunto, não acha? Então, prepare-se, pois ainda vem muito assunto interessante pela frente. Continue acompanhando.

4.4 COMPARANDO O TCP E O UDP

Neste momento, você pode perceber que os protocolos TCP e UDP possuem diferenças e semelhanças. Primeiramente, a função deles é a mesma, ou seja, transportar os dados de camadas superiores entre dispositivos finais e diferenciar as diversas conversações simultâneas por meio dos números de portas.

Ambos os protocolos possuem os campos de números de portas, checksum e dados com funções idênticas. Mas as semelhanças param por aí. Você pode observar que o protocolo TCP possui muito mais campos do que o protocolo UDP, justamente pelo fato do TCP oferecer serviços orientados à conexão com confiabilidade.

Como o TCP possui um cabeçalho muito maior que o UDP (20 e 8 bytes, respectivamente) o *overhead* do protocolo TCP é muito maior, ou seja, o UDP é um protocolo mais leve. Sendo assim, o protocolo UDP poderá ser usado em comunicações onde não seja necessário ter confiabilidade (ou não seja recomendado).



VOÇÊ SABIA?

Os protocolos FTP e TFTP usam respectivamente os protocolos TCP e UDP na camada de transporte, e por este motivo o FTP é confiável e o TFTP não.

Para entender melhor, na prática, os protocolos confiáveis e os não-confiáveis, acompanhe o Casos e relatos a seguir.



CASOS E RELATOS

Protocolos Confiáveis e Não-Confiáveis

Vicente é um desenvolvedor de sistemas que precisa criar uma aplicação para um dos seus clientes. Ele não desenvolveu mecanismos de controle de fluxo, confiabilidade e ordenação das trocas de mensagens que serão necessárias neste aplicativo, mas, pensando em garantir confiabilidade nas comunicações entre o seu aplicativo, Vicente utiliza o protocolo TCP na camada de transporte e, assim, não precisa se preocupar com questões de controle de fluxo e confiabilidade em sua aplicação.

Viu só como é importante saber a diferença entre os protocolos confiáveis e os não-confiáveis? Lembre-se que você vai entendendo cada vez mais sobre esse e outros assuntos conforme for colocando os seus conhecimentos em prática. Até o próximo assunto!



RECAPITULANDO

Neste capítulo, aprendemos vários conceitos da camada de transporte do modelo de referência OSI. Primeiramente, estudamos todas as características desta camada. Depois, estudamos também as características dos protocolos orientados à conexão e vimos as características dos protocolos não-orientados à conexão. Por último, vimos as diferenças e semelhanças entre os protocolos TCP e UDP e quando deve ser usado cada um destes protocolos. No próximo capítulo, vamos estudar as funções da camada de rede do modelo OSI e os principais protocolos que atuam nesta camada.

A Camada de Rede

5



Neste capítulo você estudará a camada de rede do modelo de referência OSI. Para iniciar, é preciso entender os conceitos desta camada, para depois estudar os protocolos IPv4 e IPv6. Em seguida, você conhecerá os protocolos ICMP e ARP, e, para concluir o capítulo, entenderá o significado de domínios de *broadcast*.

Ao final deste capítulo você terá subsídios para:

- a) Conhecer os principais conceitos da camada de rede e os protocolos que atuam nesta camada.

5.1 CONCEITOS DA CAMADA DE REDE

A camada de rede é responsável por endereçar e permitir a transferência de dados da origem até o destino de uma comunicação por meio das diversas redes que podem existir neste caminho. O grande mérito da camada de rede é permitir que os dispositivos se comuniquem pelas diversas redes.

Quando desejamos utilizar uma aplicação que depende de uma comunicação remota ao equipamento que estamos utilizando, precisamos utilizar a interligação existente entre os equipamentos, que é a rede de comunicação.

Nos modelos de referência definidos para a comunicação entre equipamentos há uma camada primordial para o perfeito funcionamento de comunicações por meio das redes, que é a camada de rede. A figura a seguir apresenta uma visão das sete camadas do modelo OSI com destaque para a camada de rede do modelo OSI.

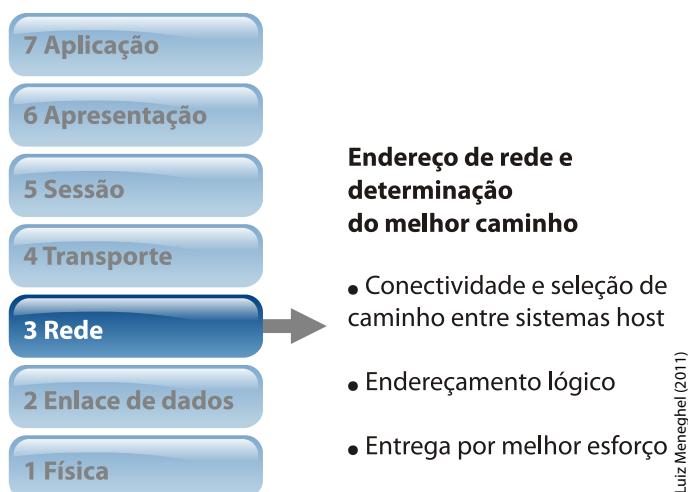


Figura 30 - A Camada de Rede
Fonte: Cisco Networking Academy (2011)

A camada de rede fornece serviços que irão permitir a transferência de dados da origem até o destino em uma comunicação de dados.

Essa camada possui quatro processos básicos bem definidos:

- b) endereçamento – é o processo de definir endereços para os dispositivos existentes em uma rede que permite a comunicação de dados. Existem padrões de endereçamento de acordo com o protocolo de camada de rede utilizado pelo dispositivo.
- c) encapsulamento – é o processo de empacotar, moldar, segmentar o fluxo de dados a ser transmitido pela rede dentro da PDU do protocolo da camada

de rede utilizado. Neste processo, são criados os pacotes com as informações a serem entregues ao destino da comunicação.

- d) roteamento – é o processo que consiste na tarefa de direcionar estes pacotes montados no processo de encapsulamento, por meio da rede de dados. O roteamento é tradicionalmente realizado por dispositivos que trabalham na camada 3 com o intuito de escolher o melhor caminho para a entrega eficiente de cada pacote ao seu destino. Normalmente, esta função é realizada por equipamentos chamados de roteadores.
- e) desencapsulamento – é o processo de desempacotar, retirar o conteúdo de dados constante no pacote recebido e entregar para a camada superior do modelo de referência OSI, no caso, a camada de transporte.

Existem diversos protocolos que foram implementados para atender às funcionalidades básicas desta camada. Estes protocolos foram criados por organismos ou empresas com o intuito de permitir a comunicação em uma rede de dados. Entre eles podemos citar:

- a) IPv4 – *Internet Protocol Versão 4*
- b) IPv6 – *Internet Protocol Versão 6*
- c) IPX – *Novell Network Packet Exchange*
- d) *Appletalk*



VOCÊ SABIA?

Que o protocolo mais utilizado atualmente que implementa a camada de rede é o protocolo IPv4, mas está sendo substituído, gradativamente, pelo protocolo IPv6, em função das necessidades de endereçamento que as redes necessitam para o seu funcionamento?

Além destes protocolos, existem outros que também atuam na camada de rede, mas com a função de auxiliar o protocolo principal a realizar suas funções, como o ICMP e o ARP, que serão vistos mais adiante. Agora, confira o protocolo IPv4.

5.2 IPV4

O protocolo IPv4 é o protocolo mais utilizado atualmente, e que faz a maior rede de comunicação existente hoje (INTERNET) funcionar e permitir todas as facilidades de roteamento e endereçamento necessárias.

¹ RFC

(Request for Comments) são documentos que descrevem os padrões dos protocolos.

Esse protocolo foi especificado ou alterado nas RFCs¹ 791, 950, 919, 922, 1349 e 2474. Uma das grandes características deste protocolo é permitir a sua utilização em qualquer tipo de rede física, permitindo com isso, uma interoperabilidade perfeita entre as diversas tecnologias de redes existentes, exatamente como o modelo de camadas define.

Cada pacote criado pelo IPv4 em uma comunicação, é tratado isoladamente durante toda a sua vida durante o tráfego na rede. Por este motivo, é dito que o IPv4 é um protocolo sem conexão, no qual seus pacotes são tratados e avaliados em cada equipamento por onde os mesmos trafegam.

Por serem tratados de forma isolada durante a comunicação, os pacotes IPs podem ser entregues no destino, não na ordem de saída, por isto, os protocolos das camadas superiores, normalmente a camada de transporte, são responsáveis por ordenar as informações recebidas, justamente como estudado no capítulo 3.

5.2.1 PACOTE IP

O pacote IP, também chamado de datagrama, é a unidade básica de transferência da camada de rede. É ele que define o *layout* dos pacotes a serem transferidos.

Dois componentes básicos estão presentes no pacote IP. Veja um exemplo a seguir.



Figura 31 - Componentes básicos do datagrama

Confira o que é cada um dos componentes:

- a) cabeçalho – é o conjunto de campos que definem diversas propriedades do pacote, permitindo com isso, o encaminhamento do pacote de forma correta até o destino.
- b) dados – é o conjunto de dados recebidos da camada superior para a camada de rede, no caso, o segmento da camada de transporte.

O cabeçalho de um pacote IP é composto por diversos campos que são utilizados para permitir o endereçamento e roteamento correto dos pacotes pela rede. Observe na figura a seguir, os campos de um pacote IP.

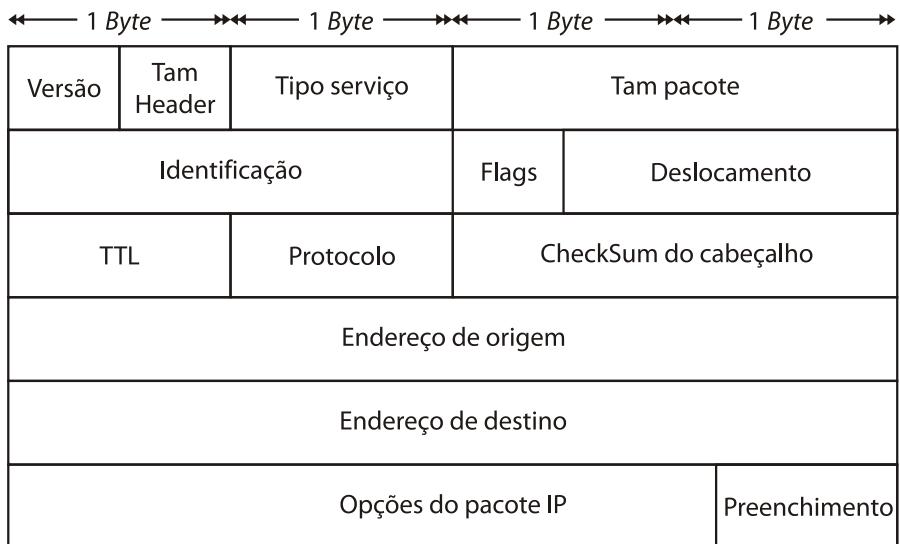


Figura 32 - Campos do pacote IP

Veja uma análise dos principais campos do pacote IP.

- Versão:** versão do protocolo, no caso 4.
- Tamheader:** corresponde ao tamanho do cabeçalho contado em números de palavras de 32 bits (4 bytes).
- Tipo serviço:** é o campo que contém a indicação de qualidade do serviço desejado para o encaminhamento do pacote. Esse campo possui 8 bits.
- Tampacote:** campo que contém o tamanho do pacote em quantidade de octetos (bytes). O valor máximo é 65.535 bits.
- Identificação:** é o campo preenchido pela origem do pacote que o identifica. É utilizado na montagem da sequência dos pacotes no destino. Um pacote que precisa ser fragmentado por outro equipamento no caminho até o seu destino, utiliza, neste campo, o mesmo valor para todos os fragmentos resultantes.
- Flags:** campo de 3 bits que identifica se o pacote pode ser fragmentado no caminho até o destino e também se já ocorreu fragmentação. O primeiro bit é sempre 0, o segundo bit indica se pode ou não fragmentar (0 = pode fragmentar, 1 = não pode fragmentar), e o terceiro bit indica se este pacote é (1) ou não é (0) o último fragmento.
- Deslocamento:** caso tenha ocorrido fragmentação, este campo indica o deslocamento dos dados do pacote em relação ao campo de dados do pacote original (antes da fragmentação). Este campo é primordial para a remontagem do pacote e considera como unidade um octeto (1byte).

- h) **TTL (Time to live)**: representa a quantidade de saltos por onde um pacote pode trafegar. Cada ativo de rede que roteia este pacote diminui o TTL de 1, sendo descartado quando este valor chega a zero.
- i) **Protocolo**: campo preenchido com um valor numérico que identifica para qual protocolo da camada superior a camada de rede deve entregar o conteúdo deste pacote, no momento em que o mesmo chegar ao destino. Exemplo: 6 – TCP, 17 – UDP, 1 – ICMP, 89 – OSPF, etc.
- j) **CheckSum do cabeçalho**: é o campo calculado e checado para cada salto que o pacote passa na rede, a fim de verificar a integridade do cabeçalho.
- k) **Endereço de origem**: é o endereço de origem do pacote, composto por 32 bits. banco (DE AVA - Gerenciamento)
- l) **Endereço de destino**: é o endereço de destino do pacote, composto por 32 bits.
- m) **Opções do pacote IP**: este campo é opcional, mas requerido para algumas implementações. A origem do pacote colocará nesse campo as opções selecionadas. Esse campo é variável em seu tamanho e vai depender das opções definidas pela origem.
- n) **Preenchimento**: é o campo para preencher o cabeçalho mantendo sempre o alinhamento do mesmo em 32 bits.

Nesse item, você conferiu, detalhadamente, os campos presentes no pacote IP. Agora, você estudará como é feito o endereçamento para o protocolo IPv4. Acompanhe!

5.2.2 ENDEREÇAMENTO IPV4

As redes encontram-se quase que todas interligadas e consistem normalmente em uma quantidade enorme de hosts e equipamentos de redes. O melhor exemplo desta integração é a Internet. Hoje temos milhões de hosts interligados por meio da Internet, trocando informações.

Um dos principais pontos que permitiram esta integração, que hoje parece tão fácil e normal, foi a estrutura de endereçamento existente no protocolo IPv4.

Quando o protocolo foi idealizado, consideraram-se diversos requisitos, como, por exemplo:

- a) cada host deverá ter um endereço único na rede;
- b) as redes poderão ser divididas em sub-redes para melhor gerenciamento e interligação de redes diferentes;

c) possibilidade de enviar informações para diversos hosts com o envio de apenas um pacote.

O endereçamento do IPv4 possui diversas características importantes que auxiliam no atendimento de alguns destes requisitos.

Uma das grandes características do endereçamento IPv4 é ser hierárquico, ou seja, conseguir identificar em uma rede cada host de maneira única e permitir com isso que, ao juntarmos redes, as mesmas consigam identificar em que parte da rede este equipamento se encontra e, a partir dos *gateways* e roteadores, conseguir entregar os pacotes ao seu destino. Podemos fazer uma analogia com o endereçamento postal, onde em qualquer endereço temos uma hierarquia que permite com que as cartas consigam ser entregues aos seus destinos.

Acompanhe uma análise do endereço do SENAI²:

Nível 6 → nº 2765

Nível 5 → Rod. Admar Gonzaga

Nível 4 → Bairro Itacorubi

Nível 3 → Florianópolis

Nível 2 → SC

Nível 1 → Brasil

Para cada nível apresentado acima, podemos considerar como um nível hierárquico dentro de uma estrutura, a partir do qual, é possível que as correspondências cheguem ao destino. Veja um exemplo na figura a seguir.

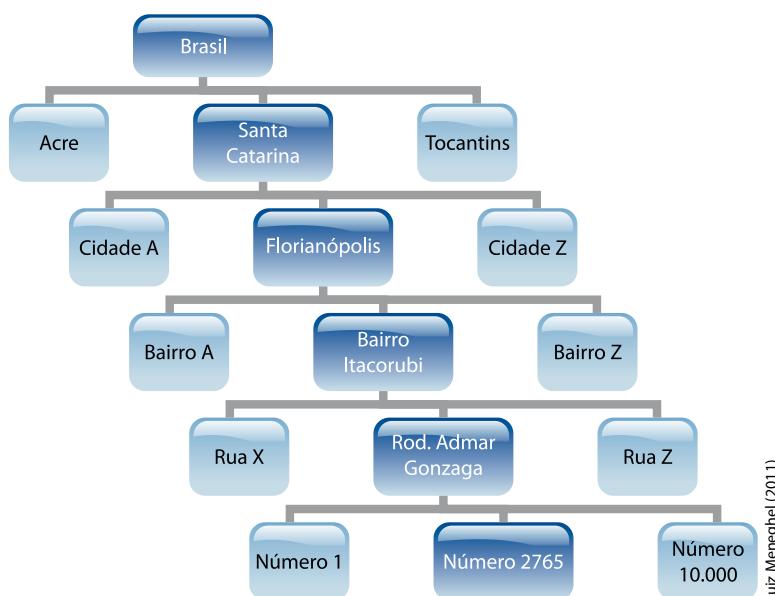


Figura 33 - Estrutura hierárquica

O endereçamento IP também segue uma estrutura hierárquica permitindo, do mesmo modo como no endereçamento postal, a localização do destino a ser alcançado. O endereço IP é representado por um conjunto de 32 bits que identificam exclusivamente o equipamento em uma rede.

O endereço IP também é representado pela divisão dos 32 bits em 4 octetos. Assim:

11000000.00001010.00001010.00000001

Estes bits podem também ser representados em formato decimal, chamado de notação decimal, separada por pontos. Por exemplo:

192.10.10.1

Este endereço é utilizado nos pacotes IPs nos campos de origem e destino para identificar o dispositivo de origem e destino do pacote. No endereçamento hierárquico do IP, o endereço dos dispositivos são divididos em duas partes, uma parte rede e a outra, Host. Veja um exemplo na figura a seguir.

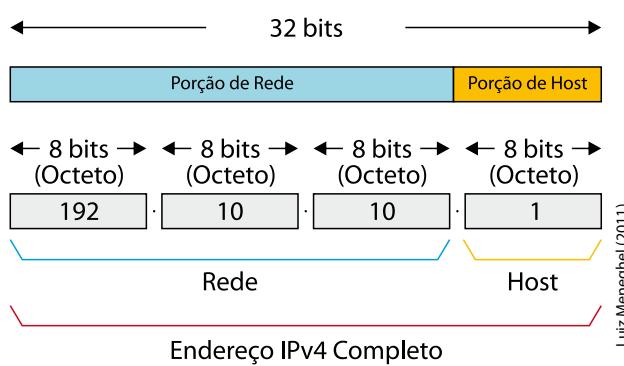


Figura 34 - Endereço IPv4
Fonte: Cisco Networking Academy (2011)

Luis Meneghel (2011)

Considerando a estrutura hierárquica, a parte rede de um endereço identifica a rede à qual pertence este dispositivo, sendo que, todos os equipamentos que pertencem à mesma rede terão esta parte do seu endereço IP iguais.

Quando os equipamentos de rede precisam descobrir como entregar os pacotes aos seus destinos, eles analisam a parte de rede do endereço. Esta, por sua vez, utiliza uma quantidade variável de bits, representada pela máscara de rede. Por exemplo:

192.10.10.1 / 24 – indica que os primeiros 24 bits do endereço representam a parte de rede deste endereço.

192.10.10.1 máscara de rede 255.255.255.0 – também identifica que os primeiros 24 bits do endereço representam a parte rede do endereço. Esta é a forma decimal da máscara.

Nessa etapa, você conferiu o que é um pacote IP e conheceu a estrutura hierárquica do endereçamento do protocolo IPv4. Todas essas informações são fundamentais para o seu dia a dia, porém, as informações não param por aqui. Acompanhe, a seguir, as classes de endereços IP.

5.3 CLASSES DE ENDEREÇOS IP

Os endereços IPs foram separados por classes criadas (A, B, C, D e E), acomodando todos os IPs possíveis. As classes A, B e C são usadas comercialmente na atribuição de endereços IPs aos dispositivos de rede. A classe D é usada para endereçamento *multicast*, conforme visto no capítulo 2, onde um único endereço representa um grupo específico de dispositivos. A classe E é utilizada para fins experimentais pela IANA³(*Internet Assigned Numbers Authority*).

Confira a demonstração das classes A, B, C e D na figura a seguir.

Tabela 2 - Classes de endereçamento IP

Classe A	Rede	Host		
OCTETO	1	2	3	4
Classe B	Rede	Host		
OCTETO	1	2	3	4
Classe C	Rede	Host		
OCTETO	1	2	3	4
Classe D	Host			
OCTETO	1	2	3	4

Os endereços de Classe D são usados para grupos *multicast*. Não é necessário alocar octetos ou bits para separar os endereços de rede e host. Os endereços de Classe E são reservados apenas para pesquisas.

Assunto interessante esse, não é mesmo? Que tal estudar um pouco mais sobre as classes A, B e C? Então, siga em frente!

Conforme você pôde observar na tabela das classes de endereçamento de IP, a classe A utiliza somente um octeto para identificar redes, sendo assim, sobram 3 octetos para identificar hosts. A classe A é uma classe para ser utilizada em redes onde a quantidade de hosts é muito grande, acima de 65534 hosts. O primeiro bit de uma rede classe A sempre será o *bit 0* (bit de ordem superior), sendo assim, poderemos ter números de 0 até 127 no primeiro octeto. Redes que comecem com 0 ou com 127 não podem ser usadas porque são reservadas para a rede padrão e endereços de *loopback* respectivamente, conforme você poderá ver na tabela seguinte (Detalhes das classes de endereçamento IP).



FIQUE ALERTA

A regra para identificar os números de hosts válidos é $2^n - 2$, onde "n" é o número de bits do campo de hosts e o "-2" é para retirar o endereço de rede e de broadcast que são endereços reservados.

Endereços de classe B utilizam os dois primeiros octetos para identificar redes e os outros dois octetos restantes representam os hosts. As redes de classe B são usadas para endereçar redes de médio à grande porte. Os primeiros dois bits de uma classe B sempre serão 10 (bits de ordem superior), sendo assim, poderemos ter até 16.384 redes.

O primeiro octeto em decimal sempre estará entre 128 e 191. Como sobraram 16 bits (dois octetos) para representar hosts, poderemos ter até 65534 endereços possíveis em uma classe B, conforme apresentado na tabela seguinte.

Já os endereços de classe C utilizam os três primeiros octetos para representar redes e somente o último octeto para representar hosts. Por este motivo, existe uma grande quantidade de redes classes C, onde cada rede destas poderá ter 254 endereços. Os primeiros três bits de uma classe C sempre serão 110 (bits de ordem superior), sendo assim, o primeiro octeto utilizará um número decimal de 192 até 223. Veja o detalhamento das classes de endereçamento IP na tabela.

Tabela 3 - Detalhes das classes de endereçamento IP

Classe de Endereços IP

CLASSE DE ENDEREÇOS	FAIXA DO PRIMEIRO OCTETO (DECIMAL)	BITS DO PRIMEIRO OCTETO*	REDE <small>N</small> E HOST <small>H</small> PARTES DO ENDEREÇO	MÁSCARA DE SUB-REDE PADRÃO (DECIMAL E BINÁRIO)	NÚMERO DE REDES POSSÍVEIS E HOSTS POR REDE
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 redes (2^7) 16,777,214 hosts por rede (2^{24-2})
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 redes (2^{14}) 65,534 hosts por rede (2^{16-2})
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 redes (2^{21}) 254 hosts por rede (2^{8-2})
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

*Bits verdes não mudam

Fonte: Cisco Networking Academy (2011)

Nessa tabela, é possível observar os intervalos do primeiro octeto em binário e decimal, a quantidade de octetos para rede e para hosts e o número de redes e hosts possíveis para cada classe. Outra informação de fundamental importância para o endereçamento IP é a máscara de rede que também é apresentada para as classes A, B e C. Observe que a função da máscara de rede é identificar a quantidade de bits que identificam o campo de rede com os bits na posição 1 (um), e a quantidade de bits que representam os hosts com os bits na posição 0 (zero).

Esses são os endereçamentos IP. Na próxima etapa, você estudará o significado de endereços públicos e privados.

5.4 ENDEREÇOS PÚBLICOS E ENDEREÇOS PRIVADOS

Uma forma de não esgotar rapidamente os endereços IPs foi a adoção da RFC 1918. Esta RFC cria um padrão para uso de faixas reservadas de endereços IPs para redes internas e privadas. Para cada classe de uso comercial, foi atribuído um grupo de endereços privados de uso exclusivo a redes internas.

Veja, na tabela a seguir, os endereços reservados para uso privado.

Tabela 4 - Endereços Privados

CLASSE	INTERVALO DE ENDEREÇOS INTERNOS RFC 1918
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Fonte: Cisco Networking Academy (2011)

As redes privadas poderão utilizar quaisquer endereços da RFC 1918 descritos na figura, desde que sejam exclusivos internamente nesta rede. Os endereços privados da RFC 1918 não são roteados pela Internet, ou seja, os roteadores de borda dos ISP (*Internet Service Provider*) não encaminharão pacotes pela Internet que contenham endereços da RFC 1918. **Resumindo, os endereços privados só poderão ser utilizados em redes internas.**

Para que os dispositivos finais de uma rede interna possam navegar na Internet será necessário o uso do NAT (*Network Address Translation*). O NAT fará a tradução de um endereço privado para um endereço público para que o pacote possa ser destinado à rede pública, sendo assim, o pacote será roteado até o destino final. Você verá com mais detalhes o NAT mais adiante, neste curso.

Os endereços públicos serão todos os endereços contidos dentro das classes A, B e C que não fazem parte da RFC 1918. Os endereços IP públicos precisam ser obtidos de um ISP ou por meio do registro “.br”.



**SAIBA
MAIS**

Para saber mais sobre registros de domínios no Brasil, acesse o endereço <<http://registro.br/>>.

Como você viu, os endereços privados só podem ser utilizados em redes internas, e, para que o endereço possa ser utilizado em uma rede pública, o NAT precisa fazer a tradução do endereço privado para público. Esse tópico finaliza as informações sobre o protocolo IPv4. Acompanhe, agora, as informações sobre o protocolo IPv6.

5.5 IPV6

Com a evolução das redes, dos novos dispositivos móveis, das populações de todos os países tendo acesso à Internet, houve a necessidade de muitos endereços de redes, para permitir o endereçamento de todos esses equipamentos.

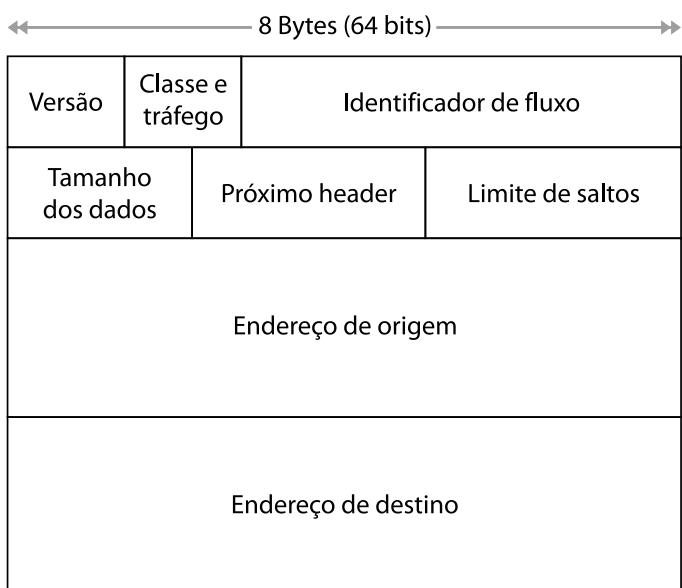
O endereçamento IPv4 em uso em todas as redes, não foi projetado para suportar toda essa necessidade de endereçamento, tornando-se esse um dos principais motivos do desenvolvimento de outro protocolo. Além das questões de endereçamento, muitas questões que não eram suportadas de forma nativa no IPv4 foram incorporadas ao novo protocolo.

Foi criado, então, o protocolo IPv6, com as seguintes características:

- a) maior espaço de endereçamento;
- b) mobilidade;
- c) segurança;
- d) auto configuração.

5.5.1 O PACOTE IPV6

O pacote IPv6, também chamado de datagrama, é composto por duas partes: o cabeçalho e os dados. Uma das grandes diferenças entre as versões do protocolo IP é o cabeçalho do pacote, que no IPv6 é mais simples e otimizado para agilizar o seu encaminhamento através das redes. Veja um exemplo de um pacote IPv6:



Luiz Meneghel (2011)

Figura 35 - Pacote IPv6

Confira, a seguir, cada um dos campos do pacote IPv6.

- a) **Versão:** é a versão do protocolo, no caso, 6.
- b) **Classe tráfego:** indica a prioridade deste pacote.
- c) **Identificador de fluxo:** QoS (*Quality of services*).
- d) **Tamanho dos dados:** informa o tamanho da parte de dados do pacote IPv6.
- e) **Próximo header:** é o campo que aponta para o próximo *header* do IPv6. Esta característica de possuir mais de um *header* foi criada para simplificar o cabeçalho padrão e, caso sejam necessárias funções especiais, cabeçalhos extras são alocados e inseridos na parte de dados do pacote IP.
- f) **Limite de saltos:** oficializando o que já acontecia com o campo TTL do IPv4, este campo limita a quantidade de dispositivos que roteiam os pacotes por onde este pacote pode passar. Caso este número chegue a zero, o pacote é descartado.
- g) **Endereço de origem:** é o endereço do dispositivo de origem representado por um campo de 128 bits.
- h) **Endereço de destino:** é o endereço do dispositivo de destino representado por um campo de 128 bits.

5.5.1 ENDEREÇAMENTO IPV6

Com relação ao endereçamento, o IPv6 utiliza 128 bits, gerando $3.4 * 10^{38}$ possíveis endereços.

Do mesmo modo que no IPv4, a representação do endereçamento não é realizada em binário representando todos os bits, pois isto seria muito difícil de representar. No IPv6, a representação do endereço é feita por meio do agrupamento de 16 em 16 bits separados por ":" (dois pontos).

Estes grupos de 16 bits são representados utilizando a notação hexadecimal, sendo que cada dígito hexadecimal representa 4 bits separados.

Então temos:

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

onde X é um dígito hexadecimal que pode ser representado pelos valores (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F)

Exemplo:

2001:0000:130F:0000:0000:01B1:2341:AA45

FF01:0000:0000:0000:0000:0000:0000:0001

Caso nos grupos de 16 bits existam valores 0 à esquerda do número, no momento da representação, estes 0s podem ser suprimidos. Por exemplo: 001A pode ser escrito com 1A.

Veja outro exemplo:

2001:0000:130F:0000:0000:**1A**:2341:AA45

Também, se tiver grupos de 4 dígitos sendo que todos os dígitos são 0, e estes grupos forem sucessivos, podemos representar apenas com o separador ":" em sequência.



FIQUE ALERTA

Esta característica de suprimir a apresentação dos 0s só pode ocorrer em uma sequência no endereço.

Exemplo:

Considerando o endereço 2001:0000:130F:0000:0000:01B1:2341:AA45 podemos representar este endereço da seguinte maneira:

2001::130F:0000:0000:01B1:2341:AA45 ou 2001:0000:130F::01B1:2241:AA45

Mas, atenção! Estará **errado** se representarmos 2001::130F::01B1:2341:AA45

O endereçamento IPv6 especifica 3 tipos de endereços possíveis: *Unicast*, *Anycast* e *Multicast*.

- a) **Unicast:** endereça apenas uma interface, ou seja, não há mais de uma interface “respondendo” ao mesmo endereço.
- b) **Anycast:** endereça um conjunto de interfaces de múltiplos dispositivos, mas, um pacote endereçado a um endereço *anycast* só será entregue para um dos elementos deste grupo. O elemento que receberá este pacote será o elemento com menor métrica para ser alcançado. Existem diversas utilidades para este tipo de endereço, podemos citar: servidores de um serviço que é servido por mais de um servidor, o servidor mais próximo da origem irá atender a esta solicitação.
- c) **Multicast:** do mesmo modo que no endereço *anycast*, o endereço *multicast* endereça um conjunto de interfaces, a grande diferença é que o pacote endereçado para um endereço *multicast* é entregue para todas as interfaces. As funcionalidades de *multicast*, são análogas às funcionalidades já existentes no IPv4.



**FIQUE
ALERTA**

Segundo *Cisco Networking Academy* (2011), com relação ao endereço de *loopback*, assim como ocorre no IPv4, foi fornecido um endereço IPv6 de *loopback* especial para testes. Os pacotes enviados para esse endereço retornam para o dispositivo de origem. Entretanto, existe apenas um endereço no IPv6 para essa função, e não um bloco inteiro. O endereço de *loopback* é 0:0:0:0:0:0:1, normalmente expresso com o uso da compressão do zero com o “::1.”

No IPv4, um endereço IP somente com zeros tem um significado especial. Ele se refere ao próprio host e é usado quando um dispositivo não souber seu próprio endereço. No IPv6, esse conceito foi formalizado, e o endereço somente com zeros (0:0:0:0:0:0:0) recebe o nome de endereço “não especificado.”

Esse tipo de endereço é usado, normalmente, no campo de origem de um pacote, o qual é enviado por um dispositivo que busca ter seu endereço IP configurado. É possível aplicar a compressão de endereços a esse endereço. Como somente contém zeros, ele se tornará simplesmente “::”.

Ainda segundo *Cisco Networking Academy* (2011), os endereços do IPv6 usam identificadores de interface para identificar as interfaces em um link. Considere-os como a “porção de host” de um endereço IPv6. Os identificadores de interface devem ser exclusivos em um link específico. Os identificadores de interface são sempre de 64 bits e são derivados dinamicamente de um endereço de Camada 2 (endereço MAC).

Você pode atribuir uma ID de endereço IPv6 estática ou dinamicamente:

- atribuição estática usando uma ID de interface manual;

- b) atribuição estática usando uma ID de interface EUI-64;
- c) configuração automática sem estado;
- d) DHCP para IPv6 (DHCPv6).



Para saber mais sobre esse assunto, dê uma olhada nas RFCs 1752 e 2460. Você tem acesso a elas, e outras mais, no site <<http://www.rfc-editor.org/>>

Nesse item você viu como escrever um endereço IPv6, utilizando os ":" (dois pontos), e conheceu, também, os três tipos possíveis de endereços: *Unicast*, *Anycast* e *Multicast*. O próximo item trata sobre o ICMP. Acompanhe!

5.6 INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

O ICMP é um protocolo que também opera na camada 3 do modelo OSI, porém, não é utilizado para a transmissão de dados, mas sim, como protocolo de controle, auxiliando o perfeito funcionamento do protocolo IP.

Quando executamos um *ping* ou *traceroute* nos roteadores ou computadores, estamos utilizando o protocolo ICMP.

O ICMP tem como funcionalidade permitir que roteadores interligados em redes possam informar erros ou problemas inesperados ocorridos durante a transmissão de pacotes.

Pode ser usado para comunicar um dispositivo final com um roteador ou com outro dispositivo final, tendo como vantagem, a utilização de um único mecanismo para todas as mensagens de controle e de informação. Tecnicamente falando, o ICMP é um mecanismo que informa os erros, possibilitando que os roteadores possam avisar destes aos transmissores, porém, o ICMP não especifica totalmente a ação a ser realizada no caso de um erro.

Suponha que, durante a transmissão, um pacote passa por vários roteadores intermediários até R1. Caso R1 receba informações erradas sobre o roteamento, este pacote irá para um roteador errado RN. Logo, RN não tem condições de enviar as informações de erro a R1, e sim ao transmissor do pacote. Pode-se concluir que, o transmissor não possui qualquer influência sobre os problemas de roteamento que possam vir a acontecer, bem como não consegue determinar qual roteador causou o problema.

Veja os tipos de mensagens implementados pelo protocolo ICMP.

TIPO	CÓDIGO	DESCRIÇÃO
0	0	<i>echo reply</i>
	0	<i>destination unreachable</i>
	0	<i>network unreachable</i>
	1	<i>host unreachable</i>
	2	<i>Protocol unreachable</i>
	3	<i>port unreachable</i>
	4	<i>fragmentation needed but don't-fragment bit set</i>
	5	<i>source route failed</i>
	6	<i>destination network unknown</i>
3	7	<i>destination host unknown</i>
	8	<i>source host isolated (obsolete)</i>
	9	<i>destination network administratively prohibited</i>
	10	<i>destination host administratively prohibited</i>
	11	<i>network unreachable for TOS</i>
	12	<i>host unreachable for TOS</i>
	13	<i>communication administratively prohibited by filtering</i>
	14	<i>host precedence violation</i>
	15	<i>precedence cutoff in effect</i>
4	0	<i>source quench (controle de fluxos)</i>
		<i>redirect</i>
	0	<i>redirected for network</i>
5	1	<i>redirect for host</i>
	2	<i>redirect for type-of-service and network</i>
	3	<i>redirect for type-of-service and host</i>
8	0	<i>echo request</i>
9	0	<i>router advertisement</i>
10	0	<i>router solicitation</i>
		<i>time exceeded</i>
11	0	<i>time-to-live equals 0 during transit</i>
	1	<i>time-to-live equals 0 during reassembly</i>
		<i>parameter problem</i>
12	0	<i>ip header bad</i>
	1	<i>required option missing</i>
13	0	<i>timestamprequest</i>
14	0	<i>timestampreply</i>
15	0	<i>informationrequest</i>
16	0	<i>informationreply</i>
17	0	<i>address mask request</i>
18	0	<i>address mask reply</i>

Quadro 6 - Tipos e Códigos das mensagens ICMP

Como você pôde acompanhar nesse item, o ICMP permite que roteadores informem erros ou problemas inesperados durante a transmissão de dados, e confere alguns códigos e mensagens ICMP. Agora, conheça o protocolo ARP.

5.7 ADDRESS RESOLUTION PROTOCOL (ARP)

A RFC826 apresenta o protocolo ARP (*Address Resolution Protocols*) que implementa uma funcionalidade que permite aos equipamentos na rede conseguirem mapear os endereços lógico e físico.

Mas, você sabe porque precisamos do endereço físico? Em uma comunicação a ser enviada em uma rede, além do endereço lógico (tradicionalmente endereço de camada de rede IPv4 ou IPv6), precisamos saber qual o endereço físico para onde os dados deverão ser enviados, permitindo a entrega dos mesmos ao seu destino.

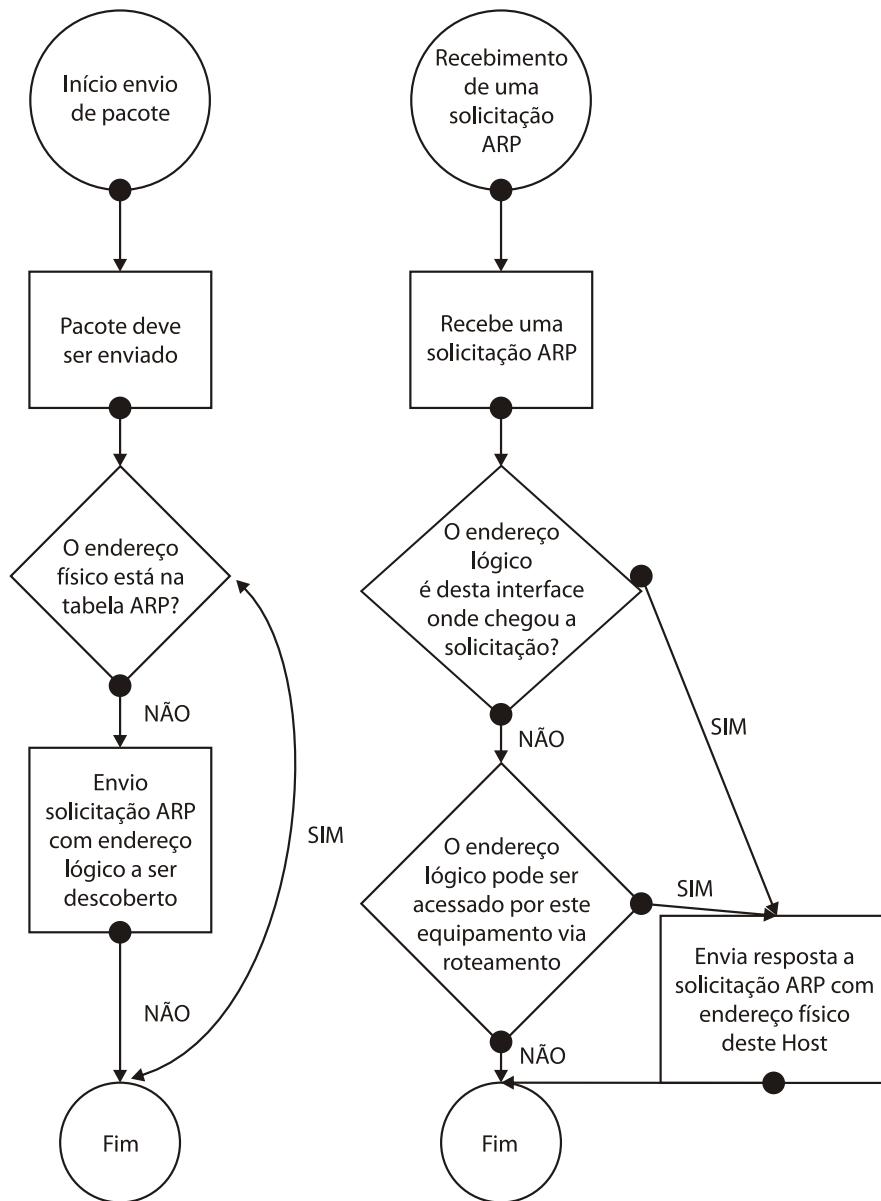
O protocolo ARP, apesar de auxiliar diretamente o protocolo da camada de rede, é um protocolo da camada de enlace.

Quando um dispositivo deseja obter o endereço físico de outro dispositivo é montada uma mensagem do tipo *broadcast*. Internamente nesta mensagem é colocado o endereço lógico (camada de rede), e essa mensagem é enviada pela rede.

O dispositivo que possuir o endereço lógico apresentado na mensagem, ou a rota para acessar aquele endereço, retornará com outra mensagem indicando o endereço físico para onde devem ser direcionados os pacotes.

Para minimizar o tráfego de *broadcast* na rede, os equipamentos implementam uma tabela ARP que armazena temporariamente a associação entre os endereços físicos e lógicos conhecidos pelos dispositivos. Com isso, antes de enviar uma solicitação ARP, o dispositivo verifica em sua tabela ARP se já não tem a informação necessária.

Observe o fluxo das solicitações ARP na figura a seguir.



Luiz Meneghel (2011)

Figura 36 - Fluxo de solicitações ARP

Como você viu, para garantir a entrega dos dados, é preciso saber o endereço físico para onde elas serão enviadas. É aí que entra o protocolo ARP. No próximo item, você conhecerá uma forma de comunicação para rede local.

5.8 DOMÍNIOS DE BROADCAST

Um *broadcast* é uma forma de comunicação em uma rede local, que tem como característica enviar uma informação para todos os equipamentos que estão alcançáveis por meio dessa rede. Essa forma de comunicação é muito utilizada por diversos protocolos, como o ARP e DHCP, entre outros, para auxiliar no funcionamento normal das redes. Um domínio de *broadcast* é representado exatamente pelos equipamentos que pertencem a um mesmo domínio de *broadcast*, ou seja, equipamentos que, caso um deles envie um *broadcast*, todos os outros receberão e terão conhecimento de seu conteúdo.

A interligação entre os equipamentos de um mesmo domínio de *broadcast* é obrigatoriamente realizada por dispositivos de camada 1 (fios, cabos, hubs) ou dispositivos de camada 2 (*bridge* e *switches*). Um domínio de *broadcast* é quebrado por um dispositivo acima da camada 2, por exemplo: roteadores, hosts, etc.

Você pode ver, na figura a seguir, um roteador separando dois domínios de *broadcast*.

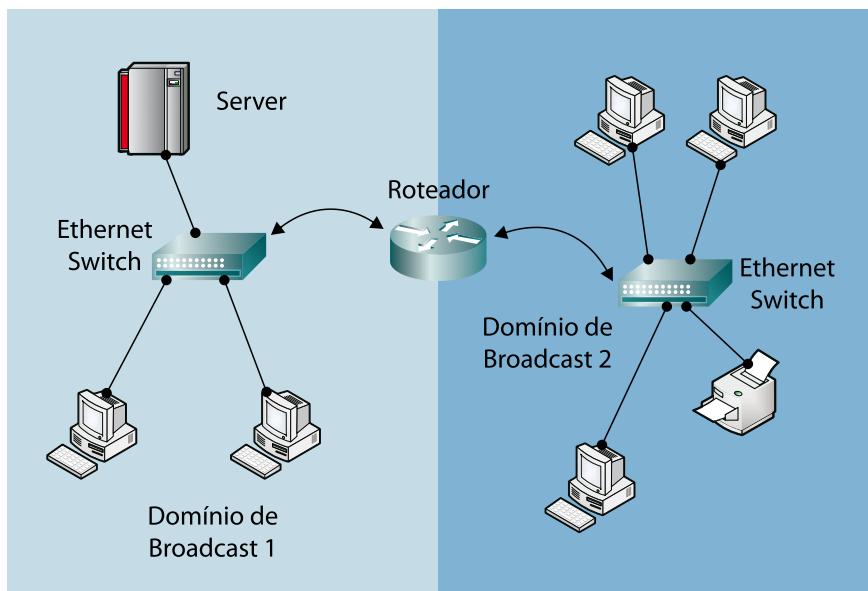


Figura 37 - Domínios de *broadcast* separados por roteador

Luiz Meneghel (2011)



**VOCÊ
SABIA?**

Um switch que seja segmentado em VLAN (LANS virtuais) criará um domínio de *broadcast* para cada LAN.

Para compreender melhor sobre o assunto *Broadcast*, acompanhe o caso relatado a seguir.



CASOS E RELATOS

Como quebrar grandes domínios de *Broadcast*

Gustavo trabalha em um escritório de advocacia como gerente da rede, e, como a quantidade de equipamento estava aumentando rapidamente, ficou preocupado com o impacto que isso teria na rede e em como ele poderia garantir a *performance*. Relendo as anotações realizadas no diário de engenharia, que ele confeccionou durante o curso no SENAI, lembrou que o maior ofensor para a *performance* da rede local seria o tamanho do domínio de *broadcast*. Lembrou então, que o professor Fábio salientou na aula que a melhor forma de dividir o domínio de *broadcast* seria com a utilização de um equipamento de uma camada superior de enlace que o divida, como um roteador ou um *firewall*, por exemplo.

Gustavo, certo das informações aprendidas no SENAI, incluiu em sua rede um roteador, diminuindo com isso o domínio de *broadcast* e melhorando com isso a *performance* da rede.

Ficou bem mais fácil de entender com esse Casos e relatos, não é mesmo? É um exemplo prático que você poderá aplicar quando for necessário

No próximo capítulo, vamos estudar as características e funcionalidades implementadas na camada de enlace de dados do modelo OSI.



RECAPITULANDO

Nesse capítulo, você conheceu os principais conceitos da camada e sua importância para toda a comunicação em uma rede. Foram detalhados os protocolos que permitem a entrega dos dados em uma rede, e, com a descrição dos protocolos IPv4 e do IPv6 e seu funcionamento, ficou muito mais fácil entender o porquê da necessidade de evolução que hoje está sendo implementada. Por fim, você estudou a importância de alguns protocolos, como o ICMP e o ARP, que auxiliam no processo de roteamento dos pacotes nas redes e o conceito de domínios de *broadcast*.

A Camada Enlace

6



Ainda, dentro do modelo de referência OSI, neste capítulo você estudará a camada enlace, que é responsável por preparar os pacotes da camada da rede para serem enviados pelos diversos meios físicos existentes nas redes. Primeiramente, você verá os conceitos da camada de enlace, e, depois, as diversas tecnologias de redes locais, com foco nas redes Ethernet. Por fim, entenderá o conceito de domínio de colisão.

Ao final desse capítulo, você terá subsídios para:

- a) conhecer os principais conceitos e tecnologias existentes na camada de enlace.

6.1 CONCEITOS DA CAMADA DE ENLACE

A camada de enlace tem como principal função fornecer um meio de comunicação comum para a troca de dados entre equipamentos. Essa camada possui algumas funções básicas. Confira:

- a) possibilitar às camadas superiores o acesso ao meio físico disponível, utilizando técnicas e métodos de enquadramento compatíveis com o meio;
- b) utilizar técnicas que permitam o perfeito acesso ao meio;
- c) detectar erros nos quadros recebidos, garantindo a integridade dos dados no nível básico.

Na figura a seguir, você pode observar a localização da camada de enlace de dados no modelo de referência OSI.

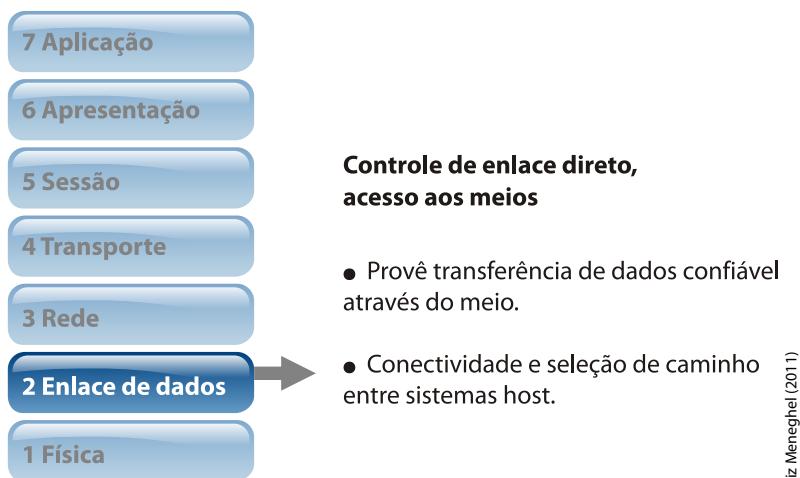


Figura 38 - Visão da camada de enlace no modelo de referência OSI
Fonte: Cisco Networking Academy (2011)

Luiz Meneghel (2011)

Seguindo a premissa de garantir a independência das camadas e do modelo de camadas, a camada de enlace gera para as camadas superiores a independência sobre que meio estará sendo utilizado para transportar os dados.

Acompanhe o relato descrito a seguir para entender melhor.



CASOS E RELATOS

A camada de enlace em um acesso à Internet

Tiago resolveu comprar um notebook e aproveitou para tirar algumas dúvidas na loja sobre o acesso à Internet. Como o Pedro, que é o administrador de redes da loja estava perto de Tiago e do vendedor, aproveitou para explicar a Tiago como funciona. A dúvida de Tiago era, após conectar um notebook pela rede sem fio, qual a diferença em utilizar a rede sem fio e a rede cabeada, e como o notebook consegue entender se precisa utilizar o cabo ou a rede sem fio? Pedro explica para o usuário que os computadores utilizam camadas para trocar informações entre origem e destino e que a camada de enlace é responsável pela codificação dos bits de dados a serem transmitidos, ou seja, quando o notebook está configurado para rede sem fio, a placa de rede codifica os dados em sinais de radiofrequência, e quando o notebook está configurado para usar a rede cabeada, a placa de rede codifica os bits de dados em sinais elétricos. Pedro explica ainda que a placa de rede é um dispositivo de camada de enlace, ou seja, transferência de dados com as redes funcionam independentes do meio físico utilizado.

Com essa explicação, Tiago sai da loja satisfeito com sua compra, e com as explicações recebidas de Pedro.

É importante salientar que, a cada segmento de rede por onde os dados transportados passam, o quadro e a forma de acesso ao meio podem ser totalmente diferentes, mas os dados que estão sendo transportados não precisam ser modificados.

Veja o exemplo a seguir de uma simples navegação para acesso a um site na Internet. O trajeto para que a solicitação chegue até o destino pode passar por diversos meios, sendo que, em cada “pedaço” de rede, o quadro pode ser diferente.

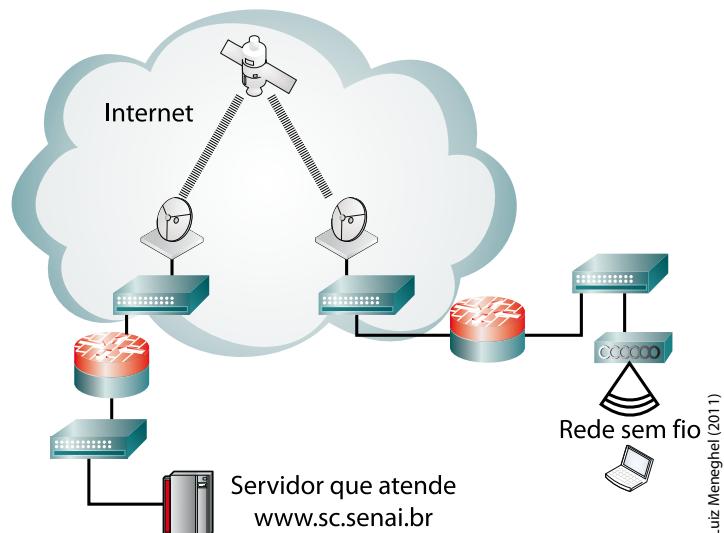


Figura 39 - Navegação na Internet



Quando precisamos nos referir à unidade de dados existente e manipulada nesta camada, chamamos de quadro. O quadro é a PDU da camada de enlace, conforme visto no primeiro capítulo.

Nos capítulos passados, você estudou como ocorre o processo de encapsulamento dos dados, onde os dados das camadas superiores foram encapsulados em vários segmentos da camada de transporte. Logo após, a camada de rede realiza o encapsulamento de cada um destes segmentos em pacotes. Agora, observe que cada pacote da camada de rede é encapsulado em um quadro na camada de enlace. Veja, na figura a seguir, que o quadro (PDU da camada 2) é composto por um cabeçalho, um campo de dados e um *trailer*.



Figura 40 - Layout de quadro

Confira as funções de cada campo:

- Cabeçalho** – contém as informações de controle do quadro, como endereçamento, de acordo com o meio utilizado.

b) **Dados** – informações a serem transmitidas, no caso, o pacote da camada de rede.

c) **Trailer** – informações anexadas no final do quadro, para controle.

Observe a figura a seguir. Ela apresenta mais detalhes sobre os campos que estão contidos dentro do cabeçalho e do *trailer*.

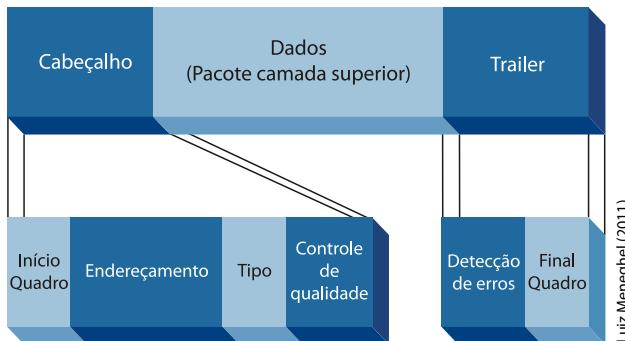


Figura 41 - Layout detalhado do quadro

Confira a função de cada campo:

- início e final do quadro** – limites que identificam e limitam o quadro;
- endereçamento** – endereçamento do quadro, de acordo com o meio utilizado;
- tipo** – tipo da PDU da camada de rede contida no quadro;
- controle de qualidade** – campo que identifica a qualidade;
- detecção de erros** – campo utilizado para validar as informações do quadro. Este campo é calculado no envio do quadro e quando do recebimento do mesmo para verificar se o quadro está íntegro.

Nas redes cabeadas que utilizam o protocolo Ethernet, a camada de enlace está embutida junto com a placa de rede. Isto acontece porque a camada de enlace está muito próxima da camada física e necessita estar de acordo com o meio físico. Por esse motivo, a camada de enlace é dividida internamente em duas sub-camadas. A seguir, você pode observar essas duas camadas.

- Sub-camada LLC (*Logical Link Control*)** – esta sub-camada é responsável por incluir e tratar as informações do quadro que tratam sobre o protocolo de rede utilizado. Sub-camada que está mais próxima da camada de rede.
- Sub-camada de Controle de Acesso ao Meio (MAC)** – esta camada fornece o endereçamento da camada de enlace de acordo com a tecnologia utilizada, e inclui o início e fim do quadro conforme a tecnologia exige.

Nesse tópico, você viu que a função da camada enlace é fornecer um meio de comunicação comum para a troca de dados entre equipamentos, e que essa camada está embutida na placa de rede e é dividida em duas sub-camadas: a LLC e a MAC. No próximo tópico, você estudará as tecnologias de rede local. Até mais!

6.1.1 TECNOLOGIAS DE REDE LOCAL

As tecnologias de redes locais disponíveis atualmente não seguem os mesmos padrões utilizando RFCs, conforme você viu no capítulo anterior. Na camada de enlace, as regras são descritas por organizações de engenharia como o IEEE, ISO, ANSI e ITU.

Nestas descrições, as organizações descrevem não somente as características físicas, mas também todas as características de acesso ao meio ligadas à camada de enlace. Observe, no quadro a seguir, os protocolos definidos por cada organização.

PROTOCOLOS	
ISO	HDLC (<i>High Level Data link Control</i>)
IEEE	802.2 (LLC)
	802.3 (Ethernet)
	802.5 (<i>Token Ring</i>)
	802.11 (<i>Wireless Lan</i>)
ITU	Q.922 (Padrão <i>frame Relay</i>)
	Q.921 (Padrão de enlace de dados ISDN)
ANSI	HDLC (<i>High Level Data link Control</i>)
	3T9.5
	ADCCP (<i>Advanced Data Communications Control Protocol</i>)

Quadro 7 - Organizações e protocolos



**SAIBA
MAIS**

Você encontra informações mais detalhadas sobre esses protocolos, acessando os sites das seguintes organizações: ISO, IEEE, ITU e ANSI. Disponíveis em: <www.iso.ch>; <www.ieee.org>; <www.itu.int>; <www.ansi.org>.

Estes protocolos definem todas as características necessárias para o perfeito funcionamento da camada de enlace. Eles definem como colocar os dados no meio utilizado (controle de acesso ao meio) e o endereçamento e enquadramento.

6.1.2 ACESSO AO MEIO

Existem diversas implementações da camada de enlace e também diferentes implementações para o controle de acesso ao meio que têm como pontos importantes e que diferenciam-se umas das outras através do meio como a transmissão é compartilhada e a topologia utilizada.

Entenda melhor cada uma dessas diferenças.

COMPARTILHAMENTO

Com relação ao compartilhamento do meio de transmissão, dependendo da tecnologia utilizada, a camada de enlace terá que definir como a comunicação ocorrerá, para que todos os componentes da mesma se entendam de forma adequada.

Em um meio compartilhado, podemos considerar o acesso ao meio como:

- a) determinístico – ou seja, cada componente da rede possui um tempo determinado dentro da rede local para transmitir. Isso definirá, inclusive, o quanto poderemos transmitir neste tipo de rede. Ex: *Token Ring*.
- b) não-determinístico – cada componente, ao transmitir, necessita verificar se o meio está disponível. É necessário, também, verificar a possibilidade de colisão, caso mais de um componente da rede necessite transmitir no mesmo momento. Para evitar o caos na transmissão, os métodos de acesso utilizam um método (CSMA – *Carrier Sense Multiple Access*) para tratar este processo.

O CSMA também é dividido em dois métodos que gerenciam o processo de colisão:

- a) CSMA/CD - (CSMA – *Carrier Sense Multiple Access/Collision Detection*) que detecta a colisão e então utiliza um processo para resolver o impasse na transmissão. Um exemplo de tecnologia que utiliza este tipo de método é a rede Ethernet cabeada.
- b) CSMA/CA - (CSMA – *Carrier Sense Multiple Access/Collision Avoid*) que previne a colisão através do processo de avaliação do meio e reserva do mesmo para a transmissão. Um exemplo de tecnologia que utiliza este tipo de método é a rede sem fio.

TOPOLOGIAS

Quando você considera as topologias em uma rede, precisa fazer uma avaliação sobre duas óticas: topologia física e topologia lógica.

A topologia física é a forma como o meio é utilizado para interconectar os dispositivos. Estas considerações são abordadas no capítulo seguinte, onde você estudará a camada física. Já a topologia lógica, é a forma como um equipamento transmite os dados entre os diversos equipamentos da rede. A camada de enlace utiliza a topologia lógica para determinar como gerenciar o processo de acesso ao meio.

As topologias lógicas mais comuns são: a ponto a ponto, multiacesso e anel. Veja mais detalhes sobre cada uma delas.

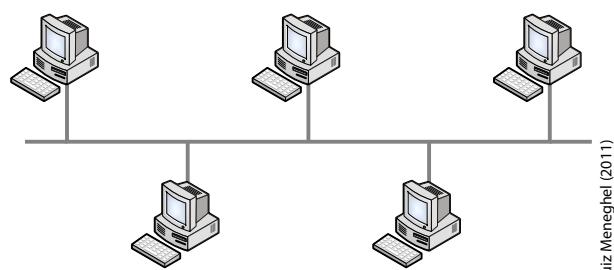
- a) Topologia ponto a ponto – conecta dois pontos diretamente. Nestes casos o protocolo da camada de enlace normalmente é mais simples, pois os dados são sempre destinados de um equipamento a outro. Veja:



Luiz Meneghel (2011)

Figura 42 - Rede ponto-a-ponto
Fonte: Cisco Networking Academy (2011)

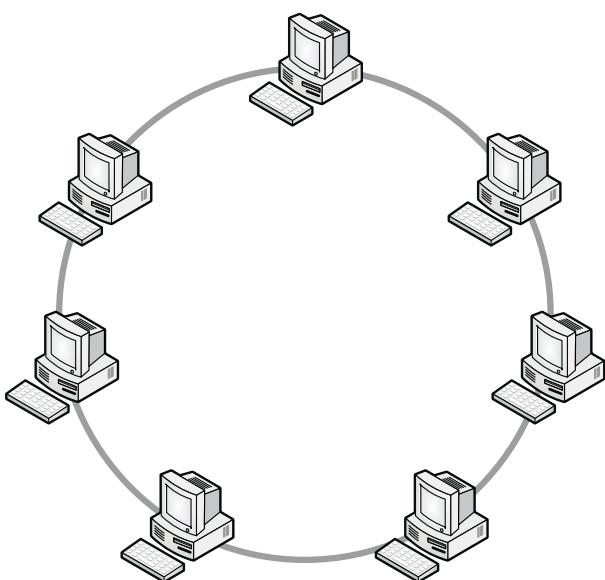
- b) Topologia multiacesso – conecta vários pontos utilizando um mesmo meio. Os dados de apenas um equipamento podem ser colocados na rede por vez. Caso mais de um equipamento decida transmitir simultaneamente, um dos métodos do controle de acesso deverá ser utilizado (CSMA/CD e CSMA/CA). A figura a seguir demonstra uma rede multiacesso.



Luiz Meneghel (2011)

Figura 43 - Rede multiacesso
Fonte: Cisco Networking Academy (2011)

c) Topologia anel – todos os equipamentos são interligados à rede na forma de anel. Os equipamentos recebem os quadros na rede e verificam se são endereçados aos mesmos, caso não sejam eles enviam adiante. O processo de transmissão é controlado por um *token* que irá indicar quando cada equipamento pode transmitir. Veja um exemplo:



Luiz Meneghel (2011)

Figura 44 - Rede em anel
Fonte: Cisco Networking Academy (2011)

Nessa etapa, você aprendeu que as redes locais podem ser determinísticas e não-determinísticas, sendo que, um exemplo de rede determinística é a rede *Token Ring*, enquanto que, o maior exemplo de rede não-determinística são as redes Ethernet. Na próxima seção, você estudará, com mais detalhes, a rede Ethernet e suas variantes.

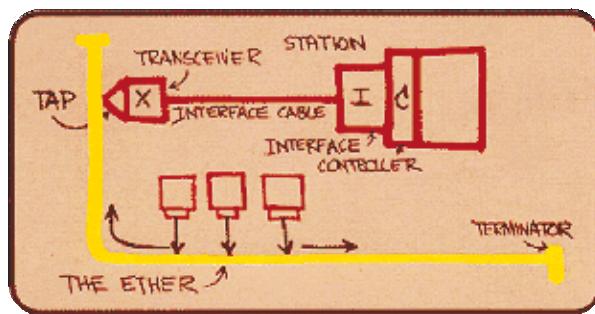


VOCÊ SABIA?

Você sabia que uma das tecnologias mais comuns e mais utilizadas em redes locais é a tecnologia Ethernet? Continue atento, pois esse material está repleto de informações interessantes. Confira!

6.2 ETHERNET (IEEE 802.3) E SUAS VARIANTES

A família de padrões Ethernet surgiu em 1980, quando um consórcio de empresas (*Digital Equipment Corporation, Intel e Xerox*) estabeleceram este padrão.



"This diagram was hand drawn by Robert M. Metcalfe and photographed by Dave R. Boggs in 1976 to produce a 35mm slide used to present Ethernet to the National Computer Conference in June of that year. On the drawing are the original terms for describing Ethernet."

Dave R. Boggs [[20-7]]

Figura 45 – Primeiro diagrama de rede
Fonte: Kurose (2006, p.42)

Em 1985, o IEEE publicou um conjunto de padrões que definiram o início de todo o protocolo Ethernet. Estes padrões começaram com o padrão 802, sendo que o padrão 802.3 atendia as camadas 1 e 2 do modelo de referência OSI.

O padrão Ethernet divide as funções da camada em duas subcamadas:

- Subcamada de modelo lógico (LLC):
 - conexão com as camadas superiores;
 - encapsula o pacote da camada de rede;
 - identifica o protocolo da camada de rede;
 - consegue permanecer independente das questões físicas.
- Sub-camada de controle de acesso aos meios:
 - delimitação do quadro, de acordo com o dispositivo físico;
 - endereçamento;
 - detecção de erros;
 - gerência do controle de acesso aos meios (transmissão, colisão etc.).

Para o IEEE, o padrão 802.2 descreve as funções da subcamada de modelo lógico, e o padrão 802.3 descreve a subcamada de controle de acesso aos meios e as funções da camada física.

Desde os seus primórdios, o padrão Ethernet utiliza como topologia lógica o barramento com multiacesso e utiliza como método de controle de acesso o CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*).

Até hoje, mesmo com as evoluções existentes na Ethernet, a topologia lógica considerada é o barramento com multiacesso. Apesar dos problemas decorrentes desta forma de acesso ao meio, a Ethernet vem evoluindo e se adaptando para conseguir atender às necessidades do mercado e à crescente demanda de altas velocidades em redes LAN.

A grande diferença da rede Ethernet, com relação a outras tecnologias e que contribuíram para o sucesso são:

- a) baixo custo de instalação e manutenção;
- b) confiabilidade;
- c) incorporação de novas tecnologias sem a necessidade de trocar toda a rede (preservação dos investimentos realizados);

Analizando os principais tipos de rede Ethernet que existem, você pode acompanhar a evolução tecnológica que ocorreu nas redes LAN.

- a) Cabeamento coaxial – todos os equipamentos conectados em um mesmo barramento.
 - a) Thicknet (10BASE5) – trabalha com cabo coaxial grosso que permita até 500 metros.
 - b) Thinnet (10BASE2) – cabo coaxial fino que permita distância de cabeamento de 185 metros.
- b) Cabeamento UTP, interligados por um ativo de rede (hub, switch).
 - a) 10BASE-TX – utiliza o hub como ponto central e os cabos UTPs; as transferências são *half-duplex*, ou seja, o equipamento envia ou recebe em um dado momento e não pode realizar as duas funções simultaneamente. Largura de banda de 10Mbps.
 - b) 100BASE-TX – permite transferências *full-duplex* de 100Mbps, ou seja, envia e recebe simultaneamente, mas com largura de banda de 100Mbps.
 - c) 1000BASE-TX – permite transferências *full-duplex* de 1000Mbps, ou seja, envia e recebe simultaneamente, mas com largura de banda de 1000Mbps.
- d) 10GBASE-T – permite transferências de 10Gbps em cabeamento UTP.

- c) Cabeamento Fibra ótica
- 100BASE-FX – permite transferência de 100Mbps.
 - 1000BASE-LX – permite transferência de 1000Mbps.
 - 10GBASE-LX4 – permite transferência de 10Gbps.

As redes de Ethernet também são conhecidas por outros nomes, de acordo com a velocidade de transmissão. Confira na tabela a seguir:

Tabela 5 - Padrões Ethernet

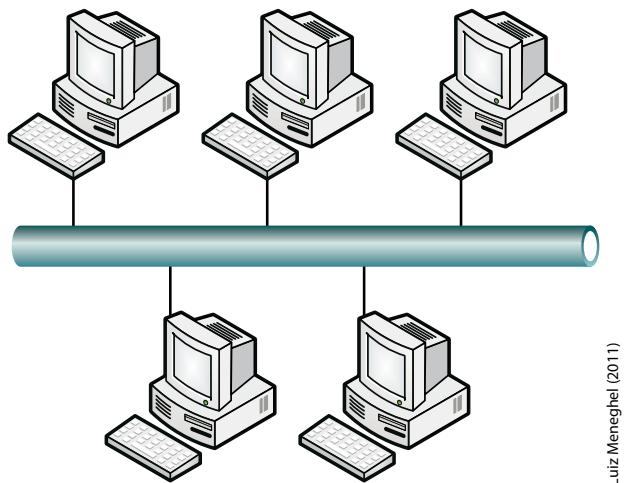
VELOCIDADE (EM MEGABITS POR SEGUNDO)	PADRÃO
10	Ethernet
100	FastEthernet
1000	GigabitEthernet
10000	10 GigabitEthernet

Nessa etapa, você conheceu como surgiu a Ethernet, seus padrões e as suas variedades. Conheceu também a nomenclatura dada à rede conforme a sua velocidade. Na próxima etapa você conhecerá os domínios de colisões. Acompanhe!

6.3 DOMÍNIOS DE COLISÕES

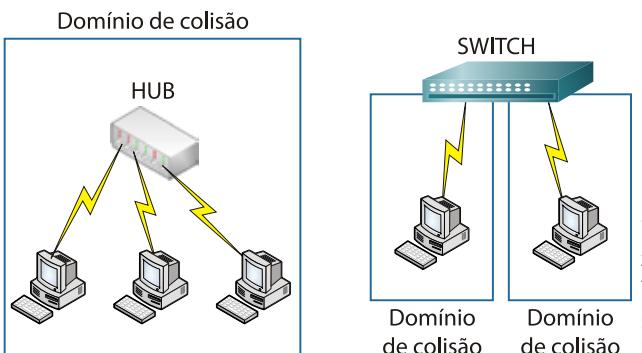
Como você já sabe, a Ethernet trabalha com o protocolo CSMA/CD, que tem como ponto forte a utilização de um meio compartilhado, otimizando os recursos na rede. Mas, a utilização deste protocolo gera um efeito colateral, todos os equipamentos que estiverem no mesmo barramento estarão sujeitos à colisão de suas tentativas de transferência.

O conjunto de equipamentos (que estiverem acessando um mesmo meio compartilhado) estarão sujeitos à colisão entre si e são considerados como estando no mesmo domínio de colisão. Analisando as possibilidades de interligação entre os equipamentos, podemos apresentar os seguintes exemplos de domínio de colisão nas duas figuras seguintes:



Luiz Meneghel (2011)

Figura 46 - Domínio de colisão em barramento



Luiz Meneghel (2011)

Figura 47 - Domínio de colisão com hub e switch

**FIQUE
ALERTA**

Quanto menor o domínio de colisão, maior a largura de banda disponibilizada para os equipamentos.



RECAPITULANDO

Nesse capítulo, você viu os principais conceitos da camada de enlace e sua importância para toda a comunicação em uma rede. Foi detalhado o principal protocolo desta camada – o Ethernet. Você viu, também, as topologias lógicas que explicam as formas de acesso aos meios das tecnologias de camada de enlace e suas características principais. Por fim, conheceu o conceito de domínio de colisão, que apresenta o impacto de uma transmissão em toda a rede e nos equipamentos associados ao mesmo domínio de colisão. No próximo capítulo, você verá os conceitos e características da camada física do modelo OSI.

A Camada Física

7



Neste capítulo, você estudará a camada física do modelo de referência OSI. Essa camada é responsável por preparar como os dados são colocados no meio físico de comunicação. Você entenderá os conceitos desta camada para, depois, estudar os diversos meios físicos de transmissão e aprenderá as topologias presentes na camada física.

Ao final deste capítulo, você terá subsídios para:

- a) conhecer os principais conceitos existentes na camada física, bem como, entender os diversos meios físicos e topologias inseridos nesta camada.

7.1 CONCEITOS DA CAMADA FÍSICA

A principal função da camada física é codificar os dígitos binários, que representam todo o quadro preparado pela camada de enlace em sinais elétricos, ópticos ou ondas de rádio para serem transmitidos pelo meio de comunicação. Veja na figura, a camada física no modelo de referência OSI.

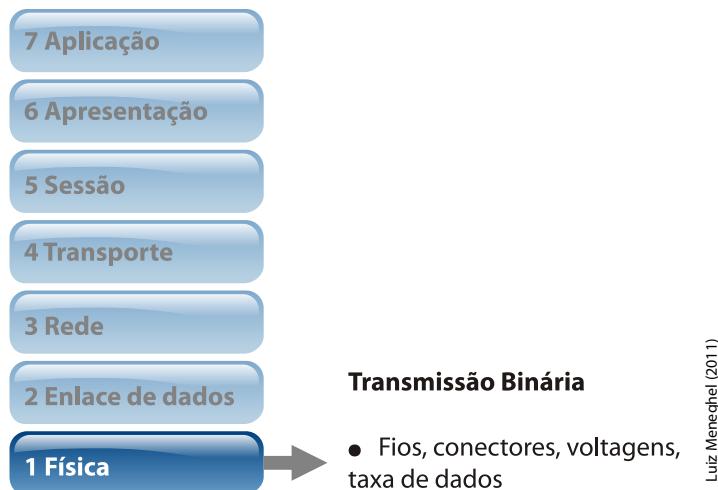


Figura 48 - Visão da camada física no modelo de referência OSI
Fonte: Cisco Networking Academy (2011)

O processo de comunicação da camada física tem alguns elementos importantes e que merecem destaque:

- os meios físicos e conectores;
- representação de bits nos meios físicos;
- codificação dos dados e informações de controle;
- circuito transmissor e receptor nos dispositivos de rede.

Por falar em meios físicos que envolvem eletricidade, componentes eletrônicos e etc., os protocolos que definem e padronizam esta camada são desenvolvidos por diversas organizações internacionais. Entre elas, podemos citar:

- ISO - *International Organization for Standardization*;
- IEEE - *Institute of Electrical and Electronics Engineers*;
- ANSI - *American National Standards Institute*;
- ITU - *International Telecommunication Union*;
- FCC - *Federal Communication Commission*;
- EIA/TIA - *Electronics Industry Alliance/Telecommunications Industry Association*.

**SAIBA
MAIS**

Todas estas organizações citadas, possuem sites na Internet que apresentam as informações detalhadas dos protocolos. Acesse e saiba mais!

Em função da gama de diferentes organizações, você encontrará diversos protocolos para esta camada (e até protocolos de organizações diferentes, mas definindo a mesma transmissão).

Os protocolos e tecnologias definidos por estas organizações devem definir quatro áreas padrões:

- a) propriedades físicas e elétricas do meio físico em questão;
- b) propriedades mecânicas (material utilizado, pinagem, dimensão, etc);
- c) representação dos bits pelos sinais (codificação utilizada);
- d) definição de sinais de informações de controle.

No processo de conversão dos bits em sinais, de acordo com a tecnologia utilizada, dois pontos se destacam: a codificação e a sinalização.

A codificação é o método de converter um conjunto de bits em um código pré-definido. Estes códigos representarão este conjunto de bits no processo de conversa entre o receptor e o transmissor. A codificação auxilia no processo de detecção de erros, pois o padrão de bits, definido por estes métodos de conversão de bits, são cuidadosamente estudados para que possam auxiliar neste processo de detecção de erros.

Quanto à sinalização, sabemos que o que será transferido são valores binários, ou seja, 0s e 1s, mas o processo de sinalização existente consiste, exatamente, em definir o que significa o valor 0 e o que significa o valor 1, de acordo com a tecnologia física em uso.

Pode-se entender, então, que transmitir um quadro da camada 2 (enlace) pela camada física não significa apenas converter 0 e 1 diretamente para o meio físico. Existe todo um processo anterior para garantir a veracidade da informação a ser transferida e o entendimento correto das informações transferidas, por parte do receptor.

**VOCÊ
SABIA?**

Cada bit a ser transferido por um meio físico possui uma representação física, de acordo com o meio físico utilizado, e esta representação tem um tempo para ocupar neste meio físico, representando este bit. Este tempo de representação é chamado de **tempo de bit**.

7.1.1 MÉTODOS DE SINALIZAÇÃO

Os métodos de sinalização criados pelos organismos internacionais, tradicionalmente alteram umas das características físicas (amplitude, frequência ou fase) para representar o bit. Todas essas características são trabalhadas de acordo com o padrão de sinalização, criado para a tecnologia em questão.

Por exemplo, na Manchester, o “0” é indicado por meio de uma transição de voltagem do nível alto para o nível baixo, no meio do tempo de bit. Já o “1” é o inverso, ocorre uma transição de voltagem do nível baixo para o nível alto.

Podemos citar como método de sinalização:

- a) Manchester;
- b) NRZ-L – não-retorno ao nível zero;
- c) NRZI.

7.1.2 MÉTODOS DE CODIFICAÇÃO

Já o processo de codificação diz respeito à forma como os bits serão agrupados antes de serem convertidos em sinal, de forma a garantir a integridade do grupo de informações a serem transferidos.

Devemos salientar que, quanto maior a velocidade desejada na transmissão, maior a probabilidade de que os bits sejam corrompidos. Os métodos de codificação são utilizados para permitir uma detecção mais rápida e eficiente de quais dados foram corrompidos.

Confira, na tabela a seguir, as vantagens e os métodos de codificação que podemos citar:

Tabela 6 - Métodos e vantagens

MÉTODOS	VANTAGENS
<ul style="list-style-type: none"> • manchester diferencial; • 4B/5B; • MLT-3; • 8B6T; • 8B10T; • 4D-PAM5. 	<ul style="list-style-type: none"> • Melhor detecção de transmissão de problemas e erros no meio físico; • Auxílio na diferenciação de bit de dados de bit de controle; • Redução de erros no nível de bit; • Economia de energia utilizada em função da codificação utilizada.

Você conheceu o conceito de camada física, e também os métodos de codificação e sinalização. Na etapa seguinte, você conhecerá os diferentes meios físicos de transmissão. Até mais!

7.2 MEIOS FÍSICOS DE TRANSMISSÃO

Podemos considerar que os meios físicos são responsáveis por transportar sinais que representam os dígitos binários, mas, estes sinais podem assumir diversas formas, como sinais elétricos, ópticos e ondas de rádio.

Dependendo do meio físico utilizado para transmissão, o sinal assumirá uma forma diferente. Hoje, temos três meios físicos comuns em redes:

- a) cabo de cobre (para sinais elétricos);
- b) fibra (para sinais ópticos);
- c) sem fio (sinais por ondas de rádio).

Confira, detalhadamente, cada um dos meios físicos citados.

7.2.1 CABO DE COBRE

O cabo de cobre é o meio físico mais utilizado, nos dias de hoje, para a transmissão em redes. Consiste em uma série de fios de cobre agrupados e dedicados às funções estabelecidas pela sinalização.

Os meios de cobre também utilizam conectores e tomadas que fornecem fácil conexão e desconexão, além de serem construídos de acordo com uma série de recomendações que auxiliarão no processo de transmissão dos dados.

Veja na figura, alguns meios físicos de cobre.

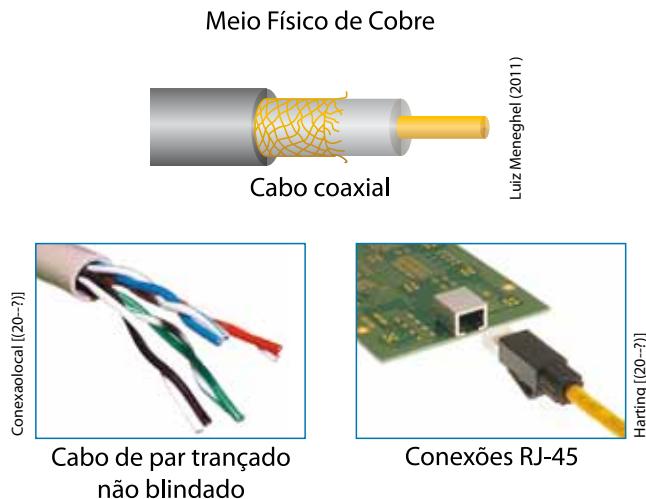


Figura 49 - Meios físicos de cobre
Fonte: Cisco Networking Academy (2011)

A transmissão ocorre no cobre por meio da transmissão de impulsos elétricos, que são codificados e decodificados pelas interfaces conectadas a estes cabos.

O grande problema na utilização de cabos de cobre diz respeito a:

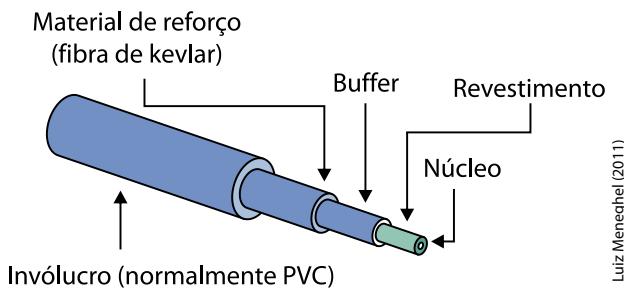
- a) atenuação do sinal (cabos muito longos, fora do padrão, fazem com que o sinal elétrico perca a força, não sendo corretamente interpretado no destino);
- b) interferência ou ruído (cabos passando muito próximos a redes elétricas, ou incorretamente conectados podem ser suscetíveis a interferências externas que fazem com que o sinal não seja corretamente interpretado no destino).

Em função destes problemas, faz-se necessário, no momento da aquisição/confecção do cabo a ser utilizado, estar atento a:

- a) seleção do cabo – é preciso selecionar o tipo de cabo mais coerente para a transmissão desejada;
- b) projeto de rede – um bom projeto de rede respeita a infraestrutura, evitando interferências externas que podem ser geradas;
- c) técnicas de cabeamento – é preciso conhecer/utilizar as corretas técnicas de cabeamento;
- d) utilização de equipamentos e ferramentas condizentes com o cabeamento desejado.

7.2.2 FIBRA

O meio físico chamado de fibra consiste na utilização de cabeamento composto por fibras feitas de vidro ou plástico, por onde são transportados sinais de luz. Os bits são codificados na fibra, como se fossem pulsos de luz. Observe um exemplo de cabos de fibra.



Luiz Meneghel (2011)



Alvaro Llorente ([20-?])

Conectores de fibra

Figura 50 - Meios físicos de fibra
Fonte: Cisco Networking Academy (2011)

A fibra tem diversas vantagens em relação ao fio de cobre:

- não é condutor elétrico, por isto, está imune às interferências eletromagnéticas;
- utiliza a luz como meio, tendo uma perda de sinal muito menor que o sinal elétrico, cobrindo distâncias maiores;

Como desvantagens, as fibras apresentam as seguintes:

- custo maior do que os fios de cobre;
- a manipulação da fibra exige um maior cuidado do que a manipulação com o cobre.

O grande segredo da solução de fibra não é apenas a fibra, mas também os lasers ou os diodos responsáveis pela emissão e recepção dos sinais de luz. Estes equipamentos detectam o sinal de luz e, de acordo com a sinalização e codificação utilizada, transformam-no em sinais digitais.

**FIQUE ALERTA**

Quando você se deparar com um cabo preso, mas com um das pontas soltas, nunca olhe diretamente para a extremidade da fibra. O feixe de luz pode danificar a sua visão. Tenha muito cuidado.

Hoje em dia, as fibras são divididas em dois tipos principais:

- monomodo – fibra que transporta um único sinal de luz, geralmente emitido por um *laser*. Um único feixe de luz, concentrado no meio da fibra, é transmitido. Estes pulsos normalmente podem ser transmitidos por longas distâncias.
- multimodo – fibra que transporta múltiplos sinais de luz, geralmente emitidos por LEDs e que, devido às características da transmissão, não permite comprimentos longos.

**VOCÊ SABIA?**

O limite de transmissão em uma fibra ainda não foi esgotado. O que limita a transferência são os dispositivos que convertem os bits em luz, e vice-versa.

7.2.3 SEM FIO

O meio físico sem fio consiste na transmissão de dígitos binários utilizando sinais eletromagnéticos nas frequências de rádio e de micro-ondas.

Uma grande característica da utilização do meio sem fio é que a transferência utilizando este meio não está restrita ao meio condutor que está utilizando, como no caso do cobre e fibra. Mas, isto também pode ser considerado um problema, pois o gerenciamento e as questões de segurança merecem atenção em projetos com esta tecnologia.

Devido a evoluções na tecnologia, já existem diversos tipos de redes sem fio, com diferentes características específicas e áreas de cobertura. Todos esses diferentes tipos estão regulamentados pela IEEE.

Confira alguns tipos de redes sem fio existentes hoje.

- Padrão 802.11 – também conhecido como Wi-Fi, muito utilizado e responsável pela difusão da utilização deste tipo de meio em redes locais. Utiliza o protocolo CSMA/CA e permite velocidades de 11 Mbps até 300 Mbps.

b) Padrão 802.15 – conhecido como WPAN ou *bluetooth*, muito utilizado nas chamadas redes pessoais. Trabalha na transmissão quando do emparelhamento de dois equipamentos.

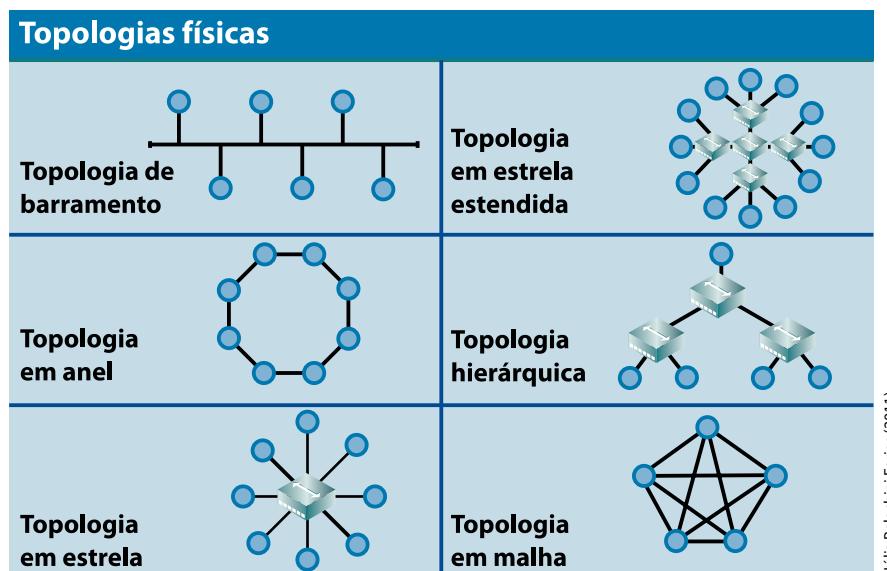
c) Padrão 802.16 – conhecido com WIMAX, utiliza uma topologia mais avançada, que permite acesso à banda larga sem fio em uma topologia ponto-multiponto.

Além de conhecer os tipos de cabos físicos para cada tipo de rede, você entendeu melhor como funciona a rede sem fio e pôde associar os tipos de rede aos nomes que você já conhece, como WI-FI e *bluetooth*.

7.3 TOPOLOGIAS

Na camada física, é possível interligar computadores de diversas formas, e essas interligações podem ser definidas como topologias físicas. Podemos entender que estas topologias físicas são a forma como os dispositivos são interligados por meio de um *layout* físico dos cabos.

A topologia escolhida deve estar associada diretamente ao tratamento da camada física no momento da comunicação entre os equipamentos de uma rede. A figura a seguir apresenta alguns exemplos de topologias físicas. Observe.



Júlia Pelachini Farias (2011)

Figura 51 - Topologias Físicas de Rede
Fonte: Cisco Networking Academy (2011)

Os tipos de topologia existentes podem ser:

- a) **totalmente conectada**: cada equipamento possui uma conexão individual para cada outro equipamento. Possui diversas vantagens como redundância e disponibilidade, mas, em função dos custos e das características técnicas que dificultam a interligação de todos com todos, a implementação deste tipo de rede é inviável na maioria das situações. É também chamada de topologia em malha.
- b) **malha**: similar à topologia totalmente conectada, porém sem a necessidade de todos conversarem com todos. Apenas deve-se garantir que a comunicação entre todos os equipamentos ocorra, mesmo que, em algumas situações, isto seja realizado por meio de outros dispositivos. É também chamada de topologia em malha parcial.
- c) **anel**: cada equipamento possui dois cabos que serão conectados em outros equipamentos, e, a partir disto, será construído um anel com estas interligações. A comunicação entre equipamentos poderá passar por outros equipamentos da rede. A transmissão sempre “trafega” em um sentido.
- d) **barramento**: cada equipamento é conectado a um barramento (cabو). Se ocorrer algum problema com o cabo, a rede deixa de funcionar. Esta é a topologia típica em redes Ethernet com cabo coaxial.
- e) **estrela**: os equipamentos são conectados em um ponto central (cabو, hub, switch). Se ocorrer algum problema com o elemento central, a rede deixa de funcionar. Esta é a topologia típica em redes Ethernet.
- f) **árvore**: consiste na interligação de diversas redes em estrela. Esta é a topologia mais comum atualmente e não deixa de ser uma rede em estrela. É também chamada de topologia em estrela estendida.
- g) **hierárquica**: semelhante a uma estrela estendida, porém, ao invés de unir os hubs ou switches, o sistema é vinculado a um computador que controla o tráfego na topologia.
- h) **sem fio**: os equipamentos se conectam à rede sem a necessidade de uso de cabos de rede. Utiliza ondas de rádio ou micro-ondas. Nesta topologia, existe um equipamento central chamado *Wireless Access Point* (WAP), utilizando para fazer a conexão entre os equipamentos que, por sua vez, possuem placa de rede sem fio.

Mas, como saber que tipo de rede escolher para uma empresa? Acompanhe o Casos e Relatos a seguir.



CASOS E RELATOS

Escolhendo o meio físico para uma empresa

João Pedro foi contratado para projetar uma rede em uma empresa que fica em dois prédios. Após analisar os requisitos do cliente, percebeu que entre os dois prédios da empresa existe uma grande interferência eletromagnética em função de um gerador, que fica entre os prédios, e que normalmente é ligado. Considerando a possibilidade de integração entre os prédios, João Pedro verificou os seguintes pontos:

- interligar a rede entre os prédios com fio de cobre, a deixa suscetível à interferência toda a vez que o gerador for ligado; ou seja, não é considerada uma solução viável;
- interligar com uma rede sem fio seria uma solução, mas também é suscetível à interferência, além de termos as questões de segurança, que deverão ser muito bem ajustadas, pois esta rede passará por uma área aberta.
- interligar com fibra tem um custo mais alto, mas não é suscetível à interferência eletromagnética, e, como serão utilizados cabos, não há problemas de segurança.

Em função destas avaliações, João Pedro decidiu que a melhor solução é interligar os prédios com fibra garantindo a qualidade, velocidade e segurança da rede.



RECAPITULANDO

Nesse capítulo, você conheceu os principais conceitos da camada física e sua importância para toda a comunicação em uma rede. Viu que existem três tipos de meios de comunicação utilizados na camada física, que são: cabos de cobre, fibra e sem fio. Também viu as diversas topologias físicas presentes nesta camada. No próximo capítulo, você estudará o modelo de Referência TCP/IP.

O Modelo TCP/IP

8



Nos capítulos anteriores, você estudou o modelo de referência OSI. Este modelo serve como base para o entendimento do funcionamento da rede e de protocolos de comunicação. Isso se torna evidente principalmente quando há a necessidade de nos referirmos ao funcionamento de dispositivos de rede, já que, ao falar em camadas, citamos as camadas do modelo de referência OSI. Neste capítulo, você estudará o modelo TCP/IP, seus conceitos, camadas e principais protocolos. Além de relacioná-lo com o modelo de referência OSI. O modelo TCP/IP é a base do funcionamento das redes atuais e é importante conhecer bem sua estrutura.

Ao final deste capítulo você terá subsídios para:

- a) conhecer os conceitos do modelo TCP/IP e sua aplicação nas redes de computadores atuais.

8.1 A PILHA DE PROTOCOLOS TCP/IP

Segundo *Cisco Networking Academy* (2011) o modelo TCP/IP é a arquitetura aberta que fornece os elementos básicos para a comunicação em rede atual. Assim como o modelo de referência OSI, o modelo TCP/IP é dividido em camadas e seu modelo leva no nome seus dois principais protocolos: o TCP (*Transmission Control Protocol*) e o IP (*Internet Protocol*). Por ser uma arquitetura aberta, teve sua adoção facilitada por fabricantes em busca da interoperabilidade de seus equipamentos com os dos concorrentes.

Ainda segundo a Cisco (2011), este modelo surgiu a partir de projetos de pesquisa financiados pela *Advanced Research Projects Agency* (ARPA), órgão financiado pelo Departamento de Defesa dos Estados Unidos. A rede inicialmente chamada de ARPANET foi concebida na década de 1970 e era uma rede de comutação de pacotes. Com o crescimento, esta rede se mostrou limitada e acabou impulsionando o desenvolvimento de novos protocolos e do modelo que hoje conhecemos como TCP/IP. Esse modelo e seus protocolos passaram a ser utilizados no início da década de 1980.

O modelo TCP/IP possui uma pilha de protocolos que ficam alocações em cada uma das camadas. A divisão deste modelo é feita em quatro camadas, sendo elas: a aplicação, transporte, Internet e acesso à rede, conforme se pode ver na figura a seguir.

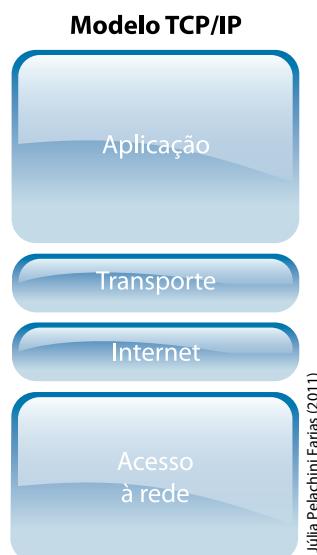


Figura 52 - Pilha TCP/IP com suas quatro camadas
Fonte: *Cisco Networking Academy* (2011)



FIQUE ALERTA

Há certa divergência com relação ao número de camadas do modelo TCP/IP, entre vários autores. Alguns autores afirmam que este modelo possui cinco camadas, acrescentando a camada física.

Vamos estudar cada uma das camadas do modelo TCP/IP, suas características, funcionalidades e principais protocolos da pilha.

8.1.1 CAMADA DE APLICAÇÃO

Nesta camada residem os protocolos que possibilitam a comunicação entre as aplicações. Quando uma aplicação depende de um protocolo desta camada, ela fará uso do protocolo para codificar os dados e encaminhá-los para a camada de transporte. A camada de aplicação fornece o serviço para que as aplicações de usuário possam interagir com a rede.

Os principais protocolos da camada de aplicação são os que você estudou no capítulo 3. O HTTP para navegação em páginas Web, o DNS para resolução de nomes, o FTP para transferência de arquivos, o SMTP/POP/IMAP para transferência de mensagens de e-mail, o DHCP para configuração de hosts e o SNMP, para gerenciamento de rede. Note que, cada uns desses protocolos utiliza um ou mais protocolos da camada de transporte.

8.1.2 CAMADA DE TRANSPORTE

No capítulo 4 você viu que a camada de transporte utiliza o número de porta para realizar o mapeamento das diversas aplicações da camada de aplicação. No caso do UDP, diferenciar a origem dos diferentes fluxos de dados da camada de aplicação está diretamente vinculado ao número de porta. No protocolo TCP, temos o conceito de *socket*. O *socket* é uma relação existente entre o conjunto de números de porta e endereço IP. Esta relação é utilizada para identificar a conexão existente entre dois hosts. Por exemplo, temos o conjunto 192.168.1.1:1893 que representa o host cliente que está no SENAI e o conjunto 172.17.103.25:80 que representa o host da Empresa X. Dessa forma, o TCP é capaz de identificar o uso simultâneo de uma mesma aplicação por dois clientes diferentes.

¹ PPP

É o acrônimo de *Point to Point Protocol*. O PPP é um protocolo de WAN utilizado na transferência de dados entre dois pontos de rede.

8.1.3 CAMADA DE INTERNET

No capítulo 4, você estudou os processos básicos da camada de rede e os detalhes sobre o IP, que é um protocolo não confiável e sem conexão. Por não oferecer garantias, o IP é conhecido como protocolo melhor esforço. Os sistemas de roteamento e dispositivos da camada farão o possível para entregar os pacotes, no entanto estes dispositivos que compõem o núcleo da rede não operam nas camadas de transporte e aplicação, deixando a cargo dos dispositivos finais a tarefa de avaliar os pacotes recebidos utilizando serviços da camada de transporte e aplicação. Apesar de não garantir, o IP é responsável pela definição de quando mensagens de erros serão geradas. Para gerar essas mensagens de erro relacionadas ao encaminhamento e entrega dos pacotes é utilizado o protocolo ICMP, também estudado no capítulo 4.

8.1.4 CAMADA DE ACESSO À REDE

A camada de acesso à rede tem como responsabilidade o encaminhamento local entre dois hosts diretamente conectados. Enquanto a camada de rede leva uma informação de uma origem até um destino qualquer, por meio de vários saltos, a camada de acesso à rede leva as informações de um salto ao outro. Ela controla como será o acesso ao meio físico. Várias tecnologias podem ser utilizadas para executar as funções desta camada e, no decorrer do trajeto, da origem ao destino. A informação pode transitar por diferentes tecnologias, como Ethernet e PPP¹. A especificação desta camada deixou a cargo da especificação dos protocolos a forma como se dará a interação com o meio físico. Desta forma, permite que a pilha de protocolos TCP/IP possa ser executada sobre qualquer tecnologia de camada física/hardware.

Nesse item você conheceu, uma a uma, as quatro camadas que o modelo TCP/IP possui. Que tal comparar essas camadas com as do protocolo OSI? Siga em frente e confira isso no próximo item.

8.2 COMPARANDO O MODELO TCP/IP E OSI

Como foi estudado em capítulos anteriores, o modelo de referência OSI possui sete camadas, enquanto o modelo TCP/IP possui somente quatro. Apesar desta divergência no número de camadas, mesmo utilizando o TCP/IP nos referimos às definições das camadas do modelo OSI, o qual continua sendo de grande importância, pois a forma como é apresentando auxilia na compreensão do funcionamento das redes de computadores e protocolos.


VOCÊ SABIA?

Apesar do modelo de referência OSI ser utilizado como base para o desenvolvimento de protocolos, o modelo TCP/IP foi definido primeiro, e muitas de suas características foram incorporadas ao modelo OSI.

O modelo TCP/IP teve uma adoção ampla, pois, apesar de ainda não estar com uma especificação madura, foi imediatamente inserido em sistemas Unix. Esta implementação levou a um grande número de usuários. Ao contrário do TCP/IP, o modelo OSI exigia que diversas etapas de maturação da especificação fossem completadas para poder implementar códigos. Essas exigências geravam uma morosidade que acarretou na falta de adesão aos protocolos do modelo OSI.

Mesmo havendo diferenças em relação ao sucesso e adoção de protocolos de cada modelo, eles compartilham muitas características. A figura a seguir mostra uma relação existente entre as camadas de cada modelo.

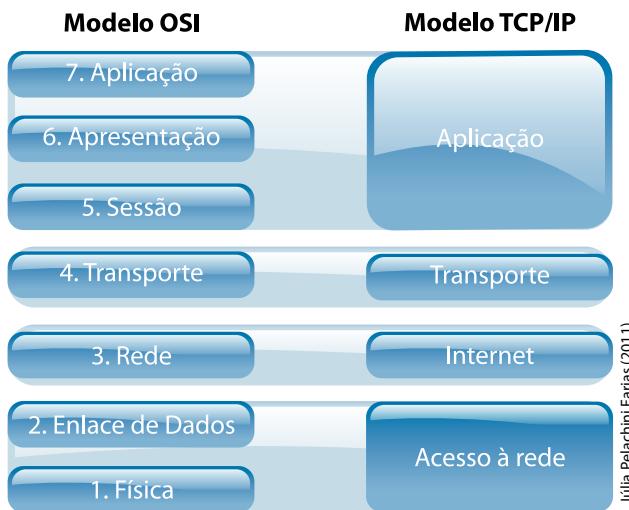


Figura 53 - Relação entre os modelos de referência OSI e TCP/IP
Fonte: Cisco Networking Academy (2011)

Podemos perceber que a relação mais significativa ocorre entre as camadas de transporte, rede e Internet. A camada de rede tem sua função bem definida em ambos os modelos, que é a capacidade de endereçar e rotear as mensagens na rede. No caso da camada de transporte, a definição considera a responsabilidade de recuperação de erros, garantia da entrega dos segmentos na sequência correta, confiabilidade na comunicação fim a fim.

Como o modelo TCP/IP possui menos camadas, algumas das funções das camadas de apresentação e sessão do modelo OSI ficam a cargo da camada de aplicação do TCP/IP. O mesmo acontece com a camada de enlace de dados e camada física do modelo OSI, que fica a cargo da camada de acesso à rede do TCP/IP.

A camada de acesso à rede elenca como deve ser feita a interação entre a camada de Internet e o meio físico, no entanto, não especifica os protocolos e nem como eles realizam esta tarefa. Todos os procedimentos para que sejam estabelecidas as conversações nesta camada são especificados pelas camadas física e de enlace do modelo OSI.



**SAIBA
MAIS**

Você pode aprender mais sobre o TCP/IP consultando o livro on-line <<http://www.tcpipguide.com/>>. Entenda melhor a diferença entre os protocolos, acompanhando o caso relatado a seguir.



CASOS E RELATOS

UDP versus TCP

Um dos seus colegas de João Pedro estuda Desenvolvimento de Sistemas. Ele tem interesse em atuar no desenvolvimento de aplicativos de comunicação de voz, mas não tem conhecimentos suficientes na área de redes de computadores. Sabendo que João Pedro é um grande conhecedor dessa área, resolve consultá-lo sobre o uso de protocolos de rede para a comunicação de voz. João Pedro sabe que as aplicações de voz exigem interação em tempo real, e de imediato descartou o TCP, devido à sua sobrecarga com informações de controle. Sugeriu ao seu colega que procurasse conhecer melhor os protocolos UDP e IP, principalmente questões de endereçamento de rede. Além disso, João Pedro sugeriu que ele também veja como funciona o protocolo de DNS, já que o uso de aplicações de rede geralmente envolve nomes de domínio. Apesar de sua excelente instrução, seu colega questionou sobre o uso de um protocolo confiável, para que a aplicação seja atualizada automaticamente quando novas versões forem lançadas. Para este caso, João Pedro sugere que ele estude sobre o TCP, pois é um protocolo que garante a entrega dos segmentos de rede.



RECAPITULANDO

Neste capítulo, você estudou a pilha de protocolos do TCP/IP e o funcionamento básico dos principais protocolos das camadas de aplicação, transporte e Internet. Os conceitos estudados ajudarão você a compreender a importância de cada protocolo, para que a comunicação seja estabelecida. Além disso, a partir de agora, você será capaz de identificar a finalidade de cada protocolo e como eles devem ser empregados para que a rede funcione corretamente. Por último, foi feita uma comparação entre os modelos OSI e TCP/IP observando suas diferenças e semelhanças. No próximo capítulo você estudará os conceitos e utilização das sub-redes.

Sub-redes

9



No capítulo 5, você conheceu os conceitos básicos relacionados ao endereçamento IPv4. Neste capítulo, você verá como utilizar melhor os endereços por meio da criação de sub-redes, ou seja, dividir um endereço IP em partes para endereçar conjuntos menores de computadores. Você entenderá o que são sub-redes e depois verá como fazer os cálculos para obter os endereços de sub-redes.

Ao final deste capítulo você terá subsídios para:

- a) entender a estrutura do endereçamento IP utilizando sub-redes e como realizar os cálculos para uma melhor utilização do espaço de endereços disponível.

9.1 O QUE SÃO SUB-REDES

Você já sabe que o endereço IPv4 é composto por 32 *bits* separados em conjuntos de 8 *bits* e é apresentado na notação decimal por pontos. Além disso, viu que o endereço IP possui uma porção dedicada à rede e outra dedicada ao host. A porção de rede nos permite endereçar redes, ou seja, um conjunto de computadores pertencentes ao mesmo grupo. Este grupo de hosts é endereçado pela porção de host, e pertence a uma das redes endereçadas pela porção de rede. Quem define qual porção pertence à rede e qual porção pertence ao host é a máscara. O número de redes e hosts é baseado no tamanho da porção de rede e da porção de host. Este tamanho é dado baseado no número de bits que são utilizados para representar cada porção.

O tamanho da porção de rede também é chamado de prefixo de rede, que é o número de bits que define a porção rede do endereço IP. Você também já estudou que os endereços IPv4 são divididos em classes A, B, C, D e E. Essa divisão em classes é chamada de endereçamento IP *classfull* ou classes cheias. As classes A, B e C são utilizadas para endereçar redes e hosts. A figura a seguir apresenta as classes com seus prefixos. Observe.

Endereço de Classe A (decimal):	10.0.0.0
Endereço de Classe A (binário):	00001010.00000000.00000000.00000000
Máscara de Classe A (Binário):	11111111.00000000.00000000.00000000
Máscara de Classe A (decimal):	255.0.0.0
Comprimento padrão:	/8
Endereço de Classe B (decimal):	172.16.0.0
Endereço de Classe B (binário):	10010001.10101000.00000000.00000000
Máscara de Classe B (Binário):	11111111.11111111.00000000.00000000
Máscara de Classe B (decimal):	255.255.0.0
Comprimento padrão:	/16
Endereço de Classe C (decimal):	192.168.100.0
Endereço de Classe C (binário):	11000000.10101000.00101010.00000000
Máscara de Classe C (Binário):	11111111.11111111.11111111.00000000
Máscara de Classe C (decimal):	255.255.255.0
Comprimento padrão:	/24

Júlia Pelachini Farias (2011)

Figura 54 - Cada classe com sua máscara padrão em binário, decimal e prefixo de rede

Cada classe é capaz de prover um determinado número de redes e um número de hosts por rede. A classe A fornece mais hosts e a classe C mais redes, conforme pode ser visto na tabela a seguir. No entanto, essa forma de utilização baseada em classes gerava um desperdício de endereços.

Tabela 7 - Número de redes e hosts por rede em cada classe

CLASSE	NÚMERO DE REDES	NÚMERO DE HOSTS POR REDE
A	128	16.777.214
B	16.384	65.534
C	2.097.152	254

Ao alocar um endereço de classe A para uma corporação, esta receberia uma rede com 16.777.214 hosts. Nem mesmo grandes empresas possuem hosts suficientes para ocupar todo o espaço de endereçamento de uma rede de classe A. No caso de uma rede classe B, são 65.534 hosts. Apesar de ser um número bem menor, ainda era bastante grande, pois alocar uma classe B para uma rede de 500 hosts deixaria 65.034 endereços sem uso. Uma classe C oferecia somente 254 hosts, ou seja, muito pouco para a maioria das empresas. Estas acabavam crescendo e necessitando de mais um endereço de rede de classe C. Muitas empresas possuem um endereço de classe A, como por exemplo, a IBM, APPLE, XEROX e HP.



**SAIBA
MAIS**

Para consultar a alocação de endereços IPv4, visite o site <<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>>, e para obter mais informações sobre o esgotamento de endereços IPv4, acesse o endereço <<http://www.nro.net/news/ipv4-free-pool-depleted>>.

O esquema de endereçamento utilizado pelo IPv4 logo se mostrou limitado, conforme a Internet crescia. Para resolver o problema da má distribuição e também da futura previsão de esgotamento de endereços, definiu-se um novo esquema de divisão em sub-redes, ou seja, repartir essas redes de classe A, classe B e classe C em redes menores. Fazendo a divisão em sub-redes, pode ser feito um uso mais eficiente do endereçamento IP, por meio da alocação mais precisa do número de redes e hosts necessários para cada organização. Também possibilita a divisão da rede de uma organização em redes menores, por exemplo, por departamentos ou por política de acesso a recursos de rede. A divisão de redes em redes menores ou sub-redes proporciona também a redução de domínios de broadcast e melhor gerenciamento da rede.



**VOCÊ
SABIA?**

Outros meios além da divisão de sub-redes permitiram evitar o esgotamento prematuro de endereços IPv4. Entre eles podemos citar o CIDR, VLSM e NAT. Estes assuntos serão abordados em uma unidade curricular posterior.

O processo de divisão de sub-redes é simples. Primeiramente se escolhe qual endereço será dividido e em quantas redes. Também pode-se fazer a divisão a partir do número de hosts desejados para cada rede, sem se preocupar diretamente com o número de redes. Você verá mais detalhes sobre o cálculo de sub-redes na seção seguinte.

Como visto anteriormente, quem define o que é porção de rede e porção de host é a máscara. Ela nos permite identificar quantos bits temos em cada porção. Para realizar a divisão, temos que obter bits da porção de host e “transferí-los” para a porção de rede. Fazendo essa transferência, estaremos criando uma porção de sub-rede, que fica entre a porção de rede e a porção de host como mostra a figura.

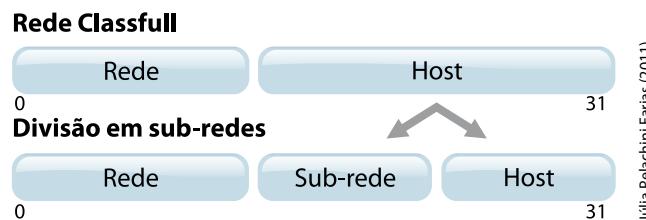


Figura 55 - Porções do endereço IP para classfull e com a divisão em sub-redes

Vamos dividir o endereço 172.16.0.0 em quatro sub-redes. Sabemos que este endereço é de classe B. Portanto, temos que pegar bits emprestados da porção de host. No endereço de classe B a porção de rede corresponde aos primeiros 16 bits e a de host, aos 16 bits seguintes. Pegaremos emprestados os bits mais significativos, ou seja, o mais à esquerda da porção de host. Para obter quatro sub-redes, temos que pegar bits suficientes para endereçá-la.

Para chegar ao número quatro usando a regra de 2^b , onde b é o número de bits que pegamos emprestados, precisaremos de 2 bits. Esses bits que foram retirados da porção de host passam a fazer parte da porção de sub-rede e são também contabilizados pela máscara de sub-rede. A máscara de sub-rede nos indica o que é porção de rede e o que é porção de host. A seguir, vamos ver o processo realizado para obter os quatro novos endereços IP.

Dividir o endereço 172.16.0.0, 255.255.0.0 ou 172.16.0.0/16 em quatro sub-redes. Precisamos de dois bits da porção de host, pois $2^2 = 4$. A máscara nos indica que a porção de rede é composta pelos dois primeiros octetos e a porção de host pelos dois octetos restantes. A figura a seguir apresenta a porção de rede e host em relação à máscara padrão e a escolha dos dois bits mais significativos que serão emprestados para criar as sub-redes.

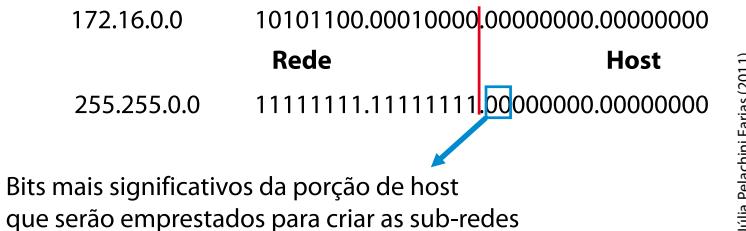


Figura 56 - Identificação da porção de rede e host e dos bits mais significativos

Júlia Pelachini Farias (2011)

Uma vez que os bits necessários para obter as quatro sub-redes foram selecionados, eles passam a fazer parte da porção de sub-rede. Além disso, ocorre uma alteração da máscara, que passa a ser denominada de máscara de sub-rede. Esta nova máscara passa a indicar uma porção de rede estendida, pois contempla os bits que foram emprestados para criar as sub-redes. A figura a seguir mostra a nova máscara, os bits emprestados para a porção de sub-rede e as três porções que compõem o endereço IP.

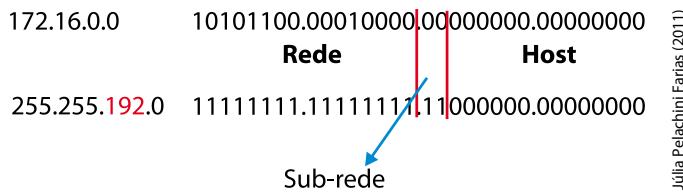


Figura 57 - Bits emprestados para criar a sub-rede e a nova máscara de sub-rede

Júlia Pelachini Farias (2011)

Tendo a nova máscara, podemos passar a criar as sub-redes. Você já sabe que o endereço de rede possui todos os bits da porção de host definidos como zero e que o endereço de *broadcast* possui todos os bits da porção de host definidos como um. Assim, já podemos identificar o primeiro endereço de sub-rede, que será o próprio endereço de rede utilizado para realizar a divisão, mas com uma nova máscara. Para identificar o endereço de *broadcast*, colocamos todos os bits da porção de host com uns binários.

A figura ilustra o primeiro endereço de sub-rede e *broadcast*.

Todos os bits da porção de host definidos como zero	
Primeira sub-rede	- 172.16.0.0
Broadcast	- 172.16.63.255
Todos os bits da porção de host definidos como um	
Máscara de sub-rede	- 255.255.192.0

Figura 58 - Primeira sub-rede

Júlia Pelachini Farias (2011)

Os outros três endereços de sub-rede são obtidos por meio da manipulação dos dois bits da porção de sub-rede. Devemos realizar todas as combinações possíveis para obter os quatro endereços de sub-rede. As próximas sub-redes são apresentadas na figura a seguir. É importante que sempre que manipularmos os bits da porção de sub-rede, façamos a conversão em decimal do octeto completo e não somente dos dois bits manipulados.

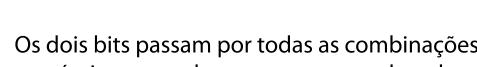
Segunda sub-rede	- 172.16.64.0 - 10101100.00010000. 01 00000.00000000
Terceira sub-rede	- 172.16.128.0 - 10101100.00010000. 10 00000.00000000
Quarta sub-rede	- 172.16.192.0 - 10101100.00010000. 11 00000.00000000
Os dois bits passam por todas as combinações possíveis para endereçar as quatro sub-redes 	
Máscara de sub-rede - 255.255.192.0 - 11111111.11111111.1100000.00000000	

Figura 59 - Bits da porção de rede e as demais redes para a divisão realizada

Júlia Pelachini Farias (2011)

Neste exemplo, foi necessário manipular somente dois bits para obter todas as combinações possíveis. No entanto, ao manipular mais bits esta tarefa será árdua. Na seção seguinte, você verá como obter as demais redes sem a necessidade de manipular os bits para a obtenção de todas as combinações.



FIQUE ALERTA

Um planejamento bem realizado permite o crescimento da rede, melhorar o roteamento da rede e economizar endereços IP.

9.2 REALIZANDO O CÁLCULO DE SUB-REDES

Como você viu, o endereço IP é composto por uma porção de rede e outra de host. Além disso, já estudou as diferentes classes de endereço, que possuem diferentes tamanhos para a porção de rede e host. Para determinar qual parte do endereço de 32 bits representa a porção de rede, é necessário utilizar a máscara. A máscara é um número de 32 bits, assim como o endereço IP, só que possui um conjunto de bits 1s contíguos, da esquerda para a direita, que indicam quais bits do endereço IP são significativos, ou seja, quais bits são de interesse para uso no roteamento. Esses bits significativos representam exatamente a porção de rede, conforme visto anteriormente.

O primeiro passo para efetuar o cálculo de sub-rede é definir qual endereço será utilizado pela organização. Esse endereço pode ser obtido de várias formas, por meio de um provedor de telecomunicações, pelo registro.br, ou podemos optar por utilizar endereços IP privados.

Uma vez obtido o endereço, é necessário determinar o número de redes ou o número de hosts desejados. O número de rede ou hosts irá nos indicar quantos bits precisamos pegar emprestados da porção de host para criar as sub-redes. Caso façamos a escolha por um determinado número de sub-redes, precisamos pegar bits emprestados da porção de host, de forma que estes sejam suficientes para endereçar o número de redes desejadas.

**FIQUE ALERTA**

Para obter o número de redes, deve-se usar a regra 2^b . Para obter o número de hosts válidos, deve utilizar a regra $2^b - 2$. A letra b indica o número de bits utilizados para endereçar a sub-rede ou hosts.

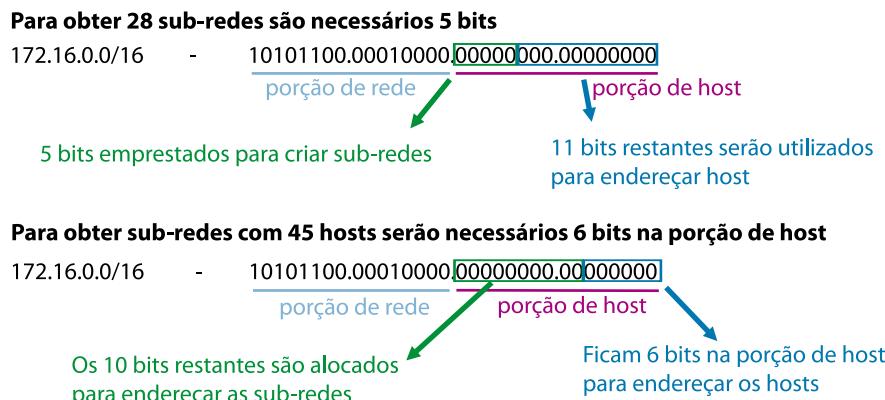
Por exemplo, se queremos 28 sub-redes, teremos que pegar 5 bits. Esses 5 bits no permitem obter 32 sub-redes, ou seja, 4 sub-redes a mais do que precisamos. No entanto, se fôssemos utilizar somente 4 bits, teríamos somente dezesseis sub-redes, número bem inferior ao necessário. Podemos considerar que usando cinco bits teremos quatro redes para um crescimento futuro.

Ao optar por redes com um número mínimo de hosts, precisamos verificar quantos bits são necessários deixar na porção de host para ter o número de hosts escolhido. Os bits restantes da porção de host serão os que pegaremos emprestado para criar as sub-redes.

**FIQUE ALERTA**

Os bits restantes da porção de host que pegaremos emprestados serão sempre os bits mais significativos, ou seja, mais à esquerda da porção de host.

Por exemplo, se desejamos 45 hosts por sub-rede teremos que deixar pelo menos 6 bits na porção de host. O restante dos bits, podemos pegar emprestados para utilizar na porção de rede. A figura a seguir ilustra os dois casos. Confira!



Júlia Pelachini Farias (2011)

Figura 60 - Alocação de bits para os dois casos: escolha pelo número de redes ou pelo número de hosts

No caso ilustrado na figura 60, quando feita a opção por 28 sub-redes, teremos na verdade 32 sub-redes. Cada uma dessas sub-redes terá 2046 hosts. Quando feita a opção por 45 hosts, teremos na verdade 62 hosts. Os 10 bits restantes são alocados para sub-rede totalizando 1024 sub-redes, cada uma delas com os 62 hosts.

Escolhido o número de bits que serão emprestados da porção de host, incluímos estes bits na máscara com a finalidade de determinar as sub-redes e os endereços de host. Finalmente, poderemos designar os endereços aos dispositivos da rede. Para o exemplo utilizado, as máscaras seriam as seguintes:

- para a opção pelo número de redes: 255.255.248.0;
- para a opção pelo número de hosts: 255.255.255.192.



FIQUE ALERTA

Ao adicionar os bits emprestados na máscara, lembre-se de utilizar a máscara padrão do endereço que está sendo utilizado como base.

Sempre que formos manipular os bits de um endereço para criar sub-redes, devemos ficar atentos à classe a qual pertence aquele endereço. Se for um endereço de classe A, a porção de rede possui 8 bits e a porção de host 24 bits. Podemos pegar bits emprestados da porção de host a partir do nono bit do endereço. No caso de um endereço de classe B, a porção de rede possui 16 bits, assim como a de host. A figura seguinte, mostra um endereço de cada classe com a máscara padrão (*classfull*). Ao pegar bits emprestados da porção de host, devemos pegar do décimo sétimo bit do endereço. Para classe C, que possui 24 bits de host, podemos pegar do vigésimo quinto em diante. Os bits devem sempre ser obtidos do mais significativo ao menos significativo, ou seja, da esquerda para a direita, em sequência, sem saltar um bit. Os bits disponíveis para empréstimo em cada classe são apresentados a seguir.

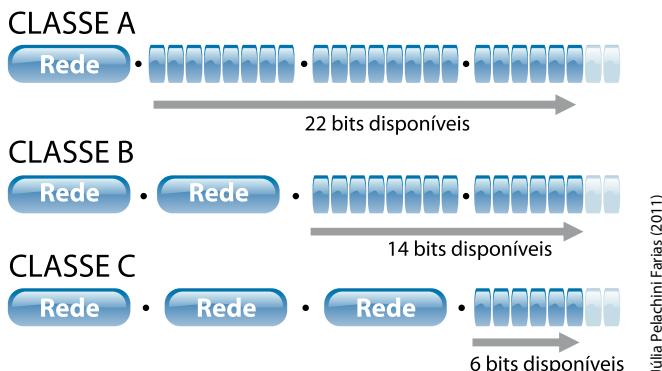


Figura 61 - Bits disponíveis para empréstimo em cada classe

Ao pegar bits emprestados, devemos tomar cuidado para deixar pelo menos dois bits para a porção host, ou seja, os dois últimos bits. Isso é necessário para ter sempre dois hosts válidos para cada rede. Dois bits nos permitem obter dois hosts, pois $2^2 - 2$ será dois, o que nos dá o número de hosts válidos para um endereço de rede que possui dois bits disponíveis na porção de host.

Veja alguns exemplos de divisão de endereços para criação de sub-redes. Nesses exemplos vamos realizar os cálculos usando como base tanto o número de redes, como o número de hosts desejados. Os endereços utilizados serão das classes A, B e C.

Para os exemplos 1 e 2 utilizaremos o endereço de classe A 10.0.0.0/8, para os exemplos 3 e 4 o endereço de classe B 172.16.0.0/16, e para os exemplos 5 e 6 o endereço de classe C 192.168.1.0/24.

EXEMPLO 1 – CLASSE A – 10.0.0.0/8

Desejamos dividir o endereço em 400 sub-redes. Utilizaremos o endereço de classe A 10.0.0.0 que tem como máscara padrão 255.0.0.0. Tendo o número de sub-redes, precisamos verificar quantos bits são necessários para termos o número 400 ou maior utilizando a regra de 2^b , onde b é o numero de bits necessários.

No caso de 400 sub-redes, precisaremos de 9 bits, pois 2^9 é igual a 512. Caso optássemos por 8 bits, teríamos somente 256 sub-redes, número insuficiente para a nossa necessidade.

Realizando este cálculo de 2^b identificamos que devemos pegar 9 bits emprestados da porção de host para que sejam utilizados na porção de sub-rede. Pegamos emprestados os 9 bits mais significativos da porção de host conforme destacado na figura a seguir. Podemos ver que a porção de host ficou com 15 bits. Estes bits serão utilizados para endereçar os hosts, totalizando 32.766 hosts por sub-rede.

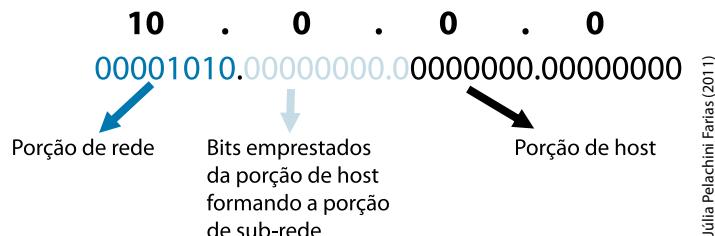
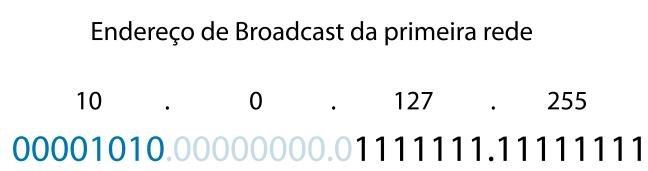


Figura 62 - Bits emprestados para obter quatrocentas sub-redes

Júlia Pelachini Farias (2011)

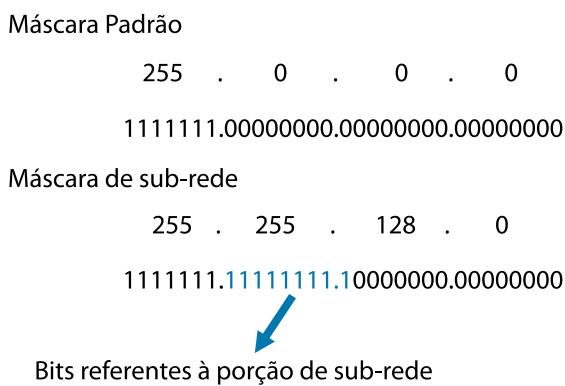
Para obter o primeiro endereço de rede e seu endereço de *broadcast*, é necessário definir todos os bits da porção de rede com 0s e 1s, respectivamente. A figura anterior apresenta a porção de host com todos os bits em zero e a figura a seguir, com todos os bits de host definidos em um.



Júlia Pelachini Farias (2011)

O primeiro endereço de host válido para a rede 10.0.0.0/17 é obtido definindo todos os bits de host como zero, exceto o último, ou seja, o menos significativo. Dessa forma teremos o endereço 10.0.0.1 como primeiro endereço válido. Para obter o último endereço, basta diminuir em uma unidade o valor do último octeto do endereço de *broadcast* e teremos o endereço 10.0.127.254 como o último endereço válido.

Além disso, temos que alterar a máscara de 255.0.0.0 para a máscara de sub-rede. Fazemos isso definindo como binários o número de bits referente à porção de sub-rede, neste caso 9 bits. A figura a seguir mostra a máscara padrão e a máscara de sub-rede.



Júlia Pelachini Farias (2011)

Figura 64 - Máscara padrão e máscara de sub-rede

Os demais endereços serão obtidos por meio da manipulação dos 9 bits emprestados para a porção de sub-rede. Devemos realizar todas as combinações possíveis de zeros e uns para obter todas as sub-redes, no entanto, realizar essa operação para muitos bits é cansativo.

Para obter o próximo endereço de rede, basta adicionar uma unidade ao último octeto do endereço de *broadcast*. Porém, ao fazer esta adição, obteremos o número 256. Como o valor de cada octeto deve estar entre 0 e 255, ao invés de colocar 256, colocamos zero e adicionamos uma unidade ao terceiro octeto. Obteremos o número 128 no terceiro octeto. O endereço obtido depois das adições será 10.0.128.0, ou seja, o segundo endereço de rede da divisão. A figura seguinte mostra o endereço de rede e de *broadcast* em binários.

O primeiro endereço válido da segunda rede será obtido da mesma forma que na primeira rede, definindo o bit menos significativo da porção de host como um. Teremos o endereço 10.0.128.1 como primeiro endereço válido para a segunda rede. No caso do endereço do último endereço válido, diminuímos uma unidade do último octeto do endereço de *broadcast*, ou seja, teremos o endereço 10.0.255.254. Veja.

Endereço da segunda rede

10 . 0 . 128 . 0	
00001010.00000000.10000000.00000000	

Endereço de broadcast da segunda rede

10 . 0 . 255 . 255	
00001010.00000000.11111111.11111111	

Júlia Pelachini Farias (2011)

Figura 65 - Endereço de rede e *broadcast* da segunda rede

Para obter o terceiro endereço de rede, o procedimento é o mesmo realizado para obter a segunda rede. Ao adicionar uma unidade ao quarto octeto, teremos o valor 256, ou seja, mudamos o octeto para zero e adicionamos um ao terceiro octeto. No entanto, o terceiro octeto também nos dará o valor 256 ao ser adicionado em um. Devemos alterar o terceiro octeto para zero e adicionar uma unidade ao segundo octeto. Teremos o valor um no segundo octeto e obteremos o terceiro endereço de rede, 10.1.0.0.

A tabela a seguir mostra os primeiros e últimos endereços de rede e seus respectivos endereços de *broadcast* para a divisão em sub-redes do endereço do exemplo 1.

Tabela 8 - Endereços de sub-rede para a divisão do exemplo 1

	ENDEREÇO DE REDE	ENDEREÇO DE BROADCAST
1º endereço	10.0.0.0	10.0.127.255
2º endereço	10.0.128.0	10.0.255.255
3º endereço	10.1.0.0	10.1.127.255
.	.	.
:	:	:
510º endereço	10.254.128.0	10.254.255.255
511º endereço	10.255.0.0	10.255.127.255
512º endereço	10.255.128.0	10.255.255.255

EXEMPLO 2 – CLASSE A – 10.0.0.0/8

Desejamos dividir o endereço de forma que tenhamos, pelos menos, 400 hosts por sub-rede. Utilizaremos o endereço de classe A 10.0.0.0/8 que tem como máscara padrão 255.0.0.0. Tendo o número de hosts desejados, precisamos verificar quantos bits são necessários para termos o número 400. Para isto, utilizamos a regra $2^b - 2$, onde b é o número de bits necessários para endereçar os hosts. No caso de 400 hosts, precisaremos de 9 bits, pois $2^9 - 2$ é igual a 510.

Realizando o cálculo de $2^b - 2$ identificamos que devemos utilizar 9 bits na porção de host para endereçar os quatrocentos hosts. Observe que, desta vez, os bits do cálculo não se referem aos bits que devemos pegar emprestados, mas sim aos bits utilizados para endereçar os hosts. Esses 9 bits serão os bits da nova porção de host. Para obter o número de bits da porção de sub-rede, devemos pegar os bits da porção de host original e subtrair os bits que necessitamos, ou seja, nove bits. Ao subtrair 9 de 24, obtemos 15. A porção de sub-rede terá 15 bits, que equivalem aos 15 bits mais significativos da porção de host original. Com os 15 bits da porção de rede, poderemos ter até 32.768 redes, cada uma com até 510 hosts. A figura a seguir ilustra as porções originais e as porções obtidas após o cálculo.

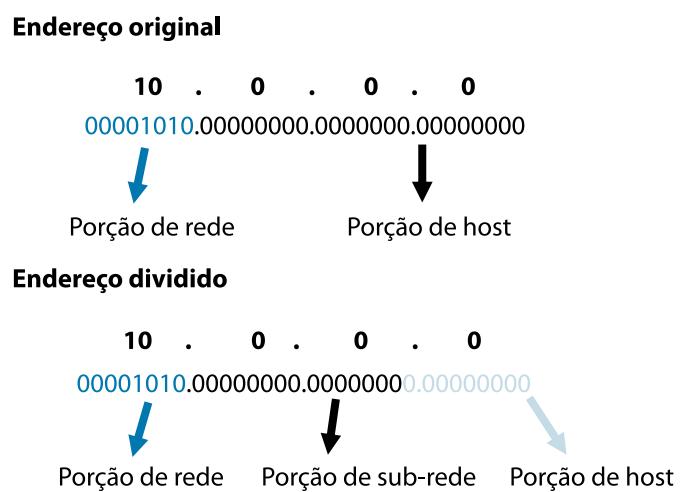


Figura 66 - Porções de um endereço IPv4 depois de dividido

Repare que, ao optar por definir o número de hosts como base para realizar o cálculo de sub-rede, os bits que serão emprestados para a porção de sub-rede são aqueles que não necessitamos para obter o número de hosts desejados. Depois de definidos quantos bits restaram para a porção de sub-rede, a obtenção dos endereços IP ocorre da mesma forma que foi apresentada no exemplo 1. Neste exemplo, a máscara de sub-rede terá 15 bits definidos como um, além dos 8 bits originais. Teremos como máscara de sub-rede em decimal 255.255.254.0, ou em binário **11111111.11111111.11111110.00000000**.

Para obtermos o primeiro endereço de rede e seu endereço de *broadcast*, necessitamos definir todos os bits da porção de rede com 0s e 1s respectivamente. A figura anterior apresenta a porção de host com todos os bits em zero e a figura a seguir, com todos os bits de host definidos em um.

Endereço de Broadcast de primeira rede

10 . 0 . 1 . 255	
00001010.00000000.00000001.11111111	

Júlia Petachini Farias (2011)

Figura 67 - Endereço de *broadcast* da primeira rede

O primeiro endereço de host válido para a rede 10.0.0.0/23 é obtido definindo todos os bits de host como zero, exceto o último, ou seja, o menos significativo. Dessa forma, teremos o endereço 10.0.0.1 como primeiro endereço válido. Para obter o último endereço, basta diminuir em uma unidade o valor do último octeto do endereço de *broadcast*. Teremos o endereço 10.0.1.254 como o último endereço válido.

Os demais endereços serão obtidos por meio da manipulação dos 15 bits emprestados para a porção de sub-rede. Devemos realizar todas as combinações possíveis de zeros e uns para obter todas as sub-redes.

Para obter o próximo endereço de rede, basta adicionar uma unidade ao último octeto do endereço de *broadcast*. No entanto, ao fazer esta adição obteremos o número 256. Devemos colocar zero neste octeto e adicionar uma unidade ao terceiro octeto. Obteremos o número um no terceiro octeto. O endereço obtido depois das adições será 10.0.2.0, ou seja, o segundo endereço de rede da divisão.

A Tabela a seguir mostra os endereços de rede e *broadcast* para as primeiras e últimas sub-redes.

Tabela 9 - Endereço de sub-rede para a divisão do exemplo 2

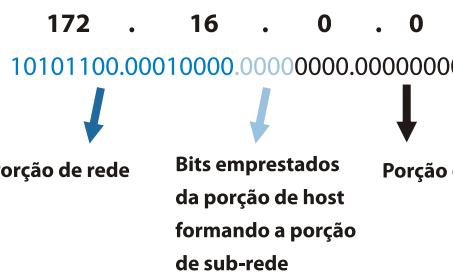
	ENDEREÇO DE REDE	ENDEREÇO DE BROADCAST
1º endereço	10.0.0.0	10.0.1.255
2º endereço	10.0.2.0	10.0.3.255
3º endereço	10.0.4.0	10.0.5.255
.	.	.
:	:	:
32766º endereço	10.255.250.0	10.254.251.255
32767º endereço	10.255.252.0	10.255.253.255
32768º endereço	10.255.254.0	10.255.255.255

EXEMPLO 3 – CLASSE B – 172.16.0.0/16

Desejamos dividir o endereço em 12 sub-redes. Utilizaremos o endereço de classe B 172.16.0.0 que tem como máscara padrão 255.255.0.0. Tendo o número de sub-redes, precisamos verificar quantos bits são necessários para termos o número doze ou maior, utilizando a regra de 2^b , onde b é o número de bits necessários. No caso de doze sub-redes, precisaremos de 4 bits, pois 2^4 é igual a 16. Caso optássemos por 3 bits, teríamos somente 8 sub-redes, número insuficiente para a nossa necessidade.

Realizando este cálculo de 2^b identificamos que devemos pegar 4 bits emprestados da porção de host para que sejam utilizados na porção de sub-rede. Pegamos emprestados os 4 bits mais significativos da porção de host, conforme destacado na figura a seguir.

Você pode ver que a porção de host ficou com 12 bits. Estes bits serão utilizados para endereçar os hosts, totalizando 4.094 hosts por sub-rede.



Júlia Pelachini Farias (2011)

Figura 68 - Bits emprestados para obter dez sub-redes

Para obter o primeiro endereço de rede e seu endereço de broadcast, precisamos definir todos os bits da porção de rede com 0s e 1s, respectivamente. A figura anterior apresenta a porção de host com todos os bits em zero e a figura a seguir com todos os bits de host definidos em um.

Endereço de Broadcast da primeira rede

172 . 16 . 15 . 255

10101100.00010000.00001111.11111111

Júlia Pelachini Farias (2011)

Figura 69 - Endereço de *broadcast* da primeira rede

O primeiro endereço de host válido para a rede 172.16.0.0/20 é obtido definindo todos os bits de host como zero, exceto o último, ou seja, o menos significativo. Dessa forma, teremos o endereço 172.16.0.1 como primeiro endereço válido. Para obter o último endereço, basta diminuir em uma unidade o valor do último octeto do endereço de *broadcast*. Teremos o endereço 172.16.15.254 como o último endereço válido.

Os demais endereços serão obtidos por meio da manipulação dos 4 bits emprestados para a porção de sub-rede. Devemos realizar todas as combinações possíveis de zeros e uns para obter todas as sub-redes.

Para obter o próximo endereço de rede, basta adicionar uma unidade ao último octeto do endereço de *broadcast*. No entanto, ao fazer esta adição obteremos o número 256. Como o valor de cada octeto deve estar entre 0 e 255, ao invés de colocar 256, colocamos zero e adicionamos uma unidade ao terceiro octeto. Obteremos o número 16 no terceiro octeto. O endereço obtido depois das adições será 172.16.16.0, ou seja, o segundo endereço de rede da divisão. A figura a seguir mostra o endereço de rede e de *broadcast* em binários.

O primeiro endereço válido da segunda rede será obtido da mesma forma do que na primeira rede, definindo o bit menos significativo da porção de host como um. Teremos o endereço 172.16.16.1 como primeiro endereço válido para a segunda rede. No caso do último endereço válido, diminuímos uma unidade do último octeto do endereço de *broadcast*, ou seja, teremos o endereço 172.16.31.254.

Endereço da segunda rede

172 . 16 . 16 . 0

10101100.00010000.00010000.00000000

Júlia Pelachini Farias (2011)

Endereço de broadcast da segunda rede

172 . 16 . 31 . 255

10101100.00010000.00011111.11111111

Figura 70 - Endereço de rede e *broadcast* da segunda rede

A Tabela 10 mostra os dezesseis endereços de sub-rede e seus respectivos endereços de *broadcast* para a divisão em sub-redes do endereço do exemplo 3.

Tabela 10 - Endereços de sub-rede para a divisão do exemplo 3

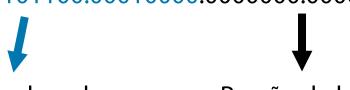
	ENDEREÇO DE REDE	ENDEREÇO DE BROADCAST
1º endereço	172.16.0.0	172.16.15.255
2º endereço	172.16.16.0	172.16.31.255
3º endereço	172.16.32.0	172.16.47.255
4º endereço	172.16.48.0	172.16.63.255
5º endereço	172.16.64.0	172.16.79.255
6º endereço	172.16.80.0	172.16.95.255
7º endereço	172.16.96.0	172.16.111.255
8º endereço	172.16.112.0	172.16.127.255
9º endereço	172.16.128.0	172.16.143.255
10º endereço	172.16.144.0	172.16.159.255
11º endereço	172.16.160.0	172.16.175.255
12º endereço	172.16.176.0	172.16.191.255
13º endereço	172.16.192.0	172.16.207.255
14º endereço	172.16.208.0	172.16.223.255
15º endereço	172.16.224.0	172.16.239.255
16º endereço	172.16.240.0	172.16.255.255

EXEMPLO 4 – CLASSE B - 172.16.0.0/16

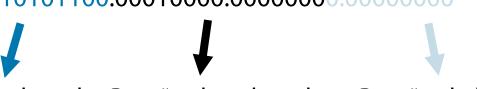
Desejamos dividir o endereço de forma que tenhamos pelos menos 200 hosts por sub-rede. Utilizaremos o endereço de classe B 172.16.0.0 que tem como máscara padrão 255.255.0.0. Tendo o número de hosts desejados, precisamos verificar quanto bits são necessários para termos o número 200. Para isto, utilizamos a regra 2^b-2 , onde b é o número de bits necessários para endereçar os hosts. No caso de 200 hosts, precisaremos de 8 bits, pois 2^8-2 é igual a 254.

Realizando o cálculo de 2^b-2 , identificamos que devemos utilizar 8 bits na porção de host para endereçar os 200 hosts. Observe que, desta vez, os bits do cálculo não se referem aos bits que devemos pegar emprestados, mas sim aos bits utilizados para endereçar os hosts. Esses 8 bits serão os bits da nova porção de host. Para obter o número de bits da porção de sub-rede, devemos pegar os bits da porção de host original e subtrair os bits que necessitamos, ou seja, 8 bits. Ao subtrair 8 de 16, obtemos 8. A porção de sub-rede terá 8 bits, que equivale aos 8 bits mais significativos da porção de host original. Com os 8 bits da porção de rede, poderemos ter até 256 redes cada uma com até 254 hosts. A figura a seguir ilustra as porções originais e as obtidas após o cálculo.

Endereço original

172 . 16 . 0 . 0
 10101100.00010000.00000000.00000000


Endereço dividido

172 . 0 . 0 . 0
 10101100.00010000.00000000.00000000


Júlia Pelachini Farias (2011)

Figura 71 - Porções do endereço IPv4 antes e depois da divisão em sub-redes

Repare que ao optar por definir o número de hosts como base para realizar o cálculo de sub-rede, os bits que serão emprestados para a porção de sub-rede são aqueles que não necessitamos para obter o número de hosts desejados. Depois de definido quantos bits restaram para a porção de sub-rede, a obtenção dos endereços IP ocorre da mesma forma que foi apresentada no exemplo 2. Neste exemplo, a máscara de sub-rede terá 8 bits definidos como um, além dos 16 originais. Teremos como máscara de sub-rede em decimal 255.255.255.0, ou em binário, 11111111.11111111.11111111.00000000.

Para obter o primeiro endereço de rede e seu endereço de *broadcast*, necessitamos definir todos os bits da porção de rede com 0s e 1s respectivamente. A figura anterior apresenta a porção de host com todos os bits em zero e a figura a seguir, com todos os bits de host definidos em um.

Endereço de Broadcast da primeira rede

172 . 16 . 0 . 255
 10101100.00010000.00000000.11111111

Júlia Pelachini Farias (2011)

Figura 72 - Endereço de broadcast da primeira rede

O primeiro endereço de host válido para a rede 172.16.0.0/24 é obtido definindo todos os bits de host como zero, exceto o último, ou seja, o menos significativo. Dessa forma, teremos o endereço 172.16.0.1 como primeiro endereço válido. Para obter o último endereço, basta diminuir em uma unidade o valor do último octeto do endereço de broadcast. Teremos o endereço 172.16.0.254 como o último endereço válido.

Os demais endereços serão obtidos por meio da manipulação dos 15 bits emprestados para a porção de sub-rede. Devemos realizar todas as combinações possíveis de zeros e uns para obter todas as sub-redes.

Para obter o próximo endereço de rede, basta adicionar uma unidade ao último octeto do endereço de broadcast. No entanto, ao fazer esta adição obteremos o número 256. Devemos colocar zero neste octeto e adicionar uma unidade ao terceiro octeto. Obteremos o número um no terceiro octeto. O endereço obtido depois das adições será 172.16.1.0, ou seja, o segundo endereço de rede da divisão. A tabela a seguir mostra os primeiros e últimos endereços de sub-rede para a divisão do endereço 172.16.0.0/16.

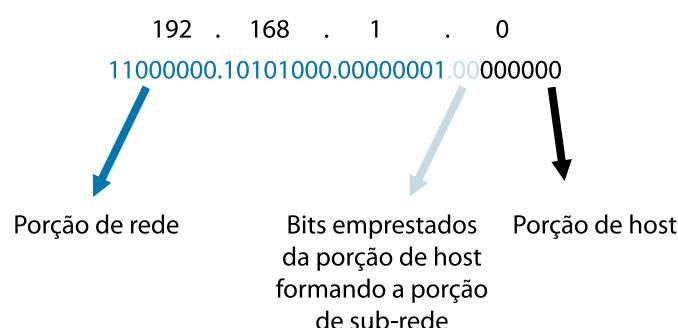
Tabela 11 - Endereço de sub-rede para a divisão do exemplo 4

	ENDEREÇO DE REDE	ENDEREÇO DE BROADCAST
1º endereço	172.16.0.0	172.16.0.255
2º endereço	172.16.1.0	172.16.1.255
3º endereço	172.16.2.0	172.16.2.255
.	.	.
:	:	:
510º endereço	172.16.253.0	172.16.253.255
511º endereço	172.16.254.0	172.16.254.255
512º endereço	172.16.255.0	172.16.255.255

EXEMPLO 5 – CLASSE C - 192.168.1.0/24

Desejamos dividir o endereço em 3 sub-redes. Utilizaremos o endereço de classe C 192.168.1.0 que tem como máscara padrão 255.255.255.0. Tendo o número de sub-redes, precisamos verificar quantos bits são necessários para termos o número 3 ou maior utilizando a regra de 2^b , onde b é o número de bits necessários. No caso de três sub-redes, precisaremos de 2 bits, pois 2^2 é igual a quatro.

Realizando este cálculo de 2^b identificamos que devemos pegar 2 bits emprestados da porção de host para que sejam utilizados na porção de sub-rede. Pegamos emprestados os 2 bits mais significativos da porção de host, conforme destacado na figura a seguir. Perceba que a porção de host ficou com 6 bits. Estes bits serão utilizados para endereçar os hosts, totalizando 62 hosts por sub-rede.



Júlia Pelachini Farias (2011)

Figura 73 - Bits emprestados para obter dez sub-redes

Para obter o primeiro endereço de rede e seu endereço de *broadcast*, necessitamos definir todos os bits da porção de rede com 0s e 1s respectivamente. A figura anterior apresenta a porção de host com todos os bits em zero e a figura a seguir, com todos os bits de host definidos em um.

Endereço de Broadcast da primeira rede

192 . 168 . 1 . 63

11000000.10101000.00000001.00111111

Figura 74 - Endereço de *broadcast* da primeira rede

Júlia Pelachini Farias (2011)

O primeiro endereço de host válido para a rede 192.168.1.0/26 é obtido definindo todos os bits de host como zero, exceto o último, ou seja, o menos significativo. Dessa forma teremos o endereço 192.168.1.1 como primeiro endereço válido. Para obter o último endereço, basta diminuir em uma unidade o valor do último octeto do endereço de *broadcast*. Teremos o endereço 192.168.1.62 como o último endereço válido.

Os demais endereços serão obtidos por meio da manipulação dos 2 bits emprestados para a porção de sub-rede. Devemos realizar todas as combinações possíveis de zeros e uns para obter todas as sub-redes.

Para obter o próximo endereço de rede, basta adicionar uma unidade ao último octeto do endereço de *broadcast*. Ao fazer esta adição obteremos o número 64. O endereço obtido depois da adição será 192.168.1.64, ou seja, o segundo endereço de rede da divisão. O primeiro endereço válido da segunda rede será obtido da mesma forma do que na primeira rede, definindo o bit menos significativo da porção de host como um. Teremos o endereço 192.168.1.65 como primeiro endereço válido para a segunda rede. No caso do último endereço válido, diminuímos uma unidade do último octeto do endereço de *broadcast*, ou seja, teremos o endereço 192.168.1.126. A figura a seguir mostra o endereço de rede e de *broadcast* em binários e apresenta os endereços de rede e *broadcast* para a segunda rede.

Endereço da Segunda rede

192 . 168 . 1 . 64

11000000.10101000.00000001.01000000

Júlia Pelachini Farias (2011)

Endereço de broadcast da Segunda rede

192 . 168 . 1 . 127

11000000.10101000.00000001.01111111

Figura 75 - Endereço de rede e *broadcast* da segunda rede

A tabela a seguir mostra os quatro endereços de sub-rede e seus respectivos endereços de *broadcast* para a divisão em sub-redes do exemplo 5.

Tabela 12 - Endereços de sub-rede para a divisão do exemplo 5

	ENDEREÇO DE REDE	ENDEREÇO DE BROADCAST
1º endereço	192.168.1.0	192.168.1.63
2º endereço	192.168.1.64	192.168.1.127
3º endereço	192.168.1.128	192.168.1.191
4º endereço	192.168.1.192	192.168.1.255

EXEMPLO 6 – CLASSE C - 192.168.1.0/24

Neste exemplo, desejamos dividir o endereço de forma que tenhamos, pelo menos, 100 hosts por sub-rede. Utilizaremos o endereço de classe C 192.168.1.0 que tem como máscara padrão 255.255.255.0. Tendo o número de hosts desejados, precisamos verificar quanto bits são necessários para termos o número 100. Para isto, utilizamos a regra 2^b-2 , onde b é o número de bits necessários para endereçar os hosts. No caso de 100 hosts, precisaremos de sete bits, pois 2^7-2 é igual a 128.

Realizando o cálculo de 2^b-2 identificamos que devemos utilizar 7 bits na porção de host para endereçar os 100 hosts. Observe que, desta vez, os bits do cálculo não se referem aos bits que devemos pegar emprestados, mas sim aos bits utilizados para endereçar os hosts. Esses 7 bits serão os bits da nova porção de host. Para obter o número de bits da porção de sub-rede, devemos pegar os bits da porção de host original e subtrair os bits que necessitamos, ou seja, 7 bits. Ao subtrair 7 de 8 obtemos um. A porção de sub-rede terá um bit, que equivale ao o bit mais significativo da porção de host original. Com o bit da porção de rede, poderemos ter até duas redes com até 126 hosts cada. A figura a seguir ilustra as porções originais e as obtidas após o cálculo.

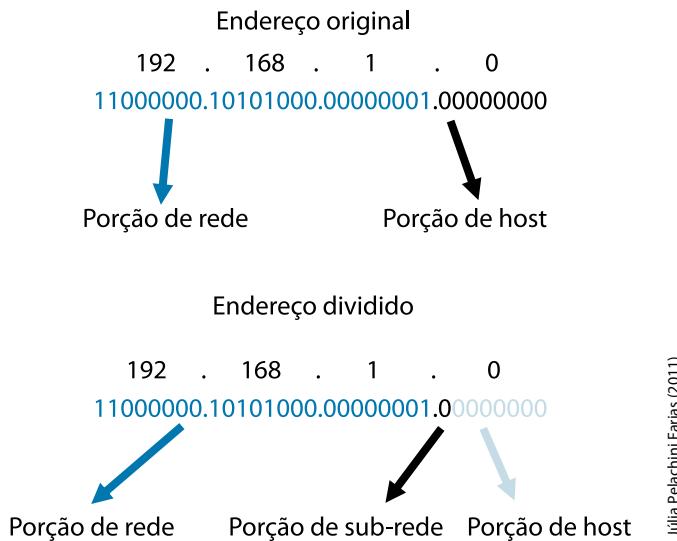


Figura 76 - Porções de um endereço IPv4 depois de dividido

Júlia Pelachini Farias (2011)

Repare que ao optar por definir o número de hosts como base para realizar o cálculo de sub-rede, o bit emprestado para a porção de sub-rede é aquele que não necessitamos para obter o número de hosts desejados. Depois de definido quantos bits restaram para a porção de sub-rede, a obtenção dos endereços IP ocorre da mesma forma que foi apresentada no exemplo 1 e 3. Neste exemplo, a máscara de sub-rede terá um bit definido como um, além dos vinte e quatro originais. Teremos como máscara de sub-rede em decimal 255.255.255.128 ou em binário 11111111.11111111.11111111.**1**0000000.

Para obter o primeiro endereço de rede e seu endereço de *broadcast*, necessitamos definir todos os bits da porção de rede com 0s e 1s respectivamente. A figura a seguir apresenta a porção de host com todos os bits em zero e a figura 80 com todos os bits de host definidos em um.

Endereço de Broadcast da primeira rede

192 . 168 . 1 . 127
11000000.10101000.00000001.**1**01111111

Figura 77 - Endereço de rede da segunda sub-rede

Júlia Pelachini Farias (2011)

O primeiro endereço de host válido para a rede 192.168.1.0/25 é obtido definindo todos os bits de host como zero, exceto o último, ou seja, o menos significativo. Dessa forma teremos o endereço 192.168.1.1 como primeiro endereço válido. Para obter o último endereço, basta diminuir em uma unidade o valor do último octeto do endereço de *broadcast*. Teremos o endereço 192.168.1.126 como o último endereço válido.

Os demais endereços serão obtidos por meio da manipulação do bit empregado para a porção de sub-rede. Devemos realizar todas as combinações possíveis de zeros e uns para obter todas as sub-redes, que neste caso pode ser somente 0 ou 1.

Para obter o próximo endereço de rede, basta adicionar uma unidade ao último octeto do endereço de *broadcast*. Obteremos o número 128, que nos dará 192.168.1.128, ou seja, o segundo e último endereço de rede da divisão. A tabela a seguir mostra os endereços de rede e *broadcast* para a divisão do exemplo 6.

Tabela 13 - Divisão de sub-redes para o exemplo 6

	ENDEREÇO DE REDE	ENDEREÇO DE BROADCAST
1º endereço	192.168.1.0	192.168.1.127
2º endereço	192.168.1.128	192.168.1.255

Acompanhe um exemplo de planejamento de endereçamento de IP no Casos e Relatos, e entenda melhor como funciona.



CASOS E RELATOS

Planejamento do Endereçamento IP

Vicente foi contratado para elaborar um esquema de endereçamento para uma pequena empresa. Esta pequena empresa possui cinco áreas de atuação e gostaria que essas áreas ficassem separadas logicamente. Cada área possui no máximo 100 hosts.

Sabendo que são necessárias cinco redes com cem hosts cada, Vicente procurou obter uma boa relação de bits para porção de rede e hosts de um endereço.

Para obter cinco redes, são necessários 3 bits, pois $2^3 = 8$. Para obter 100 hosts, são necessários 7 bits, pois $2^{7-2} = 128$. No total, Vicente utilizará 10 bits, ou seja, ele precisa escolher um endereço no qual seja possível manipular 10 bits. Um endereço de classe C possui somente 8 bits na porção de host. Neste caso, constata-se que não é possível utilizar um único endereço de classe C. Uma opção seria utilizar mais de um endereço de classe C, mas Vicente optou por utilizar um endereço de classe B, pois este possui 16 bits na porção de host. O endereço selecionado é 172.16.0.0/16. Tendo os 16 bits disponíveis, Vicente optou por realizar o cálculo com base no número de bits da porção de host, que são 7.

Restam da porção de host original 16 menos 7, ou seja, 9 bits. Haverá 512 redes com até 126 hosts cada. A máscara de sub-rede será 255.255.255.128. O primeiro endereço de rede será a própria rede escolhida, mas utilizando a nova máscara. Ficou como 172.16.0.0/25. O endereço de *broadcast* é obtido definindo todos os bits da porção de host como um, ou seja, os últimos 7 bits do endereço. Ficou 172.16.0.63/25. Para obter o segundo endereço de rede, adicionamos um ao endereço de *broadcast* da primeira sub-rede. Ficou 172.16.0.64/25. Continuando o processo de cálculo, haverá 5 redes que serão utilizadas e ainda sobram 507 redes. Se feita a opção por utilizar endereços de classe C, seria necessário utilizar três endereços de classe C. Pois, alocando 7 bits para host, pode-se endereçar duas redes com cada endereço de classe C.



RECAPITULANDO

Neste capítulo, você viu o que são sub-redes e aprendeu a realizar os cálculos para divisão em sub-redes. Esses conceitos ajudarão você a planejar o endereçamento de redes de forma a obter o melhor aproveitamento de endereços IPv4. Além disso, conhecer como se realizam cálculos de sub-redes e endereçamento IP, ajuda na compreensão do funcionamento de roteamento em redes e na solução de problemas de endereçamento e roteamento. No próximo capítulo você verá quais são os principais ativos de redes e suas funções. Até mais.

Ativos de Rede

10



Neste capítulo, você estudará os equipamentos que compõem a rede. Estes equipamentos são conhecidos como ativos de rede e são os responsáveis pela interconexão e transmissão dos dados por meio de redes de comunicação, sejam elas locais (LAN) ou de longa distância (WAN). Esses equipamentos são conhecidos por ativos porque eles atuam na manipulação dos sinais para que a transmissão dos dados seja realizada com sucesso.

Ao final deste capítulo você terá subsídios para:

- a) conhecer os ativos de rede, suas características, funcionamento e identificar como melhor aplicá-los a um projeto de rede.

10.1 TIPOS DE ATIVOS DE REDE

Os ativos de rede são componentes essenciais para o funcionamento de uma rede de comunicação. São os dispositivos eletrônicos responsáveis pela transmissão dos sinais por meio dos diversos meios físicos entre uma origem e um destino.

Para elaborarmos um projeto de rede, precisamos escolher quais ativos irão compor a infraestrutura. No entanto, a escolha dos ativos não é uma tarefa simples. Precisamos conhecer bem cada um deles, suas características e funcionamento. Dessa forma, saberemos escolher quais ativos devemos utilizar durante a elaboração de um projeto, para satisfazer as necessidades das aplicações e serviços que serão executados na rede. Essa escolha é muito importante, pois afetará o funcionamento da infraestrutura e, também, como se dará o crescimento quando houver uma necessidade de ampliação da rede.

Os principais ativos de rede em uso atualmente são os switches, roteadores, e pontos de acesso a rede sem fio. No entanto, você estudará outros dois ativos – hubs e pontes – pois estes nos ajudarão a compreender melhor o funcionamento dos demais. Além desses ativos, você conhecerá os repetidores, ainda utilizados, mas não comuns em redes corporativas locais.



FIQUE ALERTA

A escolha correta dos ativos de uma rede auxilia no projeto de uma rede escalável com bom desempenho!

Nos capítulos anteriores você estudou o modelo de referência OSI e suas sete camadas. Agora você verá que os ativos de rede operam nas diferentes camadas deste modelo, e, portanto, é importante lembrar a função de cada camada. Sempre que nos referimos a um dispositivo que atua em uma determinada camada, esta referência é feita em relação às camadas do modelo de referência OSI. Geralmente, essa referência é feita por meio de números, como por exemplo, camada 1 (física), camada 2 (enlace), camada 3 (rede) e assim por diante.

Os repetidores e hubs operam na camada física, as pontes, switches e pontos de acesso operam na camada de enlace e os roteadores na camada de rede. Existe um caso especial de switches que operam na camada de rede. Esses switches são capazes de realizar algumas tarefas de camada 3. Esse caso especial será estudado com mais detalhes em outra unidade curricular.

Para entender um pouco melhor o que você acabou de estudar, acompanhe o “casos e relatos” a seguir.



CASOS E RELATOS

Eliminando colisões na rede local

Uma determinada empresa possui uma infraestrutura de rede muito antiga, pois foi uma das primeiras a adotar o uso de redes de comunicação. O gerente de TI, sabendo que estava além de seus conhecimentos reestruturar a infraestrutura de rede, contratou Gustavo para uma consultoria. Ao iniciar os trabalhos, Gustavo procurou conhecer a infraestrutura de rede e os relatos dos usuários. Primeiramente, ele identificou que boa parte da infraestrutura era muito antiga, repleta de hubs, e que a principal reclamação dos usuários era a lentidão no acesso aos sistemas. Além disso, todos os usuários estavam compartilhando o mesmo domínio de *broadcast*. Como consultor experiente, Gustavo sugeriu a troca de hubs por switches e a adoção de um roteador, para realizar a divisão de domínios de *broadcast* por meio da segmentação da rede. Os switches evitam as colisões, pois cada porta se torna um domínio de colisão e a segmentação utilizando um roteador reduz os domínios de *broadcast*, consequentemente, o tráfego em cada domínio. Essas duas ações em conjunto refletem em um melhor desempenho da rede.

Nessa etapa, você conheceu os principais ativos de redes que estão em uso atualmente e conferiu um exemplo de uma situação real, no casos e relatos. Na etapa seguinte, você acompanhará cada um dos principais ativos, detalhadamente, conferindo além das suas características, o seu funcionamento. Lembre-se que todas essas informações são essenciais para o bom desenvolvimento de um profissional, portanto, mantenha-se atento!

10.2 FUNCIONAMENTO E CARACTERÍSTICAS

Conheça, agora, um pouco sobre os ativos de rede que atuam nas camadas do modelo OSI.

10.2.1 REPETIDOR

O repetidor é um dispositivo que atua na camada física e tem como função regenerar o sinal elétrico recebido. Ele é composto de duas interfaces. Os meios físicos de transmissão possuem limitações de comprimento, pois quanto maior a distância, maior será a atenuação do sinal. Há casos nos quais é necessário manipular o sinal recebido, de forma que ele volte a ter as mesmas características de quando foi enviado na origem. Em situações como estas, é necessário inserir um repetidor para conectar segmentos de uma mesma rede, que por questões de distância, necessitam ter o sinal regenerado.

É importante notar que regenerar significa melhorar, restaurar ou corrigir. Em nosso caso, será regenerado um sinal elétrico. Essa situação se difere do caso de amplificar, pois amplificar é dar mais força ao sinal, fazê-lo ficar maior, o que não é desejável, pois pode acabar amplificando ruídos da rede, além dos sinais de dados que foram efetivamente enviados.

Como o repetidor é um dispositivo que atua na camada de rede, ele não reconhece as informações de quadro como endereçamento ou verificação de erros. Este reconhecimento fica a cargo dos dispositivos que atuam na camada de enlace ou superiores. Além disso, não podemos adicionar repetidores indefinidamente para aumentar o alcance da nossa rede. Há uma limitação de quatro repetidores devido ao modo como foi projetado o padrão de rede para garantir o funcionamento da comunicação. Por exemplo, em rede Ethernet, temos o CSMA/CD. Atualmente, os repetidores são utilizados também para aumentar o alcance de ondas de rádios e fibras ópticas.

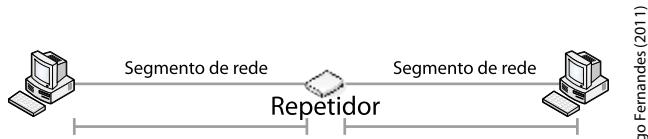


Figura 78 - Repetidor interligando dois segmentos de rede

Nessa figura você percebe dois segmentos de rede que já estão no comprimento máximo permitido pela especificação da tecnologia, utilizando um repetidor para regenerar o sinal.

10.2.2 HUB

Assim como o repetidor, o hub ou concentrador é um dispositivo que atua na camada física. No entanto, possui múltiplas portas permitindo a interconexão de diversos dispositivos através dele. Os quadros são encaminhados para todas as portas com objetivo de atingir o destino correto. O hub oferece um meio físico compartilhado, fazendo com que todos os dispositivos conectados a ele consigam trocar informações. Uma característica fundamental do hub é que os sinais inseridos em uma porta são replicados para todas as outras portas, além de serem regenerados.

Apesar da vantagem de permitir que vários dispositivos se conectem, o hub tem a grande desvantagem de compartilhar o meio físico. Os sinais de máquinas inseridos ao mesmo tempo no meio físico, mesmo que em diferentes portas, interferem uns nos outros. O uso do meio compartilhado leva ao conceito de domínio de colisão onde os sinais compartilham o mesmo meio e podem interferir uns nos outros, deturpando a qualidade da transmissão. Essa interferência é conhecida como colisão e afeta o desempenho da rede, pois o sinal não é recebido corretamente pelo destino. Os hubs reconhecem e tratam as colisões, notificando todas as portas por meio de um sinal conhecido como *Jam*. Ao receber o sinal de *Jam* os dispositivos conectados no hub reconhecerão que o sinal por eles enviado foi danificado por uma colisão e tomarão providências para retransmiti-lo. Nas redes Ethernet esse processo é chamado de *Backoff*.

Diversos fabricantes colocaram hubs no mercado, principalmente para o uso corporativo. Hubs incluíam até mesmo funções de gerenciamento com SNMP. Atualmente, pode ser encontrado à venda, mas o foco é voltado para uso em redes domésticas.

O uso de hubs gerava uma limitação no tamanho da rede devido às colisões. Para auxiliar no projeto de construção de redes com hub, utilizava-se a regra 5-4-3, ou também conhecida como 5-4-3-2-1. Essa sequência oferece uma diretriz de como estruturar uma rede Ethernet de 10 Mbps utilizando hubs. A sequência de número indica o seguinte: no máximo **5** segmentos entre dois hosts; no máximo **4** hubs; no máximo **3** segmentos populados com hosts; **2** ligações sem host; **1** domínio de colisão.

A figura mostra um exemplo no qual a regra é respeitada. Confira a seguir.

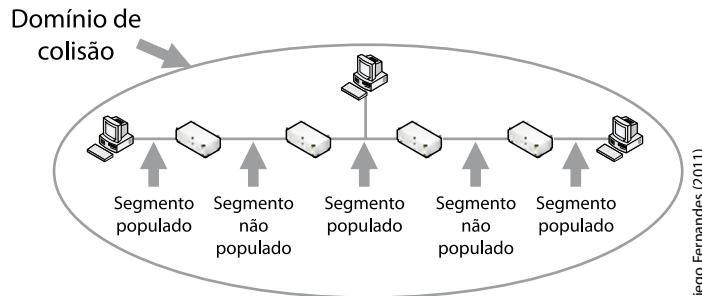
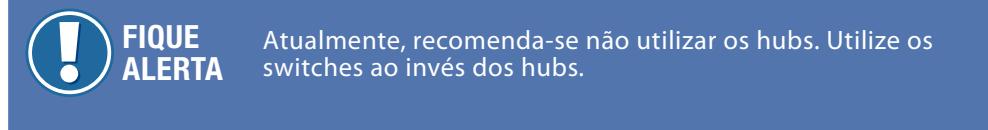


Figura 79 - Utilização de HUBs respeitando a regra 5-4-3-2-1

Hubs foram os principais ativos de rede no passado, permitindo a interconexão de estações de trabalho em redes corporativas. Atualmente, devido ao seu baixo desempenho, recomenda-se que sejam integralmente substituídos por switches.



10.2.3 PONTES

Bridge é um dispositivo que atua na camada de enlace. Em português, a palavra *bridge* corresponde à ponte. Diferentemente do hub, a ponte possui duas portas para conexão, não necessariamente na mesma tecnologia.

Como uso de pontes, é possível interconectar duas redes com tecnologias diferentes, ou redes de mesma tecnologia, mas de forma segmentada. O hub forma um único domínio de colisão, já a ponte divide a rede em dois segmentos ou dois domínios de colisão. Essa divisão é feita por meio da filtragem dos quadros de camada de enlace de dados que passam por ela. Somente podem transitar para o outro lado da ponte quadros que estão endereçados para dispositivos conectados naquele lado, quadros que ainda não foram mapeados (desconhecidos) ou quadros *broadcast*. Esse mapeamento é feito por meio de uma tabela de endereço MAC que registra os endereços conectados em cada porta.

Baseado nas informações desta tabela, a ponte irá ou não encaminhar os quadros, que são mapeados baseados no seu endereço de origem. Quando o quadro entra em uma porta, a ponte imediatamente adiciona na tabela o endereço de origem do quadro e vincula a porta de entrada ao endereço. A figura a seguir mostra a divisão dos domínios de colisão e *broadcast* com a utilização de pontes.

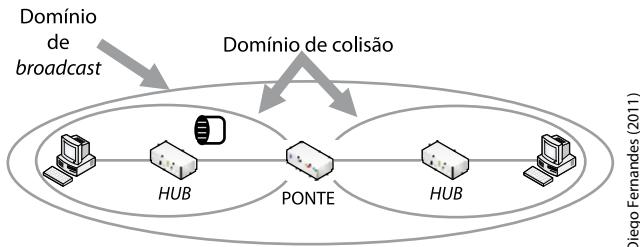


Figura 80 - Domínios de Colisão e Broadcast

Diego Fernandes (2011)


FIQUE ALERTA

As pontes somente adicionam endereços na tabela MAC baseados no endereço de origem dos quadros. Elas utilizam o endereço de destino para saber se devem ou não encaminhar o quadro por meio da ponte, comparando o endereço de destino com aqueles já constantes na tabela MAC.

A vantagem da utilização de pontes está na redução do domínio de colisão e do tráfego em cada segmento. A redução do domínio de colisão melhora o desempenho da rede. Além disso, as pontes verificam a integridade do quadro antes de encaminhá-lo para o outro segmento. No entanto, para os hosts conectados, a rede é uma só.

10.2.4 SWITCHES

O switch ou comutador é o dispositivo principal para prover a interconexão de hosts em uma rede local. Ele atua na camada de enlace, assim como a ponte. Há referências ao switch como sendo uma *bridge* multiporta. Baseado nessa colocação, podemos identificar algumas informações acerca do funcionamento de um switch.

A principal função do switch é encaminhar quadros de uma porta para outra. Considerando essa função podemos questionar qual a verdadeira necessidade de um switch se o hub já encaminhava os quadros para as demais portas? Bom, lembre-se que, além da possibilidade de encaminhar quadros entre as portas, o switch possui funcionalidades de uma *bridge*, mas com diversas portas, ou seja, além de encaminhar quadros, ele realiza a filtragem de pacotes utilizando o endereço MAC.

Do mesmo modo que a *bridge*, o switch possui uma tabela de endereços MAC que relaciona endereços com portas. Quando o switch recebe um quadro em uma determinada porta, ele analisa o endereço de origem e atualiza a tabela MAC para constar em qual porta aquele endereço está conectado. Dessa forma, o switch é capaz de enviar os quadros para a porta de destino correta, sem poluir as demais portas com quadros que não interessam aos outros dispositivos. Quando o mapeamento não existe, por exemplo, o host que possui o MAC de destino ainda não participou de uma comunicação na rede, o switch encaminha o quadro para todas as portas, exceto a porta de origem.

**VOCÊ SABIA?**

Você sabia que cada porta do switch forma um domínio de colisão?

Atualmente, a capacidade de transmissão das portas de switches está em torno de 10 Mbps a 10 Gbps, sendo que, quanto maior a velocidade e número de portas, maior o custo. Existem switches fixos, comprados com um determinado número de portas, e que não permitem adicionar mais portas, e switches modulares, que permitem adicionar portas de acordo com a necessidade. Esses switches modulares possuem limitação de número de portas, mas dependendo da marca e modelo esse número passa de 500 portas.

Além do encaminhamento de quadros entre portas, os switches atuais permitem realizar diversas outras tarefas na rede, desde o gerenciamento até funções relacionadas à segurança, divisão em redes virtuais, alimentação de energia para dispositivos como telefones IP e pontos de acesso, priorização de tráfego (qualidade de serviço), entre outros assuntos que serão abordados posteriormente no curso.

**SAIBA MAIS**

Você pode saber mais sobre os ativos de rede nos sites dos fabricantes, como <<http://www.cisco.com>>

10.2.5 PONTOS DE ACESSO A REDE SEM FIO

Os pontos de acesso à rede sem fio são dispositivos que atuam na camada de enlace e possuem rádios que operam em frequências padronizadas. Apesar de ser um dispositivo de camada 2, é importante lembrar que as ondas de rádio compartilham o mesmo meio (camada física) e há a ocorrência de colisões assim como em um *hub*. O dispositivo de rede sem fio consegue escutar todo o tráfego que está na sua frequência de operação como se fosse replicado em todas as portas. Você estudará em uma unidade curricular posterior como as colisões são evitadas e a forma como os clientes se associam ao ponto de acesso para que haja comunicação.

O uso de pontos de acesso permite que clientes se conectem uns aos outros sem a necessidade de uma conexão física por meio de um cabo. Ou seja, apesar de a comunicação ser sem fio, os clientes se comunicam através de um mediador, o ponto de acesso, e não diretamente uns com os outros. Uma grande vantagem da rede sem fio é a possibilidade de mobilidade dos usuários pelo ambiente de trabalho sem perda da conexão. Os clientes são dispositivos que possuem uma placa de rede sem fio que possibilita a comunicação como ponto de acesso. Além da mobilidade, o uso de pontos de acesso gera economia por não necessitar de cabos para cada cliente e, consequentemente, isso agiliza a implantação, pois as obras necessárias para cabeamento serão menores.

No caso das redes locais sem fio, os pontos de acesso operam nas frequências de 2.4 GHz e 5 GHz, oferecendo velocidades de conexão de 1 Mpbs até 600 Mbps. Vários são os padrões suportados pelos dispositivos sem fio, sendo que os detalhes de cada um serão estudados em uma unidade curricular posterior.



VOCÊ SABIA?

Você sabia que as frequências de rádio utilizadas para redes sem fio são regulamentadas pelo governo?

Assim como switches, é possível gerenciar os pontos de acesso e realizar alterações de configuração. A principal atividade de gerenciamento e configuração relacionada aos pontos de acesso está relacionada à segurança. As frequências de rádio não se limitam ao espaço físico de uma empresa ou escritório. Ou seja, qualquer um com uma antena consegue receptar o sinal se este estiver ao alcance. Portanto, é importante conhecer o funcionamento das redes sem fio e utilizar princípios de configuração segura, dessa forma não há problemas no uso de redes sem fio.

Geralmente o ponto de acesso sem fio vai estar conectado a uma rede cabeada para permitir o acesso a serviço de rede conforme ilustra a figura a seguir.

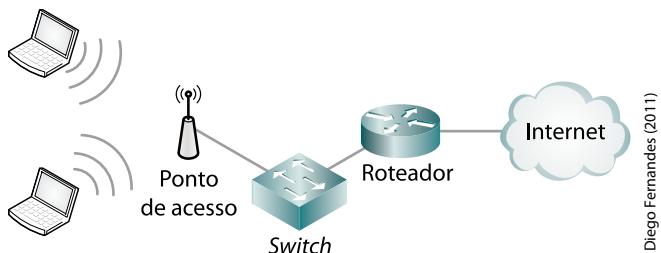


Figura 81 - Ponto de Acesso sem fio conectado a uma rede cabeada

Para os dispositivos terem acesso a redes sem fio, eles devem possuir uma placa de rede sem fio instalada. Atualmente, a maioria dos dispositivos móveis possui esta placa embutida, como notebooks e telefones móveis do tipo *smartphone*. No entanto, a conexão por rede sem fio não é exclusiva para dispositivos móveis, podem ser utilizadas em computadores de mesa, televisores, impressoras entre outros.

10.2.6 ROTEADORES

Você conheceu os ativos de redes que atuam na camada física e de enlace, repetidores, hubs, pontes, switches e pontos de acesso. Além disso, estes dispositivos permitem somente a conexão de clientes que estão na mesma rede ou no mesmo domínio de *broadcast*, pois manipulam sinais e quadros, porém, para que clientes em diferentes redes ou domínios de *broadcast* possam se comunicar, é necessário utilizar um roteador.

Os roteadores são dispositivos que atuam na camada de rede, ou seja, são capazes de realizar o encaminhamento de pacotes. Diferentemente de pontes e switches que realizam o encaminhamento baseado no endereço MAC, os roteadores usam o endereço IP.



FIQUE ALERTA

Os dispositivos que atuam na camada 2 também atuam na camada 1, assim como dispositivos que atuam na camada 3 também atuam nas camadas 2 e 1.

A principal função do roteador é interconectar diferentes redes. Para possibilitar a comunicação entre as diferentes redes, o roteador precisa determinar qual o melhor caminho para o destino do pacote e encaminhá-lo para o destino. Para definir o melhor caminho, ao invés de tabelas MAC, o roteador possui tabelas de roteamento. Essas tabelas possuem informações que indicam a interface que deve ser utilizada para o encaminhamento de um pacote com base no endereço IP de destino.

O roteador também tem a capacidade de realizar conexões de longa distância, ou seja, estabelecer a comunicação com pontos remotos distantes. Essas conexões de longa distância geralmente são estabelecidas com uso da infraestrutura de operadores de telecomunicações.

Os switches possuem porta de conexão para ligar computadores à rede local. Os roteadores, além de portas para acesso à rede local, possuem portas para acesso a diferentes tecnologias, como interfaces seriais síncronas/assíncronas para redes de longa distância em fio metálico e interfaces de fibra óptica.

Uma característica interessante dos roteadores é que eles não encaminham quadros de *broadcast*. Esses quadros somente são necessários em uma mesma rede, ou seja, dentro de um domínio de *broadcast*, portanto não há necessidade do roteador encaminhá-los, sendo muitas vezes conhecido como filtro de *broadcast* ou firewall de *broadcast*.

Diversas configurações de gerenciamento podem ser feitas em roteadores, tais como: configuração de rotas, protocolos de roteamento, configuração de interfaces, qualidade de serviço para priorização de tráfego, controle de acesso entre outras.

Você viu os principais ativos de rede e pode identificar que alguns deles são necessários para montarmos uma infraestrutura mínima para comunicação de rede. Outros já estão em desuso e devem ser substituídos. Além dos dispositivos estudados neste capítulo, diversos dispositivos existem e estão tendo seu uso indicado em rede, principalmente aqueles relacionados à segurança, como:

- a) *Firewall* – permite bloquear ou liberar acessos de uma rede a outra ou de acesso a serviços de rede; sistemas de detecção de intrusão ou sistemas de prevenção de intrusão;
- b) *Web Proxy* – para bloqueio de acesso a sites maliciosos ou inadequados para acesso no ambiente de trabalho;
- c) Filtros *anti-spam* – para o bloqueio de mensagens maliciosas no serviço de e-mail.

Esses dispositivos serão estudados em uma unidade curricular posterior, fique tranquilo!



RECAPITULANDO

Nesse capítulo você conheceu os principais ativos de redes em uso atualmente, e conferiu seu funcionamento básico e características. Conhecer a forma de operação dos ativos de rede é de extrema importância, pois ajudarão você na escolha dos dispositivos que devem ser empregados em um projeto de rede. Também ajudará a solucionar problemas que surgem no decorrer da implantação de uma rede ou na manutenção de uma rede existente. O assunto que você estudará no próximo capítulo é sobre os analisadores de protocolos. Até lá!

Anotações:

Analisadores de Protocolos

11



Nos capítulos anteriores, você estudou diversos conceitos que regem a comunicação em rede. Aprendeu que, para realizar a comunicação, são necessários protocolos e aplicações que os utilizam para estabelecer a troca de dados entre os dispositivos. A rede e as próprias aplicações podem apresentar falhas ou problemas de desempenho. Em diversos casos é necessário efetuar análises mais profundas sobre a comunicação em rede a fim de identificar a causa da falha ou problema. Estas análises envolvem o uso de ferramentas específicas que possuem a capacidade de analisar o tráfego gerado pelas aplicações, os sinais gerados por placas e antenas além de interferências eletromagnéticas.

Ao final deste capítulo você terá subsídios para:

- conhecer os conceitos relacionados à análise de protocolos de rede e as ferramentas que podem ser utilizadas para efetuar estas avaliações em busca da solução de problemas.

11.1 O QUE É UM ANALISADOR DE PROTOCOLO?

Há situações na qual necessitamos realizar uma avaliação mais específica do tráfego que transita em nossa rede em busca de causas para um desempenho ruim ou falhas. Ter conhecimento de que o tráfego é HTTP, FTP, SMTP, DNS entre outros, baseados nas portas de comunicação definidas pela camada de transporte, não é suficiente. As aplicações geralmente possuem uma porta TCP ou UDP definida como padrão que é alocada para comunicação em rede. No entanto, várias dessas aplicações possuem a capacidade de utilizar outras portas, quando suas portas padrões são bloqueadas por mecanismos de segurança de rede. Usualmente, essas aplicações procuram utilizar portas conhecidas por estarem sempre liberadas, como a porta TCP/80, utilizada para acesso a páginas web por meio do protocolo HTTP.



**SAIBA
MAIS**

É interessante você conhecer melhor as portas utilizadas por diversas aplicações. Você encontra uma lista dessas portas no site <<http://iana.org/assignments/port-numbers>> ou no arquivo <[/etc/services](#)> em sistemas Unix/Linux. Dê uma olhadinha. Vale a pena!

Para avaliar em maiores detalhes o desempenho da rede, pode ser necessário verificar se o tráfego que transita na rede é realmente aquele esperado. Algumas aplicações podem ser avaliadas para verificar falhas no desenvolvimento ou problemas de comunicação. Para que tais análises sejam realizadas, você pode utilizar os analisadores de protocolos.

Analisadores de protocolos são ferramentas que possuem a capacidade de analisar o tráfego que transita em uma rede. Estas ferramentas também são conhecidas como *sniffer* de pacotes, ou farejadores de pacotes, pois possuem a capacidade de interceptar o tráfego que transita na rede. As unidades de dados do protocolo (PDUs) são capturadas integralmente e as ferramentas de análise de protocolos conseguem decodificá-las. À medida que os quadros são capturados, estes são imediatamente exibidos na tela. Dependendo da ferramenta utilizada, gráficos com estatísticas podem ser exibidos em tempo real, no entanto, a quantidade de pacotes capturada é grande e exige que seja armazenado para uma análise posterior. Esta análise pode ser individual (de cada PDU), ou de um conjunto de PDUs, como por exemplo, analisar todo o fluxo de uma conexão TCP. Alguns analisadores de protocolos possuem a capacidade de gerar relatórios de eventos específicos na rede, do tipo de tráfego capturado, tamanho dos pacotes entre outros.

Quando falamos na análise de PDU, podemos entender que para a pilha de protocolos do modelo TCP/IP é possível identificar informações das PDU de cada camada. Para a camada de acesso à rede é possível identificar os tempos de recebimento do *frame* e o número de bits capturados, endereços físicos de origem e destino e qual o protocolo da camada superior. Para a camada de Internet é possível identificar endereços IP de origem e destino, *flags* e informações de fragmentação. Na camada de transporte, podemos identificar informações de porta de origem e destino, janelamento, número de sequência, entre outras, no caso do protocolo TCP. A camada de aplicação apresenta informações do protocolo utilizado, por exemplo, no HTTP informações da página acessada.

O mais interessante na análise de protocolos é que qualquer computador com uma placa de rede é capaz de se tornar um analisador de protocolo. Computadores portáteis se tornam um excelente analisador de protocolos, pois podem ser facilmente transportados até diferentes locais da infraestrutura de rede. Para tornar um computador um analisador de protocolos é necessário instalar uma aplicação que realiza a captura do tráfego que passa pela placa de rede deste computador. Na seção seguinte, você estudará algumas dessas aplicações.

Quando você estudou a camada de enlace, aprendeu que as interfaces de rede analisam o endereço de destino dos quadros para definir se irá processá-lo ou não. Somente os quadros que tiverem como endereço de destino o endereço da interface de rede ou o endereço de *broadcast* serão processados, os demais são descartados. Quando se fala em quadros processados, significa que estes são encaminhados para as camadas superiores.

Ao utilizar um analisador de protocolos, temos como objetivo capturar qualquer pacote que esteja em trânsito pela conexão de rede da interface, independente se este quadro está destinado para a nossa interface ou não. Para que a placa de rede seja capaz de capturar qualquer quadro, independentemente do endereço de destino, devemos colocá-la no modo promíscuo.



VOCÊ SABIA?

As ferramentas em análise de protocolos permitem que senhas sejam capturadas, caso não sejam enviadas criptografadas pela rede.

O modo promíscuo é um estado no qual a placa de rede é colocada num estado que permite que todos os quadros que passam por ela sejam capturados e encaminhados para processamento, independente do endereçamento. Geralmente, esse tráfego capturado é repassado para a aplicação que realiza a análise dos dados. Diferentes tecnologias de camada de enlace permitem a captura do tráfego, como rede Ethernet cabeada e sem fio. As próprias aplicações utilizadas

para realizar a captura dos quadros colocam a placa de rede em modo promíscuo. A figura a seguir apresenta informações de placa de rede antes da abertura da aplicação de captura e durante a execução do aplicativo. Compare as linhas em destaque. No segundo destaque, durante a execução da captura, a palavra PROMISC indica o modo promíscuo da placa de rede. Observe que a palavra estava ausente no primeiro destaque, já que não estava ocorrendo a captura de pacotes.

```
$ ifconfig
<-- informações omitidas para melhor leitura do resultado do comando -->
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether e0:f8:47:14:a2:b6
    inet6 fe80::e2f8:47ff:fe14:a2b6%en1 prefixlen 64 scopeid 0x5
        inet 192.168.0.171 netmask 0xffffffff broadcast 192.168.0.255
            media: autoselect
            status: active
<-- informações omitidas para melhor leitura do resultado do comando -->
$ ifconfig
<-- informações omitidas para melhor leitura do resultado do comando -->
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    ether e0:f8:47:14:a2:b6
    inet6 fe80::e2f8:47ff:fe14:a2b6%en1 prefixlen 64 scopeid 0x5
        inet 192.168.0.171 netmask 0xffffffff broadcast 192.168.0.255
            media: autoselect
            status: active
<-- informações omitidas para melhor leitura do resultado do comando -->
```

Figura 82 - Placa de rede no modo normal e em modo promíscuo

Diego Fernandes (2011)

Com o uso de hubs, essa captura era muito simples. Todo o tráfego do hub era repassado para todos os integrantes da rede. Com a evolução da tecnologia e a utilização de switches, essa situação deixou de ser tão simples. Na maioria dos casos, para realizar a captura de quadros, deve-se utilizar recursos dos switches de forma a definir em qual porta do equipamento o tráfego que se deseja analisar está passando. Tendo definido a porta, todo o tráfego que passa por ela é espelhado em uma porta na qual está conectado o analisador de protocolos.

A figura a seguir ilustra a situação, utilizando um hub e um switch. Repare, na parte (a) da figura, que ao utilizar um HUB o tráfego de A para B é replicado em todas as portas. Neste caso, o computador C precisa somente estar habilitado para a captura de pacotes. No caso do switch, na parte (b) da figura, o tráfego é encaminhado somente para o destino. Para realizar a captura numa infraestrutura com switch, além da máquina habilitada para capturar pacotes, devemos utilizar uma funcionalidade do switch que replica o tráfego de uma porta para outra. Observe, na figura (b), que o tráfego é replicado da porta 2, onde está conectado o computador de destino, para a porta 3, onde está conectado o analisador de protocolos.

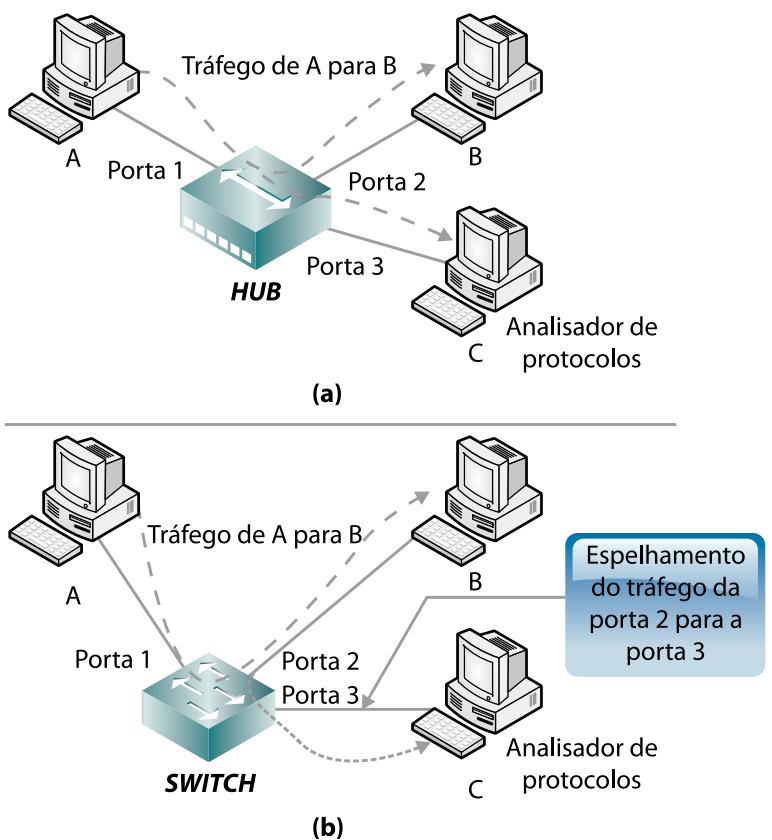


Figura 83 - Análise de protocolos utilizando hubs e switches

Diego Fernandes (2011)

Você aprendeu sobre a capacidade de um computador qualquer realizar a captura de tráfego para análise. Como viu, não é uma tarefa complicada e podemos nos questionar acerca da segurança de uma rede. O acesso a computadores pessoais, inclusive portáteis, está mais fácil e qualquer pessoa mal intencionada poderia utilizar um programa de análise de protocolos para obter dados pessoais de terceiros.


FIQUE ALERTA

Ferramentas de análise de protocolos podem ser utilizadas para finalidades ilícitas. Ao utilizar estas ferramentas, tenha cuidado para não infringir políticas das organizações.

Ao identificar uma interface de rede promíscua em uma infraestrutura de rede em que você desconhece o uso de um analisador de protocolos, verifique a máquina para possível incidente de segurança. Como você já viu, o tráfego que transita pela rede pode ser facilmente capturado. O uso desse tipo de ferramenta gera problemas de segurança na rede, no entanto, o uso de switches limita o tráfego

que pode ser capturado por uma estação analisadora de protocolos, pois o switch, diferentemente do hub, não encaminha o tráfego para toda a rede. Ainda assim, é possível obter informações importantes que podem ser mal utilizadas por alguém com má intenção.

Outro fator que também dificulta a captura de pacotes para usos ilícitos, hoje em dia, é que boa parte do tráfego é criptografado, principalmente senhas de acesso a sistemas. Essa é uma limitação das ferramentas de análise de protocolos, pois elas não possuem a capacidade de decifrar o tráfego capturado na grande maioria dos casos quando criptografados.

Como você pode perceber, nesse item, é preciso ter certo cuidado com os analisadores de protocolos para não deixar espaço aberto e caminho livre para pessoas mal intencionadas. Todo cuidado é pouco. A seguir você conhecerá alguns tipos de analisadores de protocolos.

11.2 TIPOS DE ANALISADORES DE PROTOCOLOS

Os analisadores de protocolos são divididos em dois tipos: os que são baseados em software e os que são baseados em hardware. Os analisadores baseados em software acabam utilizando um computador de propósito geral e os recursos de processamento e memória são compartilhados com outras aplicações e com o sistema operacional. Os analisadores de protocolos baseados em hardware são projetados especificamente para fornecer exclusividade ao processo de análise de protocolos, e, geralmente, conseguem oferecer funcionalidades mais avançadas do que os analisadores baseados em software.

Para realizar a análise de protocolos podemos utilizar diversos softwares disponíveis gratuitamente, necessitando somente de um computador com uma interface de rede. No entanto, diversas empresas comercializam soluções bastante completas para análise de protocolos, e também soluções para segmentos específicos. Os analisadores de protocolos baseados em hardware geralmente possuem um alto custo, pois oferecem o hardware e software com alto desempenho e com funções de análise de problemas comuns que podem facilitar em muito o dia a dia do administrador de redes. No entanto, o alto custo nem sempre compensa para a maioria das empresas. O foco no uso de aparelhos como este fica a cargo de empresas de suporte e consultoria.

Conheça, agora, três ferramentas. Uma realiza análise de redes sem fio, e as outras duas realizam análise de protocolos que necessitam de uma interface. Confira!

11.2.1 WIRESHARK

O Wireshark é uma ferramenta gratuita de análise de protocolos que realiza a captura de dados em interfaces de rede cabeadas ou sem fio. Esta ferramenta é amplamente conhecida e utilizada por empresas e no ensino de cursos de redes de computadores. Possui funcionalidade avançada de captura e análise de tráfego dos mais variados protocolos, análise off-line das capturas, suporte a diversos sistemas operacionais, capacidade de análise de arquivos de capturas de outras ferramentas de análise de protocolos, suporte a diversas tecnologias da camada de enlace como PPP, Frame-Relay, Ethernet entre outros.

A figura a seguir apresenta a tela inicial da ferramenta. Nesta figura você pode ver que ela possui uma barra de Menu, uma barra de ferramentas principal (com os ícones) e uma barra de ferramentas de filtro.

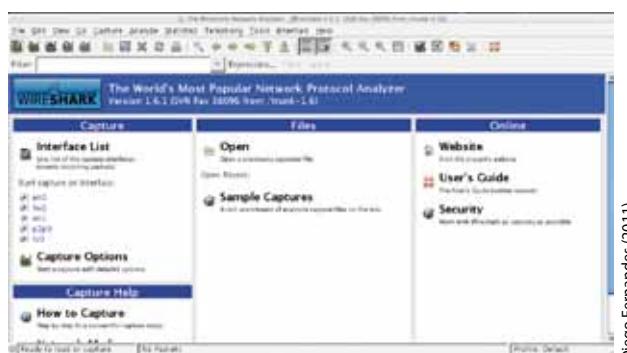


Figura 84 - Tela Inicial do Wireshark

Diego Fernandes (2011)

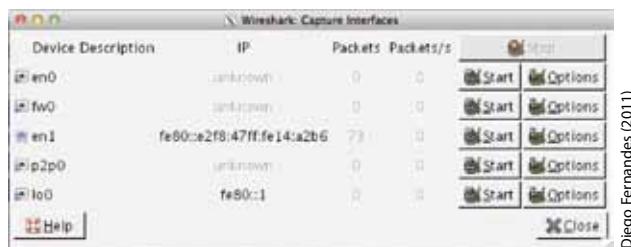
Para iniciar a captura de tráfego, basta clicar no botão de captura na barra de ferramentas principal ou por meio do Menu. Pelo menu pode-se ir à Capture, e selecionar Interfaces conforme ilustra a figura a seguir.



Figura 85 - Seleção de interface de captura no Wireshark

Diego Fernandes (2011)

Ao selecionar Interfaces, todas as interfaces de rede disponíveis na estação de análise de protocolos serão apresentadas, conforme você pode perceber na figura a seguir.

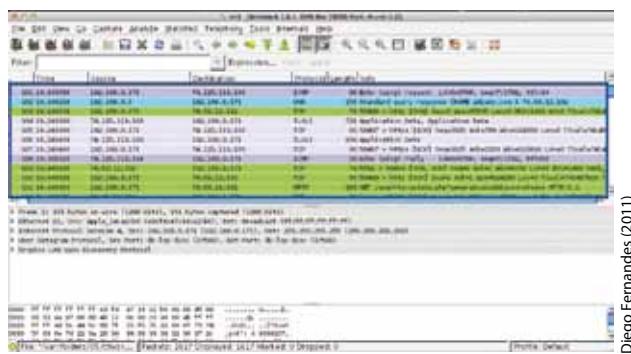


Diego Fernandes (2011)

Figura 86 - Interfaces disponíveis na estação de análise de protocolos

No caso da estação utilizada, somente as interfaces en1 (wireless) e a Loopback0 estão ativas. Selecione o botão Start da interface en1 para iniciar a captura. Note que há um botão Options, que oferece uma personalização da captura. Consulte a documentação da ferramenta para obter mais detalhes.

Uma vez iniciada a captura, poderemos ver, na janela da aplicação, diversas linhas percorrendo a tela conforme ilustra a próxima figura. Nesta figura pode-se ver na área destacada diferentes protocolos sendo capturados como ICMP, DNS, TCP, TLSv1 e HTTP. A listagem está configurada para todos os protocolos na sequência de captura, mas é possível listar por tempo, origem, destino, protocolo, comprimento e informações gerais, bastando selecionar a coluna a qual se deseja ordenar. Por exemplo, ao clicar em Protocol, esta coluna listará os protocolos alfabeticamente.



Diego Fernandes (2011)

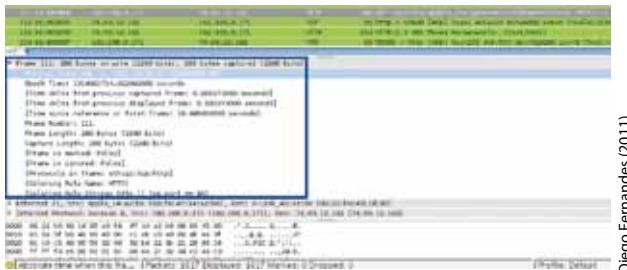
Figura 87 - Captura de tráfego com o Wireshark

Ainda na figura da captura do tráfego, logo abaixo do destaque, veja as informações para cada camada do modelo TCP/IP, como frame e Ethernet II (Acesso à rede), Internet Protocol Version 4 (Internet), User Datagram Protocol (Transpor-

te) e Dropbox Lan Syn Discovery Protocol (Aplicação). As informações mostradas para cada camada são para uma linha selecionada na área em destaque da figura, mas que não está visível.

Vamos analisar cada uma das informações apresentadas pelo Wireshark para uma requisição HTTP. Observe que a forma de apresentação das informações não permite identificar os campos das PDUs de cada camada do modelo TCP/IP.

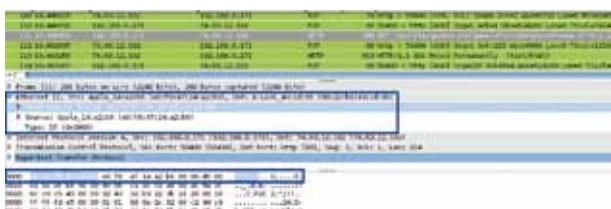
A figura seguinte apresenta as informações do frame, como hora de recebimento do frame, protocolos contidos no frame e números de bits capturados.



Diego Fernandes (2011)

Figura 88 - Informações do Frame

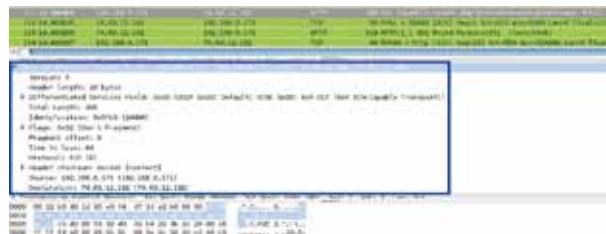
Na próxima figura, você pode ver os detalhes das informações do quadro Ethernet como Endereço de Origem e Destino (MAC Address) e o tipo do protocolo da camada superior que, neste caso, é o IP. Observe também que o endereço de destino está destacado. Ao clicar no endereço de destino, o wireshark marca as informações na área que mostra os dados originais em hexadecimal.



Diego Fernandes (2011)

Figura 89 - Informações do quadro Ethernet

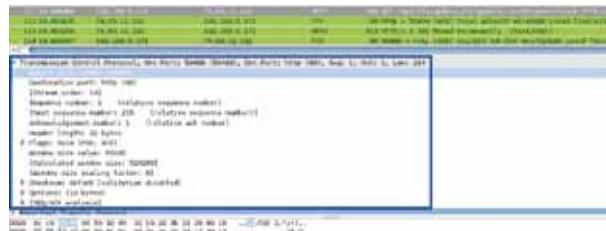
A figura a seguir mostra os detalhes do protocolo IP. Observe, na área em destaque, qual é a versão do protocolo IP, tamanho do cabeçalho, flags de fragmentação, TTL do pacote, protocolo da camada superior e endereço de origem e destino.



Diego Fernandes (2011)

Figura 90 - Detalhes do protocolo IP

O protocolo da camada de transporte é o TCP, como já esperávamos. Vimos na análise do IP que o protocolo da camada superior era o TCP. Na figura a seguir, podemos ver detalhes sobre as portas de origem e destino, número de sequência, número de reconhecimento (ACK), flags, tamanho da janela e número de verificação de erros (Checksum). Note que a porta de destino é a 80. Já sabemos que a comunicação em análise é uma requisição HTTP, mas o número da porta já seria uma indicação do tipo protocolo utilizado na camada de aplicação.



Diego Fernandes (2011)

Figura 91 - Detalhes do segmento TCP

O protocolo utilizado na camada de aplicação é o HTTP como pode ser visto na figura seguinte. No entanto, a requisição não partiu de um navegador web como o Internet Explorer ou Firefox, e sim de uma aplicação de comunicação instantânea. Esta aplicação utiliza o protocolo HTTP para verificar se existem atualizações para a aplicação. Pode identificar que a mensagem HTTP a enviar é uma requisição devido à diretiva GET e qual o endereço requisitado.



Diego Fernandes (2011)

Figura 92 - Informações do protocolo utilizado na camada de aplicação

O Wireshark suporta filtros para que somente determinados protocolos ou endereços sejam apresentados em tela ou capturados. Esses filtros podem ser inseridos diretamente na tela do aplicativo, na barra de tarefas Filter, conforme mostra a figura a seguir. Neste caso, o filtro é simples e faz com que somente requisições do ARP sejam listadas. No entanto, os filtros podem ser bem mais complexos.



Diego Fernandes (2011)

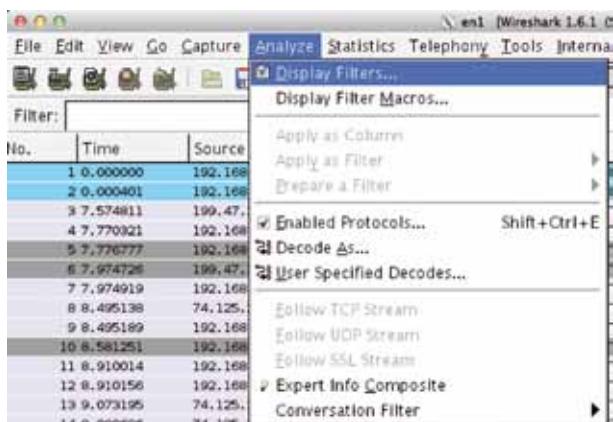
Figura 93 - Uso de filtros no Wireshark



**SAIBA
MAIS**

No site <http://media.pecketlife.net/media/library/13/Wireshark_Displau_Filters.pdf> você encontra um PDF com diversos filtros prontos para uso no Wireshark. Confira!

Além da barra de filtros apresentada na figura anterior, mais opções de análise são apresentadas na opção *Analyze* do Menu, conforme mostrado na figura a seguir. No item *Display Filters*, alguns filtros prontos são disponibilizados e outros podem ser criados. Além disso, é possível habilitar quais protocolos serão analisados selecionando o item *Enabled Protocols*.



Diego Fernandes (2011)

Figura 94 - Opções de filtragem de protocolos

Na opção de *Menu Statistics*, é possível obter diversos tipos de informações sobre o tráfego capturado. O item *Summary*, por exemplo, apresenta um resumo contendo o nome do arquivo de armazenamento da captura, a hora de início e fim da captura e quando foi finalizada. Informa também a interface utilizada na captura, número de pacotes perdidos e se foram utilizados filtros tanto na captura como na visualização. A taxa de transmissão em pacotes e bytes, o número de pacotes e o tamanho médio dos quadros são apresentados. Confira a tela das informações de resumo a seguir.

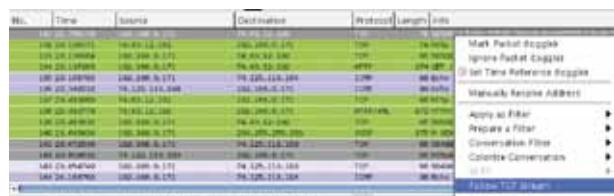


Diego Fernandes (2011)

Figura 95 - Resumo da captura de tráfego

Entre outros itens do *Menu Statistics*, está a possibilidade de criar gráficos diversos e personalizáveis das entradas e saídas por meio de filtros, verificar as conversações entre clientes baseada no endereço físico e no endereço IP, além de gráficos dos fluxos das conversações.

Uma funcionalidade bastante interessante no Wireshark é a capacidade de acompanhar um fluxo TCP. Com ele, é possível analisar todas as trocas de comunicação de um fluxo TCP, desde a inicialização (SYN) até a finalização (FIN). Para acompanhar um fluxo TCP, basta clicar com o botão direito em cima do fluxo desejado e escolher o item *Follow TCP Stream*, conforme mostra a próxima figura. Neste caso, o fluxo selecionado foi o de número 131.



Diego Fernandes (2011)

Figura 96 - Acesso a funcionalidade de seguir um fluxo TCP

Ao selecionar a função de acompanhar um Fluxo de TCP, ele irá listar na tela somente os quadros referentes ao fluxo que está sendo acompanhado como pode ser visto na figura a seguir. Note que para listar um fluxo específico, o que a seleção do item Follow TCP Stream faz é aplicar um filtro.

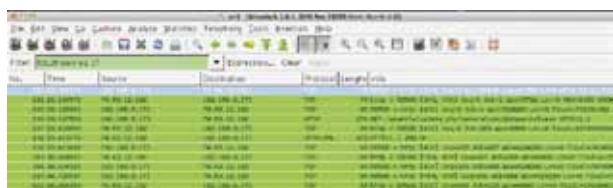


Figura 97 - Acompanhamento de um fluxo TCP

Além de listar somente os quadros correspondentes ao filtro do fluxo TCP, uma nova janela se abre. Nesta janela é possível verificar o conteúdo das mensagens do fluxo. Veja isso na próxima figura.

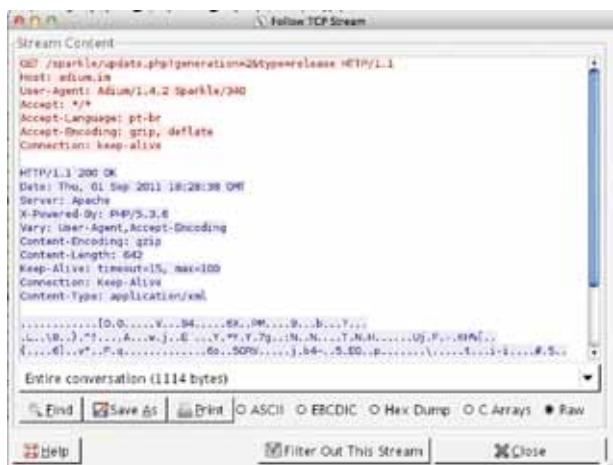


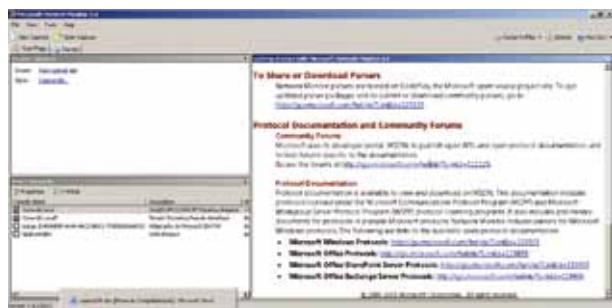
Figura 98 - Toda a troca de informações do fluxo selecionado



Não é possível cobrir a fundo o uso da ferramenta Wireshark num curso como este, mas é possível aprender muita coisa utilizando a ferramenta no dia a dia e consultando a documentação e fóruns na Internet. Para mais informações sobre a ferramenta, consulte <<http://www.wireshark.org/about.html>>.

11.2.2 MICROSOFT NETWORK MONITOR

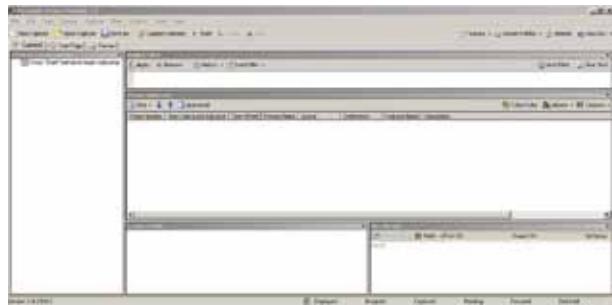
O analisador de protocolos Microsoft Network Monitor é uma ferramenta de captura e análise de tráfego assim como o Wireshark. Esta ferramenta permite realizar capturas dos principais protocolos, principalmente os protocolos da Microsoft. A tela inicial da aplicação pode ser vista na figura a seguir. A aplicação possui uma interface simples, permitindo iniciar uma captura ao clicar no botão *New Capture*.



Diego Fernandes (2011)

Figura 99 - Tela inicial do analisador de protocolos da Microsoft

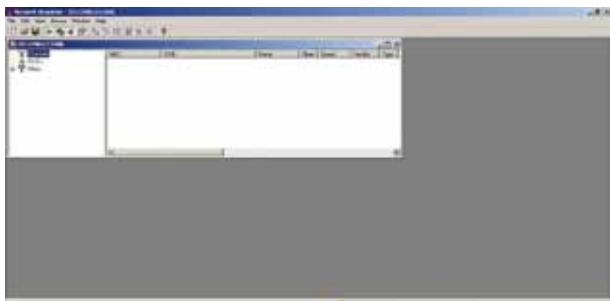
Ao clicar no botão, uma nova aba se abre. . A tela possui uma área para filtros na área superior e uma para apresentar um resumo dos quadros capturados no centro. Além disso, na parte inferior esquerda da tela, podemos ver os detalhes do quadro que for selecionado e, na parte inferior direita, os detalhes em hexadecimal.



Diego Fernandes (2011)

Figura 100 - Aba de captura do Microsoft Network Monitor

Tendo criado uma nova aba de captura, podemos iniciar a capturar pacotes. Para isso temos que clicar no botão *Start*. Ao iniciar a captura, imediatamente os quadros começam a aparecer na tela, como mostra a figura a seguir. Os detalhes do quadro são apresentados na mesma maneira que o Wireshark.



Diego Fernandes (2011)

Figura 101 - Captura de tráfego

Uma funcionalidade interessante do Microsoft Network Monitor é a apresentação das conversações no lado esquerdo da tela, assim, já sabemos de imediato que aplicações estão utilizando a rede. Além disso, na captura dos quadros, as aplicações já são listadas junto aos quadros que geraram. No caso dos quadros que não possuem a informação do nome do processo, foram as geradas pelo sistema.

Apesar de o analisador da Microsoft ser uma excelente ferramenta, o Wireshark é ainda muito superior. Possui muitas funcionalidades que não são encontradas na ferramenta da Microsoft, como por exemplo, acompanhar fluxos TCP. O aplicativo Microsoft Network Monitor somente pode ser utilizado em sistemas Microsoft Windows.

**SAIBA
MAIS**

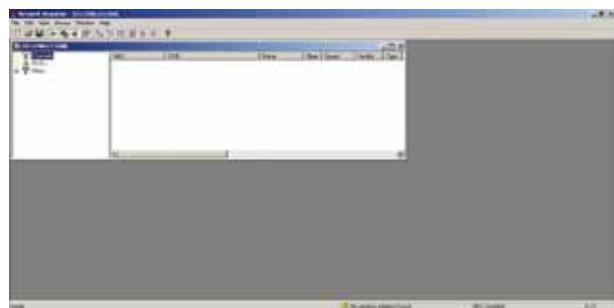
Você encontra mais informações sobre a ferramenta Microsoft Network Monitor no site <<http://www.microsoft.com/download/en/details.aspx?id=4865>>

11.2.3 NETSTUMBLER

O NetStumbler é uma ferramenta gratuita para analisar redes wireless. No entanto, não é exatamente um analisador de protocolos como o Wireshark e o Microsoft Network Monitor, tanto que é definido pelos próprios autores como uma ferramenta de auditoria de redes sem fio. Uma utilização interessante desta ferramenta é verificar a existência de pontos de acesso sem fio que não são legítimos, verificar como está a cobertura do sinal da rede corporativa ou doméstica analisando o alcance da rede e efetuar *Site Survey* básico.

O Site Survey é uma metodologia para avaliar a área de instalação de uma rede sem fio ou para solução de problemas. Geralmente utilizam equipamentos para isso, no entanto, utilizar o NetSumbler no Site Survey permite avaliar que frequências de rádio são utilizadas no local da nova rede para escolher uma frequência que não sofra interferência ou tenha a interferência minimizada. Mais detalhes sobre redes sem fio serão abordados em uma unidade curricular posterior.

A tela inicial do Netstumbler é a apresentada na figura a seguir. O aplicativo possui uma janela interna que apresenta os canais em uso, os SSID (identificadores das redes sem fio) e filtros.



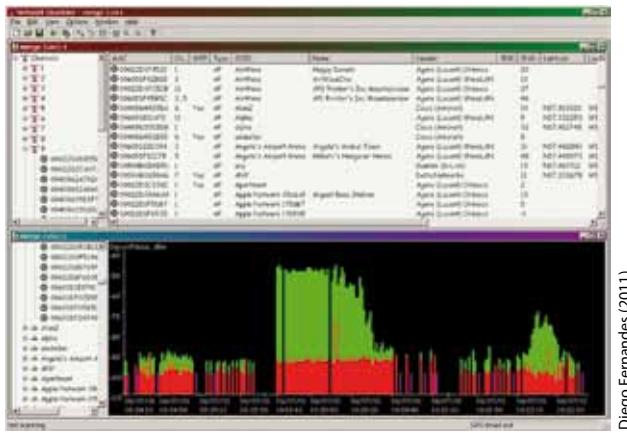
Diego Fernandes (2011)

Figura 102 - Tela inicial do netStumbler

Ao clicar no botão Play, o NetStumbler é ativado e inicia a detecção de redes sem fio e frequências em uso e as lista na janela interna conforme ilustrado na figura 106. Na listagem podemos visualizar os identificadores das redes sem fio, o canal utilizado, velocidade da rede, fabricante do ponto de acesso detectado e criptografia utilizada. Também é possível verificar a intensidade do sinal de cada rede.

MAC	SSID	Name	Chnl	Speed	Vendor	Type	Encryption
00:0C:29:01:0A:02	airmail		3	11 Mbps	D-Link	AP	WEP
00:0C:29:01:0A:03	Q_Network		3	11 Mbps	Astar	AP	WEP
00:0C:29:01:0A:04	Lynne's Network		3	11 Mbps	Apple	AP	WEP
00:0C:29:01:0A:05	laptop		3	11 Mbps	Apple	AP	WEP
00:0C:29:01:0A:06	Visitor's wireless Network		6	11 Mbps	AlpineNet/Hub	AP	WEP
00:0C:29:01:0A:07	medium		6	22 Mbps	D-Link	AP	WEP
00:0C:29:01:0A:08	wireless		6	11 Mbps	Gentoo (21.1.0)	AP	WEP
00:0C:29:01:0A:09	laptop		1	11 Mbps	Dell (Fevereiro)	AP	WEP
00:0C:29:01:0A:0A	visitors		1	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0B	visitors		6	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0C	MYFREELESS		8	11 Mbps	Microsoft	AP	WEP
00:0C:29:01:0A:0D	linksys		8	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0E	laptop		10	11 Mbps	Linksys (Bling)	AP	WEP
00:0C:29:01:0A:0F	medium		10	22 Mbps	D-Link	AP	WEP
00:0C:29:01:0A:0G	medium		8	11 Mbps	Cisco (Access)	AP	WEP
00:0C:29:01:0A:0H	medium		10	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0I	medium		4	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0J	medium		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0K	medium		6	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0L	medium		1	11 Mbps	Dell (Fevereiro)	AP	WEP
00:0C:29:01:0A:0M	medium		8	11 Mbps	D-Link	AP	WEP
00:0C:29:01:0A:0N	medium		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0O	medium		9	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0P	linksys		8	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Q	linksys		8	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0R	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0S	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0T	linksys		9	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0U	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0V	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0W	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0X	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Y	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Z	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0A	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0B	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0C	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0D	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0E	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0F	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0G	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0H	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0I	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0J	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0K	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0L	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0M	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0N	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0O	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0P	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Q	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0R	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0S	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0T	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0U	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0V	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0W	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0X	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Y	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Z	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0A	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0B	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0C	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0D	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0E	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0F	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0G	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0H	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0I	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0J	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0K	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0L	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0M	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0N	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0O	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0P	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Q	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0R	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0S	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0T	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0U	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0V	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0W	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0X	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Y	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Z	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0A	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0B	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0C	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0D	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0E	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0F	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0G	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0H	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0I	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0J	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0K	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0L	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0M	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0N	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0O	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0P	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Q	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0R	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0S	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0T	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0U	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0V	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0W	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0X	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Y	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Z	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0A	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0B	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0C	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0D	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0E	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0F	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0G	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0H	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0I	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0J	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0K	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0L	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0M	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0N	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0O	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0P	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Q	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0R	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0S	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0T	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0U	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0V	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0W	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0X	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Y	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0Z	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0A	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0B	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0C	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0D	linksys		11	11 Mbps	Linksys	AP	WEP
00:0C:29:01:0A:0E	linksys		11	11 Mbps	Linksys	AP	WEP
00:0							

O NetStumbler também permite gerar gráficos da relação de ruído e intensidade do sinal como mostra a próxima figura. Além disso, também é possível exportar os dados capturados e utilizá-los em planilhas de dados, por exemplo.



Diego Fernandes (2011)

Figura 104 - Gráfico de ruído e sinal gerado pelo NetStumbler
Fonte: WIRELESS LAN (2008)

O NetStumbler é uma ferramenta simples e de fácil utilização. Permite analisar as redes, frequência utilizadas, intensidade dos sinais e auxilia na instalação e na solução de problemas de redes sem fio.



**SAIBA
MAIS**

Você encontra mais informações sobre esta ferramenta no site <<http://www.netstumbler.com>>. Acesse e confira!

Você acabou de conhecer três ferramentas que são utilizadas para fazer a análise de protocolo, mas, sabe em que momento usar? Entenda um pouco melhor acompanhando o relato a seguir.



CASOS E RELATOS

Usando um analisador de protocolo

Lucas é o administrador de redes de uma grande empresa que possui diversas filiais. Um software de gestão foi adquirido para ser utilizado em todas as unidades da empresa. A base do sistema fica hospedada na sede. Apesar de ser um sistema novo e de conexão da rede das unidades até a central e apresentar um bom desempenho para as diversas aplicações, os usuários reclamam muito de lentidão ao utilizar a aplicação de gestão, depois das primeiras semanas de uso. Sabe-se que o desempenho da rede não é o culpado pela lentidão, e, como bom profissional, Lucas avaliará a situação. Para tanto, ele simula o uso do aplicativo de gestão realizando as mesmas tarefas realizadas pelos usuários em uma unidade remota e detecta que realmente há uma lentidão excessiva e inaceitável. Para verificar o que pode estar causando a lentidão, ele resolve, primeiramente, utilizar um analisador de protocolos para avaliar como se dá o acesso da aplicação até o servidor. Em seguida, Lucas também faz testes de transferências de arquivos utilizando o protocolo FTP, capturando os pacotes e medições de tempos de resposta dos servidores. Ao analisar o fluxo de transferência do FTP, ele observa que a transferência do arquivo foi executada na velocidade máxima permitida pela conexão, sem perda de pacotes e com raras retransmissões. Já com a aplicação de gestão, Lucas observa que apesar de não haver perdas de pacotes e de ocorrerem raras retransmissões, a taxa de transmissão é baixa. O tempo de resposta dos servidores é excelente. Identificando que a infraestrutura de rede realmente não apresenta problemas, ele aproveita que fez a captura dos pacotes para realizar uma análise aprofundada das mensagens trocadas pelo aplicativo de gestão. Como a captura de pacotes foi realizada utilizando o Wireshark, Lucas utiliza o acompanhamento de fluxos TCP e avalia os diversos fluxos trocados pelo aplicativo de gestão. Nesta análise profunda, são identificadas várias requisições ao banco de dados que foram mal formuladas e mal implementadas. Dessa forma, todo o processamento dos resultados obtidos com as requisições fica a cargo da aplicação, o que acaba gerando a lentidão. Com os resultados em mãos, Lucas elabora um relatório indicando que a causa da lentidão é da própria aplicação e não da rede.



RECAPITULANDO

Neste capítulo você viu que existem ferramentas capazes de capturar o tráfego que transita na rede e realizar a análise dos protocolos. Essas ferramentas são de grande utilidade para auxiliar na solução de problemas em redes de computadores sem fio, cabeadas e executando em diferentes tecnologias. A análise de protocolos na área de administração de redes é essencial e deve fazer parte do conjunto de ferramentas utilizadas no dia a dia. Os conceitos estudados neste capítulo auxiliaram você a iniciar no uso dessas aplicações e com o uso contínuo, aprender novos usos e recursos.

Termina aqui mais uma unidade curricular. Esperamos que você tenha gostado e aprendido bastante sobre Arquitetura de Redes. Lembre-se que nessa área o profissional precisa estar em constante aprendizado, portanto, pesquise, estude, mantenha-se informado, e tenha sucesso em sua vida profissional. Até uma próxima!

REFERÊNCIAS

CISCO NETWORKING ACADEMY. **CCNA Exploration 4.0.** Disponível em: <<http://cisco.netacad.net>>. Acesso em: 15 ago. 2011.

COMER, Douglas. **Interligação de redes com TCP/IP:** princípios, protocolos e arquitetura. 5. ed. Rio de Janeiro: Elsevier, 2006. 435 p. 1 v.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet:** uma abordagem top-down. 3. ed. São Paulo: Pearson Education do Brasil, 2006. 634 p.

ODOM, Wendell. **CCENT/CCNA ICND 1:** guia oficial de certificação do Exame. Rio de Janeiro: Alta Books, 2008. 458 p.

WIRELLES LAN. **Screenshot of NetStumbler.** 2008. il. color. Disponível em <<http://www.monolith81.de/netstumbler.html>>. Acesso em 21 out. 2011

MINICURRÍCULO DOS AUTORES

André Leopoldino de Souza, especialista em Gestão da Segurança da Informação pela Faculdade de Tecnologia do SENAI Florianópolis, onde concluiu também o curso Superior de Tecnologia em Redes de Computadores. Possui as certificações CCNA (*Cisco Certified Network Associate*) e CCAI (*Cisco Certified Associate Instructor*). Atualmente trabalha como consultor na área de segurança em transações eletrônicas de fundos aplicada à rede de dados, atua também como pesquisador e professor no SENAI de Florianópolis, onde ministra aulas nos cursos superiores de tecnologia e Cisco Network Academy. Coordena a Academia Regional Cisco e é responsável pelo treinamento dos instrutores das Academias Locais. Sua área de pesquisa está baseada em aplicações de segurança, roteamento avançado e switches multi-camadas. Cursos de qualificação realizados recentemente: Cisco CCNP-BSCI, Cisco CCNP-BCMSN, Cisco CCNP-ISCW e Cisco CCNP-ONT como parte da capacitação de docentes no projeto CCNP do SENAI. Curso VoIP, Curso Metro Ethernet, Curso Wireless e Cisco CCNA Security como parte da capacitação de docentes para o projeto Laboratório Remoto do SENAI.

Augusto Castelan Carlson, mestre em Engenharia Elétrica pela Universidade Federal de Santa Catarina e Bacharel em Ciência da Computação pela Universidade do Sul de Santa Catarina. Possui as certificações CCNA (*Cisco Certified Network Associate*) e CCAI (*Cisco Certified Associate Instructor*), além de diversos cursos na área de TI. Atualmente trabalha no Ministério Público de Santa Catarina como Analista de Sistemas, com enfoque em redes de computadores, e ministra aulas nos cursos da *Cisco Networking Academy*. Já atuou como Analista de Redes no SENAI/SC, como Analista de TI em outros órgãos do governo como SC Parcerias S/A e na Universidade do Estado de Santa Catarina. Sua área de pesquisa está direcionada para desempenho de redes de computadores. Cursos de qualificação realizados recentemente: Firewall, ASA e CSM; MS Windows Server Active Directory; e Metodologia de Ensino em cursos superiores.

Fabio Ricardo Santana, especialista em Organização de Sistemas e Métodos pela Universidade Federal de Santa Catarina, Bacharel em Ciências da Computação pela Universidade Federal de Santa Catarina. Possui as certificações CCNA (*Cisco Certified Network Associate*) e CCAI (*Cisco Certified Associate Instructor*) além de diversos cursos na área de TI. Atualmente, trabalha como Analista de Negócios na empresa Teclan Engenharia de Software. Também atua como professor no SENAI de Florianópolis onde ministra aulas nos cursos superiores de Tecnologia de Redes de Computadores e Telecomunicações além do *Cisco Network Academy* nos módulos 1, 2, 3 e 4. Sua área de pesquisa está baseada em roteamento avançado, IPv6 e PLC. Cursos de qualificação realizados recentemente: Cisco CCNP-BSCI e Cisco CCNP-BCMSN, como parte da capacitação de docentes no projeto CCNP do SENAI.

ÍNDICE

A

ARP 23, 63, 79, 80, 81, 82, 169

B

Broadcast 21, 23, 24, 70, 79, 81, 82, 123, 125, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 147, 150, 151, 154, 155, 161

D

DNS 36, 40, 41, 54, 115, 118, 160, 166

Domínio de *Broadcast* 81, 82, 147, 154, 155

Domínio de Colisão 85, 96, 97, 98, 147, 149, 150, 151, 152

E

Ethernet 85, 89, 90, 91, 93, 94, 95, 96, 98, 110, 116, 148, 149, 161, 165, 166, 167, 181

F

FTP 36, 38, 39, 54, 57, 115, 160, 176

H

HTTP 36, 37, 38, 54, 115, 160, 161, 166, 167, 168

HTTPS 37, 38, 54

Hub 20, 81, 95, 97, 110, 146, 147, 149, 150, 151, 153, 154, 162, 163, 164

I

ICMP 63, 66, 77, 78, 79, 82, 116, 166

IMAP 36, 39, 54, 115

IP 19, 29, 30, 31, 40, 41, 42, 45, 64, 65, 66, 68, 69, 70, 71, 72, 73, 74, 76, 77, 111, 113, 114, 115, 116, 117, 118, 119, 121, 122, 123, 124, 125, 126, 127, 133, 137, 141, 142, 143, 152, 154, 155, 161, 167, 168, 170, 179

O

OSI 19, 29, 30, 31, 33, 35, 36, 43, 44, 45, 47, 48, 58, 61, 62, 63, 77, 82, 85, 86, 94, 98, 101, 102, 113, 114, 116, 117, 118, 119, 146, 148

P

PDU 31, 32, 48, 56, 62, 88, 89, 160, 161, 167

POP 36, 39, 40, 54, 115

R

Roteador 154

S

SMTP 36, 39, 40, 54, 115, 160

SNMP 36, 42, 43, 115, 149

Switch 151

T

TCP 19, 29, 30, 31, 45, 47, 55, 56, 57, 58, 66, 69, 111, 113, 114, 115, 116, 117, 118, 119, 160, 161, 166, 167, 168, 170, 171, 173, 179

TCP/IP 29, 30, 31, 45, 111, 113, 114, 115, 116, 117, 118, 119, 161, 166, 167, 179

TFTP 36, 38, 39, 54, 57

Topologia Física 28

U

UDP 19, 47, 56, 57, 58, 66, 69, 115, 118, 160

SENAI - DN
UNIDADE DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA – UNIEP

Rolando Vargas Vallejos
Gerente Executivo

Felipe Esteves Morgado
Gerente Executivo Adjunto

Diana Neri
Coordenação Geral do Desenvolvimento dos Livros

SENAI - DEPARTAMENTO REGIONAL DE SANTA CATARINA

Simone Moraes Raszl
Coordenação do Desenvolvimento dos Livros no Departamento Regional

Beth Schirmer
Coordenação do Núcleo de Desenvolvimento

Caroline Batista Nunes Silva
Juliano Anderson Pacheco
Coordenação do Projeto

Gisele Umbelino
Coordenação de Desenvolvimento de Recursos Didáticos

André Leopoldino de Souza
Augusto Castelan Carlson
Fabio Ricardo Santana
Elaboração

Juliano Anderson Pacheco
Revisão Técnica

Evelin Lediani Bao
Design Educacional

D'imitre Camargo Martins
Diego Fernandes
Júlia Pelachini Farias
Luiz Eduardo Meneghel
Ilustrações e Tratamento de Imagens

Carlos Filip Lehmkuhl Loccioni
Diagramação

Juliana Vieira de Lima
Revisão e Fechamento de Arquivos

Luciana Effting Takiuchi
CRB 14/937
Ficha Catalográfica

DNA Tecnologia Ltda.
Sidiane Kayser dos Santos Schwinzer
Revisão Ortográfica e Gramatical

DNA Tecnologia Ltda.
Sidiane Kayser dos Santos Schwinzer
Normalização

i-Comunicação
Projeto Gráfico

SENAI

*Iniciativa da CNI - Confederação
Nacional da Indústria*

ISBN 978-85-7519-484-3



9 788575 194843 >