



MÓDULO DE:

PROTOCOLOS DE REDES

AUTORIA:

Ing. M.Sc./D.Sc. ANIBAL D. A. MIRANDA

Copyright © 2008, ESAB – Escola Superior Aberta do Brasil

Módulo de: PROTOCOLOS DE REDE

Autoria: Ing. M.Sc./D.Sc. Anibal D. A. Miranda

Primeira edição: 2008

Todos os direitos desta edição reservados à
ESAB – ESCOLA SUPERIOR ABERTA DO BRASIL LTDA
<http://www.esab.edu.br>
Av. Santa Leopoldina, nº 840/07
Bairro Itaparica – Vila Velha, ES
CEP: 29102-040
Copyright © 2008, ESAB – Escola Superior Aberta do Brasil

Apresentação

Familiarizar ao aluno com o conceito importantíssimo dos protocolos de comunicações e como atuam cada um deles nos diferentes níveis impostos pelo modelo de referência OSI. Saber identificar o tipo de rede pelos protocolos utilizados para a transferência de dados.

O bjetivo

Proporcionar aos participantes os conceitos de protocolos, em particular dos protocolos TCP/IP que são o motor da Internet, assim como os fundamentos, modelos e regras de endereçamento IP, tópicos TCP/IP avançados, IPX/SPX, X.25, Frame Relay, ATM, NetBEUI, PPPoE, SNA, ISDN, ADSL, ATM, SMDS & SONET/SDH.

Ementa

Protocolos; organizações padronizadas; modelo de referência OSI; Nível de:aplicação, apresentação, sessão, transporte, rede, enlace de dados, físico; modelo de referência internet; portas dos protocolos de transportes; funcionamento da comunicação TCP/IP; endereços de IP registrados; sub-redes; pilha de protocolo.

Sobre o Autor

Engenheiro eletrônico especializado nas áreas de Teleinformática e Telecomunicações.

Mestrado e Doutorado outorgados pelo Instituto Tecnológico de Aeronáutica (ITA) em 1998 e 2004 respectivamente.

A Tese de Mestrado rendeu o Primeiro premio "Comandante Quandt de Telecomunicações" na TELEXPO de São Paulo em 1999. Categoria: Trabalhos Técnicos.

Autor de softwares na área de engenharia de tráfego, principalmente para medir, analisar e emular o comportamento agregado de pacotes IP.

Autor de vários artigos técnicos apresentados em importantes congressos a nível nacional e internacional.

Boa experiência no estudo, análise, dimensionamento e implementação de projetos na área de Teleinformática

SUMÁRIO

UNIDADE 1	8
Protocolos	8
UNIDADE 2	14
Organizações Padronizadoras	14
UNIDADE 3	19
Modelo De Referência OSI	19
UNIDADE 4	23
O Nível De Aplicação	23
UNIDADE 5	27
O Nível De Apresentação.....	27
UNIDADE 6	29
O Nível De Sessão.....	29
UNIDADE 7	34
O Nível De Transporte	34
UNIDADE 8	36
O Nível De Rede	36
UNIDADE 9	39
O Nível De Enlace De Dados.....	39
UNIDADE 10	46
O Nível Físico.....	46
UNIDADE 11	49
Mais Sobre O Modelo OSI	49
UNIDADE 12	53
Modelo De Referência Internet (DoD)	53
UNIDADE 13	60
Protocolos Do Nível De Aplicação.....	60
UNIDADE 14	73
Protocolos Do Nível De Transporte: TCP.....	73

UNIDADE 15	96
Protocolos Do Nível De Transporte: UDP	96
UNIDADE 16	100
Portas Dos Protocolos De Transporte.....	100
UNIDADE 17	104
UNIDADE 18	117
Protocolos Do Nível Internet	117
UNIDADE 19	124
Como Funciona A Comunicação TCP/IP	124
UNIDADE 20	128
Formato E Categorias IP Versão 4 (Ipv4)	128
UNIDADE 21	140
Endereços IP Registrados.....	140
UNIDADE 22	144
Criando Sub-Redes.....	144
UNIDADE 23	157
IPv6	157
UNIDADE 24	170
Protocolos Do Nível Físico	170
UNIDADE 25	185
Protocolos De LAN E WAN	185
UNIDADE 26	198
Asymmetric Digital Subscription Line (ADSL)	198
UNIDADE 27	203
Asynchronous Transfer Mode (ATM)	203
UNIDADE 28	218
Pilha De Protocolos IPX/SPX.....	218
UNIDADE 29	235
Pilha De Protocolos SNA	235
UNIDADE 30	241
Pilha De Protocolos Appletalk, SMDS & SONET/SDH.....	241

GLOSSÁRIO	252
BIBLIOGRAFIA.....	276

UNIDADE 1

Objetivo: Entender o que significa e qual a importância dos protocolos de comunicações.

Protocolos

Introdução

Na área das redes de computadores, a palavra protocolo encontra-se em todo nível, isto porque, praticamente seria impossível que as redes se comuniquem umas com outras se os protocolos não existissem, ou seja, a condição necessária e suficiente para que as redes funcionem da maneira como elas funcionam atualmente é a existência de protocolos de comunicação.

Um protocolo de comunicação ou protocolo de rede é uma especificação de uma série de regras que regem a comunicação. Por isso chamamos também os protocolos de rede de protocolos de comunicação. Eles podem ser considerados software que foi desenvolvido de preferência utilizando-se um padrão ou modelo de referência; juntos esses protocolos para comunicação de computadores são organizados em diversas camadas de programas, umas sobre as outras, englobando, freqüentemente, vários protocolos.

Os diferentes tipos de protocolo executam diferentes tarefas que possibilitam a comunicação: em conjunto eles formam **pilhas de protocolo** que executam uma função maior.

Existem diversas pilhas (camadas) ou famílias de protocolos, temos entre as principais as seguintes:

- Open Systems Interconnect (OSI)
- Internet stack protocol suit (TCP/IP)
- Novell – Netware suit protocolo (IPX/SPX)

- Apple Talk
- Digital Equipment Corporation (DECnet)
- System Network Architecture (SNA)

Os protocolos mais recentes, para comunicação com a Internet, são determinados pela **IETF**, e a **IEEE** ou **ISO** para outros tipos de protocolos. A **ITU-T** controla os protocolos de telecomunicações, assim como seus formatos. Os princípios da engenharia de sistemas são aplicados na criação e desenvolvimento dos protocolos de rede.

As organizações que efetuam o desenvolvimento dos protocolos de rede estão descritas logo a seguir com seus respectivos sites para consulta; lá se encontram disponíveis documentos que descrevem como foram padronizadas determinadas funções ou implementações para rede, normalmente tais documentos são chamados de **RFC** (Request For Comments).

Qualquer proposta de padronização que é submetida passa por um processo antes de virar uma RFC. Inicialmente ela recebe o nome de **Draft Proposal**, ou algo assim como uma proposta em rascunho. As propostas são analisadas por um grupo de trabalho conforme a área que se referem e se aprovadas por votação, recebe um número e se torna uma RFC. Mesmo assim, vale a pena mencionar que um protocolo para ser utilizado na Internet não necessariamente precisa se tornar um padrão Internet.

As RFCs podem ter os seguintes status:

- S = Internet Standard
- PS = Proposed Standard
- DS = Draft Standard
- BCP = Best Current Practices
- E = Experimental

- I = Informational
- H = Historic

Abaixo segue uma tabela que contém algumas RFCs importantes e a classificação por STANDARD. O STANDARD é o agrupamento das RFC que se referem a um determinado padrão:

Classificação	STD	RFC	Descrição
Padrões	STD-1	2200	INTERNET OFFICIAL PROTOCOL STANDARDS
	STD-2	1700	ASSIGNED NUMBERS
	STD-3	1122	Requirements for Internet hosts - communications layers
	=	1123	Requirements for Internet hosts - application and support
	STD-4	1009	Requirements for Internet Gateways
		1812	Requirements for IP Routers
		1918	Address Allocation for Private Internets
		2135	Internet Society By-Laws
		2134	Articles of Incorporation of Internet Society
		2008	Implication of Various Address Allocation Policies for Internet Routing
Internet		2026	The Internet Standards Process - Rev.3
		2050	The Internet Registry IP Allocation Guidelines
	STD-5	791	IP - Internet Protocol
	=	792	ICMP - Internet Control Message Protocol
	=	919	Broadcasting Internet Datagrams
	=	922	Broadcasting Internet datagrams in the presence of subnets
	=	950	Internet standard subnetting procedure
	=	1112	Host extensions for IP multicasting - IGMP
		2101	IPv4 address Behaviour Today
		1256	ICMP Router Discovery Protocol
IP			

		2236	Internet Group Management Protocol, v.2
		1788	ICMP Domain Name Messages
		1191	Path MTU Discovery Protocol
UDP	STD-6	768	User Datagram Protocol - UDP
TCP	STD-7	793	Transmission Control Protocol
		1144	Compressing TCP headers for low speed serial links
		1323	TCP Extensions for High Performance
Telnet	STD-8	854	Telnet Protocol specification
	=	855	Telnet Option Specification
FTP	STD-9	959	File Transfer Protocol - FTP
SMTP	STD-10	821	Simple Mail Transfer Protocol - SMTP
	=	1869	SMTP Service Extensions
	=	1870	SMTP Service Extension for Message Size Declaration
		1652	SMTP Service Extensions for 8-bit MIME transport
		1891	SMTP Service Extensions for Delivery Status Notification
		2142	Mailbox Names for Common Services, Roles and Functions
Mail-Content	STD-11	822	Standard Format for ARPANET Messages
	=	1049	Content-type header field for Internet messages
NTP	STD-12	1119	Network Time Protocol v.2 - NTP
DNS	STD-13	1034	Domain names - concepts and facilities
	=	1035	Domain names - implementation and specification
	STD-14	974	Mail Routing and the Domain Name System
	STD-15	1137	A Simple Network Management Protocol - SNMP
		1034	Domain Names, concepts, facilities, implementation and specification
		, 1035	
		2100	The Naming of Hosts
		2136	Dynamic Updates in the Somain Name System
		2181	Clarifications to DNS Specification
		2182	Selection and Operation of Secondary DNS Servers

SNMP-MIB	STD-16	1155	Structure and Identification of Management Information for TCP/IP-based Internets
	=	1212	Concise MIB Definitions
	STD-17	1213	Management Information Base for Network Management of TCP/IP-based internets - MIB II
Netbios/IP	STD-19	1001	Protocol standard for a NetBIOS service on a TCP/UDP transport: Concepts and Methods
	=	1002	Protocol standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications
TFTP	STD-33	1350	Tiny FTP Protocol Rev.2
IP-SLIP	STD-47	1055	IP datagrams over serial lines: SLIP
PPP	STD-51	1661	Point-to-Point Protocol - PPP
		1662	PPP in HDLC-like Framing
		1332	IPCP - PPP IP Control Protocol
		1570	PPP LCP Extensions
		1662	PPP in HDLC Framing
		2153	PPP Vendor Extensions
POP3	STD-53	1939	Post Office Protocol v.3 - POP3
RIP		1722	RIP - Routing Information Protocol version 2
		1723	
OSPF	STD-54	2328	Open Shortest Path Protocol - OSPF v.3
		2154	OSPF with Digital Signatures
ARP		866	ARP - Address Resolution Protocol
		903	RARP - Reverse Address Resolution Protocol
		1027	Proxy ARP
ATM		1483	Multiprotocol Encapsulation Over ATM
		1577	Classic IP over ATM
BOOTP		951	BOOTP - Bootstrap Protocol
		1497	BOOTP Vendor Extensions
		1533	DHCP Options and BOOTP Vendor Extensions
BGP		1771	Border Gateway Protocol 4
		1517	CIDR - ClassLess Interdomain Router
		1518	
		1519	
		1930	Guidelines for creation, selection and registration of an Autonomous System (AS)

DHCP	2131	DHCP - Dynamic Host Configuration Protocol
	2132	DHCP Options and BOOTP Vendor Extensions
	1534	Interoperation Between DHCP and BOOTP
	2241	DHCP Options for Novell Directory Services
RADIUS	2242	Netware/IP Domain Name and Information
	2138	Remote Authentication Dial-in User Service (RADIUS)
	2139	RADIUS Accounting
HTML	1866	HTML - Hypertext Markup Language
	2110	MIME E-mail Encapsulation of Aggregate Documents such as HTML
HTTP	2068	HTTP/1.1 - Hypertext Transfer Protocol
	2109	HTTP State Management Mechanism
	2168	Resolution of Uniform Resource Identifiers using the Domain Name System
	2145	Use and Interpretation of HTTP Version Numbers
LDAP	2251	LDAP (Lightweight Directory Access Protocol) v.3
IRC	1459	IRC - Internet Relay Chat
MIME	1521	MIME - Multipurpose Internet Mail Extension
NFS	1813	NFS Version 3 - Network File System
NNTP	977	NNTP - Network News Transport Protocol
IPv6	2147	TCP and UDP over IPv6 Jumbograms
	2185	Routing Aspects of IPv6 Transition
ICP	2186	Internet Cache Protocol (ICP), v2
	2187	Application of ICP, v2
Segurança	2196	Site Security Handbook
Histórico	2235	Hobbe's Internet Timeline
Resumos	2151	A Primer on Internet and TCP/IP Tools and Utilities

UNIDADE 2

Objetivo: Saber quem define os padrões utilizados na Internet.

Organizações Padronizadoras

IETF – Internet Engineering Task Force

A **Internet Engineering Task Force (IETF)** ou a Força Tarefa de Engenharia da Internet é responsável pela formação e desenvolvimento de padrões para a Internet. Ela é aberta e se utiliza do trabalho voluntário para funcionar, não tendo uma organização formal (uma organização caórdica). Para maiores informações acesse:

- O site oficial da IETF: <http://www.ietf.org/>
- Detalhes de como é organizada a IETF: <http://www.ietf.org/rfc/rfc3160.txt>

IEEE – Institute Of Electrical And Electronics Engineer

A **IEEE - Institute of Electrical and Electronics Engineers** é uma organização sem fins lucrativos, estabelecida nos Estados Unidos. Ela é a maior em número de membros (profissionais). A IEEE foi formada em 1963 pela fusão do 'Institute of Radio Engineers' (IRE) e do 'American Institute of Electrical Engineers' (AIEE). A IEEE tem diversos escritórios em varias partes do mundo. Os seus membros são engenheiros elétricos, estudantes de ciência da computação, trabalhadores de telecomunicações, etc. O objetivo é promover a "engenharia elétrica". As suas maiores realizações se deram no campo da computação onde estabeleceram diversos padrões para software e dispositivos.

Para mais informação sobre o assunto acesse:

- O site oficial da IEEE: <http://www.ieee.org/>

- Detalhes de suas principais padronizações:

<http://info.computer.org/standards/standesc.htm>

ITU - International Telecommunication Union

A ITU-T - International Telecommunication Union é uma organização que promove os padrões para telecomunicações. Antigamente era conhecida como CCITT ou “Consultative Committee for International Telegraphy and Telephony”.

Para mais informação acesse:

O site oficial da IEEE: <http://www.itu.int/ITU-T>

ISO – International Standard Organization

ISO – International Standard Organization é uma organização não governamental, criada em 1947, estabelecida em Genebra, Suíça, é uma rede dos institutos de padrões nacionais de aproximadamente 130 países. O escritório central em Genebra coordena o sistema e publica os padrões finais.

A missão da ISO é promover o desenvolvimento da estandardização e das atividades com ela relacionadas no mundo com o objetivo de facilitar a troca de serviços e bens, e para promover a cooperação a nível intelectual, científico, tecnológico e econômico.

Todos os trabalhos realizados pela ISO resultam em acordos internacionais os quais são publicados como Standards Internacional. De onde provém o nome ISO? Muitas pessoas têm reparado na falta de semelhança entre o acrônimo em Inglês da Organização e a palavra "ISO". Mas é que ISO não é um acrônimo. Efetivamente, "ISO" é uma palavra, derivada do grego "isos", que significa "igual", raiz do prefixo "iso", que aparece numa grande quantidade de termos. De "igual" até "standard" é fácil continuar por esta linha de pensamento que foi o que levou a escolher "ISO" como o nome da Organização.

IANA – The Internet Assigned Numbers Authority

A IANA, que é operada pela ICANN, é uma das instituições mais antigas da Internet, e está em atividade desde a década de 70. A IANA é a entidade responsável por coordenar alguns dos elementos fundamentais que mantêm a Internet funcionando normalmente. Embora a Internet seja conhecida por ser uma rede mundial sem uma coordenação central, existe a necessidade técnica de que alguns componentes essenciais da Internet tenham uma coordenação global – e esse é o papel de coordenação da IANA.

- O site oficial da IANA: <http://www.iana.org/>

ICANN – Internet Corporation For Assigned Names And Numbers

A ICANN é responsável pela coordenação global do sistema de identificadores exclusivos da Internet, tais como nomes de domínio (.org, .net, .com, .edu, .mil, etc.,) e códigos de países como (.br, .uk, .ch, .at, etc.) e os endereços usados em vários protocolos da Internet que ajudam os computadores a se comunicarem pela Internet. A administração criteriosa e cuidadosa desses recursos é vital para a operação da Internet, de modo que os participantes globais da ICANN se reúnem periodicamente para elaborar políticas que garantam a continuidade da segurança e estabilidade da Internet.

A ICANN é uma entidade internacional sem fins lucrativos em benefício público.

- O site oficial da ICANN: <http://www.icann.org.br/>

Modelos De Inter-Redes

Quando as redes surgiram, estas foram desenvolvidas para comunicar equipamentos do mesmo fabricante o que causava um problema de compatibilidade entre as soluções de diversos fabricantes.

No final da década de 1970, foi criado um modelo de referência que foi chamado de OSI (Open Systems Interconnection), este sistema foi desenvolvido pela ISO (International for Standardization Organization). A proposta desse modelo era conectar diferentes tipos de redes e sistemas, criando uma referência para os fabricantes desenvolverem os protocolos e hardware adequadamente.

Pode-se dizer que ajudou bastante e até que se tem alguma compatibilidade hoje em dia, mas ainda existem soluções proprietárias que seguem padrões próprios.

A tendência dos sistemas operacionais é prover suporte para protocolos desenvolvidos nesse padrão e no padrão do modelo de referência TCP/IP.

Todavia a OSI é o modelo padrão para o desenvolvimento de arquitetura para redes. Neste modelo de referência consta tudo o que é necessário para efetuar a comunicação através das mídias de rede, até uma aplicação ou outro computador. O modelo de referência OSI separa as funções em camadas ou níveis.

O Enfoque Em Níveis

O *modelo de referência* é uma espécie de guia para orientar como as comunicações devem ocorrer. São agrupadas em níveis (camadas) as diversas funções que devem ser implementadas. Pode-se dizer que um sistema de comunicação é projetado desta forma é desenvolvido com *arquitetura de níveis*.

Uma analogia seria comparar as camadas como departamentos de uma grande empresa, cada qual efetua uma tarefa que ajuda o todo a alcançar o seu objetivo. Para que a comunicação flua de forma coerente são implementados *protocolos* que são a implementação dos procedimentos executados por uma camada. Dessa forma no enfoque em níveis cada camada pode ter um conjunto de protocolos que efetua as tarefas de forma similar conforme as necessidades da rede ou sistema operacional.

Esse tipo de desenvolvimento é aconselhável, pois se aproveita dos serviços já implementados em outras camadas; somente é necessário se preocupar com as funções do nível específico e não com as de qualquer outro nível. Se for necessário outro protocolo efetuara o tratamento dos dados para possibilitar a comunicação. Esse processo de tratamento é chamado de *vínculo (binding)*.

Vantagens Dos Modelos De Referência

As vantagens de utilizar um modelo de referência são as seguintes:

- Garante a interoperabilidade entre as tecnologias: Diferentes fabricantes podem integrar diferentes tecnologias, porque existe a padronização.
- Redução da complexidade: Através da decomposição da rede em partes menores e mais simples.
- Padronização das interfaces: Os componentes de rede são padronizados, permitindo um suporte e desenvolvimento eficiente.
- Facilita e engenharia modular: Possibilita a comunicação entre diferentes tipos de dispositivos e softwares.
- Acelera a evolução/desenvolvimento: Garante que o que foi desenvolvido em uma camada não afete a outra, mas que se possam aproveitar os serviços e funções já implementadas.
- Simplifica o ensino e aprendizagem: Fica mais fácil aprender por partes as funções das camadas associando palavras chaves à função que desempenham.

UNIDADE 3

Objetivo: Saber a definição e funcionalidades do modelo de referência de redes OSI.

Modelo De Referência OSI

Como citado anteriormente ao decorrer das décadas à quantidade de equipamentos e do tamanho das redes foi aumentando. Porém existia o problema das redes de diversos fabricantes que não se conversavam entre si, pois foram criadas se utilizando diversos padrões e equipamentos que impossibilitava a conexão entre redes.

Várias redes, no entanto, foram criadas através de implementações diferentes de hardware e de software. Como resultado, muitas redes eram incompatíveis, e a comunicação entre redes com diferentes especificações tornou-se difícil.

Para tratar desse problema, a International Organization for Standardization (ISO) realizou uma pesquisa sobre vários esquemas de rede.

A ISO reconheceu a necessidade de se criar um modelo de rede para ajudar os desenvolvedores a implementar redes que poderiam trabalhar e se comunicar juntas (interoperabilidade). Esse sistema foi criado no final da década de 1970; porém somente em 1984 a ISO lançou o modelo de referência OSI.

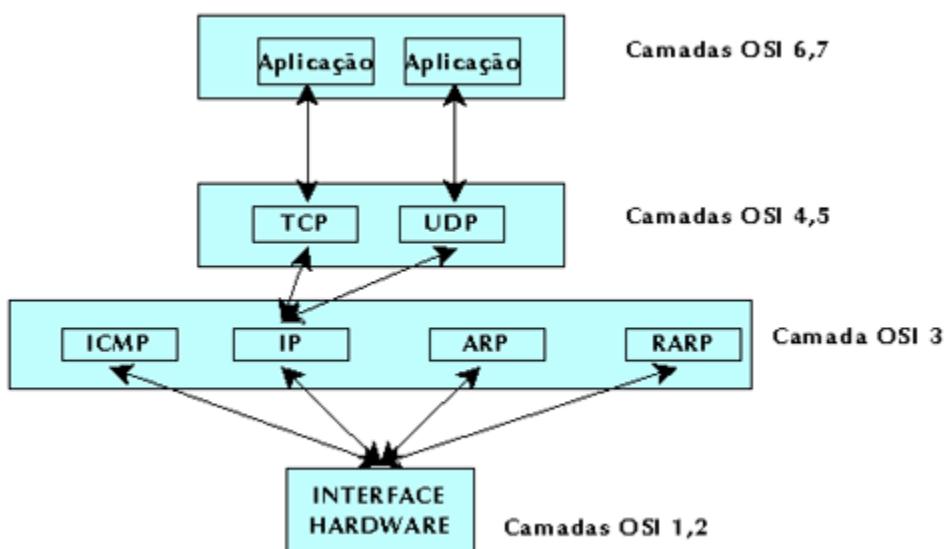
No decorrer desse módulo será explicado como funciona o modelo de referência OSI, citando quais as funções básicas que acontecem em cada camada deste modelo que é a base para entender como funcionam os protocolos de rede e a comunicação entre dispositivos.

Podem-se solucionar vários dos problemas de rede através de testes para detectar em que nível se encontra a falha de comunicação.

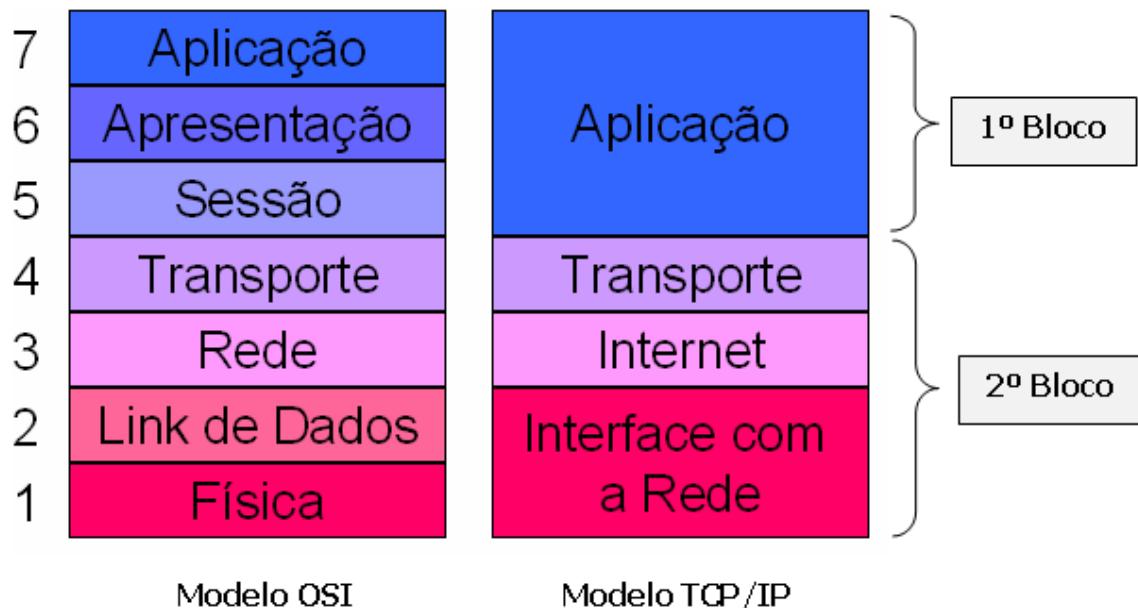
O modelo de referência OSI possui sete níveis (ou camadas):

- Nível Aplicação – nível 7 (Application Layer)
 - Nível Apresentação – nível 6 (Presentation Layer)
 - Nível Sessão – nível 5 (Session Layer)
 - Nível Transporte – nível 4 (Transport Layer)
 - Nível Rede – nível 3 (Network Layer)
 - Nível Enlace - nível 2 (Data Link Layer)
 - Nível Físico – nível 1 (Physical Layer)

Deve-se lembrar sempre que o modelo OSI não é um modelo físico e sim um conjunto de orientações que os desenvolvedores de aplicações de redes podem usar para criar e implementar ferramentas de software (e hardware) que sejam executadas em uma rede.



É possível dividir o modelo OSI em dois blocos conforme sua finalidade. O primeiro bloco define como as aplicações dentro das estações finais se comunicam entre si e comprehende as camadas superiores.



Portanto, o primeiro bloco comprehende as camadas:

- Nível Aplicação (7): Fornece uma interface com o usuário.
- Nível Apresentação (6): Apresenta os dados e fornece criptografia.
- Nível Sessão (5): Separa os dados de diferentes aplicações.

O segundo bloco define como os dados são transmitidos de uma ponta à outra e comprehende as camadas inferiores:

- Nível Transporte (4): Oferece remessa confiável ou não confiável e realiza correção de erro antes de transmitir.

- Nível Rede (3): Oferece endereçamento lógico que os roteadores utilizam para determinar o caminho.
- Nível Enlace (2): Combina pacotes em Bytes e Bytes em quadros, oferece acesso à mídia usando endereço MAC (Media Access Control) e realiza a detecção de erro, não correção.
- Nível Físico (1): Move bits entre dispositivos, neste nível são especificados parâmetros tais como a voltagem dos fios elétricos enviados, velocidade no fio e a pinagem das interfaces com os cabos.

UNIDADE 4

Objetivo: Saber as funcionalidades da camada de Aplicação.

O Nível De Aplicação

No nível de Aplicação temos os seguintes serviços básicos: Serviços de arquivo, impressão, mensagem, banco de dados, programas para aplicações de software e desenvolvimento, etc.

Este nível é aquele que faz de interface com o usuário, ou seja, quando um usuário liga um computador é com este nível que normalmente ele interage com a máquina. Este nível de Aplicação é o responsável direto por identificar se existem recursos suficientes para iniciar a comunicação com o recurso desejado.

Esse método de acesso é normalmente utilizado por aplicações como o correio eletrônico (e-mail) e os serviços de compartilhamento de arquivo que efetuam transferências de dados entre outras tarefas.

Existem outras aplicações que são utilizadas hoje em dia pelas organizações com freqüência e que exigem aplicações inter-redes:

- WWW (World Wide Web): É o nome que se da a um conjunto de informações públicas disponibilizadas na Internet por meio do protocolo HTTP (Hyper Text Transfer Protocol). Normalmente utiliza-se um programa (Browser) de interface com o usuário que permite visualizar documentos HTTP que são acessados na Internet, tais como, IExplorer, Firefox, Opera, etc.
- Gateways de e-mail: Fazem o USO do padrão SMTP (Simple Mail Transfer Protocol) e/ou do X.400 para que sejam providos serviços de mensagens.

- Utilitários de navegação Internet: Incluem aplicações como mecanismos (motores) de busca (Google, Yahoo, Altavista, etc.) e também aplicações como o Gopher que necessitam de acesso a Internet para localizar informações.

A camada de aplicação dentro do processo de comunicação é representada pelo usuário final para o Modelo OSI. Esta camada faz a conversão entre os diversos tipos de terminais, controles de operação, mapeamentos de memória para os terminais, controle de transferência de arquivos, e-mail, seleção da disciplina de diálogo e outras facilidades.

Baseado em pedidos de um usuário da rede, esta camada seleciona os serviços a serem fornecidos por funções das camadas mais baixas. Esta camada deve providenciar todos os serviços diretamente relacionados aos usuários. Alguns destes serviços são:

- Identificação da intenção das partes envolvidas na comunicação e sua disponibilidade e autenticidade
- Estabelecimento de autoridade para comunicar-se
- Acordo sobre o mecanismo de privacidade
- Determinação da metodologia de alocação de custo
- Determinação de recursos adequados para prover uma qualidade de serviços aceitável
- Sincronização de cooperação para aplicações
- Seleção da disciplina de diálogo
- Responsabilidade da recuperação de erros de estabelecimento
- Acordo na validação de dados
- Transferência de informações

Serviços De Divulgação

Faz a divulgação dos serviços disponíveis aos clientes empregando métodos ativos e passivos para divulgar os serviços. Sendo que o método ativo consiste em os servidores de serviços os divulgarem ativamente através de broadcast. Essa divulgação é válida por um tempo determinado o que obriga o Broadcast ser atualizado dentro de um tempo especificado, já que os clientes o removerão de suas tabelas de serviços, caso isso não ocorra.

Da mesma forma, os clientes podem transmitir mensagens solicitando serviços específicos, e os servidores responderão com uma lista de serviços suportados. E o método passivo, onde os serviços oferecidos encontram-se em um registro central, o qual é consultado pelos clientes, para determinar quais serviços estão disponíveis e como acessá-los.

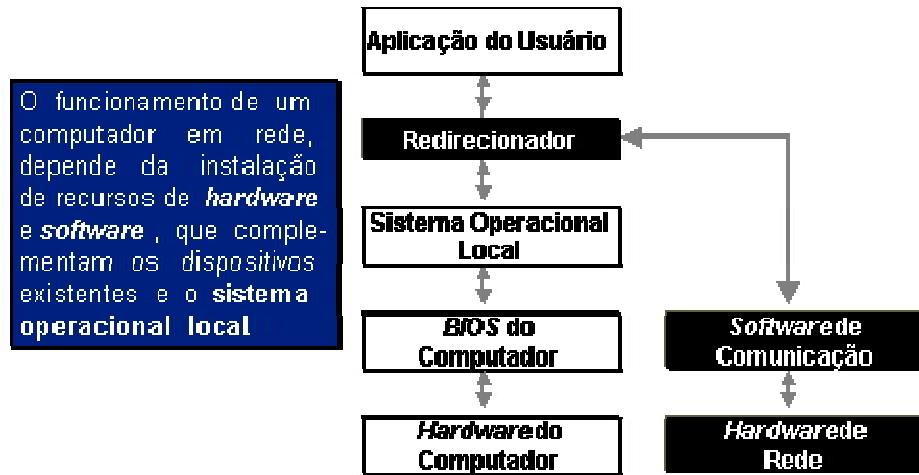
Métodos De Uso Dos Serviços

Os clientes podem acessar os serviços usando três métodos: interrupção de chamadas do sistema operacional, operação remota e cooperação. Na interrupção de chamadas, as aplicações no sistema cliente fazem uma chamada de serviço ao sistema operacional que determina se é uma chamada de recursos locais, que são resolvidos pelo sistema operacional local, ou uma chamada de recursos de rede, onde o sistema operacional envia a solicitação para o servidor apropriado.

A determinação de quem responde ao pedido de serviço do cliente é feita pelo Redirecionador (como mostrado na figura). Quando de uma operação remota, o sistema operacional da estação cliente faz uma interface direta com a rede, conectando-o a um servidor. As solicitações do sistema operacional do cliente aparecem iguais às solicitações do sistema do próprio servidor, portanto o servidor não está diretamente informado da existência independente dos sistemas clientes.

Já no processamento cooperativo, os sistemas operacionais de servidor e cliente são tão avançados que o limite entre eles fica indistinto. Os sistemas operacionais funcionam juntos

para coordenar o uso dos recursos nos dois respectivos computadores, na verdade os computadores que participam de um processamento cooperativo, compartilham todos os seus recursos. Um computador pode iniciar um processo em outro para tirar proveito de alguns ciclos de processamento livres.



Esta camada trata basicamente dos seguintes processos e métodos

Processos	Métodos
Serviços de Rede	<ul style="list-style-type: none"> • Serviços de rede comuns (arquivo, impressão, mensagem, aplicativo e banco de dados). • Serviços de rede centralizados e distribuídos
Divulgação de Serviços	<ul style="list-style-type: none"> • Ativo • Passivo
Uso de Serviços	<ul style="list-style-type: none"> • Interceptação de Chamada do OS • Operação remota • Colaborativa

UNIDADE 5

Objetivo: Saber as funcionalidades da camada de Apresentação.

O Nível De Apresentação

No nível de Apresentação, basicamente são realizados os seguintes processos, apresentação dos dados, aqui também é feito o processamento de criptografia, ou seja, este nível apresenta os dados ao nível de aplicação e é responsável pela tradução de dados e formatação de código.

A função desta camada é interpretar e fazer a manutenção da sintaxe e semântica quando da execução de aplicações remotas, estabelecendo um formato de dados comum entre nós de comunicação. É responsável por:

- Transformação de dados
- Formatação de dados
- Sintaxe de seleção

A transformação de dados é o ato de traduzir os dados entre diferentes formatos. Exemplos de diferenças entre formatos de dados incluem ordem de bytes (poderia ser lido da esquerda para a direita, ou vice-versa) e conjunto de caracteres (caracteres ASCII ou conjunto de caracteres EBCDIC, da IBM), bem como diferenças na representação numérica.

Essencialmente este nível possui uma serie de protocolos especializados em traduzir os dados que vem da camada de Aplicação, neste sentido esta camada pode definir como os dados padrões devem ser formatados.

Na parte gráfica que envolve multimídia e imagens podem ser encontrados os seguintes formatos:

- PICT
- TIFF – Tagged Image File Format
- JPEG – Joint Photographic Experts Group
- MIDI – Musical Instrument Digital Interface
- MPEG – Moving Picture Experts Group
- RTF – Rich Text Format
- QuickTime

A formatação de dados (texto, figuras, arquivos binários, etc.) serve para que o computador receptor entenda o que o computador emissor envia. Um bom lembrete para esta camada de Apresentação é a palavra **formatos**, já que é neste nível que os formatos são definidos para ser enviados e/ou recebidos das outras máquinas.

Basicamente esta camada trata dos seguintes processos e métodos:

Processos	Métodos
Conversão	<ul style="list-style-type: none"> • Ordem dos bits • Ordem dos bytes • Código de caracteres • Sintaxe dos arquivos
Criptografia	<ul style="list-style-type: none"> • Códigos públicos • Código privado

UNIDADE 6

Objetivo: Saber as funcionalidades da camada de Sessão.

O Nível De Sessão

O nível de Sessão separa os dados das diferentes aplicações das camadas superiores. A camada de Sessão tem a função de iniciar e terminar a comunicação entre dois dispositivos que querem se comunicar. Ela serve a camada de apresentação que aproveita seus serviços e também cuida da sincronia entre os diálogos entre a camada de apresentação de dois dispositivos, coordenando a troca de informações entre eles.

Oferece recursos para tornar eficiente a transferência de informações e também poderia fornecer serviços e relatórios de exceção sobre a camada de Sessão, a camada de Apresentação e a camada de Aplicação. Uma boa sugestão para se lembrar desta camada é a palavra **dialogo** e conversações.

Existem alguns protocolos e interfaces no nível de sessão como:

- NFS – Network File System
- SQL – Structured Query Language
- RPC – Remote Procedure Call
- X Window – Interface gráfica para sistemas UNIX
- ASP – Apple Talk Session Protocol
- DNA SCP – Digital Network Architecture Session Control Protocol

Esta camada gerencia todas as atividades das camadas inferiores. Ela faz isso através de conexões virtuais, que são estabelecidas quando a estação transmissora troca mensagens com a estação receptora, e diz a ela para iniciar e manter um enlace (link) de comunicação. É similar ao que acontece quando alguém se conecta a uma rede. Uma vez feito o login pelo usuário, a conexão é mantida até o logout, mesmo sem acesso contínuo à rede.

Localizada acima da camada de Transporte e abaixo da camada de Apresentação, propicia a criação e o gerenciamento de uma ou mais sessões entre as máquinas conectadas.

Ela é responsável por:

- Intercâmbio de Dados, para troca de dados entre usuários.
- Controle de Conversação, determinando quem pode falar e quando.
- Sincronização em Diálogos, possibilitando interrupções e retornos (quando ocorre algum erro, por exemplo).
- Gerenciamento de Atividades, que são unidades lógicas menores independentes em que são divididas as mensagens do usuário.
- Relatório de Exceções, permitindo que problemas sejam relatados.

Intercâmbio De Dados

O intercâmbio de dados é o recurso mais importante da camada de sessão. Ele envolve três fases: estabelecimento, utilização e liberação. O estabelecimento de sessão é feito através de um pedido de conexão à camada de transporte, e envolve a negociação entre usuários no que tange aos diversos parâmetros da conexão. Alguns destes parâmetros são pertinentes à conexão de transporte e são simplesmente passados para esta conexão sem qualquer modificação.

A liberação pode ser feita de duas formas na camada de sessão: de forma abrupta ou disciplinada. A primeira é análoga a desconexão na camada de transporte e uma vez

emitida, a conexão não recebe mais nenhum dado. Ela é utilizada para abortar conexões. A liberação disciplinada, por sua vez, utiliza um Handshake (protocolo de inicialização) completo: pedido, indicação, resposta e confirmação. Com isso, esta forma de liberação pode aceitar mensagens até que uma confirmação seja enviada.

A camada de sessão pode transmitir quatro tipos diferentes de dados, a saber: regulares e expedidos (análogos aos tipos da camada de transporte), tipificados e dados de capacidade.

Gerenciamento De Diálogos

O controle de conversação é implementado por meio de tokens, ou seja, quem o possui tem o direito de se comunicar. O token pode ser requerido, porém pode-se adotar uma política de prioridades para permitir uso desigual do token.

Existem muitas situações em que o software da camada superior está estruturado de forma a esperar que os usuários se revezem (comunicação Half-duplex). Para tal, foram introduzidos controles para determinar de quem é a vez de transmitir. O gerenciamento de diálogos foi implementado através do uso de tokens de dados. Ao se estabelecer uma sessão, pode ser utilizado um parâmetro que indique o modo (Half-duplex) e um outro parâmetro que diga qual dos lados recebe inicialmente o token. Somente o usuário que está com o token pode transmitir, enviando o token para o outro usuário assim que encerrar sua transmissão.

Sincronização

A sincronização é utilizada para devolver as entidades na camada de sessão um estado conhecido. Isso pode ser necessário no caso de ocorrerem erros ou divergências. Este serviço pode parecer desnecessário, uma vez que a camada de transporte cuida dos erros de comunicação, porém podem ocorrer erros na camada superior.

O texto na camada de sessão pode ser dividido em páginas. Estas páginas podem ser separadas por pontos de sincronização. Se ocorrer algum problema é possível reiniciar a

partir de um ponto de sincronização anterior (ressincronização). Quando essa ressincronização ocorre, o salvamento de mensagens (e a retransmissão subsequente) ocorre acima da camada de sessão.

Existem dois tipos de pontos de sincronização, a saber: principal e secundário. O ponto de sincronização principal delimita as partes logicamente significativas de trabalho, chamadas unidades de diálogo. Estas unidades podem conter vários pontos de sincronização secundários. Quando ocorre a ressincronização retorna-se até o ponto de sincronização principal mais recente, ou a um ponto de sincronização secundário desde que este não tenha sido precedido de um ponto principal.

Para a fixação de pontos de sincronização são utilizados tokens. Existem dois tokens independentes, para o ponto principal e o secundário. Estes tokens são distintos entre si e diferentes também dos utilizados para controle de dados na comunicação Half-duplex.

Gerenciamento De Atividades

O gerenciamento de atividades é utilizado para permitir que o usuário divida o fluxo de mensagens em unidades lógicas (atividades). Cada atividade é completamente independente de outra subsequente ou anterior. O usuário determina o que deve constituir cada atividade (e não a camada de sessão). Tudo o que a camada de sessão faz é transmitir para o receptor as indicações de inicio, finalização, retomada, interrupção ou descarte de uma atividade. Porém a camada de sessão não sabe quando as solicitações de atividades são feitas e como são as reações do receptor.

O gerenciamento de atividades é a forma principal de se estruturar uma sessão. Para que não ocorram pedidos simultâneos de inicio de atividades, todo gerenciamento é controlado por um token (o mesmo token utilizado para pontos de sincronização principal). Esse token pode, em princípio, ser enviado e solicitado de maneira independente de dados e de tokens de sincronização secundários.

A ISO concluiu que se um usuário iniciar uma atividade enquanto o outro estiver fazendo uma sincronização secundária, podem ocorrer problemas. Para solucionar isso, antes que uma atividade ou operação de sincronização seja iniciada a camada de Sessão do usuário deve reter os tokens de atividade, sincronização secundária e dados.

Outra questão importante é a relação entre as atividades e os pontos de sincronização. Cada vez que é iniciada uma nova atividade os números de séries dos pontos de sincronização são reinicializados e é criado um ponto de sincronização principal. Podem ser criados pontos de sincronizações adicionais, secundários ou não, dentro de atividades. Uma vez que uma atividade é iniciada, se ocorrer uma ressincronização não é possível retornar para uma atividade anterior.

Relatório De Exceções

Este serviço é utilizado para que sejam relatados erros inesperados. Se o usuário tiver algum problema, ele pode relatar este para seu parceiro explicando o que aconteceu. O relatório de exceções não se aplica apenas a erros detectados pelo usuário, mas também para problemas internos na camada de sessão ou problemas relatados pelas camadas inferiores. Porém a decisão da ação que deve ser tomada é sempre feita pelo usuário. Basicamente a camada trata dos seguintes processos e métodos:

Processos	Métodos
Controle de diálogos	<ul style="list-style-type: none"> • Simplex • Duplex Parcial (half duplex) • Duplex Completo (full duplex)
Administração de sessões	<ul style="list-style-type: none"> • Estabelecimento da conexão • Transferência de dados • Liberação da conexão

UNIDADE 7

Objetivo: Saber as funcionalidades da camada de Transporte.

O Nível De Transporte

O nível de Transporte oferece serviços de remessa (transporte) de mensagens que pode ser confiável (orientado à conexão) ou não confiável (não orientado à conexão). Realiza também correção de erro antes de transmitir.

A camada de Transporte efetua a segmentação dos dados das aplicações do nível superior quando esta no processo de envio e efetua a união ao fluxo de dados e a montagem quando recebe pacotes da camada de rede. Ela cuida do transporte de dados fim a fim e estabelece uma conexão lógica entre os computadores de envio e de destino na rede.

A camada de transporte pode ser considerada a divisão entre as camadas inferiores e superiores, pois efetua o isolamento das camadas superiores que não necessitam dos detalhes de implementação de como é feito o transporte de dados. O tipo de transporte seguro ou não dizem respeito desta camada. São criados circuitos virtuais (que são estabelecidos através dos serviços de comunicação – a camada cria e termina esses circuitos conforme sua necessidade). Existe nessa camada o controle de fluxo de dados, a detecção e recuperação de erros de transporte. Ao pensar nessa camada pense em **segmento** e em transporte confiável e não confiável.

Funcionamento Básico

A função básica da camada de Transporte é aceitar dados da camada de sessão, quebrá-los em unidades menores se necessário, passar estes para a camada de rede e assegurar que todas as peças (pacotes) chegarão corretamente ao outro extremo. Protocolos de transporte são empregados para estabelecimento, manutenção e liberação de conexões de transporte

que representam um caminho duplo (Full-duplex) para os dados entre dois endereços de transporte. O modelo OSI define três fases de operação dentro da camada de transporte:

1. **Fase de estabelecimento:** O objetivo desta fase é o estabelecimento de conexões entre funções de serviços das camadas mais altas. A qualidade dos serviços de conexão pode ser negociada durante esta fase
2. **Fase de transferência:** Esses serviços têm como objetivo a transferência de dados de acordo com a qualidade dos serviços descritos na fase de estabelecimento.
3. **Fase de terminação:** Esses serviços permitem encerrar uma sessão terminando a conexão, sendo notificadas ambas as partes

Basicamente a camada trata dos seguintes processos e métodos:

Processos	Métodos
Resolução de endereço / nome	<ul style="list-style-type: none"> • Serviço iniciado pelo solicitante • Serviço iniciado pelo provedor
Endereçamento	<ul style="list-style-type: none"> • Identificador da conexão • Identificador da transação
Desenvolvimento de segmentos	<ul style="list-style-type: none"> • Divisão e combinação
Serviços de conexão	<ul style="list-style-type: none"> • Ordem de segmentos • Controle de erros • Controle de erros de uma extremidade a outra

UNIDADE 8

Objetivo: Saber as funcionalidades da camada de Rede.

O Nível De Rede

O nível de Rede oferece endereçamento lógico que os roteadores utilizam para determinar o melhor caminho possível até o destino final.

A camada de rede é uma camada que cuida dos endereços dos dispositivos de rede (sua localização) e da seleção do melhor caminho entre dois sistemas que estão em lugares diferentes. Para lembrar dessa camada se lembre de caminho ou rota (**roteamento** e endereçamento). Absolutamente todos os Roteadores de rede atuam neste nível, algumas Bridges (Pontes) poderiam atuar também neste nível ou camada.

Existem dois tipos de pacotes que são utilizados nesse nível de rede:

- Pacotes de Dados: São os responsáveis de transportar os dados dos usuários entre os diferentes tipos de redes (inter-rede). Por exemplo, protocolos sensíveis a roteamento tais como o IP e IPX.
- Pacotes de Atualização de Rotas: São os responsáveis para atualizar a informação dos roteadores, através do anúncio e manutenção de tabelas de rotas.

Entre os protocolos que fazem manutenção de tabelas de roteamento assim como informam da disponibilidade da mesma temos o RIP (v1 e v2), o EIGRP e o OSPF.

Funcionamento Básico

Estabelece uma conexão lógica entre dois pontos, cuidando do tráfego e roteamentos dos dados da rede. Roteamento é o processo de escolha do caminho pelo qual iremos enviar os datagramas, este processo pode ser dividido em:

- **Roteamento Direto:** comunicação entre dois computadores alocados em uma mesma rede física ou rede de área local (LAN).
- **Roteamento Indireto:** conexão entre dois computadores alocados em redes distintas. Neste caso, é necessário o uso de roteadores Gateways para efetuar o encaminhamento dos datagramas (blocos de dados) à rede destino. Este tipo de roteamento é típico em redes de área estendida (WAN).

O algoritmo de roteamento IP utiliza tabelas de roteamento que contém endereços de possíveis destinos e a maneira de alcançá-los, alocadas em computadores e Gateways. Temos então uma rede de comutação por mensagens com inteligência de roteamento descentralizada.

A camada de Rede também controla o congestionamento das sub-redes, ou seja, evita os gargalos quando muitos pacotes estão presentes na sub-rede ao mesmo tempo. Outros problemas são inerentes a esta camada tais como pacotes que não chegam ao destino devido ao tamanho, incompatibilidade de endereços em redes distintas, protocolos diferentes, etc.

Esta camada ocultará da camada de transporte qualquer conhecimento a respeito dos sistemas de trânsito (retransmissões), roteamento e tecnologia utilizada no meio de comunicação (fibra óptica, comutação de pacotes, satélites, redes locais, etc.)

Basicamente a camada trata dos seguintes processos e métodos:

Processos	Métodos
Endereçamento	<ul style="list-style-type: none"> • Rede lógica • Serviço
Comutação	<ul style="list-style-type: none"> • Pacote • Mensagem • Circuito
Descoberta de Rota	<ul style="list-style-type: none"> • Vetor de distância • Estado de vínculo
Seleção de rota	<ul style="list-style-type: none"> • Estática • Dinâmica
Serviços de conexão	<ul style="list-style-type: none"> • Controle do fluxo da camada Rede • Controle de erros • Controle da ordem de pacotes
Serviços de gateway	<ul style="list-style-type: none"> • Conversão de camadas da rede

UNIDADE 9

Objetivo: Saber as funcionalidades da camada de enlace de dados.

O Nível De Enlace De Dados

O nível de Enlace combina pacotes em bytes e bytes em quadros. Oferece acesso à mídia usando endereço MAC. Realiza a detecção de erro, não correção.

A camada de enlace (data link) oferece a transmissão física dos dados e cuida da notificação de erro, topologia de rede e controle de fluxo. Ela cuida do trânsito seguro dos dados e garante que as mensagens sejam entregues ao dispositivo correto em uma rede; isto é feito através do uso dos endereços de hardware (endereçamento físico).

Esta camada de enlace providencia maneiras funcionais e procedimentos para estabelecimento, manutenção e liberação de enlace de dados entre as entidades da rede. Os objetivos são providenciar a transmissão de dados para a camada de rede e detectar, e possivelmente corrigir, erros que possam ocorrer no meio físico. As características funcionais desta camada são:

- Conexão dos enlaces, ativação e desativação. Estas funções incluem o uso de facilidades multiponto físico para suportar conexões em funções da camada de rede.
- Mapeamento de unidades de dados para a camada de rede dentro das unidades do protocolo de enlace para transmissão.
- Multiplexação de um enlace de comunicação para várias conexões físicas.
- Delimitação de unidades de transmissão para protocolos de comunicação.
- Detecção, notificação e recuperação de erros.
- Identificação e troca de parâmetros entre duas partes no enlace.

Funcionamento Básico

A principal tarefa da camada de enlace de dados é pegar uma estrutura de transmissão primária e transformá-la em uma linha que aparenta estar, para a camada de rede, livre de erros de transmissão não detectados. Ela cumpre esta tarefa fazendo com que o emissor quebre os dados de entrada em quadros de dados (tipicamente algumas centenas ou uns poucos milhares de bytes), transmita os quadros seqüencialmente e processe os quadros de reconhecimento enviados de volta pelo recebedor.

Desde que a camada física simplesmente aceita e transmite uma seqüência de bits sem qualquer relação de significado ou estrutura, é tarefa da camada de enlace criar e reconhecer limites de quadros. Isto pode ser conseguido pelo acréscimo de padrões de bit especiais ao começo e fim do quadro. Se estes padrões de bit podem accidentalmente ocorrer nos dados, um cuidado especial deve ser tomado para se estar certo de que estes padrões não são interpretados incorretamente como delimitadores de quadros. Um ruído na linha pode destruir um quadro completamente. Neste caso, o software da camada de enlace na máquina de origem pode retransmitir o quadro. Entretanto, transmissões múltiplas do mesmo quadro introduzem a possibilidade de quadros duplicados. Um quadro duplicado poderia ser enviado se o quadro de reconhecimento indo do receptor para o emissor fosse perdido.

Esta camada deve resolver os problemas causados pela danificação, perda e quadros duplicados. A camada de enlace pode oferecer diversas classes de serviço diferentes para a camada de rede, cada um com uma qualidade e preço diferente.

Uma outra questão que surge na camada de enlace (e na maioria das camadas mais altas) é como manter um transmissor rápido inundando com dados um receptor lento. Alguns mecanismos de regulamentação de tráfego devem ser empregados para que o transmissor saiba quanto de espaço de buffer o receptor tem no momento. Freqüentemente, esta regulagem de fluxo e a recuperação de erro são integradas. Se a linha pode ser usada para transmitir dados nas duas direções (modo Full-duplex), isto introduz uma nova complicação que o software da camada de enlace deve lidar. O problema é que o tráfego dos quadros de

reconhecimento de A para B compete com o uso da linha com tráfego de quadros de dado de B para A. Uma solução inteligente, conhecida como Piggyback, tem sido formulada.

Ao pensar na camada de enlace de dados pense em **frames** (quadros) e em acesso à camada física que faz uso dos meios físicos, tais como, cabos, fibras, radioenlace, etc.

Redes broadcast têm uma questão adicional na camada de ligação: como controlar o acesso no canal compartilhado. Uma subcamada especial da camada de enlace, a subcamada de acesso ao meio, lida com o problema.

O IEEE iniciou em Fevereiro de 1980 (02/80) o projeto conhecido como 802 que definiu uma série de normas para as camadas Física e Enlace do modelo de referência OSI. Sendo a camada de Enlace de dados subdividida em duas subcamadas:

1. LLC (Logical Link Control)
2. MAC (Medium Access Control)

Nesse projeto, os padrões diferem na camada física e na subcamada MAC, mas são compatíveis na subcamada LLC. As definições deste projeto foram aceitas pelos demais organismos de padronização, dentre eles a ISO (sob nome ISO 8802).

O projeto foi dividido nos seguintes grupos:

- **802.1:** Definição do gerenciamento de redes e generalidades;
- **802.2:** Descrição da subcamada LLC da camada de Enlace;
- **802.3:** Descrição da subcamada MAC e camada Física para redes com topologia em barramento e método de acesso ao meio baseado em CSMA/CD;
- **802.4:** Descrição da subcamada MAC e camada Física para as redes com topologia em barramento e método de acesso ao meio baseado em “token-passing” (Token-Bus);

- **802.5:** Descrição da subcamada MAC e camada Física para as redes com topologia em anel e método de acesso ao meio baseado em “token-passing” (Token-Ring);
- **802.6:** Descrição da subcamada MAC e camada Física para as redes metropolitanas (MAN).
- **802.11:** Descrição da subcamada MAC para as redes LAN sem fio (Wireless LAN).
- **802.12:** Descrição da subcamada MAC para redes do tipo Demand Priority.

A Norma IEEE 802.3

O padrão IEEE 802.3 é para uma LAN com CSMA/CD persistente a sua origem vem do sistema ALOHA, posto em funcionamento em 1971 para comunicação entre os computadores dos 7 campi (em 4 ilhas) da Universidade do Havaí. A comunicação era feita por ondas de rádio. Mais tarde a detecção de portadora foi adicionada, e a Xerox construiu um sistema CSMA/CD de 2.94 Mbps para conectar até 100 estações de trabalho pessoais em um cabo de até 1 Km de extensão. O sistema foi chamado de Ethernet como referência ao éter luminescente, através do qual se pensou, em certa época, que se propagavam as radiações eletromagnéticas.

A Ethernet da Xerox foi tão bem sucedida que a Xerox, a DEC e a Intel redigiram um padrão para uma Ethernet de 10 Mbps (Ethernet versão 2). Esse padrão formou a base do IEEE 802.3.

O padrão 802.3 difere da especificação Ethernet no fato de descrever toda uma família de sistemas CSMA/CD persistentes, rodando a velocidades de 1 a 10 Mbps e sob diversos meios físicos (do par-trançado à fibra óptica, passando pelo cabo coaxial), enquanto a Ethernet só o faz para 10 Mbps e com meio físico tipo cabo coaxial de 50 ohms. Outra diferença está na Ethernet especificar os serviços das camadas 1 e 2 do modelo de referência OSI, enquanto a norma IEEE 802.3 especifica a camada física (nível 1) e

subcamada MAC do nível 2 sem definir o protocolo da subcamada LLC do nível 2 (definida separadamente pela IEEE 802.2).

Vale ressaltar que ambos os padrões (Ethernet II e IEEE 802.3) podem coexistir em uma mesma LAN, mas cuidados especiais devem ser tomados para que a mesma funcione corretamente. Os formatos dos quadros (Frames) Ethernet e da IEEE 802.3 são mostrados na figura onde o tamanho dos campos está expresso em Bytes.

Ethernet

7	1	6	6	2	46-1500	4
Preamble	SOF	Endereço de destino	Endereço da fonte	Type	Dado	FCS

IEEE 802.3

7	1	6	6	2	46-1500	4
Preamble	SOF	Endereço de destino	Endereço da fonte	Length	Header 802.2 e dados	FCS

Ambos os quadros começam com um padrão alternado de “uns” e “zeros” chamado de preâmbulo (Preamble). Este informa às estações receptoras que um quadro está começando. A seguir vem um byte denominado delimitador de início de quadro (start-of-frame, SOF). Este Byte termina com 2 bits “1” consecutivos que servem para sincronizar a parte de recepção de frame de todas as estações da LAN.

A próxima informação do frame são os campos de endereço de destino e de origem (ambos de 6 bytes de comprimento). Estes endereços físicos estão contidos nas placas de rede e são únicos. O endereço de origem é sempre um endereço unicast (nó único), enquanto o endereço de destino pode ser unicast, multicast (grupo) ou broadcast (a todos os nós).

Nos quadros Ethernet, o campo de 2 bytes seguinte ao endereço de origem é o campo Type. Este campo especifica o protocolo de nível superior a receber o dado após o processamento de que o quadro Ethernet seja completado. Já nos quadros IEEE 802.3, estes dois Bytes correspondem ao campo Length, que indica o número de bytes que vem após este campo e que precede o campo Frame Check Sequence (FCS).

Seguido ao campo Type/Lenght vem o dado do frame. Depois do processamento das camadas físicas e de enlace, este dado é eventualmente enviado a um protocolo de camada superior. No caso da Ethernet, este protocolo é identificado no campo Type. No caso da IEEE 802.3, o protocolo deve ser definido dentro do campo de dado. Se o dado no quadro não for suficiente para preencher o mínimo de 64 Bytes (somados do endereço de destino até o campo FCS), alguns Bytes de preenchimento são inseridos para garantir este número mínimo de Bytes. Depois do campo de dados vem o campo FCS de 4 bytes de comprimento.

Este contém o valor de verificação de redundância cíclica (Cyclic Redundancy Check, CRC). O CRC é criado pelo dispositivo transmissor e recalculado pelo dispositivo receptor para verificar por danos aos dados que podem ter ocorrido ao frame na transmissão. As Bridges (pontes) e os Switchs atuam neste nível. Basicamente a camada de enlace possui as seguintes subcamadas as quais tratam dos seguintes processos e métodos.

Subcamada 802.2 (LLC)

Esta subcamada é conhecida como de controle de enlace lógico LLC (Logical Link Control). é a subcamada mais alta do nível de enlace (que é em si a camada 2, bem acima da camada física) no modelo OSI de sete camadas. Esta camada fornece mecanismos de multiplexação e controle de fluxo que torna possível para os vários protocolos de rede (IP, IPX) conviverem dentro de uma rede multiponto e serem transportados pelo mesmo meio da rede.

O LLC especifica os mecanismos para endereçamento de estações conectadas ao meio e para controlar a troca de dados entre os vários usuários da rede. A operação e formato deste padrão são baseados no protocolo HDLC (High-level Data Link Control).

Processos	Métodos
Topologia Lógica	<ul style="list-style-type: none"> • Barramento • Anel
Acesso à mídia	<ul style="list-style-type: none"> • Disputa • Passagem de Símbolos • Polling
Endereçamento	<ul style="list-style-type: none"> • Dispositivo Físico

Subcamada 802.3 (MAC)

Esta é a camada propriamente de Cliente MAC (Médium Access Control), isto é, de controle de acesso ao meio.

Processos	Métodos
Sincronização de transmissões	<ul style="list-style-type: none"> • Assíncrona • Síncrona • Isócrona
Serviços de conexão	<ul style="list-style-type: none"> • Controle do fluxo no nível LLC • Controle de Erros



Atividades

Antes de dar continuidades aos seus estudos é fundamental que você acesse sua SALA DE AULA e faça a Atividade 1 no “link” ATIVIDADES.



UNIDADE 10

Objetivo: Saber as funcionalidades da camada física.

O Nível Físico

O nível Físico pode movimentar os bits de informação entre os dispositivos da rede, especifica as características físicas do sinal na rede, por exemplo, nível de voltagem dos bits transferidos, assim como a velocidade no fio e a pinagem dos cabos, por exemplo, DB-9 (9 pinos para a porta serial), ou o barramento da placa de rede.

A camada física define as especificações elétricas, mecânicas, funcionais e de procedimentos para ativar, manter e desativar o link físico entre sistemas finais. Basicamente a função da camada física é transmitir dados, definindo as especificações elétricas entre a fonte e o destino conforme a especificação i.e. RS-232.

Esta camada é a responsável de prover as características físicas, elétricas, funcionais e procedimentos para ativar, manter e desativar conexões entre duas partes. Ela está ligada diretamente à transmissão de bits primários por um canal de comunicação.

Tarefas Básicas

As tarefas de planejamento desta camada devem garantir que quando um lado envia um bit 1, este seja recebido do outro lado como um bit 1, não como um bit 0. Algumas perguntas típicas são: quantos volts deveriam ser usados para se representar um 1 e quantos para um 0; quantos microsegundos um bit deve durar; se a transmissão deve proceder em ambas as direções; como a conexão inicial é estabelecida entre as partes e como ela é desfeita quando os dois lados tiverem terminado; quantos pinos o conector de rede deverá ter e qual a funcionalidade de cada um desses pinos.

As tarefas de planejamento aqui se envolvem amplamente com interfaces mecânicas, elétricas, e de procedimento, e com o mediador de transmissão física, que fica abaixo da camada física.

Esta camada é a única que possui acesso físico ao meio de transmissão da rede devendo, portanto, se preocupar com fatores como as especificações elétricas, mecânicas, funcionais e procedurais da interface física entre o equipamento e o meio de transmissão, ou seja, a camada física tem como função básica a adaptação do sinal ao meio de transmissão.

Podemos relacionar abaixo, as principais características inerentes à camada física:

- **Mecânicas:** propriedades físicas da interface com o meio físico de transmissão, incluindo, por exemplo, o tipo de conector utilizado.
- **Elétricas:** se relacionam com a representação de um bit em termos de, por exemplo, nível de tensão utilizado e taxa de transmissão de bits.
- **Funcionais:** definem as funções a serem implementadas por esta interface;
- **Procedurais:** especificam a seqüência de eventos trocados durante a transmissão de uma série de bits através do meio de transmissão

A camada física possui ainda as seguintes funções:

- **Estabelecimento/encerramento de conexões:** ativa e desativa conexões físicas mediante solicitação a entidades da camada de enlace
- **Transferência de dados:** a unidade de transmissão utilizada é o bit. O nível físico tem como função transmitir os bits na mesma ordem em que chegam da camada de enlace (no computador de origem) e entregá-los à camada de enlace na mesma ordem que chegaram (no computador de destino)

- **Gerenciamento das conexões:** gerência da qualidade de serviço das conexões físicas estabelecidas. Deve monitorar taxa de erros, disponibilidade de serviço, taxa de transmissão, atrasos do fluxo de bits, etc.

Ao pensar na camada física pense em **bits**, em sinais elétricos e meios de comunicação (cabos, fibras, radioenlace, etc.). Os repetidores e Hubs atuam neste nível / camada. Os padrões de nível físico utilizados são, por exemplo, Ethernet (IEEE 802.3), Token-Ring (IEEE 802.5), X.21, X.21 bis, V.24, V.28, RS-232C, I.430, I.431, etc.

Basicamente a camada trata dos seguintes processos e métodos:

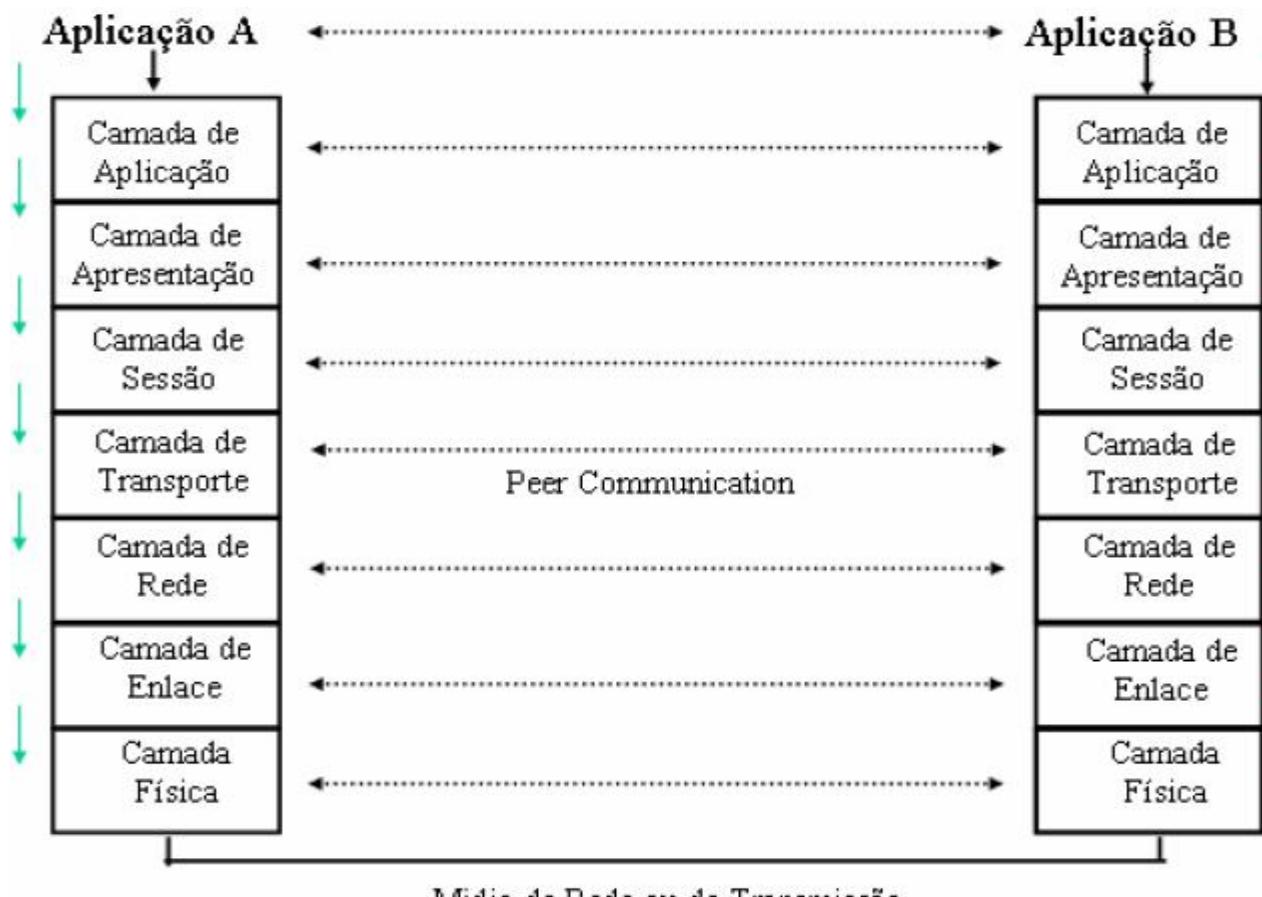
Processos	Métodos
Tipos de Conexão	<ul style="list-style-type: none"> • Ponto a Ponto • Multiponto
Topologia Física	<ul style="list-style-type: none"> • Barramento • Anel • Estrela • Malha • Celular
Sinal Digital	<ul style="list-style-type: none"> • Estado Atual • Transmissão de estados
Sinal Analógico	<ul style="list-style-type: none"> • Estado Atual • Transição de estados
Sincronização de bits	<ul style="list-style-type: none"> • Assíncrono • Síncrono
Uso da banda passante	<ul style="list-style-type: none"> • Banda-larga • Banda-base
Multiplexação	<ul style="list-style-type: none"> • FDM (Divisão de Freqüência) • TDM (Divisão de Tempo) • StatTDM (Divisão de Tempo Estatística)

UNIDADE 11

Objetivo: Entender o que mais o modelo OSI tem-nos a oferecer.

Mais Sobre O Modelo OSI

Sabe-se que as camadas do modelo OSI são 7 e cada camada (da máquina A) se comunica com a do mesmo nível (na máquina B), esse tipo de comunicação é conhecida como “Peer Communication”, ou seja, algo assim como “comunicação entre pares” de protocolos. Por exemplo, os protocolos da camada de rede (da máquina A) se comunicarão (única e exclusivamente) com os protocolos da camada de rede da máquina B, os de transporte com os de transporte, os de sessão com os de sessão e assim por diante.

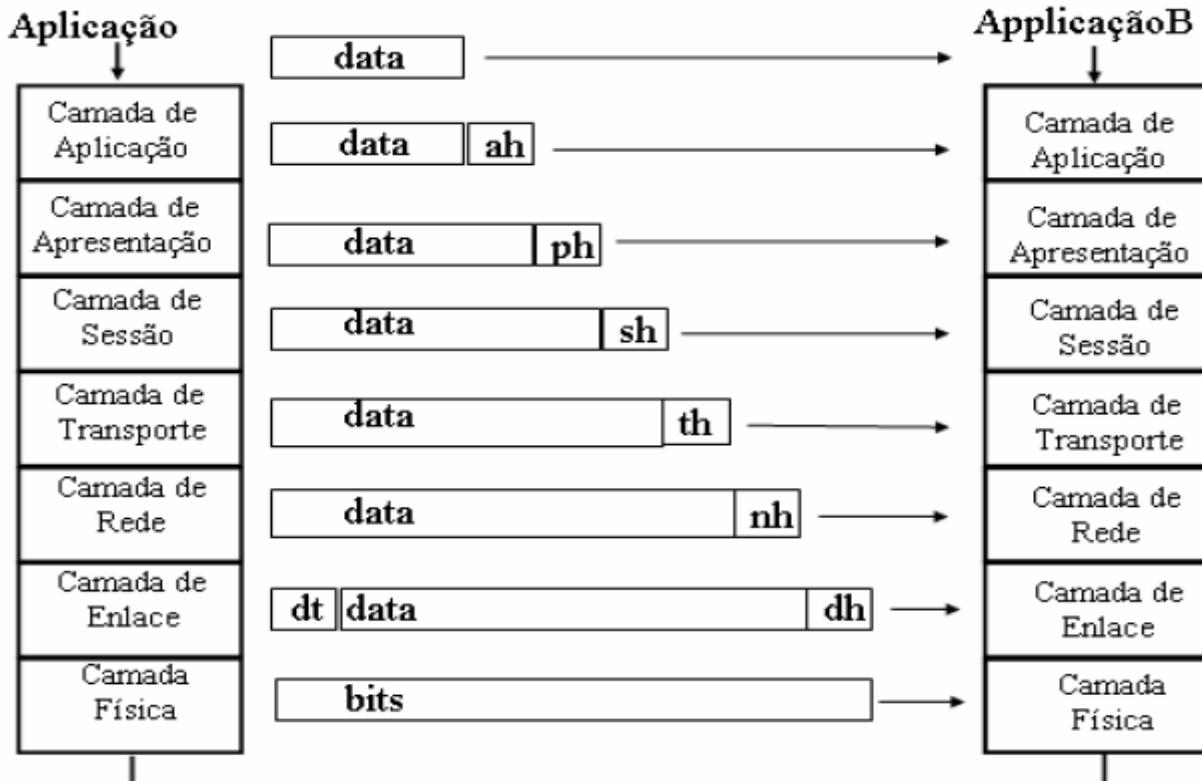


Cada camada efetua um grupo de tarefas específicas. Mas o modelo de referência OSI é um padrão, as camadas não executam nenhuma função. As implementações em software ou hardware que executam as funções associadas a uma camada da OSI (pode ser um Driver de rede).

As camadas geram pedidos (informação, dados) que são adicionados a um cabeçalho que contem as solicitações ou informações da camada em questão. Esses dados atravessam as camadas, por exemplo, da camada 7 para a 1 e daí ele vai para a mídia de transmissão (cabo, fibra, radioenlace, etc) e sobem da camada 1 para a 7. Em cada camada os dados vão experimentando algo, isto é, vai sendo adicionado (se os dados estiverem descendo) ou removido (se os dados estiverem subindo) partes do cabeçalho assim como também vão realizando-se funções da camada em que esta passando.

Esses cabeçalhos adicionam informações extras; essas informações são indispensáveis para que cada camada de aplicação consiga comunicar-se com a outra.

Cabeçalhos adicionados aos Dados



Como as camadas superiores utilizam das funcionalidades das camadas inferiores, isso se chama de pilha.

Portanto, uma pilha de protocolos é um grupo hierárquico de protocolos que funciona de forma conjunta – geralmente em um único computador. Os bits que constituem o conjunto de um pacote de dados assumem, dependendo da camada, os seguintes nomes:

- Na camada Física temos os Bits propriamente ditos.
- Na camada de Enlace de Dados temos os Quadros (ou Frames) Ethernet.
- Na camada de Rede temos os Pacotes IP.
- Na camada de Transporte temos os Segmentos (datagramas TCP ou UDP).
- Na camada de Aplicação temos as Mensagens enviadas/recebidas pelo usuário.

Observação: A descrição de cada camada em detalhes engloba uma série de aspectos técnicos que poderia consumir um tempo de leitura imenso e gerar até uma leitura redundante do que já foi visto (o modelo OSI é muito complexo se explicado em detalhe e pode deixar ao leitor uma sensação não muita agradável).

Então serão indicados Links com material “extra”, caso se opte por um aprofundamento no assunto estudado.



Dica

Uma boa idéia ou opção para se direcionar a carreira profissional é obter alguma certificação de rede. Isso além de melhorar o reconhecimento profissional por parte do empregador pode trazer novos conhecimentos e até gerar um aumento no salário.

O, porém da certificação é ter que efetuar a renovação periodicamente; para a área de redes e protocolos é interessante ter uma certificação CISCO, como a CCNA ou alguma de nível superior como o CCNP.

Materiais de estudo desse tipo certamente podem ajudar a compreender e possibilitar a configuração de equipamentos como roteadores e Switches que são muito interessantes de se lidar. Assim como outros tipos de dispositivos.



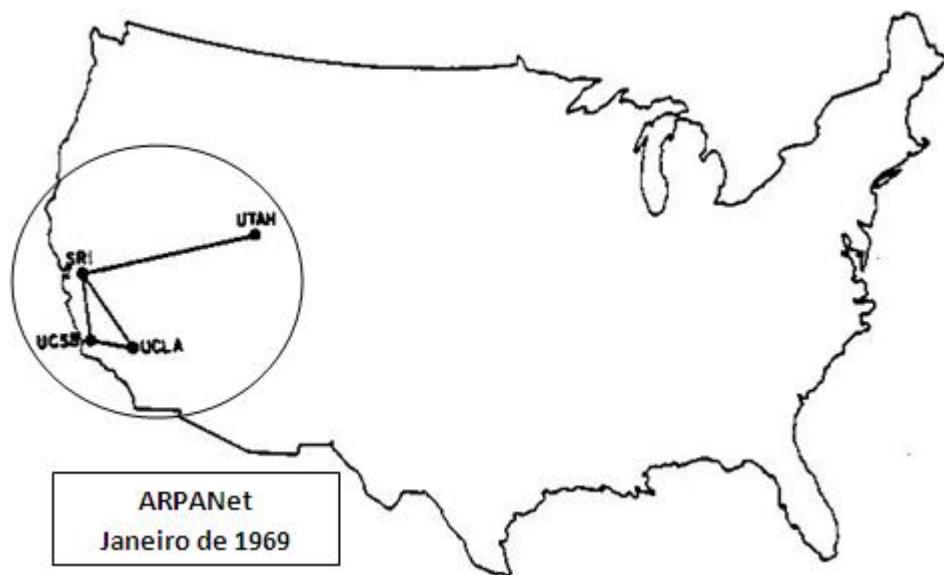
UNIDADE 12

Objetivo: Entender a pilha de protocolos TCP/IP da Internet.

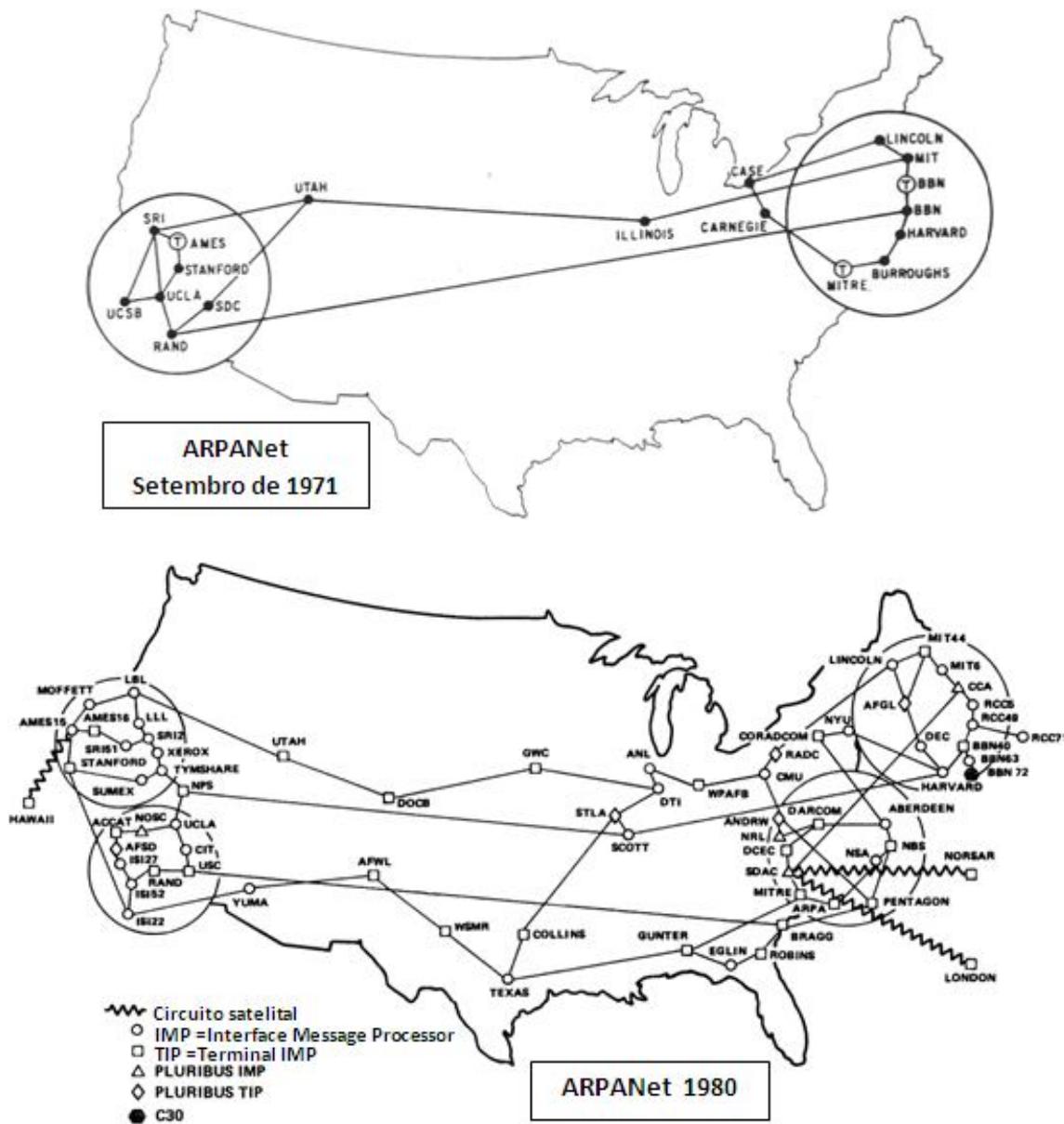
Modelo De Referência Internet (DoD)

A arquitetura TCP/IP surgiu por causa do Departamento de Defesa do governo dos Estados Unidos da América (DoD - Department of Defense), com objetivo principal de manter conectados mesmo que, apenas em parte, órgãos do governo e universidades.

A ARPANet (Advanced Research Projects Agency Network) foi a primeira rede operacional de computadores baseada na técnica de comutação de pacotes, e pode ser considerada a rede precursora da Internet atual. Nasceu com o objetivo de conectar as bases militares e os departamentos de pesquisa do governo americano.



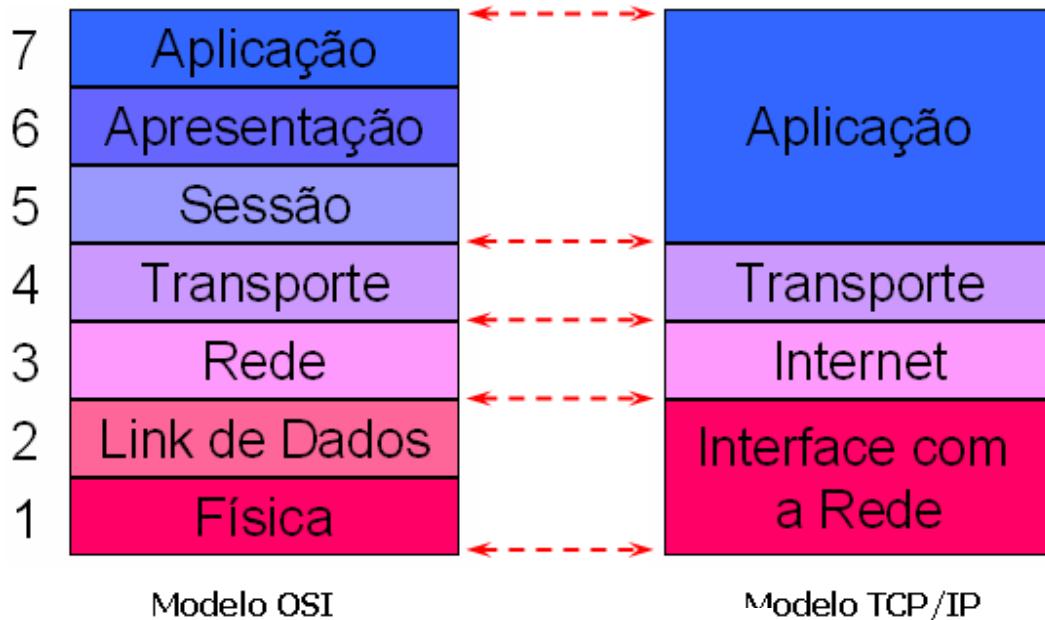
A ARPANet surgiu como uma rede que permaneceria intacta caso um dos servidores perdesse a conexão, e para isso, ela necessitava de protocolos que assegurassem tais funcionalidades trazendo confiabilidade, flexibilidade e que fosse fácil de implementar. Foi desenvolvida então, na Universidade de Berkeley na Califórnia, a arquitetura TCP/IP.



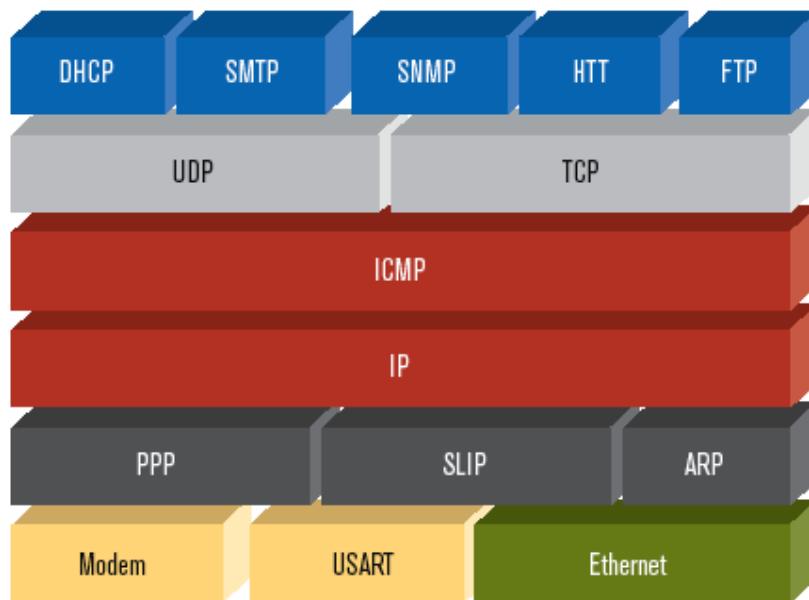
O modelo TCP/IP, quando comparado com o modelo OSI, possui duas camadas que se formam a partir da fusão de algumas camadas deste último, elas são:

1. A camada de Aplicação do TCP/IP = às camadas de Aplicação + Apresentação + Sessão do modelo de referência OSI.
2. A camada Física do TCP/IP = Data Link (Enlace de Dados) + Física do modelo OSI.

Veja na ilustração abaixo esta comparação:



A figura abaixo ilustra o modelo TCP/IP com suas camadas, e alguns dos seus vários protocolos junto com a sua ligação física.



A seguir, temos uma breve, porém completa explicação de cada uma dessas camadas do modelo TCP/IP.

O Nível De Aplicação

É formada pelos protocolos utilizados pelas diversas aplicações do modelo TCP/IP. Esta camada não possui um padrão comum. O padrão é estabelecido por cada aplicação. Isto é, o FTP possui seu próprio protocolo, assim como o TELNET, SMTP, POP3, DNS, PING, BOOTP, TFTP, HTTP, Traceroute, SNMP, etc.

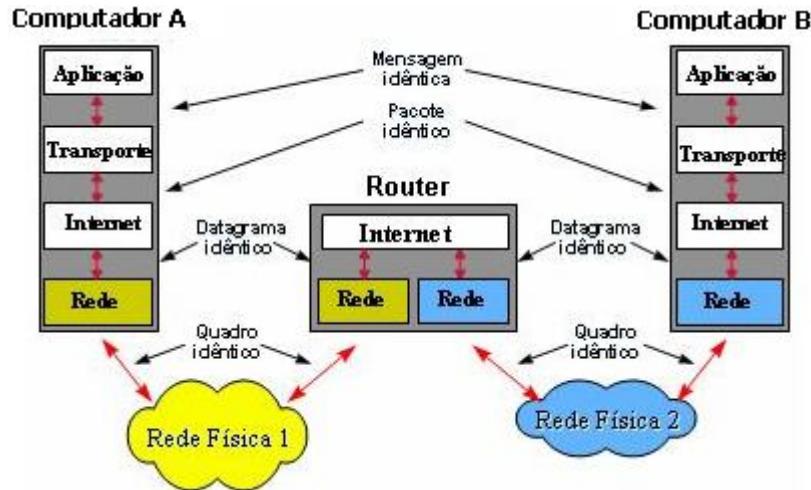
O Nível De Transporte

Camada fim-a-fim, isto é, uma entidade desta camada só se comunica com a sua entidade-par no computador destinatário. É nesta camada que se faz o controle da conversação entre as aplicações intercomunicadas da rede. Dois protocolos aqui são usados: o TCP e o UDP. O TCP é orientado à conexão e o UDP não. Por tal motivo, é usual visualizar o protocolo TCP como sendo mais confiável do que o UDP devido a que precisa de confirmação, por parte do receptor, antes de fazer o envio dos pacotes de dados. O acesso das aplicações à camada de transporte é feito através de portas que recebem um número inteiro para cada tipo de aplicação.

O Nível De Rede (ou Internet Protocol IP)

Essa camada é a primeira normalizada do modelo. Também conhecida como camada Internet, é responsável pelo endereçamento, roteamento e controle de envio e recepção. Ela não é orientada à conexão, se comunica através de datagramas. Esta camada realiza a comunicação entre máquinas vizinhas através do protocolo IP. Para identificar cada máquina e a própria rede onde estas estão situadas, é definido um identificador, chamado de endereço IP, que é independente de outras formas de endereçamento que possam existir

nos níveis inferiores. No caso de existir endereçamento nos níveis inferiores é realizado um mapeamento para possibilitar a conversão de um endereço IP num endereço deste nível.



Os protocolos existentes nesta camada de Rede são:

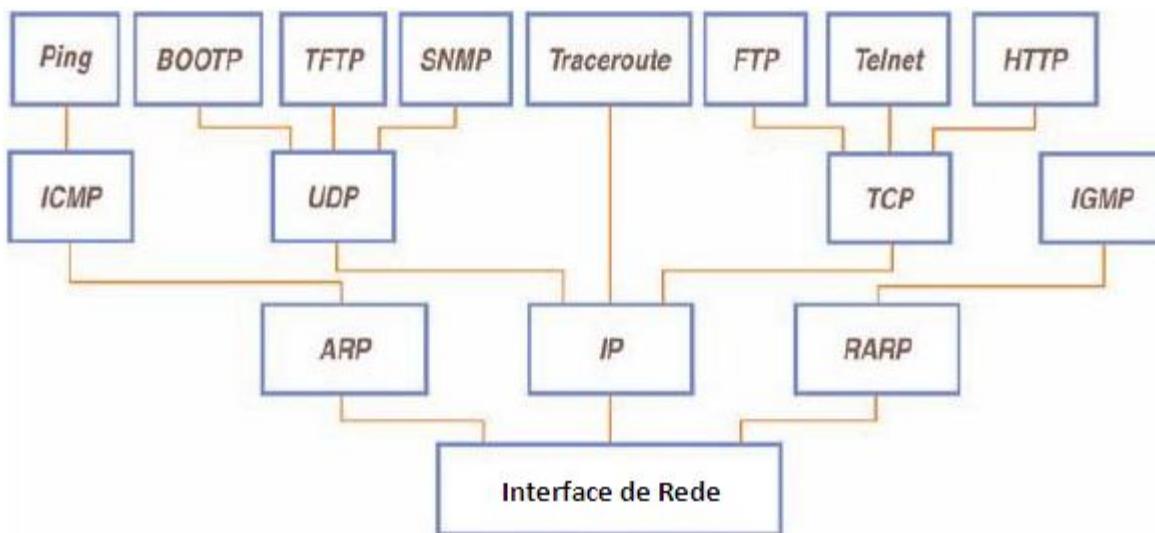
- **Protocolo de transporte de dados:** IP - Internet Protocol
- **Protocolo de controle e erro:** ICMP - Internet Control Message Protocol
- **Protocolo de controle de grupo de endereços:** IGMP - Internet Group Management Protocol.
- **Protocolos de controle de informações de roteamento:** RIP (Routing Information Protocol), OSPF (Open Shortest Path First) e BGP (Border Gateway Protocol) e IGP (Interior Gateway Protocol).

O protocolo IP realiza a função mais importante desta camada que é a própria comunicação Internet (entre redes). Para isto ele realiza a função de roteamento que consiste no

transporte de mensagens entre as diversas redes e na decisão de qual rota uma mensagem deve seguir através da estrutura de rede para chegar ao destino.

O Nível De Interface Com A Rede

Camada de abstração de hardware tem como principal função à interface do modelo TCP/IP com os diversos tipos de redes (X.25, ATM, FDDI, Ethernet, Token Ring, Frame Relay, PPP e SLIP). Por causa da grande variedade de tecnologias de rede, ela não é normalizada pelo modelo, o que provê a possibilidade de interconexão e interoperabilidade de redes heterogêneas. Cada serviço corresponde a um protocolo específico. No caso de e-mails, este serviço é atendido pelo protocolo SMTP, que, ao ser feita uma solicitação de e-mail (envio ou recebimento) ao TCP/IP, este é atendido pelo SMTP. No caso do WWW, usado para visualização de páginas, o protocolo usado é o HTTP. Existem ainda inúmeros outros.



Portanto, podemos concluir que o TCP/IP representa um conjunto de protocolos de rede projetado e desenvolvido entre as décadas de 60 e 70 (inicialmente) como um projeto do Departamento de Defesa dos EUA, e com o objetivo de interconectar redes de computadores

de universidades e sedes militares do governo americano. Nas últimas décadas foi bastante aprimorado e tornou-se um padrão “de facto”, ganhou muita popularidade com o crescimento da rede mundial de computadores, basicamente o TCP/IP é o motor da Internet.

UNIDADE 13

Objetivo: Compreender para que servem os protocolos de Aplicação.

Protocolos Do Nível De Aplicação

Telnet – Network Virtual Terminal Protocol

O Telnet é um protocolo cliente-servidor de comunicações usado para permitir a comunicação entre computadores ligados numa rede (exemplos: rede local / LAN, Internet), baseado em TCP. Basicamente este protocolo permite fazer a emulação de terminal, isto é, ele possibilita ao usuário emular o terminal de uma máquina remota; através do cliente pode acessar os recursos do servidor de Telnet.

Antes de existirem os famosos chats em IRC (Internet Relay Chat) o Telnet já permitia este tipo de serviços. Os terminais que são emulados são do tipo texto e se pode acessar uma espécie de console do servidor através desse protocolo e de seu cliente. Um bom uso é para se verificar o e-mail.

Porém para acesso a console de servidores com segurança é melhor fazer uso de outro tipo de recurso como o SSh (Secure Shell) cujo conteúdo é encriptado antes de ser enviado. A senha que é enviada ao servidor pode ser capturada em muitos casos com o modo de rede promiscuo e com o uso de um analisador de rede.

O uso do protocolo Telnet tem sido desaconselhado, à medida que os administradores de sistemas vão tendo maiores preocupações de segurança, uma vez que todas as comunicações entre o cliente e o servidor podem ser vistas, já que são em texto plano (ASCII), incluindo a senha.

FTP – File Transfer Protocol

Este protocolo possibilita a transferência de arquivos entre duas máquinas. Como o Telnet, além de um protocolo ele é também um programa que é empregado pelos usuários para efetuar as transferências de arquivo manualmente se necessário.

Pode-se utilizá-lo em conjunto com o Telnet para se obter a autenticação e a conexão de modo transparente ao servidor, após a autenticação eles pode providenciar a transferência de arquivos. É comum o uso do usuário “anonymous” com a senha idêntica ou então um endereço de e-mail como senha.

Porém os direitos são limitados nesse caso; pode-se consultar o conteúdo de diretórios, assim como efetuar a exibição de conteúdos e cópia de arquivos. Porém não é possível executar programas remotamente.

TFTP – Trivial File Transfer Protocol

Esse protocolo é uma versão reduzida / simplificada do protocolo FTP, é recomendável evitar o seu uso. Somente seu uso é justificado quando é feita a primeira carga do sistema operacional de Switches e roteadores. Após efetuar essa operação é recomendável desabilitar esse tipo de serviço, pois certos vírus poderiam se aproveitar desse tipo de recurso para se propagar e isso pode ter resultados catastróficos. Usar o TFTP tem várias desvantagens sobre o FTP, por exemplo: não se pode utilizar autenticação, não é possível fazer a listagem de diretórios ou arquivos, não é seguro, somente é utilizado para enviar e receber arquivos, mas sem garantia alguma.

SMTP – Simple Mail Transfer Protocol

Este protocolo possibilita a transferência de mensagens de e-mails. Ele utiliza um método de Spool (fila) para efetuar o envio de mensagens. Ele fica consultando o meio de

armazenamento que pode ser um disco rígido e efetuando através de software a entrega das mensagens de correio eletrônico aos destinatários.

LPD – Line Printer Daemon

Este protocolo é utilizado para compartilhamento de impressoras. Ele trabalha em conjunto com o programa LPR (Line Printer), isso possibilita se enviar um trabalho para o Spool (fila) e efetuar a impressão através de uma impressora que esteja conectada por meio de TCP/IP.

XWin – X Window

Este protocolo é utilizado para efetuar o compartilhamento da parte gráfica (GUI – Graphical User Interface) de um servidor para o cliente. Através de um emulador de X-Win é possível, por exemplo, acessar a parte gráfica do servidor Linux em uma estação Windows NT.

SNMP – Simple Network Management Protocol

O SNMP é utilizado para efetuar o controle de informações de rede, ele faz a coleta e a manipulação de dados de dispositivos de rede. Geralmente isso é feito periodicamente, fornecendo o status dos dispositivos. Ele pode ser um ótimo meio de se obter informações sobre a rede para gerenciar de forma saudável ou pode ser um transtorno caso alguém mal intencionado utilize os dados para obter informações sobre dispositivos. Ele tem um funcionamento de guarda que quando ocorre um evento, dispara uma Trap (alerta) para a estação de gerenciamento de rede.

DNS – Domain Name Service

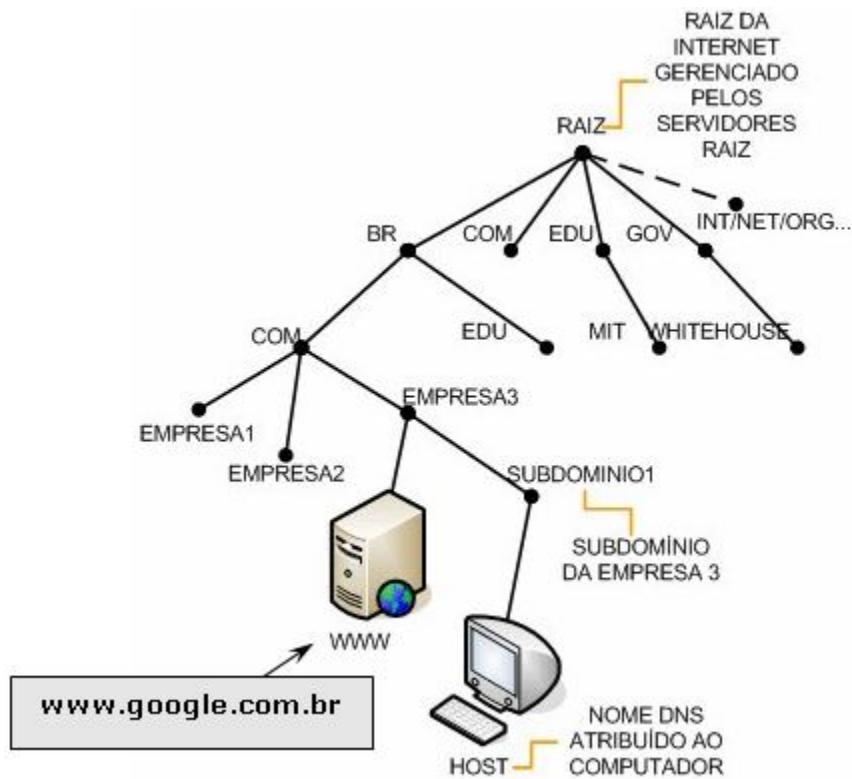
O DNS define um esquema de gerenciamento de nomes, hierárquico e distribuído. Ele define a sintaxe dos nomes usados na Internet, regras para delegação de autoridade na definição de nomes, um BD distribuído que associa nomes a atributos (entre eles o endereço IP) e um algoritmo distribuído que é utilizado para mapear nomes em endereços.

Nas RFCs 882, 883 e 973 esta definido o DNS. Como é mais fácil para os usuários digitar endereços em vez de números IP de 32 bits (que são utilizados no sentido de abrir uma conexão ou enviar um datagrama IP), o BD do DNS permite que as aplicações traduzam esse endereço para que a aplicação consiga localizar a maquina correta com a qual se comunicar. Existem servidores que mantém essa lista de nomes e endereços em um BD e que estão conectadas à Internet.

Esse tipo de informação é armazenado em um sistema de domínios (Domain System). É utilizada uma serie de servidores interconectados, ao invés de um único servidor centralizado (para garantir sua disponibilidade). Essa pratica também facilita a inserção de entradas no BD, pois se fosse centralizada em uma única instituição não haveria agilidade bastante para se efetuar todas as atualizações a nível global.

Os servidores em conjunto formam uma espécie de arvore que contem todos os domínios da estrutura institucional. Os nomes têm uma estrutura e nomeação similar conforme sua finalidade e localidade.

Um exemplo típico pode ser o motor de busca: www.google.com.br. Para poder encontrar o número IP associado a este nome pode-se passar por uma serie de servidores (até 4 servidores de nomes podem ser contatados). A primeira coisa que será consultada através do servidor central é onde se localiza o servidor br. Esse servidor é responsável pelo gerenciamento dos nomes das instituições/empresas brasileiras conectadas à Internet.



O servidor raiz traz como resultado da pesquisa o endereço IP de vários servidores de nome para o nível br (pode existir mais que um servidor de nomes em cada nível, para garantir a disponibilidade quando um deles para de funcionar). Ao se chegar a um servidor do nível br é feita a consulta que devolve o endereço IP do servidor com. Com esse endereço de servidor com é possível solicitar que ele informe o endereço da máquina Google. O resultado final da busca é o endereço Internet correspondente ao nome google.com.br. Cada um dos níveis percorridos é referenciado como sendo um domínio.

O nome completo google.com.br é um nome de domínio FQDN (Fully Qualified Domain Name). Na maioria das vezes não é necessário ter acesso a todos os domínios de um nome para encontrar o endereço correspondente, alguns dos servidores de nome possuem informações sobre mais de um nível de domínio agiliza e elimina uma ou mais consultas. Além disso as últimas consultas são armazenadas em cache e assim resolver a consulta em nível local. Isso agiliza o mapeamento de nomes em endereços, uma vez que elimina a necessidade de implementar em todas as aplicações que fazem uso do DNS, o algoritmo de

busca na arvore de domínios descrito anteriormente. O DNS não se limita somente a manter e gerenciar endereços Internet.

Cada nome de domínio é um no em um BD, que pode conter registros definindo varias propriedades. São admitidos apelidos para as maquinas (um alias ou nome alternativo) para o no. Pode-se utilizar o DNS para guardar dados sobre usuários, listas de distribuição ou outros objetos.

O DNS é vital para o sistema de correio eletrônico. No DNS estão definidos registros que identificam o servidor de e-mail que manipula as correspondências relativas a um dado nome, identificado onde o usuário recebe suas correspondências. O DNS também pode definir listas para distribuição de correspondências.

DHCP – Dynamic Host Configuration Protocol

O DHCP fornece aos protocolos TCP/IP, as informações iniciais de configuração da máquina tais como endereço IP, máscara de sub-rede, roteadores default, rotas, servidores de Boot, servidores de nome e diversas outras informações. Este protocolo pode ser utilizado pra efetuar a administração centralizada de máquinas TCP/IP. O BOOTP (Bootstrap Protocol) é o protocolo mais antigo e o DHCP (Dynamic Host Control Protocol) está aos poucos o substituindo. O DHCP é mais complexo e mais versátil e vem sendo usado para simplificar a administração de endereços e outros parâmetros de configuração de grandes instalações de máquinas TCP/IP. O DHCP consegue efetuar a configuração automática de estações, sem necessidade de criação de uma tabela de configuração para cada máquina (que é necessária no caso do BOOTP). O DHCP usa três métodos de fornecimento distinto para os endereços:

Empréstimo (leasing) de endereço aleatório por tempo limitado: Se escolhe um endereço IP de um range e se fornece ao cliente por um tempo pré-determinado.

Empréstimo de endereço aleatório por tempo infinito: O servidor atribui um endereço do range ao cliente na primeira vez que este cliente contatar o servidor. Nas demais vezes se

consultam o MAC do cliente e se fornece o mesmo endereço a este cliente, mesmo que as duas máquinas sejam desligadas e ligadas. Este método simplifica a atribuição de endereços para uma quantidade grande de máquinas.

Empréstimo de endereço fixo: Nesse tipo de fornecimento existe a associação explícita entre o endereço IP e o endereço MAC da máquina origem, estipulado em uma tabela de configuração.

O servidor DHCP poderá responder tanto às solicitações BOOTP, quanto DHCP, pois ambas possuem o mesmo formato. A mensagem DHCP possui o formato abaixo:

0	7	15	23	31				
Octeto 1	Octeto 2	Octeto 3	Octeto 4					
OP	HTYPE	HLEN	HOPS					
TRANSACTION ID								
SECONDS	FLAGS							
CLIENT IP ADDRESS								
YOUR IP ADDRESS								
SERVER IP ADDRESS								
ROUTER IP ADDRESS								
CLIENT HARDWARE ADDRESS (16 bytes)								
SERVER HOST NAME (64 bytes)								
BOOT FILE NAME (128 bytes)								
OPTIONS (Variável)								

CAMPO	INFORMAÇÕES
OP	Numa mensagem DHCP, uma solicitação e uma resposta possuem os mesmos campos. O que as diferenciam é o conteúdo deste campo. A informação um indica uma solicitação, a informação dois indica uma resposta
HTYPE	Informa o padrão de rede utilizado pelo adaptador de rede
HLEN	Informa o tamanho do endereço MAC do adaptador de rede
HOPS	Quantidade de roteadores pelos quais a mensagem deverá passar
ID DE TRANSAÇÕES	Número de identificação da mensagem
SEGUNDOS	Quantidade de tempo em segundos desde que o cliente fez a inicialização
FLAGS	Utilizado para "setar" opções especiais de resposta às solicitações
CLIENT IP ADDRESS	Em uma solicitação o cliente informa o seu endereço IP (possível quando o cliente conhece o seu endereço)

YOUR IP ADDRESS	Utilizado pelo servidor para enviar informação do endereço IP disponível para o cliente que solicitou.
SERVER IP ADDRESS	Preenchido pelo cliente quando ele quer obter uma informação de um servidor específico.
ROUTER IP ADDRESS	Preenchido pelo servidor para informar ao cliente o endereço IP do roteador da rede local
CLIENT HARDWARE ADDRESS	Informação do endereço MAC do cliente
SERVER HOST NAME	Quando esses campos não são utilizados para enviar as informações pertinentes a cada um (nome do servidor e informação do S.O. que será inicializado no cliente) o DHCP utiliza-o enviando informações adicionais transformando-os em campo de OPÇÕES, otimizando assim a utilização da mensagem.
BOOT FILE NAME	Nome do arquivo que contém a imagem de memória da(s) estação (ões) correspondente(s)
OPTIONS	Esse campo é utilizado para informar que tipo de resposta ou solicitação DHCP (DHCPDISCOVER, DHCPOFFER etc.) está sendo enviada para o cliente ou para o servidor.

A mensagem DHCP possui 8 tipos de comandos, que estão em uma opção especial de OPTIONS; a de código 53, associado a um dos comandos abaixo:

- **DHCP DISCOVER** – Uma solicitação de resposta enviada a um servidor pelo cliente.

- **DHCP OFFER** – Uma oferta de IP do servidor para o cliente. O cliente pode receber várias ofertas de diferentes servidores DHCP.
- **DHCP REQUEST** – É uma requisição de um endereço específico do servidor. Um broadcast é gerado apesar de ser endereçado a um único servidor para que os demais saibam da escolha.
- **DHCP DECLINE** – Comunica que a oferta contém parâmetros incorretos (Erro).
- **DHCP ACK** – Mensagem de OK do servidor sobre a atribuição do endereço para a requisição do cliente.
- **DHCP NAK** - Servidor rejeita o fornecimento do endereço previamente oferecido, isso ocorre por erro ou por demora do cliente a requisitar o endereço solicitado.
- **DHCP RELEASE** - Cliente libera o endereço IP utilizado. Difícil de se ver na prática, pois geralmente o cliente é desligado sem liberar o endereço. Esse endereço volta ao conjunto de endereços disponíveis no servidor devido ao estouro do tempo de leasing.
- **DHCP INFORM** - Cliente que já possui endereço IP pode requisitar outras informações de configuração respectivas àquele endereço.

NFS – Network File System

O NFS possibilita o compartilhamento de arquivos. Dois sistemas de arquivos diferentes podem conversar graças a ajuda deste protocolo. De forma transparente o cliente NFS instalado no sistema operacional entra em ação preservando a formatação do sistema operacional e possibilitando o acesso a sistemas de arquivos distintos. Um bom exemplo é uma máquina NT acessando serviços em uma máquina UNIX.

O NFS provê o acesso remoto, de forma transparente, a arquivos compartilhados em redes de computadores. O NFS foi projetado para ser portável entre diferentes plataformas de

hardware, sistemas operacionais, arquiteturas de redes e protocolos de nível de transporte. Esta portabilidade é possível graças ao uso dos protocolos RPC e XDR.

O protocolo NFS tem a intenção de ser o mais "Stateless" quando possível, liberando o servidor de manter qualquer informação de estado de protocolo dos clientes. Características importantes:

- Provê acesso a arquivos compartilhados de maneira transparente;
- Utilizado pelo TCP/IP para interconexão de computadores;
- Efetua a interface entre o S.O. e os arquivos remotos;
- Baseado na arquitetura Cliente-Servidor.

RPC – Remote Procedure Call

O RPC define um protocolo para execução remota de procedimentos em computadores ligados em rede. O protocolo RPC pode ser implementado sobre diferentes protocolos de transporte. Não cabe ao RPC especificar como a mensagem é enviada de um processo para outro, mas somente especificá-la (com XDR) e interpretá-la. A sua implementação depende, portanto, de sobre qual protocolo de transporte vai operar, vejamos

- **Sobre TCP:** Neste caso não é necessário preocupar-se com time-outs, retransmissões, duplicatas, já quem o próprio TCP fornece todos esses mecanismos (janelas de congestionamento, reconhecimentos positivos ACK+ para cada envio de dados, etc.,) para um correto controle de fluxo.
- **Sobre UDP:** Se o RPC está rodando sobre o protocolo UDP, então é necessário preocupar-se com time-outs, retransmissões, duplicatas, isto porque o protocolo de transporte UDP não fornece nenhum tipo de mecanismo de controle para o fluxo da informação entre as partes.

Uma mensagem RPC tem três campos inteiros:

- Remote Program Number;
- Remote Program Version Number;
- Remote Procedure Number.

Além, é claro, dos parâmetros específicos à chamada. A operação do RPC pode ser descrita nos seguintes passos:

- Coleta os dados dos parâmetros;
- Forma a mensagem;
- Envia a mensagem;
- Espera a resposta;
- Devolve a resposta através dos parâmetros.

Pode ser mantida a analogia entre chamadas remotas e as chamadas locais com as seguintes ressalvas:

- **Manipulação de Erros:** Falhas no servidor remoto ou na rede devem ser explicitamente manipuladas quando usamos RPC;
- **Variáveis Globais:** Como o servidor não tem acesso ao lado cliente (a seu espaço de endereçamento), não podemos usar variáveis globais, somente parâmetros.
- **Performance:** Chamadas remotas operam normalmente a uma ou mais ordens de magnitude mais lentamente.

- **Autenticação:** Pelo fato das chamadas remotas trafegarem sobre redes inseguras, a autenticação das mensagens pode (deve) ser necessária.

XDR – External Data Representation

O XDR é um padrão IETF desde 1995. Este protocolo é utilizado para codificação e decodificação de dados para o transporte entre diferentes arquiteturas de computadores (SUN, VAX, PC, CRAY, HP, SGI, IBM). Cria uma representação independente de máquina, sendo a conversão automática e transparente, sendo realizada em tempo de compilação.

A conversão da representação local para XDR é chamada de codificação e a conversão de XDR para a representação local é chamada de decodificação. O XDR é implementado com uma livraria de funções de software que é portável entre diferentes sistemas operacionais e que independe também do tipo de protocolo de Transporte utilizado.

A seguinte tabela apresenta um exemplo entre o modelo OSI e os serviços RPC e não RPC

Modelo OSI	Serviços RPC	Serviços não RPC
7. Aplicação	NFS	rlogin, rcp, tftp, etc
6. Apresentação	XDR	
5. Sessão	RPC	
4. Transporte	TCP, UDP	TCP, UDP
3. Rede	IP	IP
2. Enlace de Dados	Ethernet, Token-Ring, FDDI	Ethernet, Token-Ring, FDDI
1. Física	Ethernet, Token-Ring, FDDI	Ethernet, Token-Ring, FDDI

UNIDADE 14

Objetivo: Saber o funcionamento e quando fazer uso deste importante protocolo.

Protocolos Do Nível De Transporte: TCP

A Internet tem como base três serviços básicos que são fornecidos pela pilha de protocolos TCP/IP. Esses serviços estão agrupados nas seguintes camadas:

- Serviços de Aplicação (como os que foram vistos na sessão anterior)
- Serviços de Transporte (como os dos protocolos TCP e UDP)
- Serviços de entrega de pacotes sem conexão (ARP, ICMP e IP)

As aplicações Internet fazem sucesso, pois a arquitetura robusta contribui para sua funcionalidade. O TCP/IP também fornece bastante flexibilidade e se adapta as necessidades do usuário. O TCP tem como finalidade básica fornecer o transporte confiável, através de um circuito lógico robusto de conexão entre um par de processos. Este protocolo se preocupa exclusivamente com a parte de transporte.

Aplicações que necessitam de transporte confiável se utilizam do protocolo de transporte **TCP**, porque este verifica se os dados são enviados de forma correta, na seqüência apropriada, pela rede.

O TCP é confiável, orientado à conexão e de fluxo contínuo de Bytes (Byte Stream); resolve problemas de perdas, atrasos, duplicação e problemas semelhantes nos pacotes transmitidos.

Veja a RFC 793 para maior conhecimento sobre a especificação do protocolo TCP:
<http://www.faqs.org/rfcs/rfc793.html>.

Características Fundamentais Do TCP

- **Orientado à conexão:** A aplicação envia um pedido de conexão para o destino e usa a conexão para transferir dados.
- **Ponto a ponto:** uma conexão TCP é estabelecida entre dois pontos.
- **Confiabilidade:** O TCP garante a entrega dos dados sem perdas, duplicação ou outros erros.
- **Full-duplex:** Pode haver troca de dados em simultâneo, em ambas as direções, pelos dois pontos da conexão.
- **Interface Stream:** Fluxo contínuo de dados; o TCP não garante que os dados sejam recebidos nos mesmos blocos em que foram transmitidos.
- **3-way Handshake:** Mecanismo fiável de conexão em 3 vias, garantindo uma inicialização fiável e sincronizada entre os pontos.
- **Finalização da conexão controlada:** O TCP garante a entrega de todos os dados depois de terminada a ligação.

Utilização do IP Com o TCP

O TCP utiliza o protocolo IP para a entrega dos datagramas à rede, e os pontos de acesso à aplicação são identificados por portas, tal como acontece com o UDP, o que permite múltiplas ligações em cada computador.

As portas podem ser associadas com uma aplicação ou um processo. O IP trata o pacote TCP como dados e não interpreta qualquer conteúdo da mensagem do TCP, sendo que os dados TCP viajam pela rede em datagramas IP. Os routers que interligam as redes apenas verificam o cabeçalho IP, quando fazem o envio dos datagramas. O TCP no destino interpreta a mensagem do protocolo TCP.

Entrega Confiável

O TCP usa várias técnicas para proporcionar uma entrega confiável dos pacotes de dados, que é a grande vantagem que tem em relação ao UDP, e motivo do seu uso extensivo nas redes de computadores.

O TCP permite a recuperação de pacotes perdidos, duplicados ou atrasados, a recuperação de dados corrompidos, erros nas velocidades de transmissão, congestão e reinicio do sistema (reboot).

Segmentos e Números de Seqüência TCP

A aplicação faz a entrega ao TCP de blocos de dados com um tamanho arbitrário num fluxo (ou stream) de dados. O TCP divide estes dados em segmentos, sendo cada um dos quais ajustado a um datagrama IP. O fluxo de dados original é numerado em bytes.

Cada Byte tem seu próprio número de seqüência de tal forma que poderia ser possível (se for necessário) reconhecer cada um deles. Porém na prática os Bytes são reconhecidos em lotes, o tamanho do lote é determinado através do tamanho do campo Window (janela). O número de seqüência é um número binário de 32 bits, embora seja de tamanho considerável só um intervalo finito de números é utilizado, este intervalo vai de 0 a $2^{32} - 1$, e zera cada vez que se atinge o valor máximo.

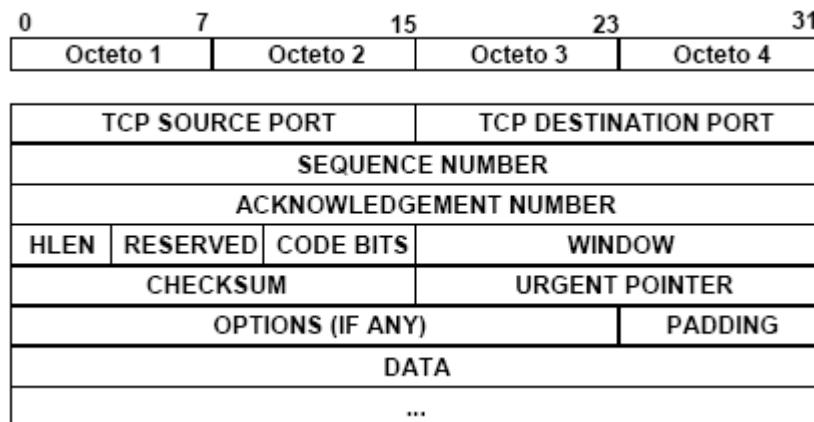
Estes números de seqüência são muito úteis para evitar que ocorra a corrupção dos dados se um pacote chegar ao destino antes de outro, ou para detectar algum pacote que porventura se perdeu no caminho entre a origem e o destino. Os números de seqüência são gerados aleatoriamente dentro das regras estipuladas na RFC 793.

Controle De Fluxo

O TCP usa o método da janela deslizante para controlar o fluxo. O receptor, à medida que recebe os dados, envia ACK, que também especificam o tamanho do buffer (janela) que resta. O transmissor pode transmitir segmentos com um número de bytes que deverá estar compreendido entre o último byte confirmado e o tamanho da janela permitido.

Pacote TCP

A estrutura do cabeçalho de um segmento TCP é ilustrada na seguinte figura.



Os campos do cabeçalho TCP estão definidos da seguinte forma:

TCP SOURCE PORT (bits 0-15): Porta origem da mensagem.

TCP DESTINATION PORT (bits 16-31): Porta destino da mensagem.

SEQUENCE NUMBER (bits 32-63): Este campo indica o número de seqüência dos dados sendo transmitidos. Se o bit SYN=1 então este número de seqüência SQN (Sequence Number) é o inicial ISN (Initial Sequence Number), ou seja, se SYN=1 então SQN=ISN que é atribuído durante o estabelecimento da conexão. Este número é utilizado nas subsequentes transmissões para determinar o próximo número a ser utilizado na seqüência (este número

nunca deve ser 0 ou 1, a seqüência começa com um valor aleatório). Quando o bit ACK=1 então o ISN passa a ser o SQN comum. Vale a pena mencionar que ambos os números de seqüência dos fluxos de dados (de A para B e de B para A) são completamente diferentes, já que os dados transmitidos por um e outro lado são diferentes.

ACKNOWLEDGE NUMBER (bits 64-95): Esse campo possui um número que significa o reconhecimento dos dados recebidos até então no sentido inverso. São trocados ACK de um sentido a outro com se levando em consideração o número de SEQUENCE NUMBER inicial praticado pela outra máquina. O valor de ACK informa sempre o próximo byte ainda não recebido do conjunto contíguo de bytes recebidos do transmissor.

HLEN ou DATA OFFSET (bits 96-99): Esse campo informa o número de palavras de 32 bits contidas no cabeçalho do TCP.

RESERVED (bits 100-103): Campo reservado para o uso futuro.

CODE BITS (bits 104-111): São formados por oito bits: CWR, ECE, URG, ACK, PSH, RST, SYN e FIN, cuja utilização é mostrada abaixo:

CWR – bit de controle de congestionamento utilizado pelo ECN (Explicit Congestion Notification – veja a RFC 3168). O bit CWR (Congestion Window Reduced) é utilizado pelo transmissor para informar ao receptor que a janela de congestionamento foi reduzida. Quando a janela de congestionamento é reduzida, implica que menos dados são enviados por unidade de tempo, isto com o único propósito de satisfazer a carga (volume total de tráfego) da rede, ou seja, na presença de congestionamento na rede o bit CWR é ativado.

ECE – bit utilizado também pelo ECN (veja a RFC 3268). O bit ECE (ECN Echo) é utilizado pela pilha de protocolos TCP/IP do receptor para dizer ao transmissor que ele recebeu um pacote com indicação de congestionamento CE. Os bits CWR e ECE inicialmente faziam parte do campo RESERVED e devido a isto alguns computadores, não estariam habilitados para entender o significado destes bits, sendo assim, eles simplesmente ignorarão ou rejeitarão os pacotes que tenham CWR = 1 e ECE = 1. Atualmente ainda existem

computadores que não conseguem processar a informação trazida por estes dois bits de controle de congestionamento.

URG – bit de Urgência: significa que o segmento sendo carregado contém dados urgentes que devem ser lidos com prioridade pela aplicação. A aplicação origem é responsável por acionar este bit e fornecer o valor do URGENT POINTER que indica o fim dos dados urgentes.

ACK – bit de Reconhecimento: indica que o valor do campo de reconhecimento está carregando um reconhecimento válido.

PSH – bit de PUSH: Este mecanismo que pode ser acionado pela aplicação informa ao TCP origem e destino que a aplicação solicita a transmissão rápida dos dados enviados, mesmo que ela contenha um número baixo de bytes, não preenchendo o tamanho mínimo do buffer de transmissão.

RST – bit de RESET: Informa o destino que a conexão foi abortada neste sentido pela origem.

SYN – bit de Sincronismo: é o bit que informa que este é um dos dois primeiros segmentos de estabelecimento da conexão.

FIN – bit de Terminação: indica que este pacote é um dos pacotes de finalização da conexão.

WINDOW (bits 112-127): Este campo informa o tamanho disponível em bytes na janela de recepção da origem deste pacote. Isso ajuda a efetuar o controle de fluxo adequado, evitando o estouro de buffer do receptor.

CHECKSUM (bits 128-143): O cálculo do Checksum de todo o cabeçalho TCP é alocado neste campo. Se o cabeçalho não finaliza em um comprimento de 16 bits, os bits que faltam (para dar 16 bits) são zerados. Durante o cálculo do checksum, este campo é zerado. Neste campo também é considerado o pseudo-cabeçalho de 96 bits que contém os campos

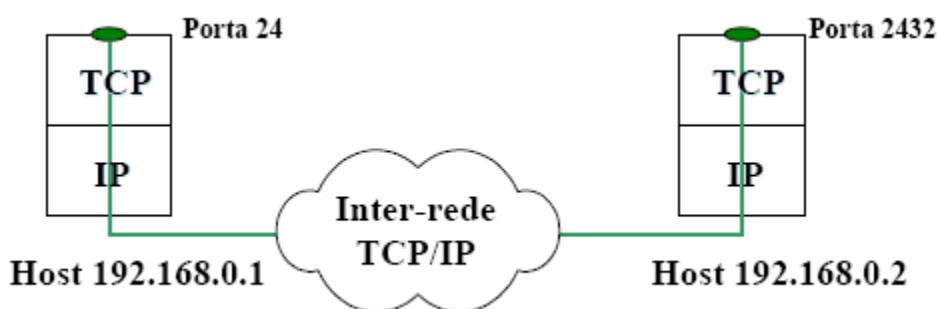
DESTINATION, SOURCE ADDRESS, PROTOCOL, e TCP LENGTH. Isto dá uma segurança extra. Diferente do protocolo UDP, no TCP o campo CHECKSUM nunca é opcional.

URGENT POINTER (bits 144-159): Este é um ponteiro que aponta para o fim dos dados os quais são considerados urgentes. Se a conexão tem dados importantes a serem processados pelo receptor, o transmissor pode ativar o bit URG e dizer que o campo URGENT POINTER aponte onde terminam os dados urgentes. Este campo indica um número positivo que corresponde ao valor de Offset do número de seqüência para este segmento em particular. Se o bit URG é 1 então este campo aponta para o número de seqüência do último Byte correspondente a uma seqüência de dados urgentes.

OPTIONS (bits 160-):** Este campo é de comprimento variável e informa sobre as varias opções que o TCP pode transmitir. Basicamente, este campo possui 3 subcampos. Um subcampo inicial que diz o comprimento do campo OPTIONS, um Segundo subcampo que diz quais as opções que estão sendo utilizadas, e finalmente temos o subcampo das opções propriamente ditas. Para mais informações sobre as opções TCP veja o seguinte Link: <http://www.iana.org/assignments/tcp-parameters>.

PADDING (bits **): Este campo também é de comprimento variável e é utilizado para assegurar que o cabeçalho TCP termine e o campo de dados inicie com um comprimento de 32 bits, se isto não ocorrer, então bits 0 serão adicionados (padded) neste campo para dar o comprimento requisitado de 32 bits.

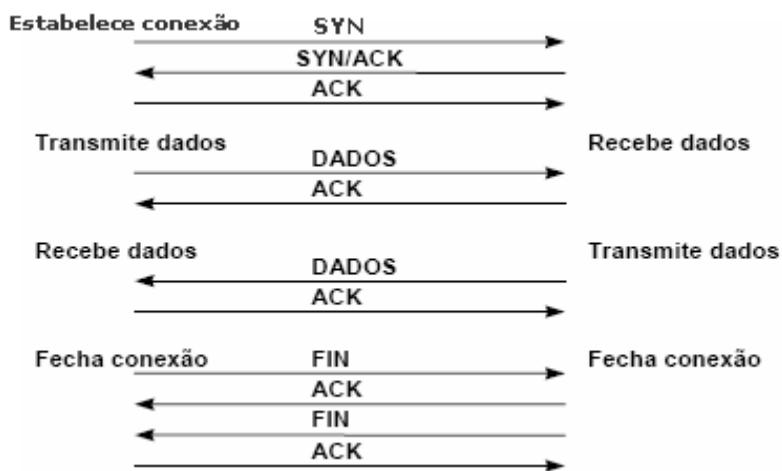
As etapas de uma conexão TCP são ilustradas na figura abaixo:



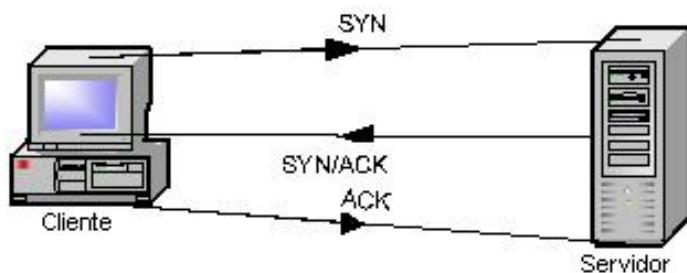
Uma conexão TCP é formada por três fases:

1. Estabelecimento de conexão
2. Troca de dados
3. Finalização da conexão

A figura mostra esses três importantes passos de toda conexão TCP:



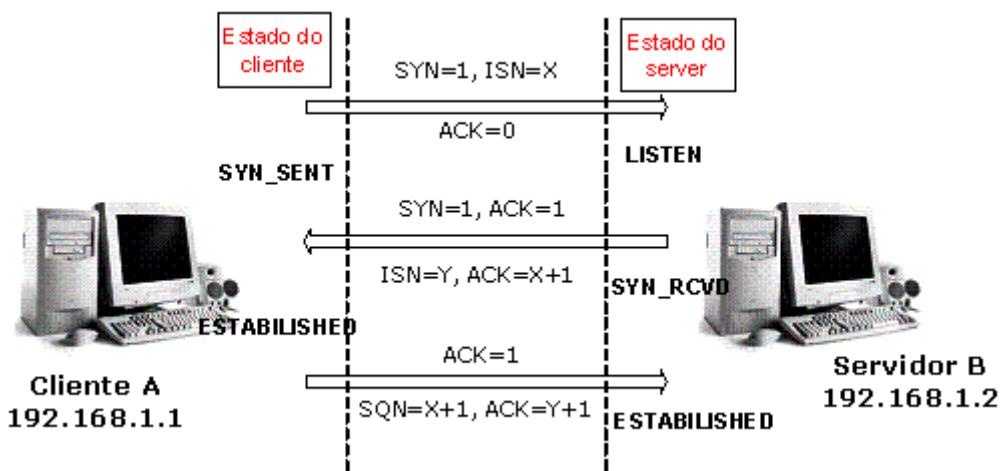
Essas três etapas que antecedem a toda conexão TCP é conhecida na literatura técnica como o mecanismo de 3-way-handshaking.



Estabelecimento De Uma Conexão TCP

O processo de conexão se inicia quando o computador cliente envia para o computador destino um segmento TCP contendo a porta de origem e destino, endereço IP de origem e destino e o bit SYN ativado. O diagrama abaixo explica o processo de abertura de sessão. Nenhum dado é trocado se este processo não for realizado.

A partir de agora os bits do campo CODE BITS serão conhecidos como flags (bandeiras) que é o nome comum que se dá a esses bits.



O primeiro segmento indica que o computador (cliente) A com endereço IP 192.168.1.1 deseja realizar uma abertura de sessão TCP na porta 80 do computador (servidor) B com endereço IP 192.168.1.2. O segmento TCP possui a porta de origem XXXX e o flag de sincronismo SYN habilitado (SYN=1) e ACK=0 (desabilitado), este segmento também envia o seu número de seqüência inicial (de 32 bits) ISN=X.

Obs.: O segmento de inicio de sessão TCP deve levar o flag de sincronismo SYN ativado, isto é, SYN=1.

O segundo segmento retorna de B para A contendo dois flags ativos (SYN e ACK) e apresenta duas situações:

O computador B aceitou o pedido de abertura de sessão na porta 80 enviando um segmento de resposta com o flag ACK habilitado (ACK=1). Isto significa que o pedido de abertura de sessão foi aceito já que o serviço existente no servidor B utiliza a porta 80 e está ativo.

No mesmo segmento é enviado o flag SYN=1 demonstrando que este computador B deseja abrir uma sessão na porta XXXX do computador A. Normalmente o TCP trabalha em modo Full-duplex, ou seja, o computador A abre a sessão no computador B e vice versa. O procedimento de enviar dois flags habilitados em um mesmo segmento é conhecido como pigg-backing.

Além de enviar os flags SYN e ACK ativados, o computador (servidor) B envia também seu próprio número de seqüência inicial ISN=Y completamente diferente do número de seqüência inicial do computador (cliente) A.

O terceiro e último segmento é enviado pelo computador (cliente) A confirmado para o computador (servidor) B a abertura de sessão na porta XXXX, através do envio de um segmento com o flag ACK habilitado (ACK=1) junto com o número de seqüência SQN=X+1 e ACK=Y+1.

Quando o processo de abertura de sessão é estabelecido através da troca de segmentos TCP pelo processo de 3-way-handshaking, os dois computadores se encontram no estado de conexão estabelecida ou “Established State” significando que uma sessão TCP foi formalmente estabelecida e os dois computadores estão em condições de transferir dados entre eles. O processo de abertura de sessão altera também uma série de parâmetros do protocolo TCP como: números de seqüência, números de ACK entre outros.

Troca De Dados Em Uma Conexão TCP

Durante a fase de transferência o TCP está equipado com vários mecanismos que asseguram a confiabilidade e robustez: números de seqüência que garantem a entrega ordenada, código detector de erros (checksum) para detecção de falhas em segmentos específicos, confirmação de recepção e temporizadores que permitem o ajuste e contorno de eventuais atrasos e perdas de segmentos.

Como se pode observar do cabeçalho TCP, existem permanentemente um par de números de seqüência, referidos como número de seqüência e número de confirmação positiva (positive ACKnowledgement) ou +ACK. O emissor determina o seu próprio número de seqüência e o receptor confirma o segmento usando como número ACK o número de seqüência do emissor. Para manter a confiabilidade, o receptor confirma os segmentos indicando que recebeu um determinado número de Bytes contíguos. Uma das melhorias introduzidas no TCP foi a possibilidade do receptor confirmar blocos fora da ordem esperada. Esta característica designa-se por ACK seletivo (selective ACK) ou apenas SACK.

A remontagem ordenada dos segmentos é feita usando os números de seqüência, de 32 bits, que reiniciam a zero quando ultrapassam o valor máximo, $2^{32} - 1$, tomando o valor da diferença. Assim, a escolha do número de seqüência inicial ISN torna-se vital para a robustez deste protocolo.

O campo Checksum permite assegurar a integridade do segmento. Este campo é expresso em complemento para 1 consistindo na soma dos valores (também em complemento para 1) do pacote. A escolha da operação de soma em complemento para 1 deve-se ao fato de esta poder ser calculada da mesma forma para múltiplos desse comprimento – 16, 32, 64 bits, etc. – e o resultado, quando encapsulado, será o mesmo. A verificação deste campo por parte do receptor é feita recalculando a soma em complemento para 1 que deveria dar 0, caso o pacote tenha sido recebido intacto.

Esta técnica do Checksum, embora muito inferior a outros métodos detectores, como o CRC é parcialmente compensada com a aplicação do CRC ou outros testes de integridade

melhores ao nível da camada 2 de rede, logo abaixo do TCP, como no caso do PPP (Point-to-Point Protocol) e Ethernet.

As confirmações de recepção (ACK) servem também ao emissor para determinar as condições da rede. Dotados de temporizadores, tanto os emissores como receptores podem alterar o fluxo dos dados, contornar eventuais problemas de congestão e, em alguns casos, prevenir o congestionamento da rede. O protocolo está dotado de mecanismos para obter o máximo de performance da rede sem congestioná-la — o envio de quadros por um emissor mais rápido que qualquer um dos intermediários ou mesmo do receptor pode inutilizar a rede. São exemplos a janela deslizante, o algoritmo de início-lento (Slow-start algorithm).

Finalização Da Conexão TCP

Da mesma forma que a abertura de sessão, o protocolo TCP também realiza um fechamento formal de uma sessão exigindo uma troca de flags entre os computadores, de maneira a confirmar, explicitamente, que a sessão TCP será fechada.

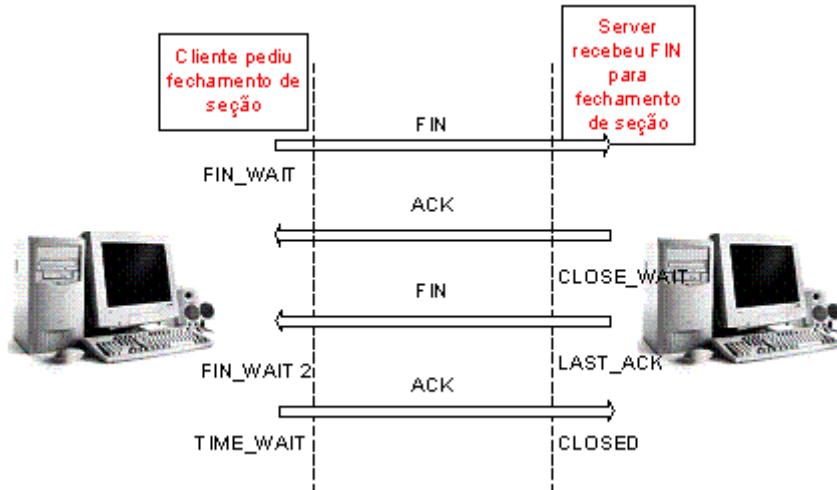
O fechamento de uma sessão TCP usa um processo um tanto diferente do 3-way-handshaking da abertura de sessão acima descrito. Lembrar, que em condições normais de funcionamento uma conexão TCP usa o modo Full-duplex, isto é, ambos os computadores falam simultaneamente.

Portanto, o processo detalhado de fechamento de uma conexão TCP pode ser resumido abaixo.

O primeiro segmento é enviado pelo computador (cliente) A quando uma aplicação como o FTP, por exemplo, não tiver mais dados para enviar, requisita da pilha TCP o encerramento da sessão que será realizada através do envio de um segmento com o flag FIN habilitado (FIN =1).

O segundo segmento é enviado pela aplicação que está sendo executada no computador (servidor) B aceitando o pedido de finalização e enviando um segmento com o flag ACK

habilitado (ACK=1). A conexão está agora fechada em uma direção (A→B) e serão ainda necessários mais segmentos para fechar a conexão no sentido inverso (B→A).



Este segmento é o pedido de fechamento de sessão no sentido inverso (B→A) que é realizado pelo computador (servidor) B enviando um segmento com o flag FIN habilitado (FIN=1).

Este é o último segmento confirmado pelo computador (cliente) A para o pedido de fechamento de sessão feito pelo computador (servidor) B. O segmento com o flag ACK habilitado (ACK=1) é enviado pelo computador A.

Obs.: A conexão TCP pode ser encerrada de maneira totalmente informal e abrupta, para isto, basta que um computador envie um segmento com o flag de RESET habilitado (RST=1).

Portas Reservadas Do TCP

O TCP introduz o conceito de porta tipicamente associado a um serviço da camada de Aplicação para fazer uma tarefa (ligação) específica. Assim, cada um dos intervenientes na

conexão dispõe de uma porta associada (com um valor de 16 bits) que dificilmente será o mesmo do interlocutor.

Alguns serviços (que fazem uso de protocolos específicos) são tipicamente acessíveis em portas fixas predefinidas denominadas como Well-known ports (portas bem conhecidas), que são aquelas portas numeradas do 1 a 1023. Além destas, existem ainda duas gamas de portas, registradas e privadas ou dinâmicas. As portas bem conhecidas são atribuídas pela IANA (Internet Assigned Numbers Authority) e são tipicamente utilizadas por processos com direitos de sistema ou super-usuário. Estas portas estão em escuta passiva os serviços triviais, tais como o HTTP, SSH, FTP, etc. Todos os protocolos da suite IP se encontram registados dentro desta gama. Nos sistemas Linux/UNIX esta escuta passiva é realizada através de processos denominados Daemons.

A gama de portas privadas segue regras de atribuição específicas do sistema operativo e serve para abrir conexões a outras máquinas, como navegar na Internet, por exemplo. As seguintes portas são alguns exemplos de portas reservadas (Well-known ports) para funções específicas de Aplicações que fazem uso do TCP:

5 RJE	43 NIXNAME
7 ECHO	53 DOMAIN
9 DISCARD	67 BOOTPS
11 USERS	68 BOOTPC
13 DAYTIME	69 TFTP
15 NETSTAT	75 Any private dial-out
17 QUOTE	77 Any private RJE ser
19 CHARGEN	79 FINGER

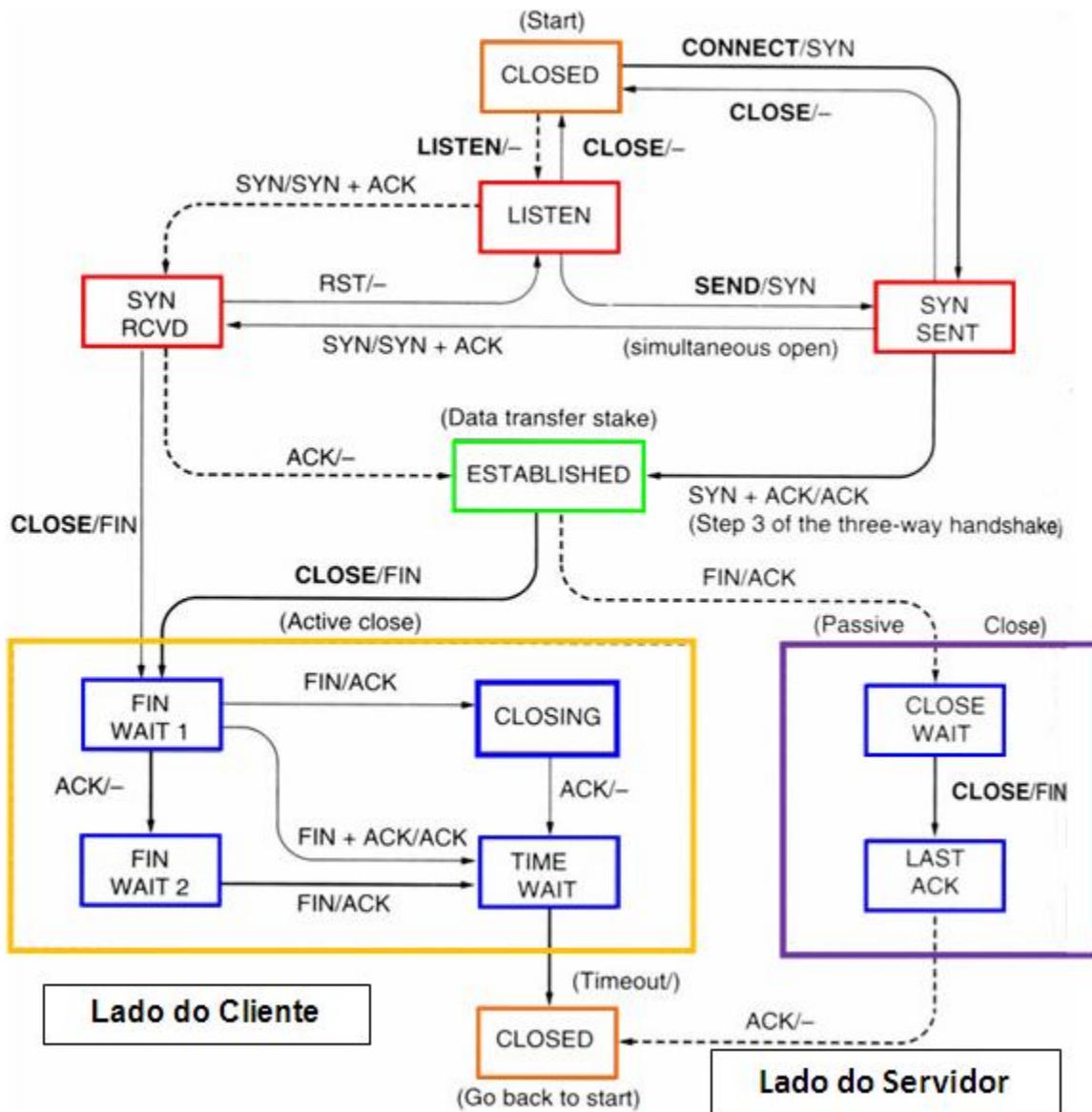
20	FTP-DATA	80	HTTP
21	FTP-CONTROL	95	SUPDUP
23	TELNET	101	HOSTNAME
25	SMTP	102	ISO-TSAP
37	TIME	113	AUTJ
39	RLP	117	UUCP-PATH
42	NAMESERVER	123	NTP

A Máquina De Estados Do TCP

Cada vez que uma conexão TCP é bem estabelecida, cria-se uma máquina de estados finita. O TCP irá de um estado para outro dependendo das condições do enlace de comunicações, portanto, cada estado é controlado por temporizadores que (quando esgotados) definirão o novo estado que o TCP deverá tomar, vale a pena lembrar que não todos os estados possuem controle por temporizadores.

Cada um dos estados de uma conexão TCP é minuciosamente descrito na RFC 793. Para entender verdadeiramente estes estados de uma conexão TCP é importante observar os muitos estágios que experimenta uma conexão TCP. Além dos estados “Established” e “Closed” apresentados, existem uma série de outros estados que devem ser entendidos por qualquer profissional de segurança, suporte e desenvolvimento.

Como o início e o fim de uma sessão de comunicação são bem definidos e o TCP acompanha o estado de suas conexões mediante Flags é importante saber quais são os vários estados pelos quais passa uma conexão TCP, nesse sentido temos a seguir uma explicação detalhada dos vários estágios que uma conexão TCP pode experimentar durante o tempo de atividade (conexão) entre um determinado cliente e um servidor (na Internet).



O reconhecimento (ACK) constitui-se no número de seqüência do próximo Byte que a entidade TCP transmissora espera receber do TCP receptor na direção oposta da conexão. Por exemplo, se o número de seqüência X for transmitido no campo Acknowledge (ACK), ele indica que a estação TCP transmissora recebeu corretamente os Bytes com os números de seqüência menores que X, e que ele espera receber o Byte X na próxima mensagem.

Os estados possíveis de estabelecimento da conexão TCP (em vermelho) são os seguintes:

- **LISTEN:** Este é o estado verdadeiro de uma conexão TCP, ele ocorre quando um computador (servidor) está esperando um pedido para iniciar uma conexão.
- **SYN-SENT:** Este estado indica que o computador enviou um SYN para iniciar a conexão e está aguardando a resposta SYN-ACK adequada.
- **SYN-RCVD:** Este estado indica que o computador enviou a resposta SYN-ACK depois de ter recebido o SYN.
- **ESTABLISHED:** Este estado (em verde) indica que a conexão foi estabelecida. O computador que iniciou a conexão entra nesse estado depois de receber o SYN-ACK e o computador que responde depois que recebe o ACK.

O processo de estabelecimento de uma conexão TCP normalmente passa pelos estados acima descritos que fazem parte do mecanismo de 3-way-handshaking, esses são os estados que os computadores (servidores) passam no processo de estabelecimento da conexão TCP. Os seis estados restantes (em azul) descrevem o desmembramento de uma conexão TCP onde os estados descritos demonstram como uma conexão é fechada e como os dados param de fluir entre os dois computadores. Os estados abaixo descritos demonstram como esse processo é realizado.

- **FIN-WAIT-1:** O estado que o computador cliente se encontra após ter enviado um pacote FIN inicial pedindo um fechamento correto da conexão TCP ao servidor.
- **CLOSE-WAIT:** O estado da conexão do servidor que recebeu um FIN inicial e envia de volta um ACK mais um FIN (final) para confirmar o FIN (inicial) do cliente.
- **FIN-WAIT-2:** O estado da conexão do cliente que recebeu a resposta ACK + FIN (final) do servidor para seu pacote FIN inicial, e indica que agora está esperando um FIN final.

- **LAST-ACK:** Este estado indica que o computador acabou de enviar seu segundo FIN, que é necessário para encerramento correto da conexão TCP, e está aguardando uma confirmação.
- **TIME-WAIT:** Nesse estado encontra-se o computador cliente que recebeu um FIN final e enviou um ACK para fechar a conexão. Nesse momento ele não irá mais receber nenhuma confirmação do ACK que acabou de enviar, portanto espera um período de tempo (em torno de 240 segundos) para fechar a conexão antes da porta ser outra vez utilizada para “escutar” (Listen).
- **CLOSED:** Este é o estado final que pode ser considerado como o estado “Sem Estado” (em laranja). Esse estado existe antes que uma conexão seja iniciada ou quando ela é finalizada. Estado que é empregado quando uma conexão usa o fechamento simultâneo iniciado pelo cliente, ou seja, a conexão ingressa neste estado depois de receber um FIN (do cliente) e o servidor o reconheça com um ACK. Vejamos a seguir como é realizado (em detalhe) o encerramento de uma desconexão TCP.

Etapas Para A Finalização De Uma Conexão TCP

Na comunicação Cliente/Servidor é necessário que existam regras, normas ou protocolos para um correto dialogo entre ambas as partes tanto para o inicio como para o fechamento das conexões, neste caso será explicado passo a passo o correto encerramento de uma sessão TCP (por favor, vide o diagrama de estados do TCP dado anteriormente).

Em condições normais de funcionamento toda conexão TCP é encerrada sempre com uma requisição por parte do cliente, esta petição de encerramento se inicia com um pacote **FIN** (inicial) enviado pelo cliente para o servidor, quando acontece isto o TCP cliente entra no estado de **FIN-WAIT 1** esperando uma das seguintes três possíveis respostas por parte do servidor:

1. Um segmento **ACK**

2. Um segmento **FIN** (final)
3. Um segmento **ACK + FIN** (final) (modo Piggyback)

Em qualquer um dos casos anteriores o servidor ingressa no estado de **CLOSE-WAIT**.

Agora o cliente, dependendo do tipo de segmento recebido (por parte do servidor), ingressará a um estado diferente, vejamos quais são esses estados após o recebimento de uma das três respostas possíveis do servidor:

1. Se o servidor enviou um **ACK**: Então o cliente ingressa no estado de **FIN-WAIT 2** e envia um novo **ACK** para o servidor que ainda se encontra no estado de **CLOSE-WAIT**, neste caso o cliente fica aguardando o **FIN** (final) do servidor.
2. Se o servidor enviou um **FIN** (final): Então o cliente ingressa no estado de **CLOSING** e envia um **ACK** para o servidor que agora se encontra no estado de **LAST-ACK**.
3. Se o servidor enviou um **ACK + FIN** (final): Então o cliente ingressa no estado de **TIME-WAIT** e envia um **ACK** para o servidor que agora se encontra no estado de **LAST-ACK**.

Pode-se observar que o servidor quando envia o segmento **FIN** (final) (seja este sozinho ou no modo Piggyback) passa do estado de **CLOSE-WAIT** para o estado de **LAST-ACK** de forma automática, como explicado nos casos 2 e 3 anteriores.

Quando o cliente se encontra no estado de **TIME-WAIT** praticamente está pronto para liberar a sessão TCP, reparar que das três situações possíveis dadas anteriormente, só a 3^a situação deixa o cliente no estado de **TIME-WAIT**. Portanto, temos ainda que explicar como o cliente chega nesse estado para as situações 1 e 2, ou seja, a 1^a é quando o servidor enviou inicialmente só um segmento **ACK** e a 2^a é quando o servidor enviou somente o segmento **FIN** (final), vejamos as explicações para cada caso:

1. O servidor (que ainda se encontra no estado **CLOSE-WAIT**) recebe o **ACK** e envia como resposta o **FIN** (final) e passa para o estado de **LAST-ACK**, quando o cliente recebe o **FIN** (final) ingressa no estado de **TIME-WAIT** e envia um **ACK** final para o servidor. Este **ACK** final tira o servidor do estado **LAST-ACK** e o coloca no estado de **CLOSED** liberando por completo a sessão TCP se posicionando automaticamente no estado de **LISTEN**.
2. O servidor (que atualmente se encontra no estado de **LAST-ACK**) recebe o **ACK** do cliente, e este lhe responde com outro segmento **ACK**. Agora temos o seguinte, esse último **ACK** (enviado pelo cliente) coloca o servidor no estado de **CLOSED** liberando assim a sessão TCP o que automaticamente leva este para o estado de **LISTEN**. Quando o cliente recebe o **ACK** (do servidor) ingressa no estado de **TIME-WAIT**.

Neste ponto o servidor já está completamente livre da sessão TCP e não tem mais nada a ver com o cliente, o servidor agora está à escuta de novas conexões de outros clientes. Portanto, o cliente dependerá só do seu próprio mecanismo TCP. Ele só entrará no estado de **CLOSED** quando o temporizador associado ao estado **TIME-WAIT** estourar, ou seja, quando ocorrer um Timeout (normalmente de 60 segundos) desse estado, somente nessa situação que o cliente entrará no estado de **CLOSED** e dessa forma ficará livre da sessão TCP iniciada por ele. Na tabela dada anteriormente se apresenta o caso quando o servidor retorna um segmento **ACK + FIN** (final) (modo Piggyback) para o **FIN** (inicial) do cliente.

Processo De Retransmissão TCP

O processo de retransmissão pode dizer muito da condição real da rede. O TCP mantém um timer interno que é inicializado e decrementado no momento que um segmento é transmitido. Se houver algum problema no processo de comunicação como link ruim, cabeamento com problema, erro causado por ruído, ou alta latência na rede e o segmento chegar com erros,

atrasado ou mesmo destruído, o computador destino simplesmente descartará este segmento, não enviando um ACK de resposta.

O que pode causar retransmissão em uma rede? Infelizmente podem ser inúmeras as causas para isto, tais como:

- Aplicações lentas e mal construídas. Muito comum em aplicações antigas como Cobol e Clipper.
- Redes com problemas na infra-estrutura física como cabeamento com problemas de ruídos e erros de transmissão.
- Dispositivos ativos (Switches, Hubs) com problemas de Hardware.
- Placas de rede com problemas de Hardware.
- Drivers de placas de rede.
- Excesso de tráfego.
- Redes com problemas de projetos.
- Como verificar se sua rede está com problemas?

Em sistemas WindowsXP/2003/2008 ou Linux, utilize o comando netstat -s e verifique as estatísticas de uma determinada conexão TCP. A estação ideal para se fazer o teste é normalmente uma máquina que enxergue a rede inteira, por exemplo, um servidor.

A seguir temos, a maneira de um exemplo ilustrativo, as estatísticas de uma dada conexão TCP:

Abertos ativos	= 489
Abertos passivos	= 25
Falha em tentativas de conexão	= 67
Conexões redefinidas	= 143
Conexões atuais	= 3
Segmentos recebidos	= 10611
Segmentos enviados	= 8872
Segmentos retransmitidos	= 140

O resultado deste comando executado em uma máquina da rede. Como você pode notar, existe uma quantidade de segmentos retransmitidos considerável. Esta informação será sempre visível para o administrador do sistema e é independente da máquina e do estado da rede na qual este comando seja executado. O procedimento para visualizar as estatísticas da sua conexão TCP é a seguinte, abra uma janela DOS (no Windows) ou uma janela Shell (do Linux) e digite (em qualquer máquina da sua rede) o comando:

- C:\>netstat -s (se estiver no Windows)
- # netstat -s (se estiver no Linux com prompt de super usuário)

Feito isso verifique a estatística de retransmissão da sua conexão TCP, se as retransmissões estão baixas e constantes (por exemplo, 5% máximo dos segmentos transmitidos) existe

algum problema mais não é grande o bastante para impactar a rede. Neste caso não precisaria de se preocupar muito em analisar a sua rede.

Digite o comando netstat -s 5 (este comando realizará um refresh a cada 5 segundos na tela). Se o número de retransmissões estiver aumentando, provavelmente você está com problemas na sua rede e com certeza você já está sentido que a rede está lenta.

Faça uma análise mais detalhada dos cabos, aplicações e dispositivos ativos. Uma boa ferramenta é um software analisador de protocolos.

Obs.: Este procedimento não lhe dará as razões exatas da lentidão da rede. São procedimentos genéricos. Para saber as razões exatas e detalhadas deve-se realizar uma análise levando em consideração os itens acima listados.

UNIDADE 15

Objetivo: Entender como e quando fazer uso do protocolo de transporte UDP.

Protocolos Do Nível De Transporte: UDP

UDP é um acrônimo do termo em inglês User Datagram Protocol que traduzido significa o protocolo de datagramas do usuário. Este protocolo de transporte pode ser considerado uma versão econômica do TCP, um protocolo que emagreceu demais e que dá às aplicações acesso direto ao serviço de entrega de datagramas.

O protocolo UDP faz o envio do datagrama, mas não garante que ele chegará efetivamente ao destino, portanto, é pouco confiável, isto devido a que é um protocolo não orientado para conexão. O "pouco confiável" significa que não há técnicas no protocolo para confirmar que os dados chegaram ao destino corretamente ou se realmente chegaram.

Na seguinte figura é apresentado o formato do cabeçalho UDP.

0	15	16	31
Porta de origem		Porta de Destino	
Tamanho		Soma de verificação (Checksum)	
Dados (se houver)			

Esse cabeçalho contém os seguintes campos:

- **PORTE DE ORIGEM:** Número da porta do computador transmissor.
- **PORTE DE DESTINO:** Número da porta da aplicação solicitada no computador receptor.
- **TAMANHO DO SEGMENTO:** Tamanho do cabeçalho UDP e dados UDP.

- **CRC:** Checagem de redundância cíclica ou soma de verificação dos campos de cabeçalho e dados do UDP.
- **DADOS:** Dados do nível superior, isto é, os dados do usuário.
- Para maiores detalhes sobre a implementação do protocolo de transporte UDP consulte o documento RFC 768.

Funcionamento Básico Do UDP

O UDP faz a entrega de mensagens independentes, designadas por datagramas, entre aplicações ou processos, entre redes. A entrega não é garantida, isto é, os dados podem chegar ao destino ou podem ser perdidos no caminho. A integridade dos dados pode ser controlada por um "Checksum" (um campo no cabeçalho de checagem por soma).

Assim como para o TCP, os pontos de acesso do UDP são geralmente designados por "Portas de protocolo" ou simplesmente "portas", em que cada unidade de transmissão de dados UDP identifica o endereço IP e o número de porta do destino e da fonte da mensagem, os números podendo ser diferentes em ambos os casos.

O UDP é o protocolo irmão do TCP. A diferença básica entre os dois é que o TCP é um protocolo orientado à conexão, que como foi estudado, inclui vários mecanismos para iniciar e encerrar a conexão, negociar tamanhos de pacotes e permitir a retransmissão de pacotes corrompidos. No TCP tudo isso é feito com muito cuidado, para garantir que os dados realmente cheguem inalterados, apesar de todos os problemas que possam existir na conexão. O lema para o TCP é "transmitir com segurança"

O UDP por sua vez é uma espécie de irmão adolescente do TCP, feito para transmitir dados pouco sensíveis, como streaming de áudio e vídeo que não requerem de retransmissões. No UDP não existem checagens e nem confirmação alguma. Os dados são transmitidos apenas uma vez, incluindo apenas um frágil sistema de CRC. Os pacotes que chegam corrompidos são simplesmente descartados, sem que o emissor sequer saiba do problema.

A idéia é justamente transmitir dados com o maior desempenho possível, eliminando dos pacotes quase tudo que não sejam dados em sí. Apesar da pressa, o UDP tem seus méritos, afinal você não gostaria que quadros fantasmas ficassem sendo exibidos no meio de um vídeo, muito menos se isso ainda por cima causasse uma considerável perda de performance.

Em geral, os programas que utilizam portas UDP recorrem também à uma porta TCP para enviar as requisições de dados a serem enviados e também para checar periodicamente se o cliente ainda está online. Ou seja, na Internet, O UDP é um protocolo de transporte que presta um serviço de comunicação não orientado a conexão e sem garantia de entrega. Portanto, as aplicações que utilizam este tipo de protocolo devem ser as responsáveis pela recuperação dos dados perdidos.

Por exemplo, o protocolo UDP é utilizado pelas Aplicações NFS (Network File System), DNS (Domain Name Service), SNMP (Simple Network Management Protocol), TFTP (Trivial FTP), etc.

Neste sentido, aplicações como o SNMP podem tirar vantagem do UDP, o SNMP faz o monitoramento de rede. Nesse tipo de serviço existe o envio de mensagens intermitentes e um fluxo constante de atualizações de status e alertas, principalmente quando esta sendo utilizado em uma grande rede.

Se ele fosse utilizado numa conexão TCP no lugar de UDP, isso geraria uma sobrecarga muito grande na rede (gerada por ter que abrir e fechar uma conexão TCP para cada uma das mensagens enviada).

Quadro Comparativo TCP vs. UDP

A seguinte tabela apresenta as principais diferenças entre ambos os protocolos de transporte mais utilizados na Internet, a saber, TCP e UDP.

TCP	UDP
Seqüenciado	Não seqüenciado
Confiável	Não confiável
Orientado a conexão	Sem conexão
Círculo virtual	Pouca sobrecarga
Three-way handshake	Sem reconhecimento
Controle de fluxo por janelas	Sem janela ou controle de fluxo

Alguns exemplos de portas que fazem uso do protocolo de transporte UDP são:

Porta UDP	Descrição
53	Consultas de nomes DNS (Domain Name System, sistema de nomes de domínios)
69	Trivial File Transfer Protocol (TFTP)
137	Serviço de nomes de NetBIOS
138	Serviço de datagrama de NetBIOS
161	SNMP (Simple Network Management Protocol)
520	Routing Information Protocol (RIP, protocolo de informações de roteamento)

UNIDADE 16

Objetivo: Entender o conceito de portas e como estas são importantes para as comunicações na Internet.

Portas Dos Protocolos De Transporte

Os pontos de acesso do TCP e UDP são geralmente designados por "Portas de protocolo" ou simplesmente "portas", em que cada unidade de transmissão de dados UDP identifica o endereço IP e o número de porta do destino e da fonte da mensagem, os números podendo ser diferentes em ambos os casos.

O servidor de cada programa que usa os protocolos de transporte escuta as mensagens que chegam ao seu número de porta conhecido.

Os números de porta de servidor TCP/UDP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela IANA. Os números de 1024 a 65535 podem ser atribuídos para outros serviços e são geralmente utilizados pelo programas-cliente de um protocolo (que podem utilizar um número de porta qualquer). Este conjunto de números tem ainda a atribuição de alguns serviços de forma não oficial, já que os primeiros 1024 números não conseguem comportar todos os protocolos TCP/IP existentes.

Para obter uma lista atualizada e completa de todas as portas TCP conhecidas e registradas atualmente, consulte o seguinte endereço: <http://www.iana.org/assignments/port-numbers>.

Definição De Porta

Para cada nível do modelo OSI existe um campo no protocolo da camada que indica para quem os dados encapsulados devem ser entregues. Por exemplo, no nível de enlace, o campo TYPE (Tipo de protocolo) indica qual é o protocolo que está encapsulado no quadro Ethernet, um valor igual a 0x0800 neste campo indica que os dados devem ser passados

para o IP. Agora, no nível de rede, o campo PROTOCOL no cabeçalho do pacote IP identifica o protocolo para o qual o datagrama deve ser repassado, por exemplo, um valor de 17 neste campo indica que o pacote deve ser transferido para o protocolo de transporte UDP e se o valor deste campo for 6 então o pacote deve ser encaminhado para o TCP.

De maneira similar, para distinguir dentre as várias aplicações das camadas superiores, o nível de transporte associa um identificador a cada processo de aplicação. Esse identificador é chamado como “Número de Porta” (PORT NUMBER).

Comunicação Através De Portas

Para que uma aplicação possa “conversar” com uma outra em uma máquina remota, é preciso conhecer não apenas o endereço Internet da máquina destino, mas também a porta associada à aplicação parceira. Uma porta é um objeto abstrato que deve ser usado para identificar processos de aplicações. Os protocolos UDP e TCP fornecem um conjunto de portas que permite a múltiplos processos dentro de uma única máquina usarem os serviços de comunicação providos pelo UDP e TCP simultaneamente.

Se observarmos ambos os cabeçalhos dos protocolos UDP e TCP, é possível verificar que o campo PORT NUMBER é um valor codificado inteiro binário de 16 bits, o que significam que podemos ter $2^{16} = 65536$ portas para efetuar o transporte de dados (começando do valor 1).

Nesse sentido, tanto o TCP quanto o UDP possibilitam o uso de 65356 portas que são empregadas pelos respectivos serviços habilitados nos computadores. Quando um determinado serviço está ativo uma porta específica é habilitada para que o processo de comunicação entre os computadores ocorra. A comunicação do TCP/UDP é baseada em um componente Cliente que busca dados em um componente Servidor.

As portas TCP e UDP são classificadas de acordo com o seguinte esquema:

- As portas do Servidor assumem valores entre 1 e 1024 e são sempre fixas. Ex: 21 para FTP, 23 para Telnet, etc.

- As portas do computador cliente assumem valores acima de 1023 e são randômicas (aleatórias) podendo ir até o valor 65536.

Em sua última atualização de 28 de setembro de 2004 o IETF e a IANA (entidades que controlam a alocação destas portas) definiram as seguintes 3 sub-regiões no intervalo de 0 a 65536, a saber, a primeira região corresponde às portas bem-conhecidas, a segunda região é das portas registradas e a terceira região das portas dinâmicas e/ou privadas, de maneira quantitativa tem-se:

- As portas bem-conhecidas são aquelas que vão desde 0 até 1023.
- As portas registradas são aquelas que vão desde 1024 até 49151.
- As portas dinâmicas e/ou privadas são aquelas que vão desde 49152 até 65535.

Portanto, as primeiras 1024 portas (e algumas com numeração superior) são predefinidas e reservadas para o acesso a serviços padrão de rede fixos pelos sistemas operacionais. Por exemplo:

- O serviço de transferência de arquivos FTP utiliza a porta 21 do TCP,
- O serviço de terminal remoto Telnet faz uso da porta 23 do TCP,
- O protocolo de hipertexto HTTP utiliza a porta 80 do TCP,
- O serviço de nome de domínios DNS utiliza a porta 53 do UDP,
- Para gerenciamento da rede o SNMP faz uso da porta 161 do UDP.
- O protocolo POP3 faz uso da porta 110 do TCP.
- O protocolo RPC pode fazer uso da porta 530 tanto do UDP como do TCP.

Vale a pena mencionar que o usuário não deve confundir as portas TCP com as portas UDP: apesar das duas terem a mesma função (identificar a aplicação da camada superior), o mesmo número de porta em ambas não necessariamente identifica um mesmo aplicativo.

Dependendo do caso, uma aplicação não precisa, necessariamente, estar restrita a um dado conjunto de portas. É possível utilizar outras, mas é necessário que isso seja especificado. É por tal motivo, por exemplo, que há determinados endereços na internet que são disponibilizados assim:

<http://www.site.com:abcd>

Onde o número **abcd** corresponde ao número da porta. Neste caso, seu computador está sendo orientado a acessar aquele endereço Internet pela porta **abcd**.

É graças ao conceito de portas que você consegue utilizar vários serviços ao mesmo tempo na Internet. No entanto, isso também pode representar um perigo, razão pela qual é importante ter controle sob o tráfego de dados nas portas TCP e UDP. O uso de Firewalls, por exemplo, ajuda a impedir que aplicações maliciosas utilizem portas abertas no computador para atividades prejudiciais. Além disso, um administrador de redes pode fazer configurações manuais para que determinadas portas fiquem bloqueadas, impedindo a conexão de aplicativos que fazem uso destas.

UNIDADE 17

Objetivo: Saber que comandos utilizar quando existem problemas de comunicação na Internet.

Existem alguns recursos que estão disponíveis através do “prompt” do DOS através de comandos de linha que ajudam aos administradores que estão familiarizados com essa interface. Até os técnicos mais experientes recorrem (em algum momento) aos recursos disponibilizados nessa interface. Nos sistemas Linux/UNIX tem-se algo parecido com o prompt do DOS, neste caso temos o Shell que faz um trabalho similar de interpretador de comandos de linha.

ICMP – Internet Control Message Protocol

Este protocolo faz parte da pilha de protocolos TCP/IP, enquadrando-se na camada de rede (nível 3), a mesma camada do protocolo IP. O seu uso mais comum é feito pelos utilitários ping e traceroute. O ping envia pacotes ICMP para verificar se um determinado computador está disponível na rede. O traceroute faz uso do envio de diversos pacotes UDP ou ICMP e, através de um pequeno truque, determina a rota seguida para alcançar um determinado computador.

Esta unidade descreve as interações entre um computador cliente e um servidor implementadas por estes dois utilitários básicos.

O Comando Ping (Packet Internet Groper)

A mais simples das ferramentas “prompt” é o utilitário denominado ping. Este comando serve para efetuar o teste de um outro endereço de IP, verificando se ele é valido e se pode ser alcançado. Essa ferramenta é utilizada para fazer um “troubleshooting”, ou seja, tentar

solucionar um problema de conectividade entre dois computadores independente da distância que os separa.

O comando ping faz o envio de um pacote de rastreamento (isso se faz através do uso do protocolo ICMP) ao endereço especificado e depois é aguardado o retorno a respeito dessa informação. Enquanto o pacote esta trafegando se registra o tempo decorrido, que será informado no momento da recepção do pacote, assim que ele for reconhecido e devolvido à origem. Se depois do tempo limite o pacote não conseguir alcançar o destino, aparecerá uma mensagem “esgotado tempo limite de pedido – destino inalcançável” para o usuário.

Quando queremos verificar se um determinado computador está disponível na rede interna ou mesmo na Internet, frequentemente fazemos uso do utilitário ping como um dos primeiros para verificar o estado da conexão. O fato de um computador não responder ao ping não quer dizer que ele esteja realmente fora da rede, pois, este serviço poderia estar desabilitado nesse computador por questões de segurança. O comando, provavelmente já conhecido pelo leitor, é:

- C:\>ping <endereço IP> (no prompt da linha de comandos do DOS)
- #ping < endereço IP> (em uma sessão Shell do Linux/UNIX como super usuário)

Exemplo:

```
[root@foofighter linux-2.6.3]# ping 192.168.0.1
```

```
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
```

```
64 bytes from 192.168.0.1: icmp_seq=1 ttl=127 time=4.22 ms
```

```
64 bytes from 192.168.0.1: icmp_seq=2 ttl=127 time=1.02 ms
```

```
64 bytes from 192.168.0.1: icmp_seq=3 ttl=127 time=1.01 ms
```

```
64 bytes from 192.168.0.1: icmp_seq=4 ttl=127 time=1.99 ms
```

```
64 bytes from 192.168.0.1: icmp_seq=5 ttl=127 time=1.03 ms
```

```
--- 192.168.0.1 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
```

```
rtt min/avg/max/mdev = 1.019/1.857/4.221/1.241 ms
```

A resposta acima indica que o computador 192.168.0.1 está disponível. Algumas estatísticas de tempo, tais como a seqüência ICMP e os tempos TTL (Time to Live) são apresentados, observe que nenhum pacote ICMP foi perdido já que a seqüência (icmp_seq) esta completa, o tempo de ida e volta, o RTT (Round Trip Time) entre os computadores, é de aproximadamente 1,03 ms.

É chamado de cliente o computador que inicia a comunicação, ou seja, a partir do qual o usuário executa o comando de teste de disponibilidade. Servidor é o alvo do teste, pois este deve possuir um serviço habilitado para ser capaz de receber o pacote do cliente e respondê-lo. O cliente envia primeiro um pacote do tipo ICMP Echo Request, ou simplesmente ICMP Echo. Abaixo está a captura deste pacote na rede. Note o tipo do protocolo no cabeçalho IP (ICMP) e o tipo do pacote no cabeçalho ICMP (Echo request).

Internet Protocol, Src Addr: 192.168.0.2 (192.168.0.2), Dst Addr: 192.168.0.1 (192.168.0.1)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 84

Identification: 0x0000 (0)

Flags: 0x04

Fragment offset: 0

Time to live: 64

Protocol: ICMP (0x01)

Header checksum: 0xb955 (correct)

Source: 192.168.0.2 (192.168.0.2)

Destination: 192.168.0.1 (192.168.0.1)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x5905 (correct)

Identifier: 0x9409

Sequence number: 0x0001

Data (56 bytes)

Quando o servidor recebe este pacote ele responde com um pacote do tipo ICMP Echo Reply. Veja abaixo a captura deste pacote.

Internet Protocol, Src Addr: 192.168.0.1 (192.168.0.1), Dst Addr: 192.168.0.2 (192.168.0.2)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 84

Identification: 0xa078 (41080)

Flags: 0x00

Fragment offset: 0

Time to live: 127

Protocol: ICMP (0x01)

Header checksum: 0x19dd (correct)

Source: 192.168.0.1 (192.168.0.1)

Destination: 192.168.0.2 (192.168.0.2)

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x6105 (correct)

Identifier: 0x9409

Sequence number: 0x0001

Data (56 bytes)

No Windows o processo de “ping” é repetido quatro vezes, a não ser que seja adicionado o parâmetro “-t” que possibilita pingar o endereço por tempo indeterminado, assim como ocorre no Linux/Unix, em ambos os casos deve-se apertar a seqüência Ctrl-c para finalizar o processo.

Pode-se utilizar o comando ping com outros protocolos, por exemplo, o NETBIOS para resolver nomes. Para obter uma ajuda rápida do comando ping no Windows digitar do prompt “C:\>ping /?”, já nos sistemas Linux/UNIX pode-se digitar no shell “\$ping --h” ou “\$man ping”.

Um dos melhores parâmetros do “ping” no Windows é o comando “ping –a w.x.y.z”. Ele faz a resolução do nome via DNS. Caso você quiser fazer isso no Unix pode se utilizar do comando “host w.x.y.z”; Não se recomenda ficar exagerando no uso do comando “ping”, pois de pacote em pacote se pode gerar um tráfego mais intenso. Por exemplo, pode-se estressar a mídia Ethernet, utilizando-se pacotes de maior comprimento.

Por exemplo, “ping –l 1472 –n 50 w.x.y.z” gera 50 datagramas com tamanho máximo de 1472 Bytes. Se a estrutura física da rede não estiver bem, se notara perda de pacotes de forma intermitente.

Portanto, é possível através de opções de comando especificar, por exemplo, quantos pacotes devem ser enviados, qual o intervalo de tempo entre eles, e até o tamanho do pacote. Na verdade a área de dados do pacote não carrega nenhuma informação útil, entretanto, pode ser aumentada para testar a rede com pacotes de tamanhos diferentes. Existe atualmente um limite para o tamanho do pacote, pois um pacote muito grande pode provocar o reboot de alguns sistemas Windows, sendo este o conhecido ping of death, ou ping da morte.

Existe a possibilidade de não se receber resposta da máquina de destino, nesse caso o serviço de resposta “eco” pode estar desabilitado (isso é bem útil para inibir o escaneamento da máquina). Pode-se fazer isso por medidas de segurança. Se for o caso pode-se optar por usar “tracert” ou “traceroute” para se chegar ao nó mais próximo do destino.

No exemplo seguinte vemos um caso em que não obtemos resposta do computador remoto.

```
[root@foofighter linux-2.6.3]# ping 192.168.0.2
```

```
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
```

```
--- 192.168.0.2 ping statistics ---
```

```
5 packets transmitted, 0 received, 100% packet loss, time 3998ms
```

Outra utilidade do ping é testar a pilha de protocolo e a própria placa de rede através do comando “ping 127.0.0.1” aqui estamos fazendo uso do endereço de loopback. Em vez de 127.0.0.1 pode-se usar localhost.

Outro meio de se descobrir informações sobre a configuração de IP da máquina é se utilizar o comando “ipconfig” que pode fornecer maiores dados, inclusive o endereço MAC. É comum o uso de “ipconfig /all” no Windows XP e W2K. No Linux/Unix se pode utilizar o comando “ifconfig”.

Sempre é bom se lembrar que no Windows o parâmetro “/?” trás mais informação de ajuda sobre o comando e no Unix/Linux o comando “man” pode auxiliar a achar manuais de ajuda.

Existem também dois comandos que podem ajudar a visualizar o estado de uso das portas de transporte. Podem-se utilizar os comandos “netstat –p TCP” e ou “netstat –p UDP”.

Também é possível visualizar os endereços físicos que foram detectados pelo TCP/IP através do comando “arp –a” que exibe uma tabela com números IP e respectivos endereços físicos. Ele exibe as máquinas da mesma sub-rede que mantiveram contato com seu computador. O prazo de expiração de uma entrada nessa tabela é de 10 minutos.

Caso utilize o DHCP e tenha algum problema de atribuição de número de endereço, pode liberar o IP utilizando o comando “ipconfig /release_all” e depois de 10 segundos pode-se solicitar um novo IP através do comando “ipconfig /renew_all”. Esse procedimento deve gerar uma nova configuração de IP (que é solicitada ao servidor DHCP). Para confirmar a configuração se pode utilizar novamente o comando “ipconfig” que exibira os dados atualizados, opcionalmente pode-se redirecionar a saída do comando para um arquivo texto para facilitar a leitura, através do comando “ipconfig > saída.txt”. O arquivo gerado saída.txt (ou outro nome que seja familiar) pode ser visualizado por qualquer editor de texto ASCII, ou pode exibir o conteúdo através do comando “type saída.txt”.

Para os administradores que tem um controle fixo de IP, que seria o caso em redes LAN, é interessante se manter um registro de nomes, com grupos de trabalho e endereço físico

atribuídos para melhor controle e para se resolver problemas futuros. Tais dados também podem ser obtidos através do uso de um scanner de rede.

Também existe o comando “route-print” (Windows) que exibe as informações sobre rotas e custos do TCP/IP consultado. No Unix pode-se utilizar o comando “netstat –r”. Caso os sistemas UNIX ou Windows estiverem trabalhando com rotas fixas, pode-se também anular, retificar ou adicionar uma rota através do comando “route add”, um exemplo deste comando é o seguinte:

```
$route add 157.0.0.0 mask 255.0.0.0 157.55.80.1 metric 3 if 2
```

Onde:

IP de destino = 157.0.0.0

Mascara de rede = 255.0.0.0

Gateway = 157.55.80.1

Métrica (metric) = 3

Interface (if) = 2

O Comando Traceroute

Um dos campos do cabeçalho IP é chamado TTL (Time to Live), este campo determina por quantas passagens em roteadores este pacote pode sobreviver. A cada passagem por um roteador intermediário este campo é decrementado de 1. Este mecanismo é utilizado para evitar que pacotes IP fiquem trafegando pela rede eternamente, rodando de um lado para outro.

Se um pacote IP possui um TTL=0 este será descartado pelo próximo router, normalmente se coloca um valor elevado para garantir que o TTL não decremente a 0 antes de atingir seu destino final. Porém, se este for o caso de que o pacote ser descartado antes de alcançar o

seu destino final, este roteador que descarta o pacote, porque o TTL=0 do mesmo, retornará um pacote ICMP do tipo ICMP Time Exceeded para o computador que o enviou. Neste pacote de resposta o roteador se identifica como origem da mensagem Time Exceeded. É nessa característica do protocolo que o utilitário traceroute se baseia para traçar uma rota entre dois pontos da rede.

Suponha que o computador 1 esteja separado do computador 2 por dois roteadores, chamados router A e router B. A partir do computador 1 é executado um traceroute para o computador 2. O utilitário cria um pacote UDP destinado ao computador 2, mas configura o seu TTL para 1. O router A recebe este pacote e, apesar de saber para onde rotear o pacote, ao decrementar o TTL este torna-se 0 (zero) o que significa que este pacote deve ser descartado, retornando um ICMP Time Exceeded para o computador 1. Quando o traceroute recebe esta resposta ele tem o endereço do primeiro roteador no caminho entre os dois computadores, portanto, só o primeiro roteador é mostrado para o usuário.

Em seguida, o traceroute cria outro pacote UDP, com o TTL de 2. O pacote sobrevive ao primeiro roteador, mas é descartado pelo segundo (roteador B). Quando o aplicativo traceroute recebe o pacote ICMP Time Exceeded do segundo roteador temos o endereço dele, portanto, este roteador B também será mostrado na saída do traceroute.

O passo seguinte é um pacote com TTL de 3 o qual alcança o computador 2. Os pacotes UDP são sempre enviados com uma porta de destino inválida, o que força que o computador 2, ao receber o pacote, retorne um pacote ICMP Destination Unreachable. O traceroute sabe então que o caminho completo foi descoberto e mostra ao usuário o endereço do host 2, indicando que o trace foi finalizado com sucesso, isto é, o computador remoto foi atingido.

Como ilustração deste procedimento, temos o seguinte exemplo para o comando traceroute a partir do IP 192.168.1.2 (computador virtual A) para o IP 192.168.0.1 (computador C). Como roteador entre essas duas máquinas está um roteador Linux (computador B) com os IP 192.168.1.1 e 192.168.0.2. Portanto, o caminho do pacote deve ser A → B → C.

O comando foi executado a partir do computador A:

```
[root@foofighter root]# traceroute -q 1 192.168.0.1

traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 38 byte packets

1 192.168.1.1 (192.168.1.1) 8.243 ms

2 192.168.0.1 (192.168.0.1) 12.298 ms

3 192.168.0.1 (192.168.0.1) 21.193 ms
```

A opção -q 1 é para que o traceroute envie apenas um pacote a cada interação, o default são 3. A opção -l também poderia ser usada para instruir que sejam usados pacotes ICMP Echo Request e não pacotes UDP.

A seqüência de troca de pacotes é a seguinte:

Seq Source → Destination Protocol Description

1 192.168.1.2 → 192.168.0.1 UDP Source Port: 33406 Destination Port: 33435 (TTL=1)

2 192.168.1.1 → 192.168.1.2 ICMP Time-to-live exceeded

3 192.168.1.2 → 192.168.0.1 UDP Source Port: 33406 Destination Port: 33436 (TTL=2)

4 192.168.0.1 → 192.168.1.2 ICMP Time-to-live exceeded

5 192.168.0.1 → 192.168.1.2 ICMP Destination unreachable

6 192.168.1.2 → 192.168.0.1 UDP Source Port: 33406 Destination Port: 33437 (TTL=3)

7 192.168.0.1 → 192.168.1.2 ICMP Destination unreachable

O primeiro pacote enviado pelo computador A e descartado pelo roteador B é apresentado a seguir.

Internet Protocol, Src Addr: 192.168.1.2 (192.168.1.2), Dst Addr: 192.168.0.1 (192.168.0.1)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 38

Identification: 0x827f (33407)

Flags: 0x00

Fragment offset: 0

Time to live: 1

Protocol: UDP (0x11)

Header checksum: 0xb4f4 (correct)

Source: 192.168.1.2 (192.168.1.2)

Destination: 192.168.0.1 (192.168.0.1)

User Datagram Protocol, Src Port: 33406 (33406), Dst Port: 33435 (33435)

Source port: 33406 (33406)

Destination port: 33435 (33435)

Length: 18

Checksum: 0xa29f (correct)

Data (10 bytes)

Note o TTL (Time to Live) igual a 1 e a porta de destino. Portanto, o roteador A gera uma resposta ICMP da seguinte forma:

Internet Protocol, Src Addr: 192.168.1.1 (192.168.1.1), Dst Addr: 192.168.1.2 (192.168.1.2)

Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

Checksum: 0x7777 (correct)

Internet Protocol, Src Addr: 192.168.1.2 (192.168.1.2), Dst Addr: 192.168.0.1 (192.168.0.1)

User Datagram Protocol, Src Port: 33406 (33406), Dst Port: 33435 (33435)

Data (10 bytes)

Podemos confirmar o ICMP Time Exceeded aqui. Após a interação seguinte, o pacote chega ao destino. Como é uma porta inválida, o computador 192.168.0.1 responde com um ICMP Destination Unreachable:

Internet Protocol, Src Addr: 192.168.0.1 (192.168.0.1), Dst Addr: 192.168.1.2 (192.168.1.2)

Internet Control Message Protocol

Type: 3 (Destination unreachable)

Code: 3 (Port unreachable)

Checksum: 0x48b6 (correct)

Internet Protocol, Src Addr: 192.168.1.2 (192.168.1.2), Dst Addr: 192.168.0.1 (192.168.0.1)

User Datagram Protocol, Src Port: 33406 (33406), Dst Port: 33436 (33436)

Veja que já no passo 5 há uma resposta de ICMP Destination Unreachable, como resposta ao pacote do passo 3, com TTL igual a 2. Entretanto, mesmo assim o traceroute inicia outra interação, enviando um pacote com TTL igual a 3. Isso aconteceu porque antes do ICMP Destination Unreachable ele recebeu, no passo 4, um ICMP Time Exceeded, o que gerou o envio imediato do terceiro pacote UDP. Pode ser interessante, para quem tem habilidades de programação, olhar o código fonte de uma implementação do traceroute.

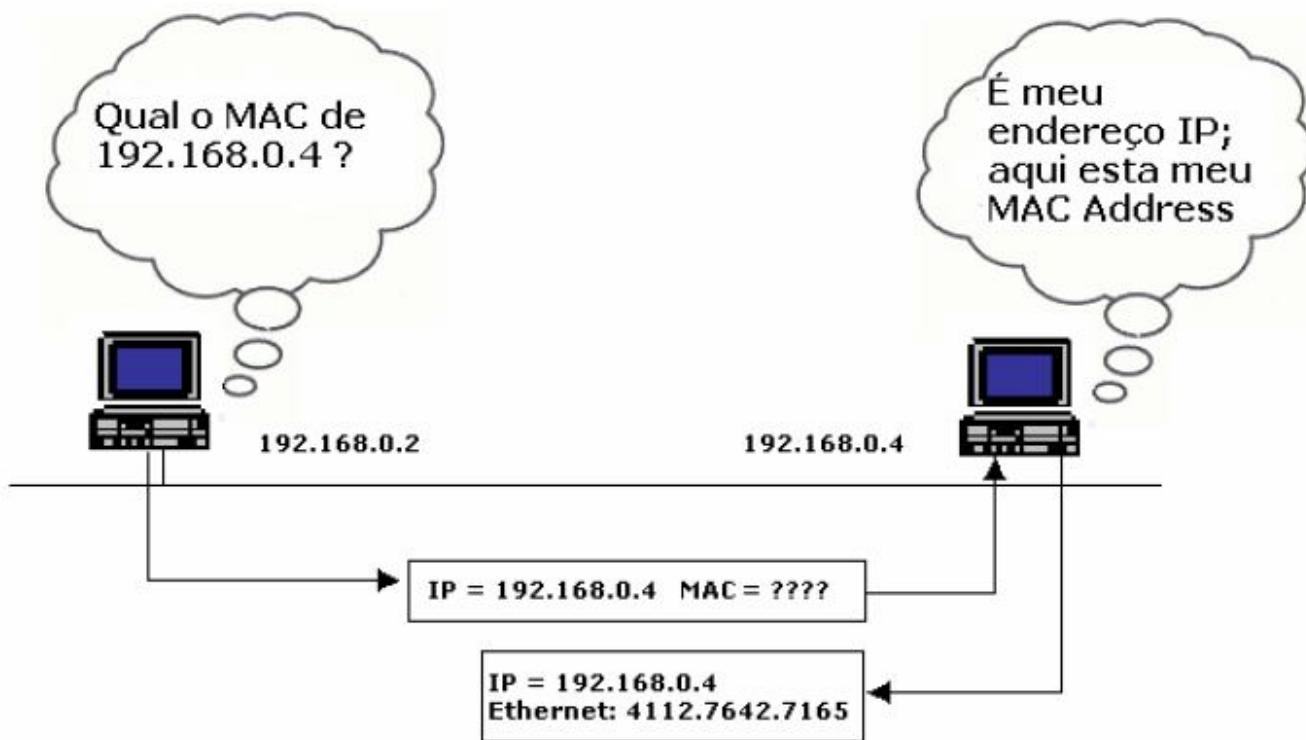
UNIDADE 18

Objetivo: Entender o funcionamento dos principais protocolos de rede.

Protocolos Do Nível Internet

ARP – Address Resolution Protocol

O protocolo ARP basicamente mapeia endereços MAC para endereços IP de forma dinâmica. O ARP faz o reconhecimento desses endereços através do disparo de mensagem em forma de “broadcast”. As informações que são detectadas são guardadas em uma tabela de “ARPcache” que armazena as informações na memória intermediaria para facilitar a consulta e evitar solicitações repetitivas.



Existe o tempo de expiração dessas entradas em caso de inatividade (o que leva aproximadamente 10 minutos). Após esse período a entrada é removida da tabela. Vale a

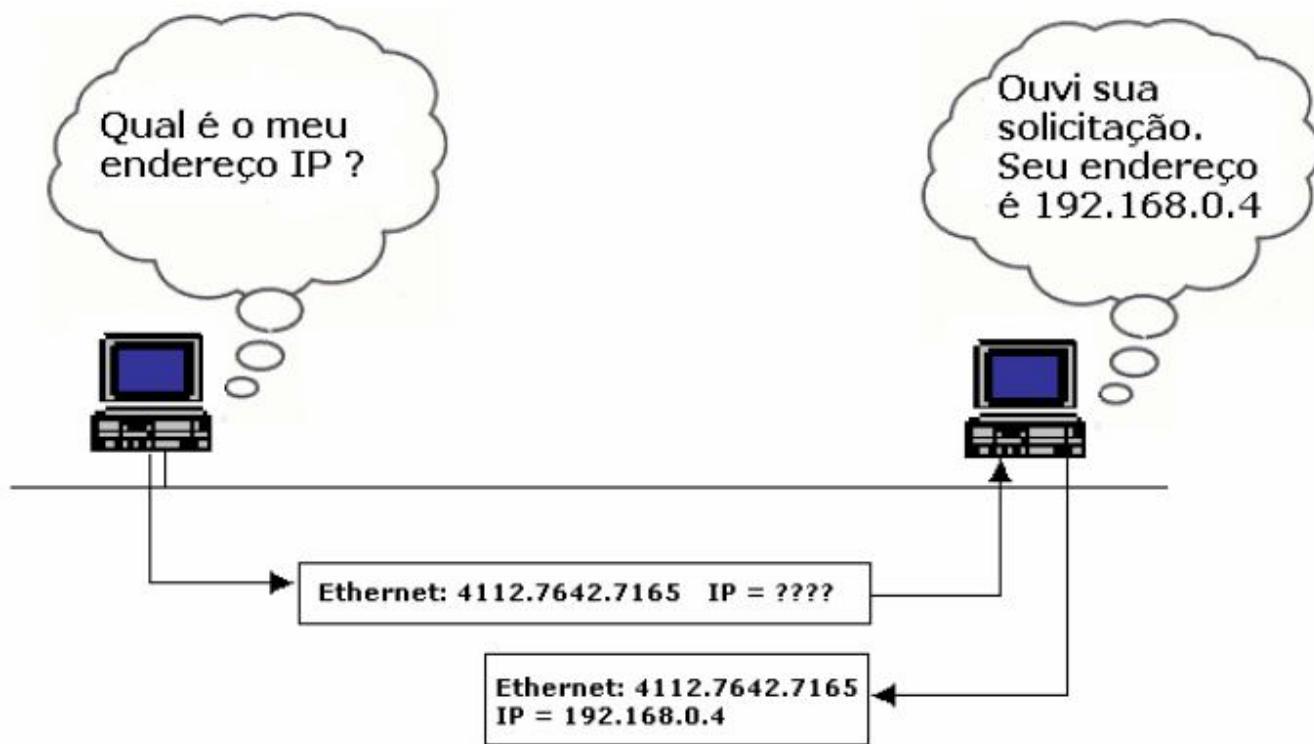
pena lembrar que o mapeamento via ARP somente é necessário em uma rede do tipo compartilhada como Ethernet, Token-Ring, FDDI, etc. Em redes ponto-a-ponto como, por exemplo, um enlace serial, o protocolo ARP não é necessário, já que há somente um destino possível.

O quadro de pacote ARP tem a aparência como apresentado na seguinte figura

	Cabeçalho físico	X bytes
Pacote Arp	Espaço de endereçamento do hardware	2 bytes
	Especo de endereçamento do protocolo	2 bytes
	Comprimento do endereço do hardware (n)	2 bytes
	Comprimento do endereço do protocolo (n)	2 bytes
	Código de operação	2 bytes
	Endereço do hardware de origem	N bytes
	Endereço do protocolo de origem	N bytes
	Endereço do hardware de destino	N bytes
	Endereço do protocolo de destino	N bytes

RARP – Reverse Address Resolution Protocol

Basicamente este protocolo de *Resolução Reversa de Endereços* associa um endereço MAC conhecido a um endereço IP, é utilizado quando uma máquina não tem disco rígido (este tipo de máquinas também é conhecida como terminal tolo), ela não tem como saber seu endereço IP, mas conhece seu endereço MAC. O RARP descobre a identidade do endereço IP para máquinas sem disco, através do envio de um pacote que inclui seu endereço MAC e uma solicitação para o endereço IP atribuído a esse endereço MAC. Uma máquina escolhida, chamada de servidor RARP, retorna a resposta e a crise de identidade termina. O RARP faz uso da informação que conhece a respeito do endereço MAC da máquina para de seu endereço IP e completar a "carteira de identidade" da máquina. Portanto, os dispositivos que usam o RARP exigem que haja um servidor RARP presente na rede para responder às solicitações RARP.

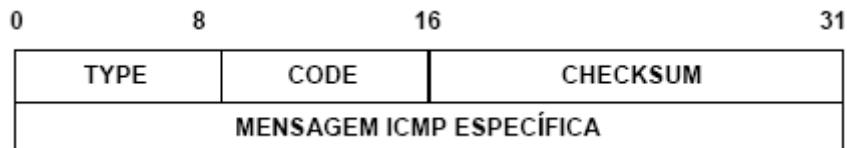


Os protocolos ARP e RARP encontram-se na camada de nível dois (Data Link) do modelo OSI e na camada de nível um (link layer) do modelo TCP/IP.

ICMP – Internet Control Message Protocol

Como estudado na anterior unidade, este protocolo é utilizado para enviar informações de controle e diagnóstico quando ocorre uma mudança ou falha na rede, de certa forma é um auxiliar ao IP, que avisa quando uma ação foi ou deve ser tomada. O ICMP está descrito pelo padrão IETF RFC 792 e têm atualizações para a versão II que estão descritas na RFC 1885 e RFC 1970. O protocolo pode realizar uma série de funções diferentes.

Como a mensagem ICMP é retornada sempre ao computador de origem, não existe nenhum mecanismo para informar erros aos roteadores no caminho ou ao computador de destino. As mensagens ICMP possuem um identificador principal TYPE (tipo) e um identificador de CODE (sub-tipo), conforme pode ser visto no formato de mensagem ICMP abaixo:



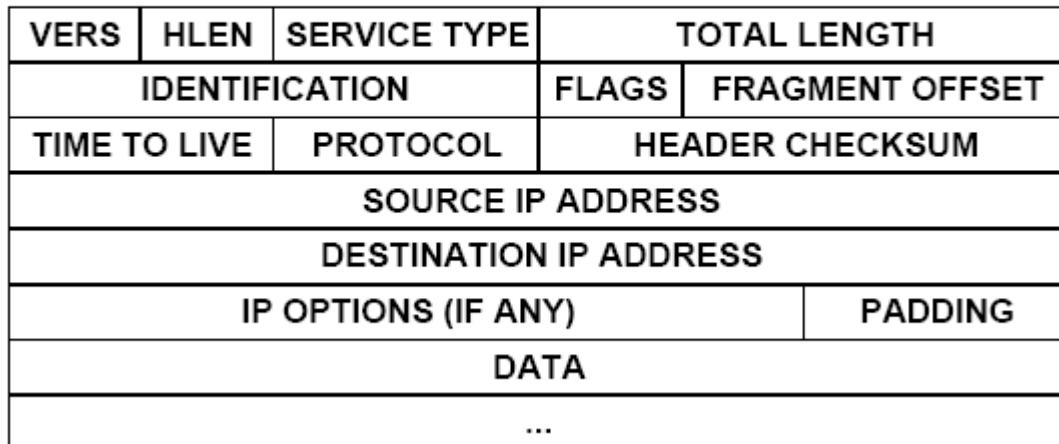
Os tipos de mensagem ICMP são listados na tabela abaixo:

Tipo	Mensagem ICMP	Categoria
0	Echo Reply	Controle
3	Destination Unreachable	Erro
4	Source Quench	Controle
5	Redirect	Controle
8	Echo Request	Controle
9	Router Advertisement (RFC 1256)	Controle
10	Router Solicitation (RFC 1256)	Controle
11	Time Exceeded for a Datagram	Erro
12	Parameter Problem on a Datagram	Erro
13	Timestamp Request	Controle
14	Timestamp Reply	Controle
15	Information Request (obsoleto)	Controle
16	Information Reply (obsoleto)	Controle
17	Address Mark Request	Controle
18	Address Mark Reply	Controle

IP – Internet Protocol

Na estrutura do pacote IP estão definidas as especificações que permitem o protocolo fazer a transmissão de dados e que possibilitam seu envio da origem ao destino. O cabeçalho de um pacote IP possui o formato descrito abaixo:

0	7	15	23	31
Octeto 1	Octeto 2	Octeto 3	Octeto 4	



Os campos mais importantes são descritos abaixo:

VERSION: Informa a versão do protocolo IP sendo carregado. Atualmente a versão de IP é 4 (mas já está em teste o IPV6).

HEADER LENGTH: Informa o tamanho do header IP em grupos de 4 bytes.

TYPE OF SERVICE: Informa como o pacote deve ser tratado, de acordo com sua prioridade e o tipo de serviço desejado como Baixo Retardo, Alta Capacidade de Banda ou Alta Confiabilidade. Normalmente este campo não é utilizado na Internet.

IDENTIFICATION: Identifica o pacote IP unicamente entre os outros transmitidos pela máquina. Este campo é usado para identificar o pacote IP no caso de haver fragmentação em múltiplos datagramas.

FLAGS (3 bits): - um bit (MF - More Fragments) identifica se este datagrama é o último fragmento de um pacote IP ou se existem mais. Outro bit (DNF - Do Not Fragment) informa aos roteadores no caminho se a aplicação exige que os pacotes não sejam fragmentados.

FRAGMENT OFFSET: Informa o posicionamento do fragmento em relação ao pacote IP do qual faz parte.

TIME-TO-LIVE: Este valor é decrementado a cada 1 segundo que o pacote passa na rede e a cada roteador pelo qual ele passa. Serve para limitar a duração do pacote IP e evitar que um pacote seja roteador eternamente na Internet como resultado de um loop de roteamento.

PROTOCOL: Informa que protocolo da camada de Aplicação está sendo utilizado (carregado) no campo de dados. O IP pode transportar mensagens dos seguintes protocolos:

- 1 ICMP Internet Control Message
- 2 IGMP Internet Group Management
- 3 GGP Gateway-to-Gateway Protocol
- 4 TCP TCP – Transmission Protocol
- 8 EGP EGP – Exterior Gateway Protocol
- 17 UDP UDP – User Datagram
- 20 HMP HMP – Host Monitoring
- 22 XNS-IDP Xerox NS IDP
- 27 RDP Reliable Data Protocol
- 28 IRTP Internet Reliable Transaction
- 29 ISO-TP4 ISO Transport Protocol Class 4
- 30 NETBLT Bulk Data Transfer Protocol
- 80 ISO-IP ISO Internet Protocol
- 86 DGP Dissimilar Gateway Protocol
- 87 TCF Transparent Computing Family
- 89 OSPF OSPF – Open Shortest Path First

HEADER CHECKSUM: Valor que ajuda a garantir a integridade do cabeçalho do pacote IP.

SOURCE ADDRESS: Endereço IP da máquina origem do pacote IP.

DESTINATION ADDRESS: Endereço IP da máquina destino do pacote IP.

PADDING (bits **): Este campo possui um comprimento variável e é utilizado para assegurar que o cabeçalho TCP termine e o campo de dados inicie com um comprimento de 32 bits, se isto não ocorrer, então bits 0 serão adicionados (padded) neste campo para dar o comprimento requisitado de 32 bits.

OPTIONS: Opções com informações adicionais para o protocolo IP. Consiste de um byte com a identificação da opção e uma quantidade de bytes variável com as informações específicas. Um pacote IP pode transportar várias opções simultaneamente.



Atividades

Antes de dar continuidades aos seus estudos é fundamental que você acesse sua SALA DE AULA e faça a Atividade 2 no “link” ATIVIDADES.



UNIDADE 19

Objetivo: Entender como a informação é transferida de um ponto a outro na Internet.

Como Funciona A Comunicação TCP/IP

Para uma melhor compreensão de como funciona a comunicação na Internet (via protocolo TCP/IP), é altamente recomendável assistir o filme (produzido pela Ericsson) chamado “Good Warriors” disponível no seguinte link:

<http://www.warriorsofthe.net/>

No site abusar.org (<http://www.abusar.org/tcp-ip3.html>) existem links para a legenda em português do filme em alta qualidade e também uma síntese do que aborda o filme que é muito interessante de se ler.

Um dos melhores programas para se ver o filme com legendas (.srt) se chama BSPlayer e pode ser encontrado em <http://www.bsplayer.org/>. Nesse mesmo site se encontram tutoriais interessantes como leitura de apoio e também comparativos entre os diversos serviços de Internet rápida e seus respectivos valores. Vale a pena perder algum tempo no site e ganhar em conhecimento.

Estrutura Do Endereço IP

Todo protocolo define um tipo de endereçamento para identificar o computador e a rede. O IP tem um endereço de 32 bits, este endereço traz o ID (identificador) da Rede e o ID (identificador) do computador dentro dessa rede.

Exemplificando o computador identifica a estação de trabalho (ou servidor ou dispositivo). Também pode ser chamado de nó ou estação. Os roteadores efetuam o trabalho de localizar os computadores na Internet se utilizando seus endereços IP (que podem ser estáticos ou dinâmicos; cada computador deve ter um endereço IP exclusivo atribuído a ele). O endereço IP de um computador tem quatro bytes divididos em duas partes:

- Um endereço de rede (que pode ter de um a três bytes).
- Um endereço de nó ou de computador (que pode ter de um a três bytes)

Para os endereços IP se utiliza o sistema binário para efetuar a representação dos números. Neste formato binário o endereço IP tem a aparência abaixo, onde os x podem ter o valor de 0 ou 1 (bits):

Byte 1	Byte 2	Byte 3	Byte 4
XXXXXX	XXXXXX	XXXXXX	XXXXXX

Por exemplo, um endereço IP completo em formato binário pode ter o seguinte formato:

11000000.10101000.00000000.00000001

Praticamente este formato binário só poderia ser entendido por um computador, ou seja, neste formato não fica claro visualizar o endereço IP, mas efetuando a conversão para o formato decimal o endereço IP torna-se legível. Nesse exemplo a conversão do endereço IP resulta igual a 192.168.0.1, que resulta muito mais familiar.

Sistema Binário

Para compreender o funcionamento do endereçamento IP é necessário rever o funcionamento de um computador que é baseado em cálculo binário. Este sistema de numeração tem a base 2 e é formado por dois dígitos: 0 e 1.

Os dígitos 0 e 1 são designados por bits e um número binário constituído por 8 bits é chamado de Byte. Um número binário de 16 bits pode ser denominado de “int” (inteiro), um número de 32 bits pode ser chamado de “double int” e números binários de 64 bits são chamados de “long”.

As pessoas no dia a dia preferem fazer uso do sistema decimal por ser mais fácil e familiar, mas é possível efetuar a conversão de um sistema para outro de maneira simples e rápida, por exemplo, se utilizarmos a tabela de conversão de números binários em decimais como apresentada abaixo:

Binário	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	Resultado em Sistema Decimal
Decimal	128	64	32	16	8	4	2	1	255
00000001	0	0	0	0	0	0	0	1	1
00000011	0	0	0	0	0	0	1	1	3
01000100	0	1	0	0	0	1	0	0	68

A soma de todos os números na tabela decimal totaliza 255.

Os números binários são convertidos elevando-se onde existe 1 o seu correspondente a potencia de 2.

Por exemplo, no primeiro caso somente o primeiro bit tem o valor 1 que indica que seu valor é 2^0 que equivale a 1. No segundo caso somente temos os dois primeiros bits como sendo 1, ou seja, utilizando a tabela temos o seguinte valor $2^0 + 2^1 = 1 + 2 = 3$, logo o valor decimal desse número binário $00000011 = 3$. No terceiro caso temos o número binário 01000100, procedendo da mesma forma que no exemplo anterior temos $2^6 + 2^2 = 64 + 4 = 68$, ou seja, o valor binário 01000100 equivale a 68 em decimal.

É altamente aconselhável decorar as potências de 2 e a tabela de conversão básica, pois alguns exames dos maiores fabricantes de software e equipamentos de rede se utilizam de exercícios para criar sub-redes dentro de uma rede, ou seja, dividir a rede em pedaços menores. O efeito de subdividir a rede reduz o tráfego e também acaba com as limitações de

números de computadores disponíveis para uma rede IP. A versão 4 do protocolo IP (IPv4) tem um número limitado de endereços validos para a Internet que estão (aos poucos) se esgotando.

UNIDADE 20

Objetivo: Entender como saber endereçar por Classes uma determinada rede LAN.

Formato E Categorias IP Versão 4 (Ipv4)

A versão 4 do protocolo IP pode suportar 5 classificações para endereçar redes e computadores na Internet, a saber, essa classificação IP é dada por redes Classe A, B, C, D e E.

Normalmente na Internet são utilizados os endereços de classe A, B e C. As redes tipo Classe D e E são reservadas e serão explicadas mais adiante. O que diferencia entre um e outro tipo classe é o número de Bytes que serão utilizados para a identificação da rede e para a identificação do computador dentro dessa rede.

Redes Classe A

Esta classe foi definida como tendo o primeiro bit do número IP como sendo igual a zero. Com isso o primeiro número IP somente poderá variar de 1 até 126 (na prática até 127, mas o número 127 é um número reservado, conforme explicado mais adiante). Observe, no esquema a seguir, que o primeiro bit sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) a que se chega é de 127:

0	1	1	1	1	1	1	1	1
Multiplica por:	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	0x128	1x64	1x32	1x16	1x8	1x4	1x2	1x1
Resulta em:	0	64	32	16	8	4	2	1
Somando tudo:	0+64+32+16+8+4+2+1							
Resulta em:	127							

O número 127 não é utilizado como rede Classe A, pois é um número especial, reservado para fazer referência ao próprio computador. O número 127.0.0.1 é um número especial, conhecido como localhost ou endereço de loopback. Ou seja, sempre que um programa fizer referência a localhost ou ao número 127.0.0.1, estará fazendo referência ao computador onde o programa está sendo executado.

A máscara de sub-rede padrão de uma rede Classe A, foi definida como sendo: **255.0.0.0**.

Com esta máscara de sub-rede observe que temos 8 bits para o endereço da rede e 24 bits para o endereço da máquina dentro da rede. Com base no número de bits para a rede e para as máquinas, podemos determinar quantas redes Classe A podem existir e qual o número máximo de máquinas por rede. Para isso utilizamos a fórmula a seguir:

$$2^n - 2$$

Onde “n” representa o número de bits utilizado para a rede ou para a identificação da máquina dentro da rede. Vamos aos cálculos:

Número De Redes Classe A

Sabe-se que o número de bits para esta classe é 7. Como o primeiro bit sempre é zero, este não varia. Por isso sobram 7 bits (8-1) para formar diferentes redes, fazendo uso da fórmula anterior temos o seguinte resultado:

$$2^7 - 2 = 128 - 2 = 126 \text{ redes Classe A}$$

Número De Máquinas Em Uma Rede Classe A

O número de bits para identificar o endereço da máquina dentro da rede é 24, isto é

$$2^{24} - 2 = 16777216 - 2 = 16777214 \text{ máquinas em cada rede classe A}$$

Como é possível observar, pelos cálculos anteriores, nas redes Classe A existe apenas um pequeno número de redes disponíveis, porém um grande número de máquinas em cada rede.

Já podemos concluir que este número de máquinas, na prática, jamais será instalado em uma única rede. Com isso observe que, com este esquema de endereçamento, teríamos poucas redes Classe A (apenas 126) e com um número muito grande de máquinas em cada rede. Isso causaria desperdício de endereços IP, pois se o endereço de uma rede Classe A fosse disponibilizado para uma empresa, esta utilizaria apenas uma pequena parcela dos endereços disponíveis e todos os demais endereços ficariam sem uso. Para resolver esta questão é que passou-se a utilizar a divisão em sub-redes, assunto este que será visto mais adiante.

Redes Classe B

Esta classe foi definida com os dois primeiros bits do número IP sendo sempre iguais a 1 e 0. Com isso o primeiro número do endereço IP somente poderá variar de 128 até 191. Como o segundo bit é sempre 0, o valor do segundo bit que é 64 nunca é somado para o primeiro

número IP, com isso o valor máximo fica em: $255 - 64 = 191$. Observe, no esquema a seguir, que o primeiro bit sendo 1 e o segundo sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) a que se chega é de 191:

1	0	1	1	1	1	1	1	1
Multiplica por:	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	1×128	0×64	1×32	1×16	1×8	1×4	1×2	1×1
Resulta em:	128	0	32	16	8	4	2	1
Somando tudo:	$128+0+32+16+8+4+2+1$							
Resulta em:	191							

A máscara de sub-rede padrão de uma rede Classe B, foi definida como sendo: **255.255.0.0**.

Com esta máscara de sub-rede temos 16 bits para o endereço da rede e 16 bits para o endereço da máquina dentro da rede. Com base no número de bits para a rede e para as máquinas, podemos determinar quantas redes Classe B podem existir e qual o número máximo de máquinas por rede.

Número De Redes Classe B

O número de bits para esta classe de rede é 14. Como o primeiro e o segundo bit são sempre 10, fixos, não variam, sobram 14 bits ($16-2$) para formar diferentes redes:

$$2^{14} - 2 = 16384 - 2 = 16382 \text{ redes Classe B}$$

Número De Máquinas Em Uma Rede Classe B

O número de bits para identificar o endereço da máquina dentro da rede é 16.

$$2^{16} - 2 = 65536 - 2 = 65534 \text{ máquinas em cada rede classe B}$$

Pode-se observar que as redes Classe B possuem um número razoável de redes, com um bom número de máquinas em cada rede.

O número máximo de máquinas, por rede Classe B já está mais próximo da realidade para as redes de algumas grandes empresas tais como Microsoft, IBM, HP, GM, etc. Mesmo assim, para muitas empresas menores, a utilização de um endereço Classe B, representa um grande desperdício de números IP. Neste sentido é possível usar um número diferente de bits para a máscara de sub-rede, ao invés dos 16 bits definidos pela máscara padrão da Classe B (o que também é possível com Classe A e Classe C). Com isso posso dividir uma rede classe B em várias sub-redes menores, com um número menor de máquinas em cada sub-rede, como será estudado mais adiante.

Redes Classe C

Esta classe foi definida com os três primeiros bits do número IP sempre iguais a 110. Com isso o primeiro número do endereço IP somente poderá variar de 192 até 223. Como o terceiro bit é sempre 0, o valor do terceiro bit que é 32 nunca é somado para o primeiro número IP, com isso o valor máximo fica em: $255 - 32 = 223$.

Observe, no esquema a seguir, que o primeiro bit sendo 1, o segundo bit sendo 1 e o terceiro bit sendo 0, o valor máximo (quando todos os demais bits são iguais a 1) é igual a 223:

1	1	0	1	1	1	1	1	1
Multiplica por:	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
equivale a:	128	64	32	16	8	4	2	1
Multiplicação:	1x128	1x64	0x32	1x16	1x8	1x4	1x2	1x1
Resulta em:	128	64	0	16	8	4	2	1
Somando tudo:	128+64+0+16+8+4+2+1							
Resulta em:	223							

Número De Redes Classe C

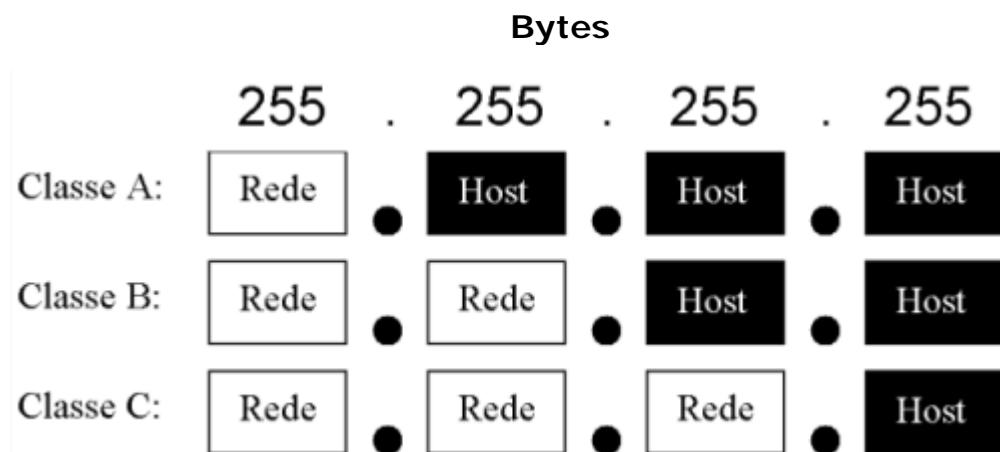
O número de bits para a este tipo de rede é 21. Como o primeiro, o segundo e o terceiro bit são sempre 110 e fixos, não variam, sobram 21 bits (24-3) para formar diferentes redes:

$$2^{21} - 2 = 2.097.152 - 2 = 2.097.150 \text{ redes Classe C.}$$

Número De Máquinas Em Uma Rede Classe C

O número de bits para identificar a máquina: 8, portanto, $2^8 - 2 = 256 - 2 = 254$ máquinas em cada rede classe C

Observa-se que em redes Classe C temos um grande número de redes disponíveis, com, no máximo, 254 máquinas em cada rede. É o ideal para empresas de pequeno porte. Mesmo com a Classe C, existe um grande desperdício de endereços. Imagine uma pequena empresa com apenas 20 máquinas em rede. Usando um endereço Classe C, estariam sendo desperdiçados 234 endereços. Conforme já descrito anteriormente, esta questão do desperdício de endereços IP pode ser resolvida através da utilização de sub-redes.



Redes Classe D

Esta classe de redes foi definida com os quatro primeiros bits do número IP iguais a 1110. A classe D é uma classe especial, reservada para os chamados endereços de Multicast. Com esse valor de bits iniciais temos para esta classe os endereços desde 224.0.0.0 a 239.255.255.255.

Redes Classe E

Esta classe foi definida com os quatro primeiros bits do número IP sempre iguais a 1111. A classe E é uma classe especial e está reservada para uso futuro e/ou funções especiais.

Resumo Para As Classes De Endereço IP

A seguir é apresentada uma tabela com as principais características de cada Classe de Endereços IP:

Classe	Primeiros bits	N.º de redes	N.º de hosts	Máscara padrão
A	0	126	16.777.214	255.0.0.0
B	10	16.382	65.534	255.255.0.0
C	110	2.097.150	254	255.255.255.0
D	1110	Utilizado para tráfego Multicast		
E	1111	Reservado para uso futuro		

Ao configurar uma rede LAN, você pode escolher a classe de endereços mais adequada. Por exemplo, para uma pequena rede, uma faixa de endereços de classe C é a mais apropriada, pois você precisa se preocupar em configurar apenas o último Byte do endereço ao atribuir os endereços. Em uma rede de maior porte, com mais de 254 micros, passa a ser necessário

usar um endereço de classe B, onde podemos usar diferentes combinações de números nos dois últimos Bytes, permitindo um total de 65.534 endereços.

É muito difícil encontrar uma situação onde seja necessário usar uma faixa de endereços de classe A, pois redes muito grandes acabam sendo divididas em vários segmentos diferentes, interligados por roteadores. Neste caso, cada segmento é endereçado como se fosse uma rede separada, usando faixas de classe C ou B.

Na internet, todos os endereços IP disponíveis já possuem dono. A entidade responsável pelo registro e atribuição dos endereços é a ARIN (<http://www.arin.net/>). As operadoras, carriers e provedores de acesso à Internet (ISP) pagam uma taxa anual, que varia de acordo com o volume de endereços requisitados e embutem o custo nos enlaces (links) de comunicações revendidos aos clientes. Os valores cobrados são apenas as taxas da ARIN pelo uso dos endereços, não incluem o custo dos enlaces.

Ao contratar algum tipo de conexão você recebe um único endereço (como numa linha ADSL) ou uma faixa de classe C inteira (ao alugar um backbone, por exemplo). Os endereços de classe B são reservados às grandes empresas e provedores de acesso, enquanto os endereços de classe A são praticamente impossíveis de se conseguir, mesmo para grandes corporações.

Por exemplo, ao alugar um backbone vinculado a uma faixa de endereços classe C, você receberia uma faixa de endereços, digamos, 203.107.171.X, aqui os valores dos três primeiros Bytes dados por 203.107.171 é o endereço de sua rede na Internet, e o último Byte dado por "X" é a faixa de 254 endereços válidos que você pode usar para identificar seus servidores.

Endereços Especiais

Observe que existem endereços reservados para teste, entre os endereços de classe A e B existe o 127. A série de endereços IP iniciada com o número 127 é reservada para testes internos. O endereço de loopback é dado pelo número 127.0.0.1 e é utilizado para fazer

testes e determinar se a comunicação da placa de rede com o meio de transmissão funciona corretamente.

Existem outros números IP reservados descritos abaixo:

1. **10.0.0.0 a 10.255.255.255**
2. **172.16.0.0 a 172.31.255.255**
3. **192.168.0.0 a 192.168.255.255**

Essas faixas de endereços IP são recomendadas para redes privadas, ou seja, para roteamento interno (por exemplo, da nossa Intranet) e não são endereços IP válidos para roteamento externo, ou seja, não podem ser acessados desde fora da corporação.

Apipa (Automatic Private Ip Addressing)

A implementação da pilha de protocolos TCP/IP no sistema operacional WindowsXP Professional suporta conceder o endereço IP para configurações de uma rede básica. Esse mecanismo é uma extensão do endereço IP dinâmico concedido para os adaptadores de rede, ativando as configurações do endereço IP sem usar um endereço IP concedido pelo servidor DHCP. O APIPA é ativado por padrão no WindowsXP Professional para que usuários domésticos ou usuários de pequenas redes possam usar uma única sub-rede, baseado em uma rede TCP/IP sem ter que configurar o protocolo TCP/IP manualmente ou configurar um servidor DHCP.

A seguir apresenta-se o processo básico que o APIPA usa para conceder um endereço IP:

- Quando o Windows XP Professional é inicializado, ele tenta localizar um servidor DHCP sobre a rede para obter um endereço IP dinamicamente.

- Na ausência de um DHCP Server durante a inicialização do computador, o cliente não poderá obter um endereço IP.
- Neste caso, o APIPA gera um endereço IP no intervalo 169.254.0.0 até 169.254.255.255, e uma Máscara de sub-rede 255.255.0.0.
- Agora o cliente consegue alcançar outros clientes que estejam configurados com o APIPA, porém limitando-se somente à rede 169.254.0.0.

Endereços IP Não Válidos

Veja alguns exemplos de endereços IP inválidos:

- **0.xxx.xxx.xxx:** Nenhum endereço IP pode começar com zero, pois ele é usado para o endereço da rede. A única situação em que um endereço começado com zero é usado é quando um servidor DHCP responde à requisição da estação. Como ela ainda não possui um endereço definido, o pacote do servidor é endereçado ao endereço MAC da estação e ao endereço IP "0.0.0.0", o que faz com que o Switch o envie para todos os micros da rede.
- **127.xxx.xxx.xxx:** Nenhum endereço IP pode começar com o número 127, pois este número é reservado para a interface de loopback, ou seja, são destinados à própria máquina que enviou o pacote. Se por exemplo você tiver um servidor de SMTP e configurar seu programa de e-mail para usar o servidor 127.0.0.1, ele acabará usando o servidor instalado na sua própria máquina. O mesmo acontece ao tentar acessar o endereço 127.0.0.1 no navegador: você vai cair em um servidor Web habilitado na sua máquina. Além de testes em geral, a interface de loopback é usada para comunicação entre diversos programas, sobretudo no Linux e outros sistemas UNIX.
- **255.xxx.xxx.xxx, xxx.255.255.255, xxx.xxx.255.255:** Nenhum identificador de rede pode ser 255 e nenhum identificador de computador pode ser composto apenas de endereços 255, seja qual for a classe do endereço, pois estes endereços são usados

para enviar pacotes de broadcast. Outras combinações são permitidas, como em 65.34.255.197 (em um endereço de classe A) ou em 165.32.255.78 (endereço de classe B).

- **xxx.0.0.0, xxx.xxx.0.0:** Nenhum identificador de computador pode ser composto apenas de zeros, seja qual for a classe do endereço, pois estes endereços são reservados para o endereço da rede. Como no exemplo anterior, são permitidas outras combinações como 69.89.0.129 (classe A) ou 149.34.0.95 (classe B).
- **xxx.xxx.xxx.255, xxx.xxx.xxx.0:** Nenhum endereço de classe C pode terminar com 0 ou com 255, pois, como já vimos, um computador não pode ser representado apenas por valores 0 ou 255, já que eles são usados para o envio de pacotes de broadcast.

Se você não pretende conectar sua rede LAN na Internet, pode utilizar qualquer faixa de endereços IP válidos e tudo irá funcionar sem problemas. Mas, a partir do momento em que você resolver conectá-los à Web, os endereços da sua rede poderão entrar em conflito com endereços válidos já usados na Web.

Para resolver este problema, basta utilizar uma das faixas de endereços reservados. Estas faixas são reservadas justamente ao uso em redes internas, por isso não são roteadas na internet. As faixas de endereços reservados mais comuns são **10.X.X.X** e **192.168.X.X**, onde respectivamente o 10 e o 192.168 indicam o endereço da rede, cabe ao administrador do sistema colocar os endereços das máquinas da melhor forma que ele achar conveniente.

A tabela abaixo lista endereços com significado especial e não deve ser utilizada jamais na atribuição de endereços:

Endereço	Utilidade/Função
Rede 0.0.0.0	Este endereço é utilizado para rota default. É usada para simplificar as tabelas de roteamento por IP.
Rede 127.0.0.0	Reservado para loopback. Se utilizando desse endereço se pode testar o micro local como se fosse um host remoto.
Endereço com todos os bits de rede definidos como 0	Serve para se referir a um host da mesma rede. Por exemplo, 0.0.0.18 endereçaria o nó 18 para rede de classe A local.
Endereço com todos os bits de host definidos como 0	Serve para se referir a própria rede. 10.65.0.0 pode ser utilizado para referir-se à rede 10.65. Pode-se encontrar esse tipo de referência na tabelas de roteamento.
Endereço de rede ou de nó com todos os bits definidos como 1	Referente a todos os hosts (nós)
255.255.255.255	Broadcast para todos hosts da rede.

UNIDADE 21

Objetivo: Saber quais são os endereços da Internet que estão registrados.

Endereços IP Registrados

Conforme explicado existem poucos números de endereço IPv4 disponíveis, pois somente é possível navegar na Internet publica através de um número exclusivo. As numerações reservadas para redes internas não possibilitam esse tipo de facilidade e para conseguir acessar algum endereço publico ou disponibilizar algum tipo de serviço que possa ser acessado globalmente é necessário efetuar o registro do número de IP para que seja evitada a sua duplicação.

Atualmente é possível compartilhar a Internet através de um único número IP para que através desse ponto central de acesso através de NAT (Network Address Translator) ou um servidor de Proxy/cache. Este dispositivo ou equipamento funciona como um roteador encaminhando e recebendo pacotes entre a rede interna privada e a internet publica.

O NAT esta definido na RFC 1631, e para mais informação sobre o mesmo entra no seguinte link: <http://www.abusar.org/nat.html>.

Quem é responsável pela atribuição de endereços IP é a Internic (ou se preferir NSI – Network Solutions, Inc). Por força de habito são alocados grandes faixas de endereços de IP primeiramente para os provedores de acesso (ISPs).

Os provedores de acesso disponibilizam ou alocam partes de endereços IP a outros provedores menores ou empresas. E ai esses provedores menores ou empresas disponibilizam o acesso aos usuários finais.

Na historia da Internet ocorreu um corte no orçamento dos EUA em relação à alocação de endereços IP que gerou organizações autoregulamentadas e independentes (sem fins lucrativos) que administraram a atribuição de endereços IP disponibilizados pela InterNIC.

A ARIN (American Registry for Internet Numbers) segue o padrão do RIPE (Reseaux IP Europeans) que administra endereços IP na Europa, na Ásia a APNIC (Ásia Pacific Network Information Center) administra os endereços IP na região do Pacífico Asiático.

Para mais informação sobre o registro IP em diversas regiões é recomendável acessar os sites abaixo:

- ARIN – <http://www.arin.net>
- RIPE – <http://www.ripe.net>
- APNIC – <http://www.apnic.net>

Vale a pena lembrar que esta cada vez mais difícil obter números IP diretamente das organizações de registro, devido a sua escassez.

Porque Criar Sub-Redes IP

Quando se recebe um endereço registrado pode ser que seja necessário fazer uma subdivisão da rede em segmentos menores, conhecidos como sub-redes. Os administradores de rede geralmente criam sub-redes pelos motivos abaixo descritos:

- **Para efetuar a expansão da rede:** Pode ser que seja necessário extrapolar as limitações físicas da rede e que seja necessário adicionar mais computadores e efetuar a criação de uma sub-rede com dispositivos como um roteador inclusive.
- **Para reduzir o congestionamento:** O tráfego entre computadores (nós) em uma rede utiliza parte da banda da rede. Nesse sentido, quantos mais computadores ou dispositivos a rede possuir, mais banda será consumida. A divisão de uma rede em várias redes (menores e separadas) reduz o número de computadores numa mesma rede. Eles podem se comunicar somente com os computadores necessários nessa rede menor e por consequência o congestionamento é drasticamente reduzido.

- **Para reduzir o uso da CPU:** Mesmo que um pacote de rede não seja endereçado a um computador em específico a placa de rede faz a análise do mesmo antes de efetuar o descarte do pacote. Então quantos mais computadores existirem em uma rede maior será o Broadcasts entre os equipamentos; Esta característica de broadcasting pode ser utilizada para, por exemplo, divulgar serviços ou para efetuar descobertas de computadores. O broadcasting é uma característica típica de uma rede Ethernet. Todos os computadores recebem os quadros Ethernet que trafegam pelo cabo da rede, e cada quadro recebido (mesmo aqueles que não sejam dirigidos a eles) deve ser verificado, então nesse processo de aceitar e/ou descartar quadros que uma boa parte dos recursos da CPU é consumida.
- **Facilita a resolução e isola os problemas de rede:** Depois de subdividida a rede é possível identificar com maior facilidade problemas com relação a um computador em específico. Por exemplo, se um computador estiver utilizando uma placa de rede defeituosa, ela pode gerar tempestades de broadcast que poderiam fazer a rede reduzir a sua performance (se chama de placa “tagarela” esse tipo de placa). Até alguns computadores (nós) podem deixar de responder ou parar, pelo excesso de atividade gerada pelo disparo de vários pacotes. Defeitos como os de infra-estrutura física também podem ser mais facilmente identificados (como defeitos físicos, por exemplo, um terminador desconectado).
- **Melhoria da Segurança de Rede:** Com um analisador de protocolo de rede (ou Sniffer) e a configuração adequada (por exemplo, para um switch se efetuar a propagação das difusões para uma porta específica para análise – gerando um ponto central onde se pode ouvir a rede literalmente) Pode-se observar todo o funcionamento dos protocolos de rede e inclusive é possível capturar senhas e dados confidenciais. A Ethernet naturalmente é uma mídia que efetua broadcasting, o que possibilita que todos os computadores tenham acesso aos pacotes de rede (o Switch diminui esse problema, mas poderia se comportar como um hub caso necessário). As sub-redes não são visíveis fora da rede da organização; pode-se encaminhar o pacote a outras sub-redes caso seja necessário ou para se redirecionar a rede correta.

- **Combinar diferentes tipos de mídias:** Podem-se utilizar diferentes tipos de mídias, assim se torna possível combinar sub-redes com diferentes implementações. Equipamentos que usam tecnologias de rede incompatíveis podem ser interconectados dessa forma.

O uso dos endereços de rede local tem aliviado muito o problema da falta de endereços IP válidos, pois uma quantidade enorme de empresas e usuários domésticos, que originalmente precisariam de uma faixa de endereços de classe C para colocar todos os seus micros na internet, pode sobreviver com um único IP válido, compartilhado via NAT entre todos. Em muitos casos, mesmo provedores de acesso chegam a vender conexões com endereços de rede interna nos planos mais baratos, como, por exemplo, alguns planos de acesso via rádio enlace, onde um roteador com um IP válido distribui endereço de rede interna (conexão compartilhada) para os assinantes.

UNIDADE 22

Objetivo: Entender em detalhe como projetar e endereçar uma rede IP.

Criando Sub-Redes

Basicamente, para a criação de sub-redes devem ser tomadas em consideração 3 tópicos, a saber:

1. Determinar o número de bits de máquina a serem usados para sub-redes.
2. Listar as novas identificações de sub-redes.
3. Listar os endereços IP para cada nova identificação de sub-rede.

Determinar o número de bits de computadores a serem usados para sub-redes. Uma das primeiras tarefas é determinar o número de computadores a serem alocados em uma sub-rede. Existem casos em que se pode dividir uma rede classe C (254 computadores, geralmente se descarta o “0” e o “255”) em redes menores que podem comportar menos máquinas. Também existem casos em que se pode necessitar de sub-redes com mais de 256 equipamentos, neste caso devemos fazer uso de mais bits de máscara para cobrir a demanda de computadores.

A principal mudança que se nota ao mexer com sub-redes é uma mudança na máscara do endereço IP que irá variar conforme a quantidade de bits usada para o endereçamento de sub-rede. Inclusive é bom pensar muito bem antes de escolher o número de bits de máquina, pois se deve levar em conta o crescimento da rede (número de computadores) e a quantidade de sub-redes a serem criadas (para evitar transtornos ou o trabalho de trocar os dados IP).

Como estudado anteriormente, o número de sub-redes disponíveis é $2^n - 2$, onde “n” é o número de bits disponíveis para utilização no endereço de sub-rede. A subtração feita por 2 é porque tanto os endereços com os bits 0 assim como os endereços com os bits 1 são reservados nas redes TCP/IP. Normalmente o endereço com os bits 0s é o próprio endereço de rede e o endereço com os bits 1 é o endereço de broadcasting da rede. As RFC 1122 e RFC 950 determinam esse tipo de restrição (No entanto alguns sistemas operacionais conseguem utilizar esse tipo de endereço caso o roteador consiga ser direcionado para uma sub-rede zero).

A seguir seguem as tabelas para criação de sub-redes para as redes Classe A, B e C.

Rede classe A – Subdivisões de Rede			
Nº de Sub-redes	Nº de bits para sub-rede	Máscara de sub-rede	Nº de hosts por sub-rede
1-2	1	255.128.0.0 ou /9	8,388,606
3-4	2	255.192.0.0 ou /10	4,194,302
5-8	3	255.224.0.0 ou /11	2,097,150
9-16	4	255.240.0.0 ou /12	1,048,574
17-32	5	255.248.0.0 ou /13	524,286
33-64	6	255.252.0.0 ou /14	262,142
65-128	7	255.254.0.0 ou /15	131,070
129-256	8	255.255.0.0 ou /16	65,534
257-512	9	255.255.128.0 ou /17	32,766
513-1,024	10	255.255.192.0 ou /18	16,382
1,025-2,048	11	255.255.224.0 ou /19	8,190
2,049-4,096	12	255.255.240.0 ou /20	4,094
4,097-8,192	13	255.255.248.0 ou /21	2,046
8,193-16,384	14	255.255.252.0 ou /22	1,022
16,385-32,768	15	255.255.254.0 ou /23	510
32,769-65,536	16	255.255.255.0 ou /24	254
65,537-131,072	17	255.255.255.128 ou /25	126
131,073-262,144	18	255.255.255.192 ou /26	62
262,145-524,288	19	255.255.255.224 ou /27	30
524,289-1,048,576	20	255.255.255.240 ou /28	14
1,048,577-2,097,152	21	255.255.255.248 ou /29	6
2,097,153-4,194,304	22	255.255.255.252 ou /30	2

Rede classe B – Subdivisões de Rede

Nº de Sub-redes	Nº de bits para sub-rede	Máscara de sub-rede	Nº de hosts por sub-rede
1-2	1	255.255.128.0 ou /17	132,766
3-4	2	255.255.192.0 ou /18	16,382
5-8	3	255.255.224.0 ou /19	8,190
9-16	4	255.255.240.0 ou /20	4,094
17-32	5	255.255.248.0 ou /21	2,046
33-64	6	255.255.252.0 ou /22	1,022
65-128	7	255.255.254.0 ou /23	510
129-256	8	255.255.255.0 ou /24	254
257-512	9	255.255.255.128 ou /25	126
513-1,024	10	255.255.255.192 ou /26	62
1,025-2,048	11	255.255.255.224 ou /27	30
2,049-4,096	12	255.255.255.240 ou /28	14
4,097-8,192	13	255.255.255.248 ou /29	6
8,193-16,384	14	255.255.255.252 ou /30	2

Rede classe C – Subdivisões de Rede

Nº de Sub-redes	Nº de bits para sub-rede	Máscara de sub-rede	Nº de hosts por sub-rede
1-2	1	255.255.255.128 ou /25	126
3-4	2	255.255.255.192 ou /26	62
5-8	3	255.255.255.224 ou /27	30
9-16	4	255.255.255.240 ou /28	14
17-32	5	255.255.255.248 ou /29	6
33-64	6	255.255.255.252 ou /30	2

Cálculo de Sub-Redes

Para poder criar sub-redes em uma rede, a única forma é alterar a máscara de rede padrão, isto é, devemos **emprestar** um ou mais bits 0 que correspondem ao endereçamento dos computadores dentro da rede, esses bits emprestados farão parte dos **bits de rede** (bits 1).

Por exemplo, temos o endereço de rede dado por **192.168.1.0**, este endereço corresponde a uma rede Classe C. Agora, para se ter duas sub-redes em esta rede Classe C basta emprestar um único bit do grupo de bits de máquina (bits 0) e invertê-lo para que faça parte do grupo de bits de rede (bits 1).

Lembremos que para este tipo de redes Classe C a máscara padrão é de 24 bits “1”, esses 24 bits correspondem ao endereço de rede e os 8 bits 0 correspondem para endereçar os computadores dentro dessa rede, ou seja,

11111111.11111111.11111111.00000000 = 255.255.255.0

Agora, empresta-se um bit dos “bits de máquina” (bits “0”) para, assim, termos 25 “bits de rede”, ou seja, 25 bits “1”, o resultado seria uma nova máscara de rede dada por:

11111111.11111111.11111111.10000000 = 255.255.255.128

Com esta nova máscara de rede é possível criar duas sub-redes internas à nossa rede total. Vejamos como foi emprestado só um bit e como estamos trabalhando com uma rede Classe C, então fazemos uso desse único bit para fazer a diferença entre as duas redes, portanto, a primeira sub-rede é dada pelo endereço 192.168.1.0 e a segunda sub-rede é dada pelo endereço 192.168.1.128. Mas estes endereços são os endereços das sub-redes, para endereçar as máquinas temos os endereços da primeira sub-rede a partir de 192.168.1.1 até 192.168.1.126, e os endereços para os computadores da segunda sub-rede vão desde 192.168.1.129 até 192.168.1.254. Claramente vemos que cada sub-rede suportará 127

máquinas. Os endereços de broadcasting dessas duas sub-redes são: 192.168.1.127 e 192.168.1.255.

Um site onde se pode encontrar uma calculadora de sub-redes esta no seguinte link:
<http://www.warriorsofthe.net/utils/index.html>.

Exemplo De Cálculo De Sub-Redes

Considerar o endereço de rede Classe A 11.1.2.64, pede-se trabalhar esse endereço como se fosse uma rede Classe C e crie duas sub-redes utilizando dois bits do grupo de bits de máquina (bits 0), mostre os endereços de broadcasting para essas sub-redes e calcule quantos computadores cada uma delas suportará.

Como o exemplo pede para trabalhar essa rede Classe A como se fosse uma rede Classe C então podemos, em princípio, assumir a máscara padrão de uma Classe C, isto é, inicialmente teríamos 24 bits 1, ou seja:

11111111.11111111.11111111.00000000 = 255.255.255.0

Como ainda o exemplo pede para utilizar dois bits do grupo de bits de máquina (bits 0) a nova máscara de sub-rede será:

11111111.11111111.11111111.11000000 = 255.255.255.192

Para facilitar as contas vamos diferenciar os 26 bits de rede (em azul) dos bits de máquina (em vermelho).

00001011.00000001.00000010.01000000 = 11.1.2.64

Endereço De Broadcast

Para calcular este endereço basta colocar, após o último bit 1 do endereço de rede original (11.1.2.64), todos os bits como sendo bits 1, assim para este exemplo, o endereço de Broadcasting fica da seguinte forma:

00001011.00000001.00000010.0111111 = 11.1.2.127

Cálculo Das Sub-Redes

Para criar as sub-redes devemos utilizar os bits que fazem parte do endereço de rede do último Byte, neste exemplo pedem para usar somente dois bits do grupo de bits de máquina (bits 0). A pergunta que surge imediatamente seria porque usar só 2 bits? A resposta esta no fato que essa rede Classe A esta sendo usada como uma rede Classe C, se a nossa intenção seria trabalhar com essa rede como se fosse uma rede Classe B então teríamos a liberdade de utilizar também todo o terceiro Byte para criar as sub-redes que vejamos convenientes.

Portanto, contamos somente com dois bits (do último Byte) para poder criar as sub-redes, isto é, com 2 bits podemos ter $2^2 - 2 = 2$ sub-redes válidas, a seguinte Tabela mostra quais são elas:

2 Bits de Sub-rede	Endereços de Sub-rede
00	Endereço usado para a máscara de Sub-rede
01	Endereço de Sub-rede válido
10	Endereço de Sub-rede válido
11	Endereço usado para Broadcasting

Desses 4 valores somente os valores 01 e 10 são válidos, os valores 00 e 11 não são válidos para endereçar máquinas porque com 00 temos o próprio endereço da sub-rede 11.1.2.64 e com 11 temos o endereço de Broadcasting, consequentemente só temos duas sub-redes cujos endereços são:

00001011.00000001.00000010.**01000000** = **11.1.2.64**

e

00001011.00000001.00000010.**10000000** = **11.1.2.128**

Cada uma das subredes pode suportar $2^6 - 2 = 62$ computadores, aqui subtraímos os endereços de Broadcasting e de rede já que estes não contam como endereços válidos para as máquinas, o termo 2^6 surge do fato de só possuirmos 6 bits para endereçar as máquinas.

Sub-rede 11.1.2.64:

Os endereços de máquina IP válidos para esta sub-rede vão:

Desde 11.1.2.65 = 00001011.00000001.00000010.**01000001**

Até 11.1.2.126 = 00001011.00000001.00000010.**01111110**

Sub-rede: 00001011.00000001.00000010.**01000000** = **11.1.2.64**

Broadcasting: 00001011.00000001.00000010.**01111111** = **11.1.2.127**

Sub-rede 11.1.2.128:

Os endereços de máquina IP válidos para esta sub-rede vão:

Desde 11.1.2.129 = 00001011.00000001.00000010.**10000001**

Até 11.1.2.190 = 00001011.00000001.00000010.**10111110**

Sub-rede: 00001011.00000001.00000010.**10000000** = 11.1.2.128

Broadcasting: 00001011.00000001.00000010.**10111111** = 11.1.2.191

Listando as Faixas de Endereços Dentro de Cada Sub-Rede

Vamos entender esta questão através de um exemplo prático como explicado a seguir. Deseja-se dividir a seguinte rede classe C: 129.45.32.0/255.255.255.0. As especificações são as seguintes: ter como mínimo 10 sub-redes. Nestas condições, pede-se determinar o seguinte:

Quantos bits serão necessários para fazer a divisão e obter pelo menos 10 sub-redes?

Quantos números IP (para as máquinas) estarão disponíveis em cada sub-rede?

Qual a nova máscara de sub-rede?

Listar a faixa de endereços de cada sub-rede.

Para responder a questão do item **(a)**, fazemos uso da fórmula:

$$\text{Número de sub-redes} = 2^n - 2$$

Aqui vamos testando o valor de n (o número de bits emprestados) por valores sucessivos, até atingir ou superar o valor de 10. Por exemplo, para n=2, a fórmula resulta em 2, para n=3, a fórmula resulta em 6, para n=4 a fórmula resulta em 14. Como 14 é maior a 10 a questão do item **(a)** está respondida, temos que emprestar quatro bits do quarto Byte para fazer parte da máscara de sub-rede. Lembre-se que o quarto Byte corresponde aos endereços das máquinas (bits 0).

Portanto, quantos bits serão necessários para fazer a divisão e obter pelo menos 10 sub-redes? A resposta é: 4 bits.

Como vamos a utilizar quatro bits do último Byte (além dos 24 bits dos três primeiros Bytes, os quais já faziam parte da máscara padrão da rede Classe C original), sobraram apenas 4 bits para os endereços IP que devem ser alocados para os computadores em cada sub-rede. Novamente fazemos uso da fórmula:

$$\text{Número de endereços IP dentro de cada sub-rede} = 2^n - 2$$

Substituindo n por 4, vamos obter um valor de 14. Com este resultado já podemos responder o item **(b)**, isto é, quantos endereços IP para os computadores estarão disponíveis em cada sub-rede? A resposta é: 14.

Como foram utilizados quatro bits do quarto Byte para fazer a divisão em sub-redes, os quatro primeiros bits foram definidos iguais a 1 (bits de rede). Basta somar os respectivos valores, ou seja: $128 + 64 + 32 + 16 = 240$. Ou seja, com os quatro primeiros bits do quarto Byte sendo iguais a 1, o valor do quarto Byte passa para 240, com esse resultado podemos responder o item **(c)** que diz: Qual a nova máscara de sub-rede? A resposta é dada por

$$11111111.11111111.11111111.11110000 = 255.255.255.\mathbf{240}$$

É importante lembrar que esta será a máscara de sub-rede utilizada por todas as 14 sub-redes.

Agora vamos listar a faixa de endereços de cada sub-rede. Esta é a novidade do item **(d)**. Como saber de que número até que número vai cada endereço IP. Observe o último bit definido para a máscara. No nosso exemplo é o quarto bit do quarto Byte. Qual o valor decimal do quarto bit? 16 (o primeiro é 128, o segundo 64, o terceiro 32 e assim por diante, conforme explicado na Tabela anterior).

O valor do último bit é um indicativo das faixas de variação para este exemplo. Ou seja, na prática temos 16 computadores em cada sub-rede, embora o primeiro e o último não devam ser utilizados, pois o primeiro é o endereço da própria sub-rede e o último é o endereço de

broadcast da sub-rede. Por isso é que só será possível alocar 14 computadores por sub-rede, devido ao ‘-2’ na fórmula anterior, pode-se observar que esse ‘-2’ significa: o primeiro e o último.

Ao listar as faixas, porém consideramos os 16 endereços, só lembrando que o primeiro e o último endereços não são utilizados para identificar uma máquina. Com isso a primeira sub-rede vai do 0 até o 15, a segunda sub-rede do 16 até o 31, a terceira do 32 até o 47 e assim por diante.

Finalmente apresentamos a divisão da rede em 14 sub-redes, onde cada sub-rede fica com 16 endereços IP para distribuí-los nas máquinas, sendo que a primeira e a última sub-rede não são utilizadas e o primeiro e o último endereço IP, dentro de cada sub-rede, também não são utilizados:

Sub-rede 01:129.45.32.0	→	129.45.32.15
Sub-rede 02:129.45.32.16	→	129.45.32.31
Sub-rede 03:129.45.32.32	→	129.45.32.47
Sub-rede 04:129.45.32.48	→	129.45.32.63
Sub-rede 05:129.45.32.64	→	129.45.32.79
Sub-rede 06:129.45.32.80	→	129.45.32.95
Sub-rede 07:129.45.32.96	→	129.45.32.111
Sub-rede 08:129.45.32.112	→	129.45.32.127
Sub-rede 09:129.45.32.128	→	129.45.32.143
Sub-rede 10:129.45.32.144	→	129.45.32.159
Sub-rede 11:129.45.32.160	→	129.45.32.175
Sub-rede 12:129.45.32.176	→	129.45.32.191

Sub-rede 13: 129.45.32.192	→	129.45.32.207
Sub-rede 14: 129.45.32.208	→	129.45.32.223
Sub-rede 15: 129.45.32.224	→	129.45.32.239
Sub-rede 16: 129.45.32.240	→	129.45.32.255

CIDR – Classless Inter-Domain Routing

A divisão tradicional, com as classes A, B e C de endereços IP fazia com que um grande número de endereços fossem desperdiçados. Entender as classes de endereços A, B e C é importante para compreender o uso das máscaras de sub-rede e por isso elas ainda são muito estudadas, mas é importante ter em mente que, na prática, elas são uma designação obsoleta. Atualmente é utilizado o sistema CIDR, onde são utilizadas máscaras de tamanho variável, que permitem uma flexibilidade muito maior na criação das faixas de endereços.

O conceito de CIDR foi introduzido em 1993 como um refinamento para a forma como o tráfego era conduzido pelas redes IP. Permitindo flexibilidade acrescida quando dividindo margens de endereços IP em redes separadas, promoveu assim um uso mais eficiente para os endereços IP cada vez mais escassos. O CIDR está definido no RFC 1519.

Os endereços IP (versão 4) IPv4 têm 32 bits de comprimento e estão separados em duas partes: o endereço de rede (que identifica toda a rede ou sub-rede), e o endereço do computador (que identifica uma ligação a uma máquina em particular ou uma interface para essa rede). Máscaras de sub-rede são máscaras de bits que mostram onde o endereço de rede termina (bits 1) e o endereço de máquina começa (bits 0).

A notação CIDR padrão começa com o endereço de rede, na direita com o número apropriado de Bytes:

- 4 para IPv4,
- E (campos hexadecimais de) 8 Bytes de 16 bits para IPv6.

Tudo isto é seguido por um prefixo **/n** que indica o comprimento, em bits, que define o tamanho do campo de sub-rede em questão, este prefixo é, na verdade, o comprimento da máscara de sub-rede. Portanto, a nomenclatura CIDR para o IPv4 é: X.Y.Z.W/n, onde X, Y, Z e W são os 4 Bytes comuns de endereço Internet, e o prefixo **/n** indica quantos bits (de valor 1) serão utilizados para o endereço de rede.

Temos a maneira de exemplo o seguinte:

192.168.0.0 **/24** representa os 256 endereços IPv4 de 192.168.0.0 até 192.168.0.255 inclusive, sendo este último (192.168.0.255) o endereço de broadcast para a rede.

192.168.0.0 **/22** representa os 1024 endereços IPv4 de 192.168.0.0 até 192.168.3.255 inclusive, com 192.168.3.255 sendo o endereço de broadcast para a rede.

2002:C0A8::**/48** representa os endereços IPv6 de 2002:C0A8:0:0:0:0:0:0 até 2002:C0A8:0:FFFF:FFFF:FFFF:FFFF, inclusive.

Para o IPv4, uma representação alternativa usa o endereço de rede seguido da máscara de sub-rede, escrito na forma decimal com pontos:

192.168.0.0 **/24** pode ser escrito como 192.168.0.0 **255.255.255.0**

192.168.0.0 **/22** pode ser escrito como 192.168.0.0 **255.255.252.0**

UNIDADE 23

Objetivo: Entender o que é, e porque foi desenvolvida uma nova versão do protocolo IP.

IPv6

A Importância Do IPv6

O endereçamento de redes IP é sempre um tema importantíssimo, já que é justamente um bom endereçamento de rede que permite ao enorme número de computadores (que formam a Internet) possam se comunicar uns com os outros.

Como se sabe, o atual IPv4, que utilizamos na grande maioria das situações, é um número de 32 bits (4 Bytes) que equivale a nada menos do que $2^{32} = 4.294.967.296$ combinações. Destes, pouco mais de 3.7 bilhões de endereços são aproveitáveis, já que os endereços iniciados com 0, 10, 127 e de 224 em diante são reservados.

Além disso, a maior parte das faixas de endereços de classe A, que englobam as faixas iniciadas com de 1 a 126 são propriedade de grandes empresas, que acabam utilizando apenas uma pequena faixa deles. Por exemplo, apenas a HP, sozinha, tem direito a duas faixas inteiras, uma ganha durante a distribuição inicial das faixas de endereços IP classe A e a segunda herdada com a compra da DEC.

No início de 2007, já restavam apenas 1.3 bilhões de endereços disponíveis. Se a procura se mantiver nos níveis atuais, teremos o esgotamento dos endereços disponíveis em 2014. Caso ela cresça, impulsionada pela popularização das conexões 3G, uso do ADSL em países desenvolvidos, aumento do número de servidores Web, popularização do ADSL nos países mais pobres e assim por diante, podemos chegar a uma situação caótica ainda em 2012!

Um dos fatores que vem reduzindo a pressão sobre os escassos endereços disponíveis é o uso do NAT. Graças a ele, você pode compartilhar uma única conexão (e,

conseqüentemente, um único endereço), entre vários micros. É possível até mesmo adicionar um segundo, terceiro, quarto, ou mesmo quinto nível de compartilhamento, recompartilhando uma conexão já compartilhada.

É muito comum, por exemplo, que um provedor de acesso via rádio use um único IP para um prédio inteiro, dando endereços de rede interna para os assinantes. Muitos destes criam redes domésticas e compartilham novamente a conexão, adicionando uma segunda camada de NAT, e assim vai.

Apesar disso, o NAT não é a solução para tudo. Você não pode usar NAT em um Datacenter, por exemplo, precisa de um endereço "real e válido" para cada servidor disponível para o mundo exterior.

Chegamos então ao IPv6, que promete colocar ordem na casa, oferecendo uma faixa muito maior de endereços e uma migração suave a partir do padrão atual (IPv4). Embora só recentemente o tema tenha ganhado popularidade, o IPv6 não é exatamente um projeto novo. O padrão vem sendo desenvolvido desde 1995, quando a Internet (como a conhecemos agora) ainda engatinhava. Entre os dois existiu o "IPv5", que era um padrão de Streaming que nunca chegou realmente a ser usado.

Endereçamento IPv6

O IPv6 é a nova versão do Protocolo de Internet, a qual deverá substituir progressivamente o protocolo atual da Internet, o IPv4, estendendo o espaço de endereçamento corrente para (nada mais nem nada menos do que) 128 bits.

No Brasil, toda a rede nacional de pacotes (RNP) está apta a operar com o protocolo IPv6 em modo nativo. Para obter serviços de conexão IPv6, a instituição deve estar localizada em um dos estados servidos por esta rede e ser cliente da RNP. Endereços IPv6 de produção para o Brasil podem ser obtidos no LACNIC: <http://www.lacnic.net>.

Prevendo o tamanho do problema que seria ter que futuramente migrar novamente para um novo padrão, o IETF (o órgão responsável) resolveu não correr riscos. O número de endereços disponíveis no IPv6 é simplesmente absurdo. Seria o número 340.282.366.920 seguido por mais 27 casas decimais!

Já existem projetos de uso do IPv6 em larga escala em países como o Japão, China e Coréia do Sul e a adoção tende a se acelerar rapidamente no decorrer dos próximos anos.

Nos endereços IPV4, dividimos os endereços em 4 grupos de 8 bits, cada um deles representado por um número de 0 a 255, como em "206.45.32.234". Usar esta mesma nomenclatura seria inviável para o IPV6, pois teríamos nada menos do que 16 Bytes, criando endereços enormes, como por exemplo:

"232.234.12.43.45.65.132.54.45.43.232.121.45.154.34.78", algo impraticável.

Por tal motivo, os endereços IPv6 utilizam 8 quartetos de caracteres em Hexadecimal separados por "dois pontos" (:).

Como é sabido cada caráter Hexadecimal, representa 4 bits (16 combinações). Além disso, a numeração Hexadecimal consta dos valores alfanuméricos dados por A, B, C, D, E e F, que representam os números decimais 10, 11, 12, 13, 14 e 15 respectivamente.

Um exemplo de endereço IPv6, válido atualmente na Internet, seria:

2001:BCE4:5641:3412:341:45AE:FE32:65.

Como se pode ver, a idéia de usar os caracteres em Hexadecimal reduz o número de caracteres necessários, mas em compensação complica um pouco as coisas em relação à notação do IPv4, com a qual estamos acostumados.

Uma forma de compreender melhor, seria imaginar que cada quarteto de números Hexadecimais equivale a 16 bits, que poderiam ser representados por um número de 0 a

65.535. Você pode usar uma calculadora que suporte a exibição de números em Hexadecimal para converter números decimais. Portanto, fazendo a conversão, o endereço dado acima por: 2001:bce4:5641:3412:341:45ae:fe32:65

Equivaleria aos números decimais "8193 48356 22081 13330 833 17835 65034 101".

Um atenuante para esta complexidade dos endereços IPv6 é que eles podem ser abreviados de diversas formas. Graças a isso, os endereços IPv6 podem acabar sendo incrivelmente compactos, como "::1" ou "FEC::1".

Em primeiro lugar, todos os zeros à esquerda dentro dos quartetos podem ser omitidos. Por exemplo, em lugar de escrever "0341", pode-se escrever apenas "341"; em lugar de "0001" apenas "1" e, em lugar de "0000" apenas "0", sem que o significado seja alterado. É por isso que muitos quartetos dentro dos endereços IPv6 podem ter 3, 2 ou mesmo um único dígito. Os demais são zeros à esquerda que foram omitidos.

É muito comum que os endereços IPV6 incluam seqüências de números 0, já que atualmente poucos endereços são usados, de forma que os donos preferem simplificar bastante as coisas. Por tal motivo, o endereço "2001:BCE4:0:0:0:0:1" poderia ser abreviado para apenas "2001:BCE4::1", omitimos todo o trecho central "0:0:0:0".

Ao usar o endereço, o sistema sabe que entre o "2001:BCE4:" e o ":1" existem apenas zeros e faz a conversão internamente, sem problema algum.

É possível observar que as mudanças no sistema de endereçamento é uma das inovações mais importantes do IPv6. Como já dito, este passa a ser de 128 bits (contra os 32 bits do IPv4).

Teoricamente, o número de endereços IP pode chegar a ultrapassar de maneira simples a casa dos trilhões, vejamos $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$, um número astronômico! Mas esse número binário de 128 bits possibilita um método mais simples de auto-configuração através do uso da identificação EUI-64 da maior parte das interfaces de rede.

A tabela abaixo apresenta alguns exemplos de endereçamento IPv6 tanto na sua representação extensa como na forma abreviada:

Endereço	Representação Extensa	Forma Abreviada
Unicast	3FFE:3102:0:0:8:800:200C:417A	3FFE:3102::8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:43	FF01::43
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

A terceira opção é utilizada na representação de endereçamento compatível IPv6-IPv4, sendo útil no período de migração e de coexistência de ambos os protocolos. Assim utilizamos a representação X:X:X:X:X:X:Z.Z.Z.Z, onde os "X" indicam números hexadecimais (16 bits) e os "Z" são valores que representam os 8 bits referentes ao endereço IPv6

0:0:0:0:0:192.168.1.1 (IPv6) = :192.168.1.1 (IPv4)

Graças a isso, determinados equipamentos poderão ter mais de um IP. Assim, será possível fazer com que certos serviços sejam executados simultaneamente numa mesma máquina e para cada um haverá uma conexão exclusiva.

Para o uso de mais de um IP em um mesmo dispositivo, foram criados os seguintes esquemas: Unicast, Multicast e Anycast descritos a seguir.

Unicast

Neste esquema, um determinado dispositivo pode ter mais de um endereço. Portanto, tais endereços são divididos em grupos. Foram definidos vários tipos de endereços unicast, que são:

unicast (1:1)



- **Global Provider-based:** É o endereço unicast que será globalmente utilizado. Seu plano inicial de alocação baseia-se no mesmo esquema utilizado no CIDR (RFC 1519) definido em (RFC 1887). Seu formato possui um prefixo de 3 bits (010) e cinco campos: Registry ID, para registro da parte alocada ao provedor; Provider ID, que identifica um provedor específico; Subscriber ID, que identifica os assinantes conectados a um provedor; e Infra-subscriber, parte utilizada por cada assinante.
- **Unspecified:** Definido como 0:0:0:0:0:0:0:0 ou "::", indica a ausência de um endereço e nunca deverá ser utilizado em nenhum nó de rede. Este endereço só poderá ser utilizado como endereço de origem (Source Address) de estações ainda não inicializadas, ou seja, que ainda não tenham aprendido seus próprios endereços.
- **Loopback:** Representado por 0:0:0:0:0:0:0:1 ou "::1". Pode ser utilizado apenas quando um nó envia um datagrama para si mesmo. O Loopback não pode ser associado a nenhuma interface.
- **IPv4-based:** Um endereço IPv6 com um endereço IPv4 embutido. Formado anexando-se um prefixo nulo (96 bits zeros) a um endereço IPv4 como, ::172.16.25.32, por exemplo. Este tipo de endereço foi incluído como mecanismo de transição para computadores e roteadores fazerem o tunelamento de pacotes IPv6

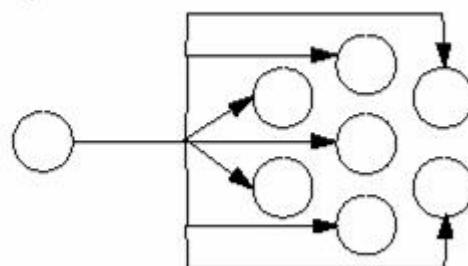
sobre roteamento IPv4. Para computadores sem suporte a IPv6, foi definido um outro tipo de endereço (IPv4 mapped IPv6) da seguinte forma, ::FFFF:172.16.25.32.

- **NSAP:** endereço de 121 bits a ser definido, identificado pelo prefixo 0000001. Endereços NSAP (Network Service Access Point) são utilizados em sistemas OSI.
- **IPX:** endereço de 121 bits a ser definido, identificado pelo prefixo 0000010. Endereços IPX (Internal Packet eXchange) são utilizados em redes Netware/Novell.
- **Link-Local:** endereço identificado pelo prefixo de 10 bits (1111111010), definido para uso interno num único link. Estações ainda não configuradas, ou com um endereço provider-based ou com um site-local, poderão utilizar um endereço link-local.
- **Site-Local:** endereço identificado pelo prefixo de 10 bits (1111111011), definido para uso interno numa organização que não se conectará à Internet. Os roteadores não devem repassar pacotes cujos endereços origem sejam endereços do tipo site-local.
- Também está reservado 12,5% de todo espaço de endereçamento IPv6 para endereços a serem distribuídos geograficamente (Geographic-based Addresses).

Multicast

Neste esquema, um único dispositivo consegue identificar várias interfaces na rede, permitindo o envio individual de pacotes.

multicast (1: n)

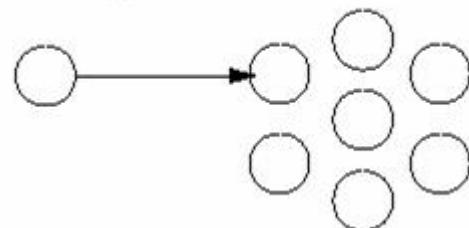


Igualmente ao endereço anycast, este endereço identifica um grupo de interfaces, mas um pacote destinado a um endereço multicast é enviado para todas as interfaces do grupo. As funcionalidades de multicasting foram formalmente incorporadas ao IPv4 em 1988, com a definição dos endereços classe D e do IGMP (Internet Group Management Protocol), e ganhou força com o advento do MBONE (Multicasting Backbone), mas seu uso ainda não é universal. Desta vez, estas funcionalidades foram automaticamente incorporadas ao IPv6. Isto significa que não mais será necessário implementar túneis MBONE, pois todos os computadores e roteadores IPv6 deverão suportar multicasting.

Anycast

Este tipo é uma variação do multicast, onde o endereço IP pode estar atribuído a mais de uma interface, ao invés de uma individual.

anycast (1: nearest)



Identifica um grupo de interfaces de nós diferentes. Um pacote destinado a um endereço anycast é enviado para uma das interfaces identificadas pelo endereço. Especificamente, o pacote é enviado para a interface mais próxima de acordo com a medida de distância do protocolo de roteamento. Devido à pouca experiência na Internet com esse tipo de endereços, inicialmente seu uso será limitado para:

- Um endereço anycast não pode ser utilizado como endereço de origem (Source Address) de um pacote IPv6;

- Um endereço anycast não pode ser configurado em um computador IPv6, ou seja, ele deverá ser associado a roteadores apenas.

Este tipo de endereçamento será útil na busca mais rápida de um determinado servidor ou serviço. Por exemplo, pode-se definir um grupo de servidores de nomes configurados com um endereço anycast; o computador acessará o servidor de nomes mais próximo utilizando este endereço.

O Cabeçalho IPv6

O endereço IP possui um cabeçalho com várias informações essenciais para a troca de informações entre sistemas e computadores. No IPv6, o cabeçalho sofre alterações. A principal é seu tamanho, que passa a ser de 320 bits, o dobro do IPv4 (12 campos dando um total de 160 bits). Além disso, alguns campos do cabeçalho foram retirados, enquanto outros se tornaram opcionais.

Version 4 bits	Traffic Class 1 byte	Flow Label 20 bits		
		Payload Length 2 bytes	Next Header 1 byte	Hop Limit 1 byte
				Source Address 16 bits
				Destination Address 16 bits

- **Version:** campo com tamanho de 4 bits utilizado para identificar a versão do protocolo utilizado no caso do IPv6 o valor deste campo é 6.
- **Traffic Class:** este campo substitui o campo Type of Service do IPv4. Utilizado para identificar certos tipos de tráfego que tem maior prioridade do que outros como tráfegos multimídia e dados relacionados a dados de aplicações de tempo real.
- **Flow Label:** este campo tem tamanho de 20 bits utilizado para identificar conjuntos de pacotes que requerem o mesmo tipo de tratamento por parte dos roteadores. Este campo facilita o tráfego de aplicações de tempo real, pois somente o cabeçalho do primeiro pacote é processado para identificar o tipo de tratamento que deve ser dado ao conjunto de pacotes. Os demais pacotes serão tratados com as mesmas opções identificadas pelo primeiro pacote do conjunto e isto possibilita um aumento de performance. O fluxo de pacotes é identificado pelo rótulo do fluxo e os endereços de origem e destino dos pacotes. Nós de rede que não tem suporte a rótulos de fluxo tem que encaminhar os pacotes sem processá-los e no caso de estarem recebendo o pacote devem desconsiderar este campo. Todos os pacotes que pertencem a um fluxo devem obrigatoriamente ter o mesmo endereço de origem e destino.
- **Payload Length:** este campo especifica o tamanho do dado carregado após o cabeçalho IP. Diferentemente do campo de tamanho do IPv4 que inclui no cálculo o tamanho do cabeçalho, o payload length é calculado a partir dos dados existentes após o cabeçalho IPv6. Os cabeçalhos de extensão são considerados parte do payload e, portanto são incluídos no cálculo. Como este campo tem tamanho de 2 bytes isto limita o tamanho máximo do pacote a 64 KB. No caso da quantidade de dados for maior que este valor o protocolo IPv6 possui um cabeçalho de extensão chamado Jumbograma que prove o suporte a pacotes de tamanhos maiores. Este tipo de cabeçalho de extensão só será necessário se o computador estiver atrelado a um link com capacidade superior a 64 KB.
- **Next Header:** este campo tem tamanho de 1 byte e representa o antigo campo Protocol Type Field do IPv4. No caso o campo foi renomeado. Este campo contém os

mesmos números utilizados para identificar os protocolos no protocolo IPv4, a tabela a seguir ilustra alguns valores. No caso do pacote IPv6 possuir um cabeçalho de extensão este campo irá conter o tipo do cabeçalho de extensão.

Valor	Descrição
0	In an IPv4 header: reserved and not used
1	Internet Control Message Protocol (ICMPv4)—IPv4 support
2	Internet Group Management Protocol (IGMPv4)—IPv4 support
4	IP in IP (encapsulation)
6	TCP
8	Exterior Gateway Protocol (EGP)
9	IGP - any private interior gateway (used by Cisco for their IGRP)
17	UDP
41	IPv6
43	Routing header
44	Fragmentation header
45	Interdomain Routing Protocol (IDRP)
46	Resource Reservation Protocol (RSVP)
50	Encrypted Security Payload header
51	Authentication header
58	ICMPv6
59	No Next Header for IPv6
60	Destination Options header
88	EIGRP
89	OSPF
108	IP Payload Compression Protocol
115	Layer 2 Tunneling Protocol (L2TP)
132	Stream Control Transmission Protocol (SCTP)
134 – 254	Unassigned
255	Reserved

- **Hop Limit:** este campo tem tamanho de 1 byte e representa o antigo campo TTL (Time To Live) do IPv4. O conteúdo deste campo indica a quantidade de roteadores que o pacote pode passar antes de se descartado. Cada vez, que é encaminhado por um roteador, o outro nó que esteja encaminhando o pacote, o valor deste campo é reduzido em uma unidade.
- **Source Address:** contém o endereço de 16 bits do host que enviou o pacote.
- **Destination Address:** contém o endereço, 16 bits, do host que pretende receber o pacote. No caso do protocolo IPv4 este campo sempre continha o endereço do último destino do pacote. Entretanto no IPv6 este campo não contém o endereço do último destino se o cabeçalho de roteamento, que é um dos cabeçalhos de extensão, estiver presente.
- De maneira geral, o cabeçalho ficou mais simples e essa mudança não serve somente para adaptar-se aos novos padrões do IPv6, mas também para permitir que os roteadores não tenham que processar determinadas informações do cabeçalho. Como consequência, a transmissão se torna mais eficiente.

O Futuro Da Internet

O IPv6 é uma padrão que promete resolver vários problemas da internet, inclusive alguns relacionados a segurança que não foram citados nesta unidade. Ainda em teste, esse novo tipo de endereçamento IP deve começar a ser usado em alta escala dentro de alguns anos. Enquanto isso não ocorre, testes e aperfeiçoamentos são realizados.

Obviamente, adaptações nos sistemas operacionais atuais serão necessários, portanto, o IPv6 não substituirá o IPv4 de uma hora para outra. Cogita-se até mesmo que o IPv4 não seja descartado após uma implementação significante do IPv6.

Para alguns, o IPv6 trará complexidades até então não existentes aos administradores de rede, mas deve-se observar que este protocolo terá algumas auto-configurações e outros meios que facilitarão a montagem de uma rede.

E agora? Você já sabe o que vai mudar em sua vida com a chegada do IPv6? Percebe-se claramente que muita coisa irá mudar: nova terminologia, novas e interessantes características, novo processo de roteamento com o IDR (Inter-Domain Routing Protocol), mais qualidade de serviços (QoS), etc.

Para os que trabalham diretamente no projeto e implementação de redes de computadores TCP/IP, a adaptação a esta nova tecnologia será inevitável. E, para não ter que pegar o "bonde" andando, a preparação para essa revolução deve ser iniciada desde agora, tendo-se em vista um planejamento criterioso de ações para o processo de transição e implementação do 6-BONE.

Por fim, se você se perguntou por que IPv6 ao invés de IPv5 saiba que este último esteve em testes, mas não foi considerado apropriado para a Internet. Para mais informações e/ou explicações mais técnicas, visite o seguinte site <http://www.ipv6.org>.



Atividades

Atividade Dissertativa

Evolução do Protocolo da Internet (IP): do IPv4 ao IPv6

Comprimento: duas folhas (no mínimo)



UNIDADE 24

Objetivo: Conhecer quais são os principais protocolos do Nível Físico do modelo OSI.

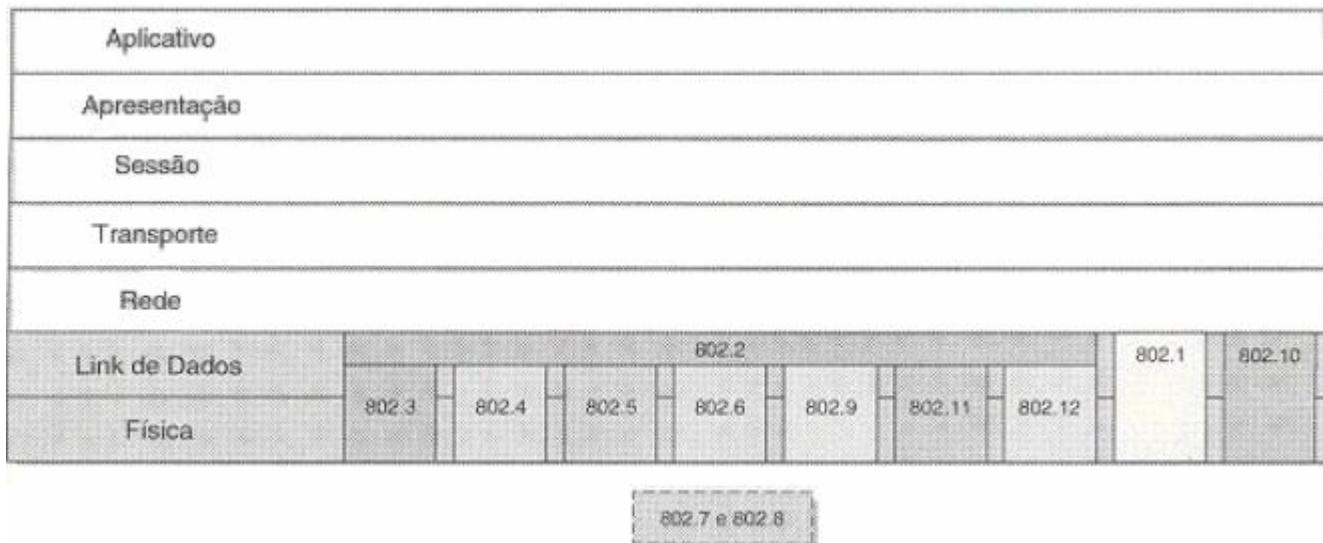
Protocolos Do Nível Físico

Ethernet (IEEE 802.3)

A Ethernet é a tecnologia mais utilizada nas redes locais, tendo sido especificada e padronizada pela norma IEEE 802.3, foi inicialmente desenvolvida pela Xerox vindo posteriormente a ser desenvolvida pela Xerox, DEC e Intel.

A Ethernet é uma tecnologia baseada na difusão (broadcasting) de quadros. Esta tecnologia define cabeamento e sinais elétricos para a camada física, e formato dos quadros e protocolos para a camada de controle de acesso ao meio (Media Access Control – MAC) do modelo OSI. A partir dos anos 90, vem sendo a tecnologia de LAN mais amplamente utilizada e tem tomado grande parte do espaço de outros padrões de rede como Token Ring, FDDI e ARCNET.

Este protocolo opera na camada física e de enlace do modelo OSI, existem ainda nesta camada de enlace duas subcamadas: a subcamada de acesso à mídia (MAC 802.3) e a subcamada do cliente LLC (Logical Link Control – 802.2). Nos “drivers” de rede (o software que permite o uso da placa de rede no sistema computadorizado) estão embutidos os suportes necessários a essas subcamadas.



Começa em fevereiro de 1980 (daí surgiu o número 802) o trabalho de definir os padrões de tecnologia LAN para a camada física e de enlace do modelo OSI. A IEEE (Institute of Electrical and Electronic Engineers) definiu uma série de padrões 802.x que interoperam com vários protocolos da camada superior e até com redes diferentes.

Protocolos Da Camada IEEE 802.X

Existem diversos protocolos na 802.x, entre eles:

- **IEEE 802.1:** Faz a definição da camada física e da camada de enlace da OSI para que os dispositivos de LAN IEEE 802 consigam se comunicar com uma LAN ou WAN.
- **IEEE 802.2:** É onde está definida a LLC (Logical Link Control) que é vital para o funcionamento das redes da série IEEE 802.x. Essa camada acrescenta campos de cabeçalho para fazer a identificação de que protocolo das camadas superiores está sendo utilizado no frame (quadro) e também indica quais os processos da camada de rede estão sendo utilizados pela origem e destino do quadro.

- **IEEE 802.3:** Faz a especificação de uma serie de opções da camada física, inclusive diferentes modos de sinalização (banda-base e banda-larga), dos tipos de mídia, tipos de tipologias e taxa de dados. Aqui é definido o método de acesso CSMA/CD (Carrier Sense Multiple Access/Collision Detection) que detecta colisões na mídia compartilhada e possibilita o funcionamento da rede, através de seu modo de tratar com esse tipo de erro.
- **IEEE 802.4:** Especifica um padrão de topologia física com método de acesso à mídia por token, mídia de banda-base e banda larga e cabeamento do tipo CATV de 75 ohms (também pode ser utilizada fibra ótica). Ele atende principalmente as necessidades de uma LAN.
- **IEEE 802.5:** Foi desenvolvido com base na Token Ring da IBM. Ele utiliza um método de acesso a mídia por token e consegue efetuar transmissões de dados nas velocidades de 1, 4 ou 16 Mbps. A diferença entre a especificação 802.5 e a da IBM é que a mídia de transmissão não esta especificada explicitamente assim como o método de transmissão (o que gera flexibilidade e não uma imposição de meio ou topologia).
- **IEEE 802.6:** Tem uma tecnologia denominada DQDB (Distributed Queue Dual Bus) que é utilizada para transferência de dados, ela permite o tráfego síncrono e assíncrono que suporta voz, vídeo e dados.
- **IEEE 802.7:** É um padrão que determina como são feitas as instalações de teste de banda-larga. Uma espécie de manual de referencia para os projetistas.
- **IEEE 802.8:** Faz a definição de grupos de trabalho para desenvolver trabalhos na tecnologia 802 em padrões de fibra ótica.
- **IEEE 802.9:** Define a Ethernet Isócrona que tem como foco a integração de transmissões de voz com dados e o suporte de tráfego esporádico e padronizado.

- **IEEE 802.10:** Faz a definição de métodos de criptografia para os serviços, protocolos, formatos de dados e interfaces. Esta definida também nele as informações sobre gerenciamento e distribuição das informações sobre criptografia que independem de qualquer algoritmo específico ou meio de transmissão.
- **IEEE 802.11:** Faz a especificação de padrões para uso com LAN Wireless (sem fio), que se utilizam transmissões com infravermelhos e de espectro amplo.
- **IEEE 802.12:** Traz a definição de um padrão de rede em forma de estrela e com taxa de transmissão 100 Mbps que é baseada em contenção (AnyLAN de 100 VG). A diferença é que o hub ou dispositivo que controla o tráfego pode consultar a prioridade dos pacotes e dar preferência a um tráfego que tem uma prioridade mais alta. São suportados quadros do tipo Ethernet e Token Ring.
- No site da IEEE é possível achar mais informação sobre os diferentes protocolos: <http://www.ieee.org>.

IEEE 802.3 e A Ethernet

Modelo OSI

Aplicação
Apresentação
Sessão
Transporte
Rede
Enlace
Física

Modelo IEEE 802.3

Cliente MAC Acesso à mídia (MAC)	802.2 802.3
Física	Mídia de Transmissão

A estrutura do IEEE 802.3 Ethernet tem a aparência acima, ela juntamente com o IEEE 802.2 especifica padrões para a camada física e a de enlace do modelo OSI.

Existem diversos tipos de opções com relação a camada física, que pode incluir diferentes tipos de mídia, topologia e sinalização (banda-base e banda larga).

	Padrões							
Parâmetros	Ethernet	IEEE 10BASE5	10BASE2	1BASE5	10Baset	10BRODA	10BASEF	
Taxa de Dados Mbps	10	10	10	1	10	10	10	
Comprimento Máximo do Segmento – metros	500	500	185	250	100(UTP)	1800	500-2000	
Mídia	50 ohms coaxial (Grosso)	50 ohms coaxial (Grosso)	50 ohms coaxial (Fino)	Cabos Trançados Não-Blindados	Cabos Trançados Não-Blindados	75 ohms Coaxial	Fibra ótica	
Topologia	Barramento	Barramento	Barramento	Estrela	Estrela	Estrela	Estrela	

A Tabela acima descreve os padrões da camada física do IEEE 802.3

LLC – Logical Link Control (IEEE 802.2)

O padrão IEEE 802.2 refere-se ao protocolo para a subcamada de enlace LLC (Logical Link Control). A camada de enlace (Data Link) foi subdividida em duas subcamadas com a única finalidade de possuir um nível independente da topologia, dos meios de transmissão e dos métodos de acesso utilizados na rede local, de forma que, se alterações fossem realizadas nestes itens, o protocolo de enlace não seria alterado. Este nível é o LLC.

Esta subcamada LLC é responsável em implementar a interface do nível de enlace com o nível de rede, fornecer serviços como multiplexação e o controle do fluxo e dos erros.

A multiplexação do acesso ao meio físico no nível de enlace é realizada através da identificação dos usuários do enlace, isto é, da identificação dos pontos de acesso a serviços (Service Access Points - SAPs). Desta forma, o protocolo LLC deve identificar qual o ponto de acesso origem (SSAP - Source Service Access Point) e qual o ponto de acesso destino (DSAP - Destination Service Access Point).

A subcamada de enlace LLC pode fornecer ao nível de rede de três tipos de serviço distintos:

1. Sem conexão e sem reconhecimento.
2. Orientado a conexão.
3. Sem conexão e com reconhecimento.

MAC – Medium Access Control (IEEE 802.3)

A preparação do quadro MAC é completada após receber o pacote da subcamada LLC (Logical Link Control). A subcamada MAC adiciona o endereço do nó de origem, e alguns bits requisitados para completar o campo de dados. Uma seqüência de checagem do quadro (FCS) é então calculada e anexada ao final do pacote.

O IEEE 802.3 utiliza um método de transmissão de contenção que permite que os dispositivos possam efetuar a transmissão de dados sempre que necessário, porém ocorrem colisões nesse tipo de método que são tratados conforme descrito abaixo:

O nó que quer se comunicar “escuta” a mídia de transmissão para determinar se existe algum sinal que a mesma está sendo utilizada no momento.

Se ele detectar que existe um sinal, espera um período aleatório de tempo que é determinado pelo tráfego existente da rede e por um gerador de número aleatório. Se não existir sinal o nó transmitira seus pacotes para a rede.

Se ocorrer de outro nó executar os passos 1 e 2 ao mesmo tempo (o que não é difícil), ocorrerá a colisão.

Quando isso ocorre se envia um sinal de congestionamento. Daí os nós esperam um período de tempo aleatório e em seguida tentam transmitir novamente.

Esse tipo de método é chamado de CSMA/CD que é utilizado em todas as implementações baseadas no padrão Ethernet. O quadro Ethernet de uma rede IEEE 802.3 tem o aspecto da figura.

Bytes	7	1	6	6	2	46-1500	4	
Preâmbulo		Destino	Origem	Comprimento	LLC	Dados	Pad	FCS

Quadro Ethernet IEEE 802.3

O protocolo CSMA/CD tem uma propriedade muito interessante que permite aumentar ou diminuir o tamanho da rede sem que a performance e confiabilidade da rede se degradem o que facilita o seu gerenciamento. Está especificada na norma IEEE 802.4u.

IEEE 802.3u – Fast Ethernet

A passagem da tecnologia 10Base-T para 100Base-T é fácil uma vez que ambas utilizam o protocolo CSMA/CD. Muitos dos adaptadores de rede suportam comunicações a 10 e 100 Mbps sendo a detecção da velocidade feita automaticamente. A passagem de 10 Mbps para 100 Mbps reduz o tamanho máximo que a rede pode ter para um comprimento máximo de 500 metros a 10 Mbps passa-se para cerca de 200 a 100 Mbps. Para se conseguirem distâncias superiores a 205 metros numa rede a 100 Mbps é necessário instalar repetidores em cada 200 metros.

Este padrão determina um tipo de rede que pode transferir dados binários a 100 Mbps. A FastEthernet Alliance determinou que as seguintes especificações devem ser utilizadas no padrão IEEE 802.3u:

Topologias Física E Lógica

- MII (Media Independent Interface)
- AUTONEG (Auto Negotiation)
- MAC (Media Access Control)

A topologia da rede determina que cada dispositivo tenha um cabo que vai da placa de rede a um ponto de conexão em comum. Se este ponto for um hub se recomenda não efetuar o cascamenteamento (2 ou mais hubs); sempre é melhor usar Switches. A topologia como no IEEE 802.3 é de barramento lógico.

MII – Media Independent Interface

O MII especifica que se devem utilizar transceptores ou PLD (Physical Layer Devices) para as conexões de rede. Existem 3 PLDs que são especificados pela camada física: 100Base-TX, 100Base-T4 e 100Base-FX. Deve se observar que a mídia de cobre ainda tem a limitação de 100 metros e que um cabo UTP de 0,5 metros pode ser utilizado para conectar a placa de rede a um transceptor externo. O tamanho máximo do cabo de link entre repetidores é de 5 metros.

A rede 100Base-FX está limitada a um tamanho de segmento de 412 metros (sem repetidores) para fibra no modo Half-duplex e 2.000 metros para a fibra no modo Full-duplex.

AUTONEG – Negociação Automática

A função de AUTONEG é uma parte opcional do padrão Ethernet que permite que os dispositivos troquem informações a respeito de suas capacidades através um segmento de ligação. Isto, por outro lado, permite que os dispositivos realizem uma configuração

automática para alcançarem o melhor modo de operação possível através de uma conexão. No mínimo, a AUTONEG provê uma comparação automática das velocidades dos dispositivos de múltipla velocidade de cada ponta da conexão. Assim interfaces Ethernet de múltipla velocidade podem aproveitar a velocidade mais alta oferecida por uma porta de hub de múltipla velocidade.

Isto significa que os adaptadores de rede para FastEthernet (IEEE 802.3u) operam em modo de compatibilidade com a Ethernet (IEEE 802.3) convencional.

O protocolo de AUTONEG também provê sensibilidade automática para outras capacidades. Por exemplo, um hub que suporta operações a Full-duplex em algumas de suas portas pode informar este fato através do protocolo de AUTONEG. Assim interfaces conectadas ao hub que também suportam operações Full-duplex podem se configurar para usar o modo Full-duplex nas interações com o hub.

A AUTONEG é possível usando-se sinais FLP (Fast Link Pulse). Estes sinais FLP são uma versão modificada do NLP (Normal Link Pulse) usados para verificar a integridade da ligação, definido na especificação 10Base-T.

Os sinais FLP foram projetados para coexistirem com os sinais NLP, de tal forma que os dispositivos 10Base-T, que usam sinais NLP, continuarão detectando a integridade do seu próprio link mesmo quando ligado a um hub de AUTONEG que envia sinais FLP. Como o NLP, os sinais FLP trafegam durante intervalos em que o link da rede está ocioso, não interferindo no tráfego normal. Ambos os sinais são especificados somente para par trançado, o que significa que segmentos de fibra ótica não podem participar de processos de AUTONEG.

Os sinais FLP são usados para enviar informações sobre as capacidades do dispositivo. O protocolo de AUTONEG contém regras para a configuração do dispositivo baseada nestas informações. É assim que um hub e o dispositivo ligado a este hub negociam e configuram-se automaticamente para usar o modo de operação de máxima performance.

A característica de AUTONEG é opcional e inclui uma interface de gerenciamento opcional que permite a desabilitação da AUTONEG, ou força um processo negociação manual. Pode-se também selecionar um modo operacional específico para uma determinada porta do hub.

Repetidores De Fast Ethernet

Vale a pena lembrar que é possível se utilizar de repetidores para interconectar segmentos de rede. Porém cada tipo se utiliza de um tipo diferente de protocolo (100Base-TX, 100Base-T4 ou 100Base-FX).

Inclusive eles utilizam sinais de freqüência diferentes. Então os repetidores utilizados têm que efetuar a conversão de freqüência para conseguir interconectar segmentos 100Base diferentes (observar se pelo menos nas duas pontas existe o mesmo tipo de conector e se existem saídas para outro tipo no mesmo dispositivo para não passar aborrecimentos, em todo caso dois Switches diferentes podem ser interconectados por um cabo cross Ethernet).

IEEE 802.5 – Token Ring

Nesse padrão de rede que é compatível com a rede Token-Ring da IBM são especificados padrões para a camada Física e para a subcamada MAC. A rede em forma de anel é controlada pelo Token.

As estações geralmente são conectadas a MSAU (Unidade de Acesso a Estações Múltiplas) que formam o anel de rede onde trafega o Token. Podem-se utilizar cabos patch entre os dispositivos e as MSAU (inclusive utilizando-se patch panel); o que não muda o formato de tráfego em forma de anel.

MAC – Token Ring

Nesse padrão o controle de acesso à mídia é feito por um Token que é especificado pelo protocolo IEEE 802.5; o Token funciona como uma permissão para transmitir dados na rede. Analogamente os índios utilizavam o Token para saber de quem era a vez de falar e somente o passavam quando se sentiam compreendidos (nesse caso era um bastaõ e não um pacote especial).

O dispositivo que recebe o token gera um frame que percorre todo anel até a origem e depois é removido do anel e daí é gerado um novo token pelo dispositivo de transmissão original. Existe o método early token release (que faz a liberação antecipada do token), quem transmite gera o novo token imediatamente após o encerramento da transmissão do último frame com dados.

Sempre um nó atua como monitor ativo no anel e determina se remove o frame (para evitar loops) ou deixa-o passar, inclusive efetuando outras tarefas de manutenção do anel. Qualquer nó tem potencial para ser monitor ativo, se ninguém se oferecer algum nó será forçado a exercer esse papel.

Beaconing

Esse processo gera uma espécie de tolerância a falhas no anel, caso tenha alguma interrupção é gerado um frame MAC de beacon com o motivo da falha e se inicia um processo de reconfiguração automática para as transmissões de rede ao redor da área afetada.

FDDI – Fiber Distributed Data Interface

O FDDI é um padrão ANSI que inclui especificações da camada física da OSI e da subcamada MAC e de gerenciamento de estação (SMT). Ele não pressupõe outros protocolos da camada superior e funciona como um auxiliar do IEEE 802.2 que utiliza seus serviços.

Geralmente a fibra óptica supre as necessidades de banda passante que são exigidas por aplicações multimídia e de voz, fornece um backbone eficiente e consegue conectar ate mainframes com eficácia.

Assim como o IEEE 802.5 ele tem o acesso na forma de token e seu meio físico é imune a EMI (Electro Magnetic Interference). A taxa de dados da FDDI leva muita vantagem sobre o padrão IEEE 802.5. As redes em FDDI possuem dois anéis que tem fluxos de dados em rotações contrárias e quando ocorre uma falha no anel primário o anel secundário, além de continuar a gerenciar a rede, presta ajuda ao anel primário a encaminhar o tráfego corretamente.

Existem estações classe A e classe B, a diferença é que as classe B somente se conectam ao anel primário e as classe A ao primário e secundário (com o único propósito de fornecer uma tolerância elevada a falhas do anel primário).

MAC – FDDI

O nível MAC utiliza uma técnica baseada em token e tem uma topologia em anel, contudo existem algumas diferenças relativamente ao Token-Ring (IEEE 802.5).

O token é liberado imediatamente após o envio do último quadro, sem esperar que este complete a volta pelo anel (Early Token Release) esta técnica é usada também em algumas implementações 802.5. Como consequência disto podem existir quadros de vários transmissores circulando simultaneamente no anel. Quando um quadro é recebido o nó tem de analisar o endereço de origem, se for o seu, o quadro deverá ser eliminado.

O protocolo MAC das redes FDDI é conhecido por TTP (Timed Token Protocol). Quando um token circula pelo anel, trata-se de uma variante da técnica usada para o MAC Token-Ring 802.5 em que é dado maior relevo ao controlo de tempos. Assim o tempo que o token demora a descrever o anel é controlado, se ultrapassa certo limite nenhum nó o pode capturar. Por outro lado e semelhante com o 802.5 o tempo que o token pode estar retido por um nó é limitado.

O formato de quadro FDDI é semelhante ao dos quadros 802.5, contudo o campo Access Control é eliminado e no inicio do quadro surge um campo adicional de 16 bits ou mais para sincronização do receptor. Em conjunto com o campo delimitador de inicio de quadro (Start Delimiter – SD) constituem o SFS (Start Frame Sequence).

O campo FC (Frame Control) tem o formato CLFFZZZZ:

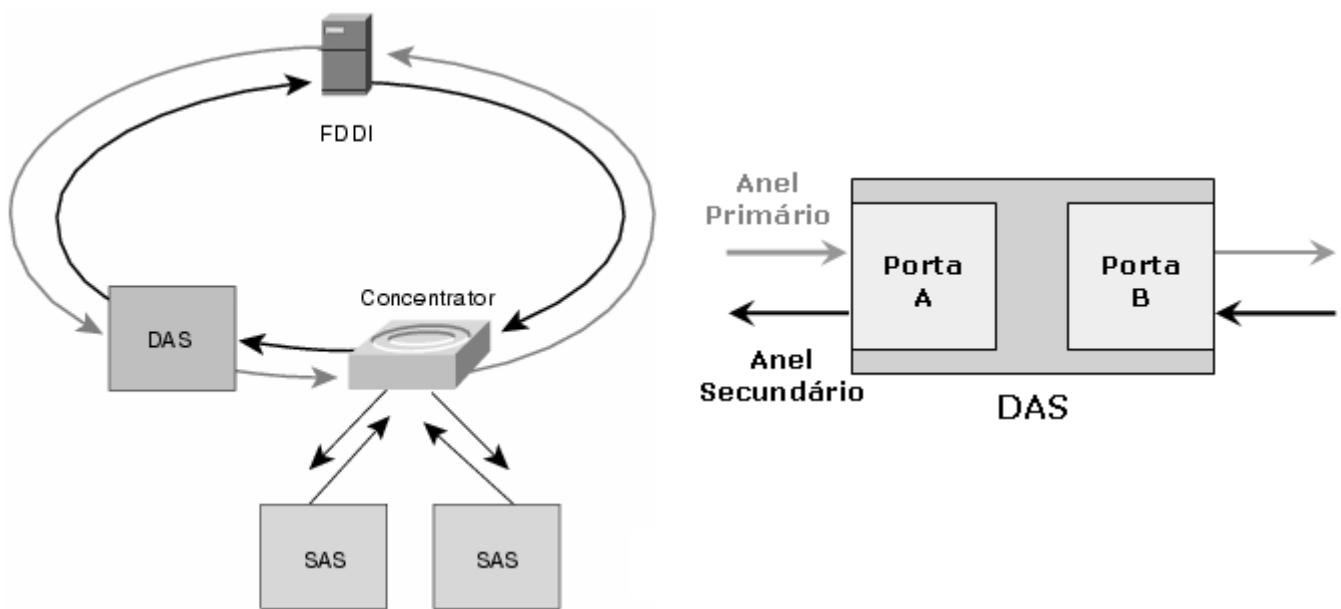
- O bit C tem o valor 1 para transmissões síncronas e o valor 0 para transmissões assíncronas.
- O bit L permite a distinção entre endereços de 2 bytes (valor 0) e de 6 bytes (valor 1).
- Os bits FF indicam o tipo de quadro, valor 00 para um quadro MAC e valor 01 para um quadro LLC, os outros dois valores são reservados.
- Quando se trate de um quadro MAC os bits ZZZZ indicam o seu tipo.

O nível físico FDDI é dividido nos níveis já descritos para o 100BaseT. No nível mais baixo (Physical Medium Dependent – PMD) são usados dois anéis de fibra óptica para transmitir sinais, a informação circula em sentido inverso por cada anel. Aos anéis é possível ligar estações diretamente ou em alternativa concentradores aos quais são depois ligadas as estações.

Qualquer nó FDDI (estação ou concentrador) pode estar ligado a um ou ambos os anéis.

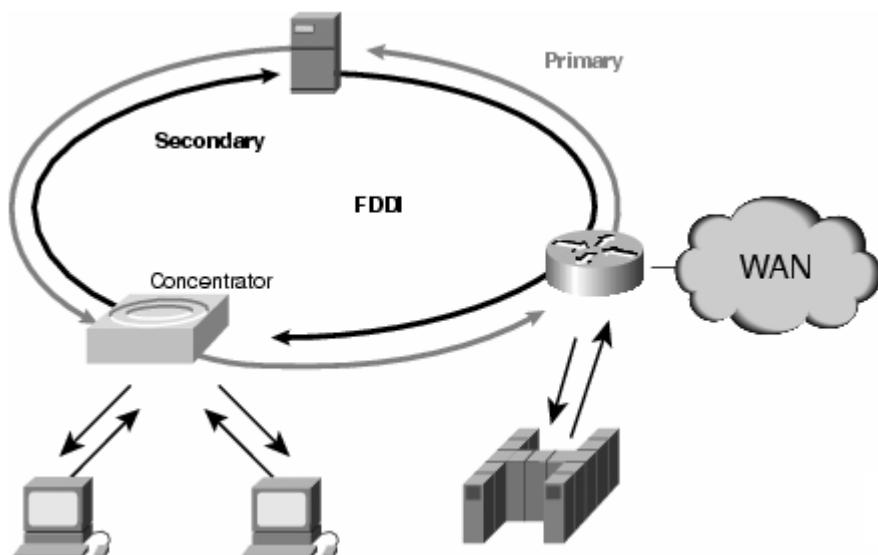
Temos por isso os seguintes tipos de nó:

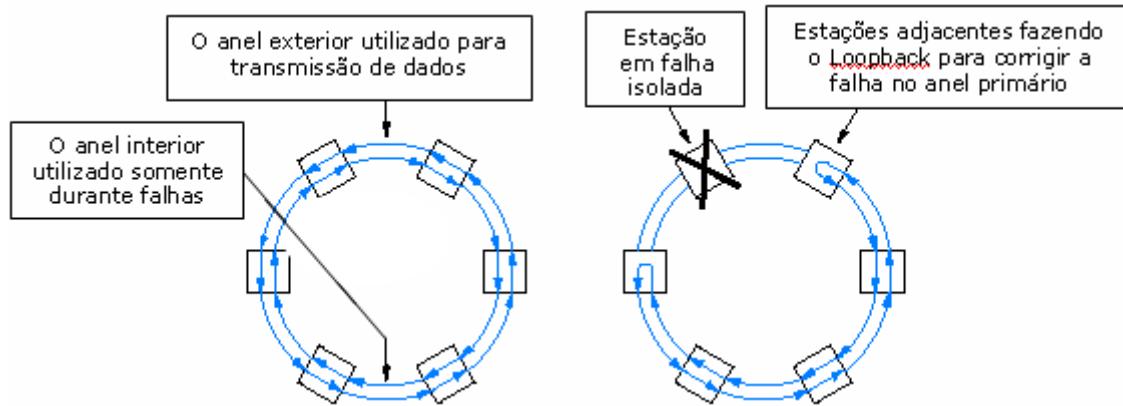
- SAS - Single Attachment Station
- DAS - Dual Attachment Station
- SAC - Single Attachment Concentrator
- DAC - Dual Attachment Concentrator



A existência de dois anéis permite a solução automática de problemas, se há uma falha num cabo de ligação entre dois nós, cada um deles faz um curto circuito dos dois anéis (para que isto seja possível devem ser nós do tipo DAS ou DAC).

No limite, em caso de falhas de ligações em pontos distintos passam a existir dois ou mais anéis:





Tal como no caso do Token-Ring, todos os nós são repetidores, no caso da fibra óptica a distância máxima entre repetidores é de 2 Km, com um máximo de 500 nós permite alcançar distâncias de 100 Km, e tudo isto a uma taxa de 100 Mbit/s.

Uma alternativa para o PMD é a utilização de cabos de cobre, o CDDI (Copper Distributed Data Interface) e o SDDI (Shielded Distributed Data Interface) são dois exemplos onde a fibra óptica é substituída por cabos de par trançado, respectivamente com e sem blindagem.

UNIDADE 25

Objetivo: Saber as diferenças entre um protocolo de LAN e um protocolo de WAN.

Protocolos De LAN E WAN

Protocolos De LAN: NetBEUI

O NetBEUI é uma espécie de “vovô protocolo”, pois foi lançado pela IBM no início da década de 80 para ser usado junto com o modelo IBM PC Network, um micro com configuração semelhante à do PC XT, mas que podia ser ligado em rede. Naquela época, o protocolo possuía bem menos recursos e era chamado de NetBIOS. O nome NetBEUI passou a ser usado quando a IBM estendeu os recursos do NetBIOS, formando o protocolo complexo que é usado atualmente.

Ao contrário do IPX/SPX (da Novell) e do TCP/IP (dos sistemas UNIX), o NetBEUI foi concebido para ser usado apenas em pequenas redes, e por isso acabou tornando-se um protocolo extremamente simples. Por um lado, isto fez que ele se tornasse bastante ágil e rápido e fosse considerado o mais rápido protocolo de rede durante muito tempo.

Para se ter uma idéia, apenas as versões mais recentes do IPX/SPX e TCP/IP conseguiram superar o NetBEUI em velocidade. Mas, esta simplicidade toda tem um custo: devido ao método simples de endereçamento usado pelo NetBEUI, somente é possível usa-lo em redes de no máximo 255 micros.

Outra causa para essa rapidez é a seguinte, o NetBEUI não suporta enumeração de redes (para ele todos os micros estão ligados na mesma rede). Isto significa que se você tiver uma grande Intranet, composta por várias redes interligadas por roteadores, os micros que usarem o NetBEUI simplesmente não serão capazes de enxergar micros conectados em outras redes, mas apenas os micros a que estiverem conectados diretamente.

Devido a esta limitação, dizemos que o NetBEUI é um protocolo “não roteável”

Protocolos De WAN

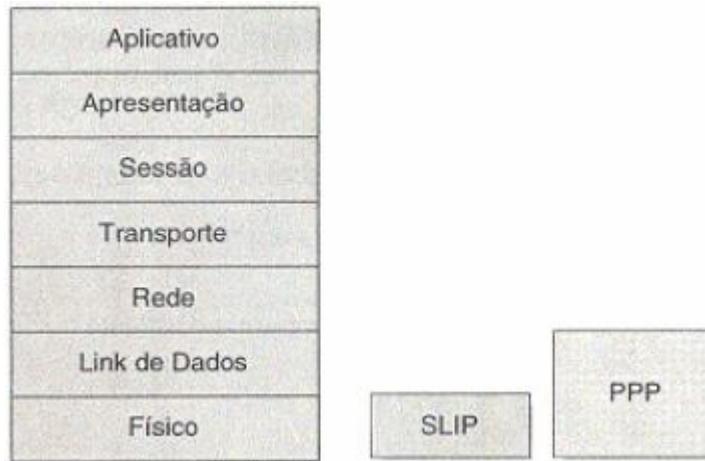
Existem protocolos que são utilizados para esses tipos de rede, os mais utilizados são:

- SLIP – Serial Line IP Protocol
- PPP – Point-to-Point Protocol
- X.25
- Frame Relay
- ISDN e B-ISDN
- ATM

SLIP e PPP

Estes dois protocolos foram projetados para permitir conexões de computadores via linhas telefônicas de uma rede pública de comutação de circuitos, este método é conhecido como conexão Dial-up utilizando o protocolo TCP/IP adaptado para este propósito.

O protocolo SLIP é mais velho do que o protocolo PPP, este último contém muitas mais funcionalidades e características. Porém, a tarefa básica de ambos é semelhante, por isso, ambos os protocolos são geralmente referidos de forma conjunta como SLIP/PPP.



A figura acima mostra o SLIP e PPP em relação a camada OSI.

Como o protocolo SLIP foi desenvolvido antes que o PPP este apresenta uma serie de deficiências, como não conseguir executar várias funções e transferências de protocolos. Para ter mais detalhes consultar o seguinte link:

<http://penta2.ufrgs.br/tp951/protocolos/slip-cur.html>.

O protocolo PPP é o sucessor do SLIP e foi desenvolvido para corrigir as falhas e deficiências deste último. Basicamente o PPP consegue efetuar as seguintes tarefas:

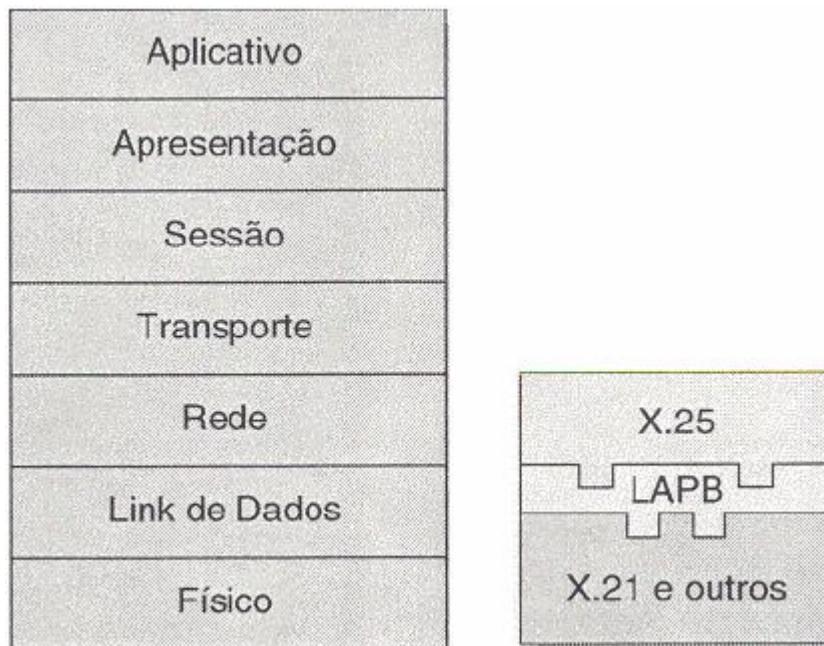
- Endereçamento IP dinâmico
- Suporte para vários protocolos no mesmo link
- Senha de login
- Controle de erro

Nem todas as implementações de PPP são 100% compatíveis entre si, então é negociado o nível de serviço antes de se efetuar a transmissão de dados. Maiores detalhes consultar:
<http://penta2.ufrgs.br/tp951/protocolos/11ppp.html>.

X.25

Esse protocolo pode ser utilizado para criar links contínuos e confiáveis entre redes distantes. O X.25 é um padrão que agrupa o computador fisicamente a uma rede de comutação de pacotes. Suas funções estão divididas em três níveis:

1. Nível 1 – Trata das regras da camada Física que são especificadas por outros padrões como o X.21, X.21 bis e X.32 e outros.
2. Nível 2 – Aqui está o LAPB que faz o trabalho de criar um caminho para os dados orientado a conexão. Esse nível corresponde a LLC do modelo OSI.
3. Nível 3 – Define as regras para o envio de pacotes entre o equipamento de terminal de dados (Data Terminal Equipment – DTE) e o equipamento de terminação de circuito de dados (Data Circuit-terminating Equipment – DCE).



O X.25 possui uma interface padrão para redes de comutação de pacotes e seu uso é recomendado para WAN e ele tem uma série de recomendações embutidas para a transmissão de dados (inclusive somente sendo recomendado para esse fim).

O X.25 não tem especificado detalhes referentes às transmissões de rede. A rede X.25 cria circuitos virtuais que podem ser permanentes (Permanent Virtual Channels – PVC) ou comutados (Switched Virtual Channels – SVC).

Os DTEs podem operar com vários circuitos ao mesmo tempo e a rede X.25 opera com uma janela de controle de fluxo e controle de erro para cada um desses circuitos.

Frame Relay

A tecnologia "Frame Relay" é uma adaptação das redes X.25 à realidade atual que exige uma tecnologia de comunicação de dados em alta velocidade, principalmente utilizada para interligar aplicações do tipo LAN, SNA, Internet e voz.

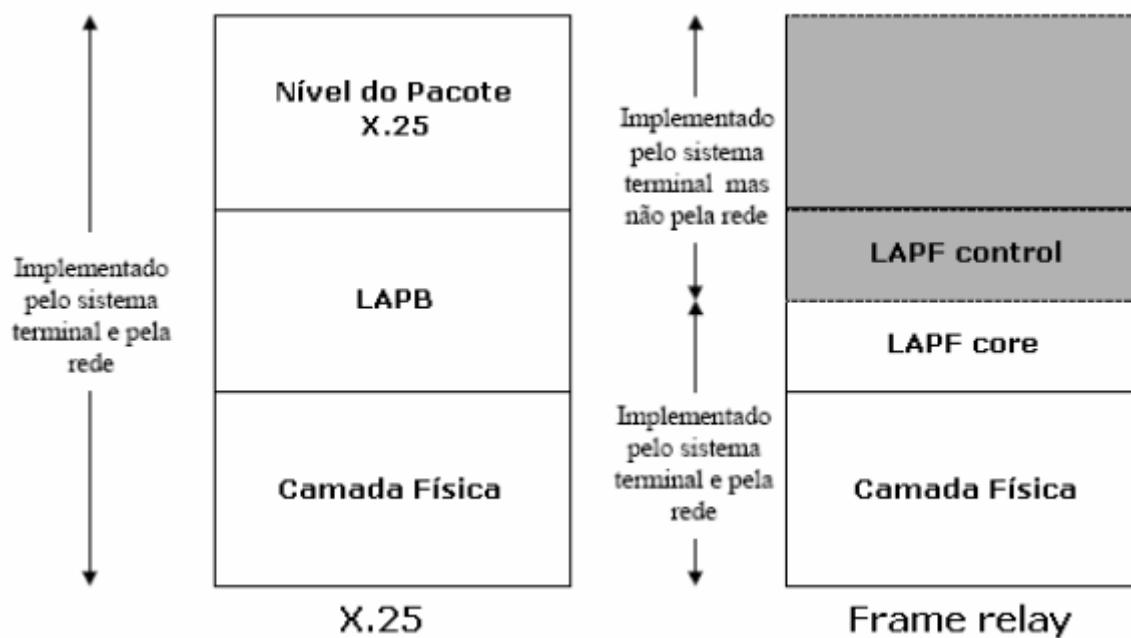
As exigências em termos de taxa de transmissão são claramente superiores e adaptáveis às necessidades, o "Frame Relay" disponibiliza taxas de transmissão variáveis, com valores múltiplos de 64 Kbps (podendo chegar até a velocidade de 2Mbps e sobre circuitos E3 em 34 Mbps).



O frame Relay está mapeado para a camada OSI conforme a figura acima.

Como nas redes X.25 é utilizado uma variante do protocolo HDLC, o novo protocolo LAP-F (Link Access Protocol/Procedures - Frame-Relay), que assegura a definição de circuitos virtuais. Assim ao contrário do LAP-B e HDLC, o LAP-F, não implementa as funções de controle de fluxo e erros, em seu lugar implementa circuitos virtuais (Virtual Link), através do campo o DLCI (Data Link Connection Identifier) que substitui os habituais números de seqüência do controle de fluxo/erros.

Não existe controle de fluxo e de erro, lance e o controle de fluxo e de erro Fim-a-Fim; se existe a necessidade de utilizá-los, uma camada mais elevada assume essa responsabilidade (utilizando de protocolos do nível superior). Esta evolução torna-se possível graças a um aumento da qualidade das linhas de transmissão, que tem como consequência a redução das taxas de erros. Essas simplificações tornam a rede de Frame-Relay cerca de 50% mais eficiente que as antecessoras redes X.25.



A figura acima é um demonstrativo de comparações entre o X.25 e o Frame Relay.

Outro fato que colabora para a melhor velocidade é que a multiplexação e comutação das conexões lógicas ocorrem na camada 2, assim se efetua uma eliminação de uma camada inteira de processamento.

	TDM	X.25	Frame Relay
Multiplexação em Tempo	sim	não	não
Multiplexação Estatística (Círculo Virtual)	não	sim	sim
Compartilha portas	não	sim	sim
Alta velocidade (por \$)	sim	não	sim
Atraso (delay)	muito baixo	alto	baixo

A tabela acima demonstra a comparação entre os circuitos de TDM (tecnologia convencional de multiplexação) do X.25 e do Frame-Relay.

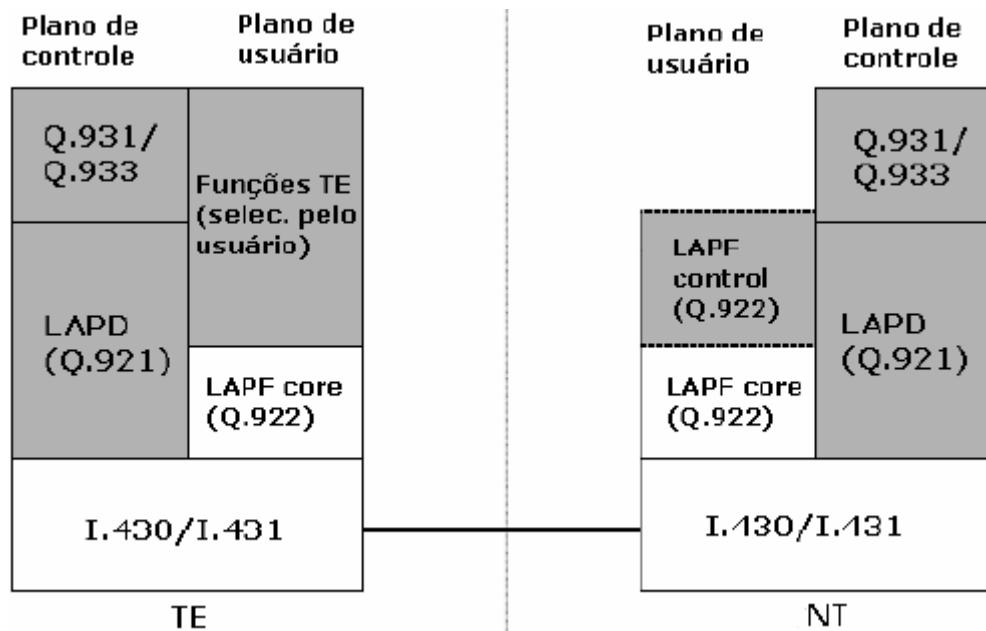
A tecnologia de TDM do Frame-Relay prove um mecanismo mais eficiente para a transmissão para redes de distância através de múltiplas conexões virtuais, onde se podem compartilhar recursos e inclusive a banda do meio físico (mídia de transmissão).

Para efeitos de controle, é usado um protocolo separado, o LAP-D. O LAPD assemelha-se mais ao HDLC "normal", existindo por isso controle de erros e fluxo. Este protocolo é usado para todas as operações relacionadas com o estabelecimento e terminação das ligações virtuais, inicialização de nós, etc.

No momento de estabelecimento de um circuito virtual numa rede Frame Relay é negociada o valor mínimo de débito de dados pretendido, este valor negociado é designado por CIR (Committed Information Rate) em bps, trata-se de uma negociação da qualidade de serviço (QoS), embora elementar porque apenas considera um parâmetro. Embora seja permitido ultrapassar o CIR durante períodos curtos, os pacotes que o fazem são assinalados, sendo ativado o bit DE (Discard Eligibility), no cabeçalho, quando o pacote passa na interface da rede.

Os dados que circulam numa rede Frame-Relay (LAP-F) não estão protegidos por mecanismos de controlo de fluxo e erros, os protocolos de nível superior (rede) deverão encarregar-se dessa tarefa, contudo as redes Frame-Relay implementam controle de congestão básico.

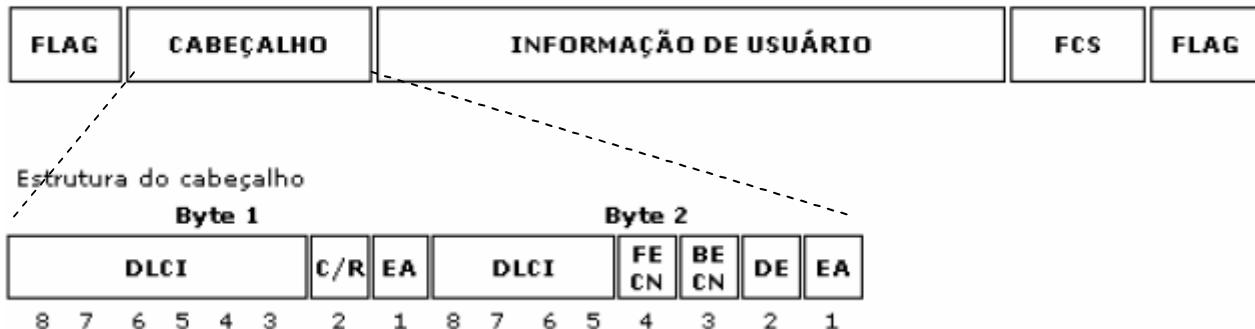
Quando os buffers de um nó intermédio ficam cheios e alguns pacotes têm de ser eliminados, o nó elimina primeiro os pacotes que transgrediram o seu CIR (bit DE ativo). Além do controle do CIR, se o débito ultrapassar determinados limites máximos, os pacotes podem ser eliminados logo na interface.



Nesta figura acima esta descrita a arquitetura do protocolo Frame Relay.

Pacotes Frame Relay

Estrutura do frame



A figura acima demonstra a estrutura do frame e do cabeçalho no Frame-Relay.

- **DLCI** – é um campo de 10 bits denominado de identificador DLCI que define o endereço do PVC ao qual pertence o quadro.
- **C/R** – é um campo que define se o quadro é um comando ou uma resposta.
- **EA** – é um campo de dois bytes que fornece um espaço adicional de endereçamento (EA significa Endereço estendido ou Extended Address).
- **FECN** – é o campo de notificação de congestionamento (FECN = Forward Explicit Congestion Notification).
- **BECN** – é um campo de notificação de congestionamento (BECN = Backward Explicit Congestion Notification)
- **DE** – elegibilidade para descarte ou Discard Eligibility.
- **Informação de Usuário** – conteúdo da unidade de protocolo da camada superior.

Os dois bytes (FCS) do quadro são ocupados pelo campo CRC, destinados ao cálculo do CRC a partir dos dados contidos no quadro entre os “flags”. O restante do quadro contém os dados do usuário.

Os frames podem ter comprimento variável e, dependendo do tipo de informação da aplicação do usuário, seu tamanho pode variar de alguns poucos até milhares de caracteres.

Isso faz com que o atraso (delay) varie em função do tamanho do frame. Entretanto, a tecnologia Frame Relay tem sido adaptada para atender até mesmo as aplicações sensíveis aos atrasos, como é o caso de aplicações em tempo real tipo tráfego de Voz.

Os pacotes são enviados através de circuitos virtuais (DLCI), cada um tem um caminho permanente da origem ao destino; estabelecidos esses circuitos se pode comunicar com diversas localidades. Existem também os caminhos permanentes chamados de PVC e os caminhos chaveados chamados de SVCs. Os DLCIs são configurados pela operadora de rede conforme as necessidades do usuário (quantidade de tráfego a disponibilidade por exemplo).

Em momentos de alto tráfego (congestionamento) os campos de descarte podem agir por isso se faz necessário o uso de um protocolo de nível mais alto para cuidar desse tipo de erro (pode ser TCP/IP, IPX ou HDLC, por exemplo).

Para finalizar com o assunto do Frame-Relay, vale a pena lembrar que além dos protocolos acima ele pode tratar também o SNA, porém existem outras implementações que podem efetuar o controle de tráfego assíncrono assim como o transporte de VoFR (Voz comprimida).

No TCP existem dois modos de configuração:

1. **Group mode:** Um único endereço IP é mantido para todos os circuitos se formando uma sub-rede IP.
2. **Point-to-point-mode:** Cada DLCI é configurado com seu endereço IP dedicado.

Recomenda-se a leitura para informações adicionais sobre as redes Frame Relay no seguinte Link: <http://www.teleco.com.br/tutoriais/tutorialfr/>

ISDN ou RDSI – Rede Digital De Serviços Integrados

O padrão ISDN é muito utilizado por fornecer uma perfeita integração entre múltiplos serviços digitais e consegue suprir a demanda de aplicações de voz, texto, dados e multimídia.



O ISDN está mapeado para o Modelo de referência OSI como mostra a figura acima. Existem dois tipos básicos de ISDN:

1. **BRI – Basic Rate Interface** (dois canais 64kb/s B e um de 16Kbps D para controle – totalizando 144 kbps).
2. **PRI – Primary Rate Interface** (23 canais B e um canal de 64 kbps D para controle – totalizando 1536 kbps).

O PRI é utilizado por usuários com grandes requerimentos de transmissão. Na Europa o PRI consiste de 30 canais B e um canal de 64 kbps D o que dá um total de 1984 kbps. É possível utilizar varias linhas PRI (muito útil para uso de videoconferência).

O protocolo de controle de controle de canais D que servem para sinalização seguem as recomendações da ITU e ocorre em três camadas e executa as seguintes funções:

- **Camada 1:** Responsável pela transmissão das informações de controle pelo canal D.
- **Camada 2:** Assegura a transmissão das informações de controle e sinalização.
- **Camada 3:** Estabelecimento e termino das conexões pela sinalização do usuário conforme as características da rede ISDN.

A ISDN pode utilizar a ISDN-API CAPI (que são interfaces de software) para criar aplicações que permitam utilizar a transmissão sem utilizar o protocolo TCP/IP.

Um exemplo de aplicação digital se utilizando o CODEC tipo GSM por meio da ISDN BRI pode ser encontrado no Link: www.isdnaudio.com.

Existe o padrão H.323 que é utilizado para videoconferência que permite trafegar com qualidade para voz e imagem em apenas dois canais B de 64 kbps.

Vale a pena lembrar que existem os canais H que possibilitam agregar vários canais B. Eles são implementados da seguinte forma:

- H0 = 384 kbps (6 canais B)
- H10 = 1472 kbps (23 canais B)
- H11 = 1536 kbps (24 canais B)
- H12 = 1920 kbps (30 canais B) - Internacional (E1) unicamente

Outro fato que faz a rede ISDN ganhar importância é pela possibilidade de integrar tecnologias como acesso a redes ATM (que é de banda larga) que são uma proposta de redes digitais de serviço integrado sobre banda larga que é chamado de B-ISDN.

Pode-se utilizar a ISDN como uma solução para backup de dados devido a sua característica de conexões comutadas e também se pode utilizar até em provedores de acesso a Internet fornecendo um link de 300 kbps bidirecional de alta disponibilidade e robustez.

Devido ao surgimento da tecnologia xDSL (a ADSL é um exemplo disso) algumas pessoas consideram obsoleta essa tecnologia.

Protocolos ISDN

Na tecnologia ISDN, existem basicamente quatro protocolos significativos para o usuário. Todos os protocolos são utilizados no canal útil e não no canal de dados. São eles:

- **V.110:** o protocolo de velocidade V.110 é um processo de transmissão que existe desde os princípios da tecnologia ISDN. Os dados são transmitidos em até 38.400 bps. O restante da capacidade (até 64 kbps) fica ocupado com pacotes de dados redundantes;
- **V.120:** é o sucessor do V.110 e possui poucas diferenças em relação ao primeiro. A principal é que nele os dados são transmitidos em até 54.000 bps;
- **X.75 e T70NL:** ambos são mais recentes e conseguem aproveitar integralmente a capacidade de transmissão do Canal B. Foram estes protocolos que permitiram à tecnologia ISDN ser uma solução viável para acesso à Internet.

UNIDADE 26

Objetivo: Saber o funcionamento desta importante tecnologia de alta velocidade via telefone.

Asymmetric Digital Subscription Line (ADSL)

O termo ADSL foi concebido em 1989 e não se refere a uma linha, mas a modems que convertem o sinal padrão do fio de telefone par trançado em um duto digital de alta velocidade. Os modems são chamados "assimétricos" porque eles transmitem dados desde a casa do assinante em uma velocidade menor do que recebe.

Mesmo assim, o termo Asymmetric Digital Subscription Line, pode ser traduzido como a "Linha Digital Assimétrica de Assinante". É uma tecnologia que permite a transferência de dados em alta velocidade utilizando apenas linhas telefônicas comuns.

É o tipo de tecnologia que cada vez mais usuários adotam para a conexão à Internet e vem sendo utilizado em larga escala no Brasil (um exemplo de serviço que utiliza a ADSL é o Speedy da telefônica).

A tecnologia ADSL divide a linha telefônica em três canais virtuais:

- Canal de Voz
- Canal para Download (com velocidade alta)
- Canal para Upload (com velocidade media)

A velocidade de download pode variar de 256 kbps até 6.1 Mbps. No caso do upload pode variar de 16 kbps até 640 kbps. Essas características que fazem a tecnologia levar o nome de assimétrica, pois existe uma velocidade maior para download do que para upload.



A voz e dados utilizam diferentes freqüências ao serem transportadas pela linha telefônica, conforme demonstrado na figura acima.

O canal de voz permite ao usuário estar conectado à Internet e ainda conseguir conversar pelo telefone. Porém é necessário o uso de um aparelho chamado Splitter para efetuar essa separação de voz e dados na linha telefônica. Na central telefônica existe também um Splitter que ajuda no encaminhamento da voz para a rede telefônica de comutação de circuitos públicos (Public Switched Telephone Network – PSTN).

Quando se utiliza a Internet o sinal é encaminhado ao DSLAN – Digital Subscriber Line Access Multiplexer que faz a limitação da velocidade do usuário conforme o plano contratado (ele pode fazer a união de varias linhas ADSL em uma); este equipamento envia o sinal para uma linha ATM (Asynchronous Transfer Mode) de alta velocidade que tem link com a Internet.

O dispositivo DSLAN que faz a mágica de juntar todas as conexões de usuário a uma única conexão, suportando vários usuários ao mesmo tempo.

Um detalhe importante é que se pode trafegar 6 Mbps até a distância máxima de 4 km. e 8 Mbps até a distância máxima de 2 km. A distância máxima da central telefônica ate a residência pode alcançar o limite de 5 km.

Acima disso o ADSL se torna inviável para o usuário, em outras palavras, quanto menor a distancia da central telefônica para a sua casa melhor. Pode-se botar a culpa na mídia de cobre que ocasiona perdas de sinal (apesar da operadora oferecer o serviço).

HDSL

No Brasil existe também a solução HDSL (High-bit-rate Digital Subscriber Line) que pode ser usada para transporte de linhas E1 e ISDN PRI. O HDSL é uma tecnologia de transmissão de alto desempenho para implementação de acessos a 2 Mbit/s na rede existente, simetria Upstream/Downstream.

O HDSL foi desenvolvido como uma tecnologia alternativa sem repetidores para disponibilizar serviços T1. O HDSL opera em modo Full-duplex através de cada par de fios em cabos de 1, 2 ou 3 pares. Isto é conhecido como Dual-duplex.

Taxa por par: 2.336 Kbps (um par), 1.168 Kbps (dois pares) ou 784 Kbps (três pares), neste último caso cada par de fios carregam 784 Kbps, ou seja, metade da largura de banda do T1 (1544 Kbps) mais um pequeno montante de overhead.

Pelo fato de seus dados serem enviados com a metade da velocidade do T1 normal, você consegue duas vezes a distância. Em virtude de o HDSL usar dois pares de fio, você ainda consegue a taxa de transferência do T1.

Diferencia-se de outras tecnologias xDSL, porque proporciona transmissão simétrica, ou seja, a mesma taxa de transmissão em ambas as direções (Download e Upload).

Vantagens

- Instalação do serviço mais rápida e barata.
- Redução de manutenção.
- Aproveitamento de transmissão superior ao do HDB3.
- Fomentar o surgimento de novos serviços.
- Reutilização de equipamentos.
- Fornecimento de E1 fracionário em um único par

Aplicações

Acesso a comunicações móveis, acesso a PABX digital, acesso primário RDSI, acesso de usuário a 2 Mbps.

Estágio de linha remota (ELR): O ELR é uma extensão da central local, localizada mais próximo dos assinantes. O ELR é controlado através da central local, que neste caso também é denominada de central-mãe. Vários ELR's podem ser interligados a uma mesma central-mãe, caracterizando-se, portanto, como um sistema distribuído de comutação. O entroncamento ELR – central-mãe pode ser feito com cabo óptico ou par metálico. O raio médio entre o ELR e o assinante é de cerca de 1 km. O ELR é indicado para aplicações em pequenas localidades, áreas rurais, grandes clientes, central de quarteirão e condomínios, para soluções rápidas ou em lugares nos quais a rede a expandir está saturada.

O Protocolo PPPoE

O ADSL permite uma conexão permanente usando unicamente o modem, porém fica a pergunta de por que (em muitos casos) é necessário usar um programa para se conectar à Internet.

É necessário utilizar um protocolo para encapsular os dados do micro de origem até a central telefônica. O protocolo mais utilizado para essa finalidade é o PPPoE (Point-to-Point over Ethernet RFC 2516).

Isso acontece porque o ADSL é somente um meio físico de acesso à rede (um meio de conexão). A autenticação através do protocolo PPPoE permite a conexão e aquisição de um endereço IP válido para a máquina do usuário.

Com a autenticação é mais fácil identificar o usuário conectado e controlar suas ações. Esse protocolo trabalha com a tecnologia Ethernet, que é usada para ligar sua placa de rede ao modem.

O protocolo PPPoE é relativamente novo, mas basicamente sua função é encapsular pacotes PPP em quadros Ethernet que serão desencapsulados pelo agregador (provedor de Internet ou ISP).

Vale a pena dar uma olhada no link abaixo, principalmente por causa do protocolo PPPoE:
http://www.cg.org.br/grupo/cable_v1.0.htm.

O link abaixo tem um tutorial completo de ADSL e com tabelas de comparação entre a família xDSL: http://www.abusar.org/tutorial_adsl.html.

Como mencionado o PPPoE é a versão do PPP que é utilizada por vários provedores de serviços de banda larga, entre eles o Speedy da Telefonica. Em todos os casos temos uma placa de rede Ethernet no PC ou porta serial universal (USB port) ligada ao modem ADSL. O PPPoE entra em cena na hora de estabelecer a conexão, permitindo que cada usuário precise fornecer seu login e senha para se conectar à rede.

O PPPoE é um padrão aberto, suportado tanto no Windows quanto no Linux e outros sistemas. No caso do Windows o suporte veio com o Windows XP e no Linux com o Mandrake 8.1, Red Hat 7.2, Debian 2.2r6, etc. Em versões anteriores do Windows é preciso instalar o software fornecido pelos provedores, enquanto no Linux basta instalar o pacote RP-PPPoE, que pode ser baixado em vários lugares, entre eles no seguinte Link:
<http://www.roaringpenguin.com/pppoe/>.

UNIDADE 27

Objetivo: Entender o que significa e para que serve uma rede com tecnologia ATM.

Asynchronous Transfer Mode (ATM)

A tecnologia ATM foi desenvolvida devido às tendências na área de redes. O parâmetro mais relevante é o grande número de serviços emergentes de comunicação com diferentes, algumas vezes desconhecidas, necessidades e características.

Nesta era da informação, usuários requisitam cada vez mais um número grande de serviços. Dentre estes serviços podemos citar alguns, tais como: High Definition TV – HDTV, vídeo conferência, transferência de dados com alta performance, multimídia, videofonia, biblioteca de vídeos, educação a distância, vídeo sob demanda, telemedicina, etc.

Este amplo espectro de serviços introduz a necessidade de uma rede universal comum suficiente para suportar esta demanda. Dois outros fatores que estão relacionados com o desenvolvimento da tecnologia ATM são: a rápida evolução das tecnologias de semicondutores e componentes ópticos e a evolução das idéias de concepção de sistemas de comunicação que transfere para a borda da rede as funções complexas de transporte da informação, por exemplo, definição de rotas. Assim sendo, tanto a necessidade de flexibilidade nas redes de comunicações, como o progresso tecnológico e conceitual de sistemas, levaram ao desenvolvimento das bases da tecnologia ATM.

Com o passar dos anos, diante do surgimento de novas tecnologias de alta performance em redes, entre as que podemos citar principalmente a FastEthernet (100BaseT IEEE 802.3u) e a GigaEthernet (1000BaseT IEEE 802.3z) e o uso cada vez maior de aplicações baseadas em IP, a visão geral da tecnologia ATM passou por várias fases. Nos últimos anos a opinião dos técnicos e engenheiros mudou sobre a tecnologia: de mais uma planificação para empresas de telefonia à inevitável utilização futura em telecomunicações; de uma complexa

tecnologia, fadada a ser substituída pela GigaEthernet, a uma promissora perspectiva de ser parte importante na ligação entre redes locais (LAN).

O ATM é um protocolo de alta velocidade que possibilita o transporte de vários tipos de tráfego pela rede. Ela possibilita a transmissão simultânea de dados, voz e vídeo em uma rede de alta velocidade.



O ATM está mapeado para a camada OSI conforme a figura acima.

O ATM pode interoperar com outros protocolos e aplicações como Frame Relay, TCP/IP, xDSL, Gigabit Ethernet, tecnologia Wireless e outros. Também pode dar suporte (através de agregação) a vários tipos de transmissão (de vários tipos de mídia) em um único meio de transmissão (como RDSI-FL, RDSI, B-ISDN, ADSL).

A principal característica é o uso de blocos de dados de tamanho fixo de 53 bytes (5 para o cabeçalho e 48 para os dados) que são chamados de células ATM. A transmissão é assíncrona e orientada a conexão através de circuitos virtuais estabelecidos, a entrega e comutação são efetuadas pela rede com base no cabeçalho das células.

O ATM apresenta uma série de atrativos com relação ao seu aproveitamento nas redes de comunicações de dados atuais (altas taxas de transmissão, baixa latência, qualidade de

serviço, etc.). Este aproveitamento está condicionado à capacidade do ATM de interoperar com as redes disponíveis atualmente.

Dentro deste contexto, foi criado o LAN Emulation, ou ELAN. Este serviço foi concebido para permitir que o maior número possível de aplicações usadas atualmente possa usar o ATM sem necessitar de modificações e ao mesmo tempo, que as estações ligadas nas redes antigas se comuniquem com as ligadas em ATM de forma transparente.

A grande maioria da base instalada de comunicação de dados é baseada em redes LAN (IEEE 802.x), tais como, Ethernet e Token Ring. Os serviços oferecidos pelo ATM são bastante diferentes dos oferecidos pelas redes LANs. As principais diferenças são as seguintes:

- As redes locais enviam quadros sem estabelecer conexões, enquanto que o ATM é orientado a conexão;
- As redes locais se caracterizam por ter o meio compartilhado, o que facilita muito o broadcast e o multicast. O ATM possui multicast, mas não oferece broadcast;
- O endereçamento ATM é hierárquico, ou seja, reflete a topologia da rede. As redes locais se baseiam nos endereços MAC, que são endereços físicos independentes da topologia.

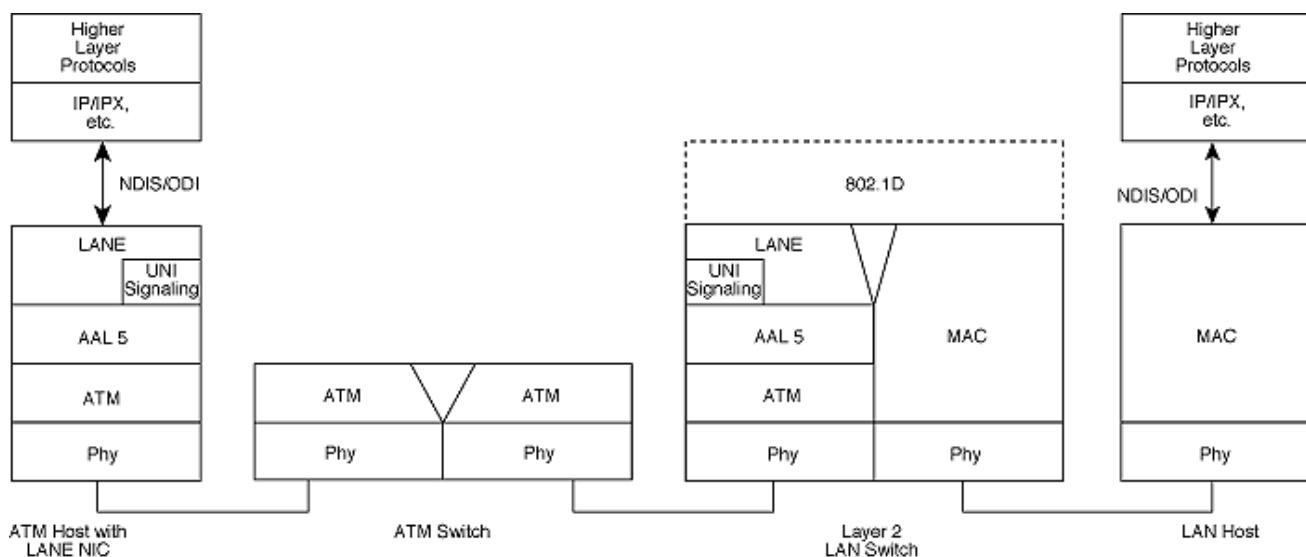
O LAN Emulation, ou ELAN, é um serviço implementado por meio de uma camada de software em qualquer estação que possua uma interface ATM, seja ela um computador, um Switch ou roteador.

Sua função básica é oferecer ao protocolo camada rede uma interface idêntica à oferecida por uma rede LAN tradicional. Isto é feito no sentido de que não seja necessário modificar os protocolos de rede para se operar uma rede ATM. Além disso, o ELAN define o bridging entre o ATM e os protocolos LAN, permitindo que as estações ligadas às duas redes se comuniquem de forma transparente.

LAN Emulation (LANE)

Como o nome próprio indica, o ELAN permite a implementação de LANs emuladas (Emulated LANs – ELANs) sobre uma rede ATM. Este conceito de ELAN provê a transmissão de quadros de dados entre seus usuários, de maneira semelhante a uma LAN física. Pode-se ter várias e independentes ELANs em uma mesma rede ATM. Para que estações em ELANs diferentes se comuniquem, é necessário o uso de um roteador. Para otimizar esta comunicação inter-ELAN foi definido pelo ATM Forum um outro serviço, chamado Multiprotocol over ATM (MPOA), que será visto mais adiante.

Existem dois tipos de ELAN: Ethernet e Token Ring. Uma ELAN é composta por um conjunto de LECs (LAN Emulation Clients) e pelo serviço, que consiste de três servidores distintos: o LECS (ELAN Configuration Server), o LES (LAN Emulation Server) e o BUS (Broadcast and Unknown Server). A interface entre os clientes e o serviço é definida pelo protocolo LUNI (LAN Emulation User to Network Interface), que é o objeto da norma de LAN Emulation. A interface entre os elementos do serviço será definida na norma LNNI (ELAN Network Node Interface). A comunicação dentro de uma ELAN é feita através de circuitos virtuais (VCCs - Virtual Channel Connections). Há VCCs de controle e de transmissão de dados. A interface LUNI (ELAN User Node Interface) usa circuitos virtuais comutados (SVCs) ponto a ponto e ponto a multiponto. O ELAN não especifica o suporte a circuitos virtuais permanentes (PVCs).

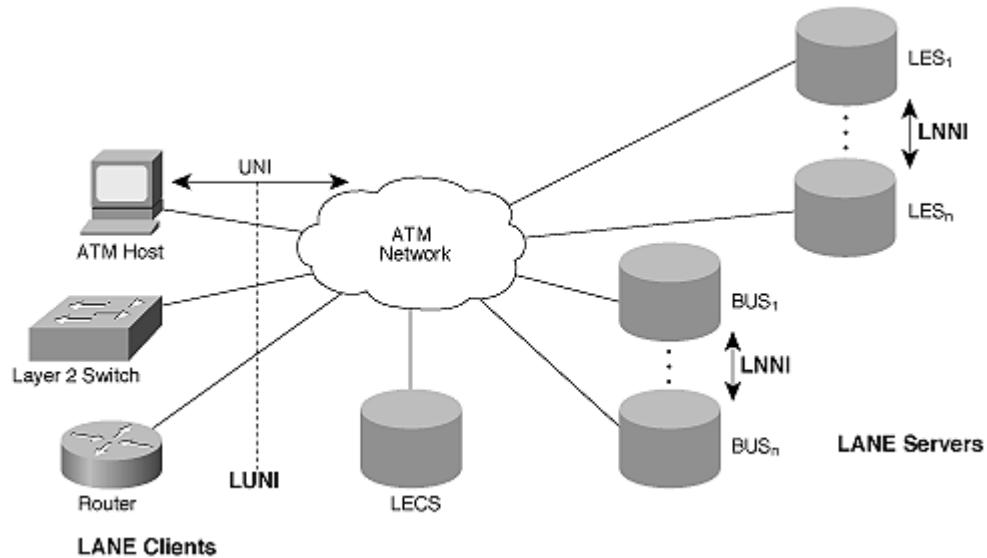


O LEC oferece ao protocolo acima dele um serviço de transmissão e recepção de quadros semelhante ao de uma rede local, de modo a mascarar do protocolo de rede as complexidades da rede ATM subjacente. Abaixo do LEC está a AAL5. O serviço de LAN Emulation usa somente a AAL5, visto que esta é a mais adequada para a transmissão de dados. O LEC passa à AAL5 um quadro semelhante ao quadro Ethernet (ou Token Ring), excluindo apenas o campo FCS (Checksum), já que a AAL5 faz um código de correção de erros semelhante.

É importante notar que o ELAN é definido acima da camada ATM, o que o torna transparente para a rede ATM, ou seja, para os Switches. O ELAN utiliza os protocolos de sinalização padrões do ATM (UNI 3.0, UNI 4.0 ou superior).

Componentes De Uma ELAN

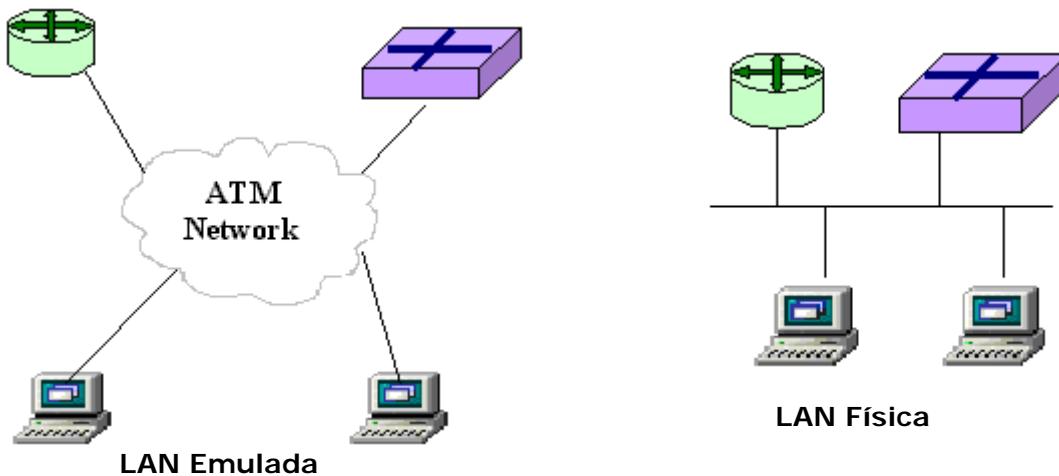
Como mencionado anteriormente, várias ELANs podem ser estabelecidas em uma rede ATM. Uma ELAN é composta pelas seguintes entidades:



- **LAN Emulation Client (LEC):** O LEC é a entidade em uma estação ATM que desempenha as funções de transferência de dados, resolução de endereços, provê a emulação do serviço de rede local para o protocolo camada rede. Um LEC somente

pode ser membro de uma ELAN. Uma estação ATM pode participar de mais de uma ELAN, desde que suporte vários LECs, um para cada ELAN. Cada LEC é identificado por um endereço ATM único, associado a um ou mais endereços MAC. No caso de um host ATM, o seu endereço ATM estará associado ao seu endereço MAC unicast e aos endereços multicast que ele desejar receber. Já no caso de um módulo ATM em um switch Ethernet, o endereço ATM do seu LEC estará associado a cada um dos endereços MAC das estações acessíveis através dele.

- **LAN Emulation Server (LES):** O LES implementa a função de controle e coordenação de uma ELAN. O LES provê serviços de registro e resolução de endereços MAC para endereços ATM. Cada LEC registra os endereços MAC que deseja receber (unicast ou multicast) junto ao LES. Os LECs também contatam o LES para resolver endereços MAC em endereços ATM para que possam estabelecer uma conexão virtual.
- **Broadcast and Unknown Server (BUS):** O BUS centraliza o envio de quadros em broadcast, multicast e também envia dados em unicast enquanto a resolução de endereços não foi completada, e, portanto o transmissor ainda não possui o endereço ATM destino desejado. No ELAN versão 1.0, cada LEC só veria um BUS, embora pudesse haver mais de um BUS por ELAN. Na versão 2.0, cada BUS pode ter mais de uma interface (ou seja, mais de um endereço ATM), sendo uma para cumprir as funções básicas do BUS e as outras específicas para determinados endereços multicast (multicast seletivo).
- **LAN Emulation Configuration Server (LECS):** O LECS é a entidade que associa um LEC a uma determinada ELAN. Um LEC sempre tem que contatar o LECS para entrar em uma ELAN. Feito este contato, se no pedido não houver qualquer violação das políticas do LECS, ele retorna ao LEC o endereço ATM do LES da ELAN desejada, permitindo ao LEC se registrar na ELAN. Somente um LECS pode ser configurado por domínio, e ele serve todas as ELANs dentro deste domínio.



Conexões

As entidades definidas pelo ELAN se comunicam através VCCs (Virtual Channel Connections). A versão 2.0 introduz o conceito de fluxo de dados, que está relacionado à multiplexação no nível LLC. Um VCC multiplexado pode transportar um ou mais fluxos, enquanto que um VCC não-multiplexado só carrega um fluxo. A versão 1.0 não suporta multiplexação.

Se um LEC deseja transmitir dados para um determinado endereço ATM, ele tem que estabelecer um VCC para aquele endereço. Se este VCC será multiplexado ou não depende se a outra parte suporta esta característica. Se for desejado estabelecer um novo fluxo de dados, ele pode ser alocado no mesmo VCC, se este for multiplexado.

Analogamente, ao encerrar um fluxo de dados, o VCC é mantido, a não ser que ele seja o único fluxo de dados presente naquele VCC. Isto causa um problema: um LEC pode encerrar um fluxo e a outra parte não tem como saber que ele foi encerrado, pois o VCC ainda existe. Assim, a especificação afirma que um LEC tem de ser capaz de receber pacotes por um fluxo mesmo já o tendo encerrado, se o VCC ainda existir.

Podem-se dividir as conexões do ELAN basicamente em dois tipos: VCCs de dados e VCCs de controle. Eles podem ser ponto a ponto ou ponto a multiponto, unidirecionais ou bidirecionais. Os tipos de conexão definidos na LUNI estão listados abaixo.

Vccs De Controle

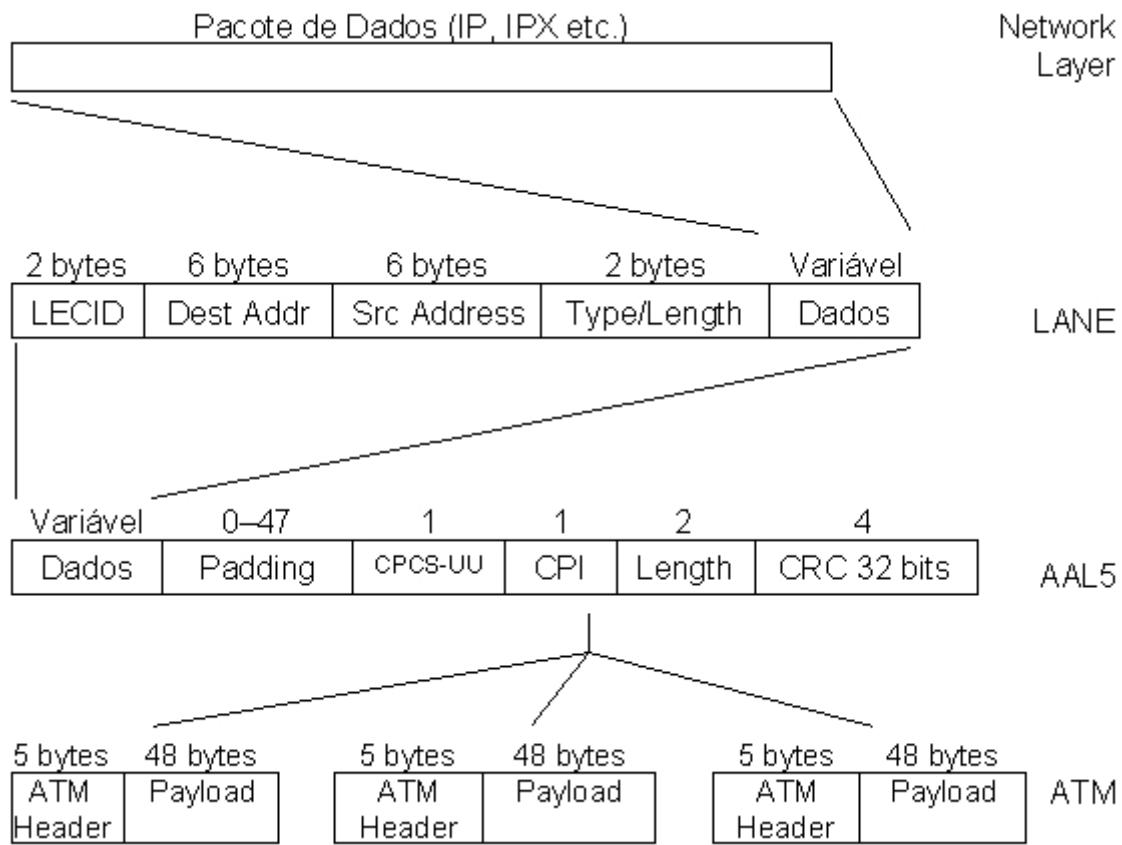
- **Configuration Direct:** É estabelecido entre um LEC e o LECS, na fase de inicialização, para obter informações de configuração, como o endereço ATM do LES. É bidirecional. Em geral, este VCC é encerrado após a obtenção destas informações, mas isto não é obrigatório.
- **Control Direct:** É estabelecido entre o LEC e o LES, na fase de inicialização, para troca de frames com informações de controle. É bidirecional.
- **Control Distribute:** É um VCC ponto a multiponto estabelecido pelo LES para todos os clientes de uma ELAN, na fase de inicialização. É usado para distribuição de informações de controle, se o LES preferir não usar o Control Direct para este fim.

VCCs de Dados

- **Data Direct:** É estabelecido entre LECs para troca de dados unicast. É bidirecional e ponto a ponto. A versão 2.0 implementa mecanismos que permitem às camadas superiores estabelecer parâmetros de qualidade de serviço (QoS) para este tipo de conexão. Também na versão 2.0, pode ser multiplexado.
- **Multicast Send:** É estabelecido entre um LEC e o BUS, para envio de dados em broadcast ou multicast, além de transmissão unicast para um destino cujo endereço ATM ainda não foi encontrado. A versão 2.0 define o Default Multicast Send, que é associado com o endereço de broadcast (todos os bits '1'). Podem ser estabelecidos para o mesmo BUS VCCs para endereços de grupo específicos, chamados Selective Multicast Send. O BUS pode optar por usar o Multicast Send para envio de dados para o LEC, portanto ele deve ser bidirecional.
- **Multicast Forward:** É um VCC multiponto estabelecido pelo BUS para os LECs. O BUS pode estabelecer mais de uma conexão deste tipo para um dado LEC, com a finalidade de enviar multicasts seletivos.

Formato Dos Quadros De Dados

Como foi dito anteriormente, o LEC passa à AAL5 um quadro de formato semelhante ao dos quadros Ethernet e Token Ring. Para simplificar, este trabalho abordará somente ELANs Ethernet. A figura a seguir descreve a trajetória de um pacote de dados desde a camada de rede (nível 3 do modelo OSI) até a camada ATM (nível 1, camada Física do modelo OSI).



É fácil perceber que o frame usado pelo ELAN é semelhante ao Ethernet, isto para facilitar a comunicação com as redes LAN tradicionais. As diferenças são:

- Não existe preâmbulo nem delimitador de início de quadro, pois a rede ATM tem seus próprios mecanismos de sincronização.
- Acrescenta-se o campo LEC ID, cuja utilização será vista mais adiante.

- Não há o 'trailer' com o FCS (Frame Check Sequence), pois a camada AAL5 já inclui um código de detecção de erros.
- Uma bridge (switch LAN) ao passar um quadro da rede ATM à rede LAN tem de refazer o quadro, incluindo o preâmbulo e o FCS e retirando o LEC ID (que não terá mais utilidade, já que o quadro estará saindo da rede ATM). Para passar da LAN à rede ATM realiza as operações inversas.

Há também outros tipos de quadros usados no ELAN. Na versão 2, introduziu-se a multiplexação no nível LLC. Os quadros usados para este tipo de transmissão são iguais aos quadros de dados normais, acrescidos de um cabeçalho específico do multiplexador LLC.

MPOA – Multi Protocol Over ATM

Como já foi dito, o tráfego entre ELANs tem que ser comutado na camada rede, o que geralmente é feito através de roteadores. O problema que isto apresenta é que os protocolos de nível 3 em geral oferecem serviços datagrama e calculam a rota para cada pacote enviado. Isto acarreta um atraso inaceitável para uma rede ATM. Se os dois computadores estão na mesma "nuvem" ATM, deve ser possível aproveitar esta rede para transferir dados entre eles.

O MPOA é um serviço definido pelo ATM Forum para complementar o ELAN e que visa a otimizar a transferência do tráfego entre ELANs. Ele faz uso do protocolo de roteamento NHRP (Next Hop Resolution Protocol) para criar atalhos entre as ELANs, evitando o processo de cálculo de rotas no roteador. Cada ELAN é configurada como uma LIS (Logical IP Subnet), ou seja, uma sub-rede IP.

O MPOA possui dois componentes:

- O MPOA Client (MPC).

- O MPOA Server (MPS).

O MPC é implementado nas estações e switches de borda, enquanto que o MPS é implementado nos roteadores. Ele funciona da seguinte forma:

- Inicialmente, um pacote para outra ELAN é enviado ao roteador.
- O MPC monitora o tráfego através do LEC, tentando identificar fluxos; como identificar os fluxos é deixado a critério do implementador.
- Quando se configura um fluxo, o MPC envia um aviso ao seu MPS, pedindo que se crie um atalho.
- O MPS vai propagando o aviso pelos MPSs (roteadores), até chegar ao que serve ao MPC destino.
- O MPC responde com o endereço ATM do LEC destino, que vai sendo propagado de volta pelos MPSs.
- De posse do endereço ATM destino, o MPC inicial cria um atalho, que nada mais é que um VCC através da rede ATM até o destino.

A partir daí, os dados são enviados pelo atalho, que fica estabelecido até que passe muito tempo sem atividade.

Deve-se notar que as entidades do MPOA (MPC e MPS) trocam informações através do serviço LAN Emulation. Cada MPC e MPS tem de ter um LEC associado, e a troca de dados do MPOA ocorre como qualquer outra troca de dados. Para que uma estação suporte o MPOA, ela tem de possuir um LEC versão 2.0.

Futuro Do LAN Emulation

O LANE foi desenvolvido para levar até as redes corporativas de dados (baseadas em LANs) os benefícios do ATM, que é em sua essência uma tecnologia de WAN. As diferenças fundamentais entre os serviços de uma LAN e do ATM fazem com que a sua interconexão seja muito complexa. Além disso, o LANE deverá ser usado juntamente com o MPOA para aumentar sua escalabilidade, permitindo que se construam backbones corporativos maiores usando a rede ATM. Isso agrega ainda mais complexidade à rede. Aliás, a complexidade não é uma característica somente do LANE e do MPOA, ela pode se estender para o ATM e seus serviços de forma geral.

Apesar desta complexidade, os preços dos equipamentos ATM vêm caindo de forma considerável nos últimos anos. Mesmo assim, ainda são maiores que os dos competidores. No caso de backbones corporativos, o principal destes é o Gigabit Ethernet. Este apresenta como sua maior vantagem a simplicidade na migração, já que é uma extensão do Ethernet. Desta forma, ele se integra facilmente à base instalada.

Por outro lado, espera-se que o ATM tenha mais facilidade de se integrar às MANs e WANs, à medida que as operadoras e provedores de serviço forem oferecendo redes públicas ATM a preços cada vez mais competitivos.

O grande argumento em favor do ATM, no entanto, é a garantia de QoS. Foi um grande avanço da versão 2.0 disponibilizar esta característica. Entretanto, os protocolos e aplicações existentes ainda têm de ser modificados para poderem usar esse serviço. O desenvolvimento de APIs que usam ATM em modo nativo também é promissor, pois assim poderão ser criados aplicativos que usem diretamente os benefícios do ATM.

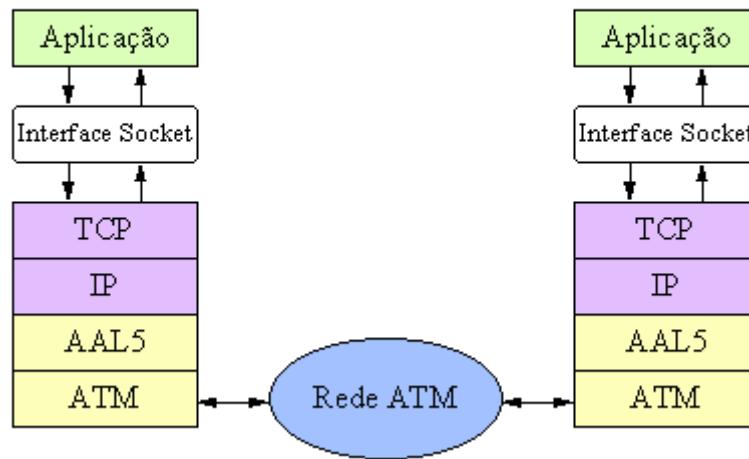
TCP/IP Sobre ATM

O trabalho conjunto entre o protocolo de transporte TCP sobre uma infra-estrutura ATM é de fundamental importância para o sucesso das redes ATM, devido a esse motivo é que foi desenvolvido o LAN Emulation suportando múltiplos protocolos. A pergunta de quem

controlará quem ainda não está bem respondida, isto é, o controle de congestionamento continuará com a camada de Transporte (pontos finais da rede) ou será controlado pela rede, para tal fim o comportamento do protocolo TCP sobre o protocolo ATM deve ser entendido, a seguir fazemos um breve análise deste assunto tão importante.

Para serviços de taxa constante (Constant Bit Rate – CBR) e taxa variável (Variable Bit Rate – VBR), as redes ATM provêm garantias para uma Qualidade de Serviço (QoS) a partir de parâmetros como banda e atraso. Para estes serviços, o controle de congestionamento é realizado pelo controle de admissão e alocação de banda, sendo que as conexões são rejeitadas no chamado tempo de estabelecimento da conexão.

TCP sobre ATM



Para serviços que fazem uso da banda disponível (Available Bit Rate – ABR), com características do melhor atendimento possível (best-effort), os requisitos não são especificados, e a rede deve prover dinamicamente uma fatia justa da banda disponível. É neste caso onde se encaixa o TCP, e o controle de congestionamento deve ser, portanto, realizado por mecanismos reativos.

Como os quadros de protocolos de camadas superiores são fragmentados em células ATM, a perda de uma única célula torna a transmissão dos restantes daquele quadro em um

desperdício de banda. Para evitar este desperdício, podem ser empregados os mecanismos EPD (Early Packet Discard) e PPD (Partial Packet Discard), onde as demais células que compõem o quadro corrompido são descartadas.

O TCP depende das perdas de pacotes (Timeout para retransmissão ou três ACKs repetidos) como indicação de congestionamento, podendo receber mensagens ICMP (Source Quench) mas que são raramente utilizadas devido ao consumo de banda. Como em redes de alta velocidade, filas grandes representam atrasos maiores, é importante uma forma explícita de retroalimentação para indicar congestionamento antes da formação de enormes filas nos buffers.

Uma forma para complementar o controle de congestionamento a nível de camada de transporte (nível 4 do modelo OSI) é a utilização de um mecanismo de prevenção de congestionamento nos roteadores, como o Gateway RED (Random Early Detection), e o de notificação explícita de congestionamento ECN (Explicit Congestion Notification).

Com RED, o Gateway indica congestionamento através da marcação ou descarte randômico de um pacote assim que for ultrapassado o tamanho médio de fila. Outras vantagens do RED são: a prevenção de sincronização global e a prevenção de descarte desnecessário de células ATM de pacotes TCP.

Com RED e ECN, pode-se ter o controle de congestionamento independente do ATM notificando o TCP, de forma mais eficiente do que por perda de pacote, nas bordas da rede ATM.

Como a tecnologia ATM ainda não teve o sucesso como originalmente seus projetistas tivessem desejado muita pesquisa esta sendo desenvolvida para poder adaptar as redes atuais com redes ATM.

O desempenho de conexões TCP em redes ATM de alta velocidade é fundamental considerando a importância do protocolo TCP/IP nas transferências de dados. A partir dos mecanismos de controle de congestionamento da camada ATM, percebe-se a preocupação em obedecer a requisitos de perda de células através de mecanismos reativos.

A forma do controle de congestionamento com abordagem por taxa influenciará definitivamente o desempenho de controles de congestionamento de camadas superiores. A interação entre o TCP e os controles de congestionamento da camada ATM é relevante também para outros protocolos da camada de transporte como IPX, NFS, etc. De forma que o entendimento das causas do fraco desempenho do TCP sobre ATM possa ajudar na definição de modificações no TCP e no controle de congestionamento do ATM.

Existe um ótimo tutorial sobre a tecnologia ATM no seguinte Link:

<http://www.teleco.com.br/tutoriais/tutorialatm/default.asp>.

Também existe uma apostila para download em:

<http://www.apostilando.com/download.php?cod=207&categoria=Redes>.

UNIDADE 28

Objeto: Entender o funcionamento básico de uma rede Netware da Novell.

Pilha De Protocolos IPX/SPX

Os protocolos IPX/SPX foram desenvolvidos pela Novell com base em um conjunto de protocolos XNS (Xerox Network Systems) da Xerox.

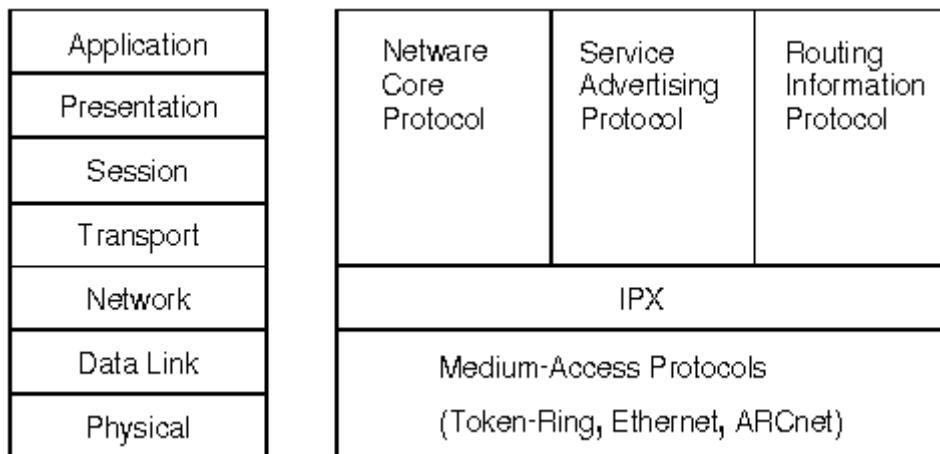
Esse protocolo era muito utilizado em versões anteriores ao Netware 5 e depois foram gradativamente substituídas pelo protocolo TCP/IP.

Antigamente ate o TCP/IP era suportado através do IPX/SPX. A principal função do IPX (Internetwork Packet Exchange) é receber pacotes através da internetwork. Conforme as estações efetuam a transmissão de dados pela internetwork, o IPX anexa um cabeçalho ao inicio dos dados.

A maior parte das aplicações que são nativas para um ambiente IPX/SPX puro fazem uso do IPX para melhor controle sobre as informações e a transferência de arquivos.

O SPX (Sequenced Packet Exchange) foi projetado com base no SPP (Sequenced Packet Protocol) da Xerox. O SPX oferece a entrega de pacotes garantida (orientada pela conexão). Quando o protocolo é orientado para conexão, exige mais requisitos de espaço no buffer e pacotes/segundo.

As redes Novell usam uma variedade de protocolos. Muitos dos quais foram desenvolvidos especialmente para redes Netware. A arquitetura de protocolos necessários para a comunicação entre máquinas servidoras e clientes NetWare são definidos a seguir:



O protocolo SPX é utilizado para proporcionar a segurança e confiabilidade da transmissão do pacote para o protocolo IPX.

Atribuição De Endereços IPX

O endereçamento de pacotes de forma adequada é um dos fatores mais importantes para que o roteamento seja efetuado corretamente em uma internetwork. A figura abaixo mostra o esquema de roteamento IPX.

Rede

Nó

10268043	00002B3FD5FB
----------	--------------

Endereçamento IPX

Para reencaminhar um pacote o IPX usa os seguintes elementos de endereçamento:

- Endereço de rede
- Endereço de rede interna

- Endereço de nó (físico - MAC)
- Número do soquete

Elementos De Endereçamento Em Redes IPX

O endereço de rede é um número hexadecimal de 8 dígitos (4bytes) que faz a identificação de uma rede lógica. O endereço deste tipo serve como base para o roteamento internetwork IPX.

O endereço de rede é atribuído quando se vincula um protocolo à placa de rede. Deve-se tomar bastante cuidado ao atribuir um número exclusivo numa rede Novell para evitar possíveis transtornos e para garantir o endereçamento adequado.

A diferença principal entre o IPX e o XNS está no uso de diferentes formatos de encapsulamento Ethernet. A segunda diferença está no uso pelo IPX do Service Advertisement Protocol (SAP), protocolo proprietário da Novell.

O endereço IPX completo é composto de 12 bytes, representado por 24 dígitos hexadecimais.

Por exemplo:

AAAAAAA	00001B1EA1A1	0451
IPX External	Node Number	Socket
Network	Number	Number

Por sua vez, o SPX é protocolo de transporte das redes Netware que incrementa a confiabilidade do protocolo IPX mediante a supervisão do envio de dados através da rede. O SPX é orientado a conexão, ele verifica e reconhece a efetivação da entrega dos pacotes a

qualquer nó da rede pela troca de mensagens de verificação entre os nós de origem e de destino.

A verificação do SPX inclui um valor que é calculado a partir dos dados antes de transmiti-los e que é recalculado após a recepção, devendo ser reproduzido exatamente na ausência de erros de transmissão. O SPX é capaz de supervisionar transmissões de dados compostas por uma sucessão de pacotes separados. Se um pedido de confirmação não for respondido dentro de um tempo especificado, o SPX retransmite o pacote envolvido.

Se um número razoável de retransmissões falharem, o SPX assume que a conexão foi interrompida e avisa ao operador.

Como o NetBEUI, o IPX/SPX é um protocolo relativamente pequeno e veloz em uma LAN. Mas, diferentemente do NetBEUI, ele suporta roteamento um legado do XNS. A Microsoft fornece o NWLink como sua versão do IPX/SPX. É um protocolo de transporte e é roteável. Pode haver conflitos tanto de nome como o de endereço, por exemplo.

Endereço De Rede Interna

O endereço de rede interna é constituído de um número hexadecimal de 8 dígitos (4 bytes) que possibilita ao servidor a função de roteamento interno de serviços para protocolos da camada superior. A atribuição de numero para uma rede interna IPX é feita quando se efetua a nomeação do servidor Netware.



Endereço Do Nô

O endereço nó (endereço físico) é um número hexadecimal de 12 dígitos (6 bytes). O IPX faz o uso do endereço MAC que esta atribuído para cada placa de rede como o endereço de nó. Este endereço especifica a conexão entre a placa de rede e a mídia de transmissão.

Um detalhe é que sempre quando o pacote é endereçado à rede interna, este pacote tem o endereço de nó como 000000000001.

Número De Soquete

O IPX faz uso de um número adicional para determinar o destino do pacote dentro de um dispositivo. O número de soquete é um exemplo desse tipo de numero. Os números de soquete representam os processos, assim como os serviços que operam dentro de um nó.

Na parte de endereçamento inicial da rede e do servidor deve ser planejado o endereçamento para evitar a perda dos pacotes (melhor fazer isso sempre na implementação inicial).

Ao fazer a definição de endereços IPX, siga as seguintes regras simples:

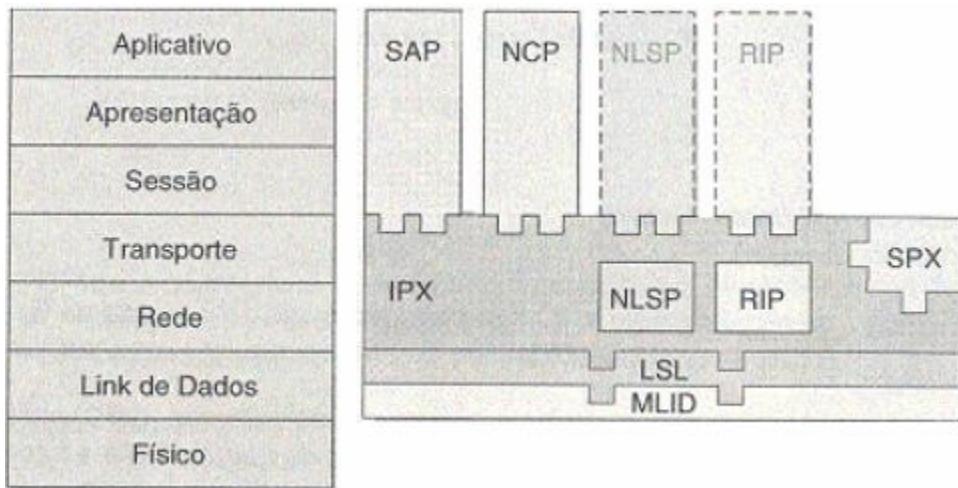
- Cada rede lógica que existe em uma internetwork deve ter um número de rede exclusivo para que opere corretamente. Isso também inclui os números atribuídos a uma rede interna do servidor Netware.
- Os dispositivos de uma rede lógica devem ter um endereço de nó exclusivo.

Obs.: Assim como no endereçamento IP existem endereços que não estão disponíveis para endereçamento de rede, são estes endereços o 00000000 e o FFFFFFFF e o FFFFFFFF (estes endereços são utilizados para finalidades especiais).

O Modelo OSI E A Pilha De Protocolos IPX/SPX

Os protocolos IPX e SPX, apesar de serem modulares e organizados em camadas, não se ajustam perfeitamente às camadas do modelo OSI.

Por tal motivo, é freqüente que as implementações dos fabricantes acabem satisfazendo suas próprias necessidades e utilizam métodos similares aos requeridos pelo modelo de referência OSI, os protocolos estão agrupados como na figura abaixo:



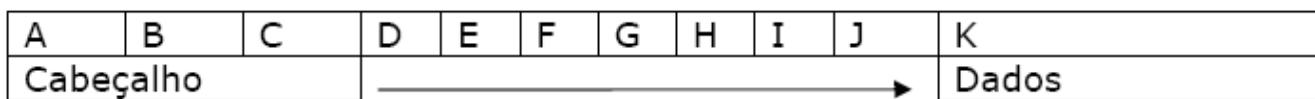
NCP – NetWare Core Protocol

O NCP define o controle da conexão e dos códigos de requisição de serviço que tornam possíveis a interação entre clientes e servidores. Associado com o sistema operacional de rede Netware, partes do NCP foram implementadas em outras plataformas como Linux, Windows e vários sistemas UNIX.

O NCP é utilizado para acessar arquivos, diretórios, sincronização de relogio, execução de comandos remotos e outras funções para serviços de rede. Aplicações utilizando o protocolo TCP/IP fazem uso da porta 524 (TCP/UDP) e dependem do protocolo de localização de serviços (Service Location Protocol - SLP) para a resolução de nomes. O diretório eletrônico (eDirectory) da Novell utiliza o NCP para sincronizar mudanças de dados entre os servidores em uma árvore de serviços de diretório.

Protocolo IPX

O formato do pacote IPX é como apresentado abaixo.



Onde cada letra indica um campo:

A = Checksum (16 Bits)

G = Soquete de Destino (16 Bits)

B = Comprimento (16 Bits)

H = Rede de Origem (32 Bits)

C = Controle de Transporte (8 Bits)

I = Máquina de Origem (48 Bits)

D = tipo de Pacote (8 Bits)

J = Soquete de Origem (16 Bits)

E = Rede de Destino (32 Bits)

K = Dados

F = Máquina de Destino (48 Bits)

O protocolo IPX é um protocolo da camada de Rede sem conexão que efetua as tarefas de endereçamento e roteamento entre redes Netware.

O IPX em caso de dados externos passa os datagramas completos para o software adequado que efetua o controle da interface de rede. As estações intermediarias fazem uso do IPX para efetuar o roteamento dos pacotes para o destino final.

Quando os pacotes atingem uma estação de trabalho ou um servidor de destino, o IPX faz a verificação se os dados do pacote atingem o processo adequado da camada superior.

A principal função do IPX é a de roteamento. Ele toma decisões com base nas informações sobre alcance de rede que são compiladas pelo protocolo RIP (Routing Information Protocol) ou NLSP (Netware Link Services Protocol).

Protocolo SPX

O formato do segmento SPX é apresentado abaixo.

A	B	C	D	E	F	G	H	IK
Cabeçalho	→							Dados

Onde cada letra indica um campo:

A = Cabeçalho IPX (30 Bits)

B = Controle de Conexão (8 Bits)

C = Tipo de Fluxo de Dados (8 Bits)

D = ID da Conexão de Origem (16 Bits)

E = ID da Conexão de Destino (16 Bits)

F = Número de Seqüência (16 Bits)

G = Número de Confirmação (16 Bits)

H = Número de Alocação (16 Bits)

I = Dados

O SPX oferece a entrega de pacotes orientada pela conexão. O IPX é utilizado como meio de transporte. O SPX faz o aprimoramento do protocolo IPX, gerando uma entrega confiável. Ele dispõe de serviços de segmentação, reconstrução e seqüência de segmentos para transmissões que são grandes demais para se ajustarem ao tamanho de frame, como os que são impostos pela camada de enlace.

O SPX faz uso de circuitos virtuais que são indicados como conexões. Elas recebem identificadores específicos (IDs) de conexão, conforme é definido no cabeçalho do protocolo SPX. Existe a possibilidade de se anexar diversos IDs de conexão em um único soquete.

Roteamento Com RIP/SAP

O IPX e seus protocolos de roteamento podem fazer a notificação para as estações sobre os serviços que estão disponíveis na rede, além de efetuar o trabalho de reencaminhar pacotes.

O RIP é um protocolo de roteamento de vetor de distância IPX; o SAP é um protocolo que faz a divulgação de serviço.

Os protocolos de divulgação de serviço podem ser utilizados para criar e manter as tabelas de Informações sobre Roteamento e Serviços, que são utilizadas pelo protocolo IPX. Quando se quer efetuar uma transmissão o dispositivo sempre solicita a rota mais rápida até o destino. O roteador que tem essa rota responde com seu endereço de rede e de nó no cabeçalho de rede.

Roteamento De Vetor De Distância: IPX RIP E SAP

O SAP e o RIP executam um trabalho de equipe para ajudar os servidores e nós de rede a localizarem os serviços de rede e as rotas para cada serviço de rede disponível em uma rede.

O RIP é um protocolo de vetor de distância que efetua o roteamento e consegue aprender e manter uma tabela de informações sobre roteamento de forma dinâmica. O SAP também pode aprender sobre informações de serviços.

RIP – Routing Information Protocol

O protocolo de roteamento RIP facilita o intercambio de informações entre computadores de uma rede NetWare. Assim como o IPX, o protocolo RIP tem origem no XNS. Entretanto, um campo extra, "número de saltos" (Hop Number), foi adicionado à estrutura dos pacotes para melhorar o critério de decisão quando na seleção da rota mais rápida para o destino do pacote. A inclusão deste campo proíbe uma integração do RIP de NetWare com a implementação do XNS.

O protocolo RIP fornece o método mais comum para transferir as informações de roteamento entre os roteadores que estão localizados na mesma rede. O RIP é um dos protocolos pioneiros de roteamento (que inclusive é utilizado em redes IP), ele é orientado seguindo o

conceito do vetor de distância (Distance Vector) para efetuar o cálculo das distâncias para um determinado destino. O RIP permite que os roteadores usem esse protocolo para atualizar suas tabelas de roteamento em intervalos programáveis, normalmente a cada trinta segundos.

Entretanto, como ele está constantemente conectando roteadores vizinhos, isso pode gerar um aumento de tráfego na rede. O RIP permite que os roteadores determinem que caminho deva ser utilizado para enviar os dados. Sempre que os dados trafegam por um roteador, ou seja, através de um número de rede, considera-se que trafegaram um salto. Nesse sentido, um caminho que tem um contador de saltos de quatro, por exemplo, indica que os dados que trafegam esse caminho devem passar por quatro roteadores antes de alcançar o destino final na rede.

Se existirem vários caminhos para um destino, o roteador, usando o RIP, seleciona o caminho com o menor número de saltos. Entretanto, como o contador de saltos é a única medida de roteamento usada pelo RIP para determinar melhores caminhos, ele não é necessariamente o caminho mais rápido. Todavia, o RIP continua muito popular e é amplamente implementado. Isso se deve principalmente ao fato de ter sido um dos primeiros protocolos de roteamento a ser desenvolvido.

Outro problema com o uso do RIP é que um destino pode estar localizado muito distante para que os dados o alcancem. Com o RIP, o número máximo de saltos pelos quais os dados podem trafegar é de quinze. Por isso, se a rede de destino estiver a mais de quinze roteadores de distância, será considerada inalcançável.

Existe a versão II do RIP que implementa algumas funções adicionais:

- Máscara de rede em ambientes de sub-redes de tamanhos variáveis
- Autenticação para atualizações do RIP
- Intervalos variáveis e configuráveis
- “Hold-down timer” permite agrupar e consolidar múltiplas alterações

O RIPv2 foi criado para controlar o fluxo das informações em circuitos de discagem sobre demanda, como: linhas discadas e ISDN. Essa implementação pode ser encontrada nas RFCs 1721, 1722, 1723 e 1724.

Propagação RIP

A propagação de pacotes RIP permite:

- As estações localizarem a rota mais rápida para aquele número de rede;
- Que roteadores solicitem informações (de outros roteadores) para atualizarem suas próprias tabelas internas;
- Que roteadores respondam às solicitações de estações e de outros roteadores;
- Que roteadores tenham certeza de que todos os roteadores estão compatíveis com a configuração das redes envolvidas;
- Que os roteadores detectem as modificações na configuração das redes.

SAP – Service Advertising Protocol

O protocolo SAP habilita os nós provedores de serviço, tais como servidores de arquivos, servidores de impressão, servidores de rotina, e servidores de aplicação. Os pacotes SAP existem para divulgar os serviços disponibilizados pelos servidores que estão disponíveis na rede.

O SAP faz com que estes servidores anunciem seus serviços e endereços. O SAP realiza a tarefa de adicionar e remover serviços na dinâmica entre redes. Como os servidores estão ativos, eles anunciam seus serviços usando SAP; quando eles estão sendo desligados eles anunciam que seus serviços não estarão mais disponíveis. (nesse caso via broadcast para o segmento local).

Os pacotes SAP podem ser de três tipos em uma rede Netware:

- Broadcasts Periódicos de Informações sobre SAP
- Consultas de Serviço SAP
- Respostas de Serviço SAP

Propagação Do SAP

Através do SAP, os clientes de uma rede podem identificar quais serviços estão disponíveis na rede e obtém o endereço dos servidores de onde eles podem acessar aqueles serviços. Isto é uma função importante, porque uma estação não pode iniciar uma sessão com um provedor de serviço sem que o primeiro conheça o endereço do servidor.

Um servidor Gateway, por exemplo, propagará pacotes SAP com uma freqüência de 60 segundos (o período é definido para todos os servidores que anunciam via SAP) para o segmento da rede no qual está conectado. O agente SAP em cada roteador daquele segmento copia a informação contida no pacote SAP para uma tabela interna do servidor gateway. Uma vez que o agente SAP em cada roteador mantém a informação sempre atualizada nos servidores disponíveis, um cliente que precise localizar um servidor gateway pode acessar o roteador mais próximo para obter o endereço IPX correto.

Aprender Sobre Serviços

O SAP e o RIP usam os mesmos métodos para manter suas tabelas. Abaixo segue os passos que descrevem como o SAP aprende sobre os serviços:

- O roteador faz a divulgação de seus serviços, se houver algum.

- O roteador faz o envio de um broadcast de um pacote de solicitação de serviço, que solicita uma lista dos serviços disponíveis na internetwork. Os roteadores vizinhos e os demais respondem com as informações de serviços conhecidos na internetwork.
- O roteador que fez a solicitação inclui as informações na sua tabela de Serviços.
- O roteador faz a divulgação das informações aprendidas sobre os serviços.

Após esse processo de aprendizado de rotas e serviços, o roteador pode responder a solicitações de serviço e rotas e fazer o reenvio de pacotes.

Link Da Rede WAN E Filtragem SAP

Tem que se tomar cuidado com o crescimento de tráfego na rede, conforme ele cresce o SAP pode ter dificuldades em divulgar serviços e o esforço pode consumir muita banda passante de forma desnecessária. Este tipo de tráfego também pode ser um problema em links de WAN.

Pode-se efetuar a filtragem de pacotes SAP para que os serviços não sejam divulgados na rede inteira. O tráfego pode ser filtrado nos dois sentidos, o de entrada e saída.

Roteamento IPX Com NLSP

- O NLSP (Netware Link Services Protocol) é um protocolo de roteamento de estado de link que substitui o RIP/SAP entre roteadores IPX. Ele é utilizado para trabalho entre redes Netware grandes e complexas, e não tem as limitações do RIP/SAP.
- O NLSP faz o uso de menos banda passante, é mais rápido na atualização das tabelas de informações sobre roteamento e é mais eficiente para uso em redes grandes.

- O NLSP usa um conjunto de termos de roteamento de estado de link próprios, são eles:

Adjacência – Indica Os Vizinhos Imediatos Do Roteador

- Link – O link é estabelecido quando os roteadores vizinhos se reconhecem e se confirmam. É uma espécie de conexão física entre dois roteadores adjacentes.
- Roteador Designado (DR) – Uma espécie de roteador líder que tem responsabilidades especiais e representa todos os outros roteadores.

Informações Sobre Como Manter Rotas E Serviços

O NLSP é responsável pela confirmação de que o BD (Banco de Dados) de cada roteador contenha as informações mais atuais. O NLSP pode ser utilizado para as finalidades abaixo:

Sincronizar Os Roteadores Em Uma Rede

Efetuar a notificação para todos os roteadores (na internetwork) de uma alteração que ocorreu na rede.

O roteador designado (Designated Router – DR) é responsável da verificação de que os roteadores estejam sincronizados com o mesmo BD de estado do link. O processo inclui os seguintes passos:

A cada 30 segundos o DR envia um CSNP (Complete Sequence Number Packet) a todos os roteadores que esta representando na rede. Um CSNP faz o resumo das entradas que o DR tem no BD de estado de link. Ele não faz a cópia do BD por inteiro.

Depois que o roteador recebe um CSNP ele faz o seguinte:

- Se o CSNP detectar uma entrada que não tem ou alguma atualização, faz o envio de um PSNP (Partial Sequence Number Packet) que faz a solicitação de informações

adicionais ao DR. O DR recebe a solicitação e envia um LSP para todos os roteadores com as informações que foram solicitadas.

- Se as informações do CSNP estiverem desatualizadas, o roteador que receptor efetuara a marcação e os novos LSPs serão enviados a todos os roteadores da rede.
- Se as informações do CSNP forem iguais as do BD do roteador, ele não fará nada.

Roteadores DR e IPX RIP/SAP

O protocolo NLSP é compatível com o RIP/SAP, mas somente o DR pode efetuar a conversão e a divulgação das informações sobre o RIP/SAP em uma internetwork NLSP. Se o ambiente for híbrido com roteadores RIP/SAP e NLSP, as rotas RIP serão consideradas “rotas externas”.

Comparação NLSP e RIP

Tanto o RIP quanto o NLSP utilizam a contagem de saltos e tiques para determinar a melhor rota para um pacote. A diferença é o número de saltos que cada um pode fazer até o destino.

RIP = 15 Saltos (16 é uma rota inatingível)

NLSP = 126 Saltos (127 é uma rota inatingível)

Os roteadores NLSP utilizam informações de primeira mão referente às rotas disponíveis, isso resolve o problema de contagem infinita que acontece quando se utiliza o RIP.

O fato do NLSP não enviar broadcasts periódicos se traduz em menos consumo de banda e o torna mais eficaz que o RIP que faz broadcasts e envia tabelas inteiras de roteamento periodicamente.

O NLSP por ser um protocolo de roteamento de estado de link, acaba atendendo as situações de WAN com maior eficiência. A banda passante do link é melhor utilizada a diferença do que acontece com o SAP.

UNIDADE 29

Objetivo: Conhecer este importante grupo de protocolos de rede desenvolvido pela IBM.

Pilha De Protocolos SNA

A arquitetura SNA (Systems Network Architeture) é uma arquitetura proprietária de rede desenvolvida pela IBM. Essa arquitetura não define somente uma pilha de protocolos, ela é um trabalho completo que possibilita a interconexão. Inclusive serviu de base para o modelo OSI, que foi desenvolvido uma década mais tarde. A arquitetura SNA é uma das arquiteturas mais antigas que ainda sobrevivem.

Essa arquitetura inicialmente somente suportava redes organizadas de forma hierárquica, com computadores, controladores de comunicação, controladores de cluster e terminais. Na atualidade ela suporta o processamento distribuído, internetwork, gerenciamento de rede e outros recursos avançados.

APPN – Advanced Peer-to-Peer Networking

Na década dos 90 a IBM baseou-se na arquitetura SNA para desenvolver uma arquitetura SNA do tipo Peer-to-Peer que foi chamada de APPN (Advanced Peer-to-Peer Networking). Ela explora os recursos de processamento dos computadores que estão distribuídos pela rede na forma de mainframes, microcomputadores e sistemas de PC.

A arquitetura APPN é uma melhora da arquitetura original SNA da IBM. A APPN, a qual inclui um grupo de protocolos e processadores, gerencia estabelecimentos de sessões entre nós pares (peer nodes), faz o cálculo de rotas de forma transparente e dinâmica. Um grupo de computadores utilizando a arquitetura APPN pode ser configurado automaticamente por um dos computadores que faz o papel do controlador de rede, de tal maneira que programas (do

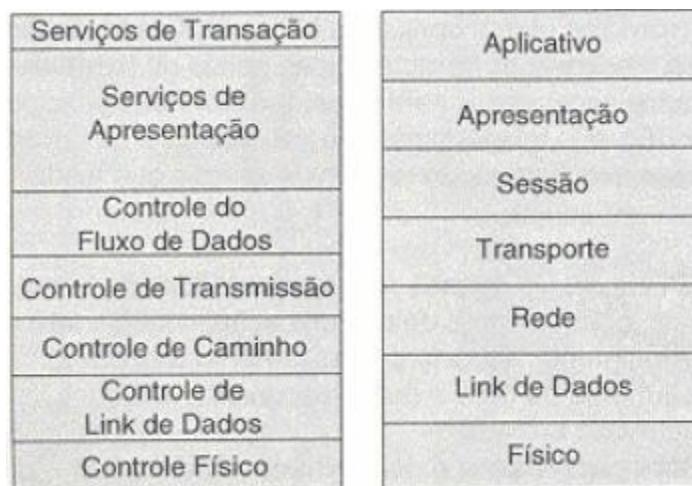
tipo peer) distribuídos em vários computadores do grupo podem se comunicar uns com outros utilizando o enrotamento de rede especificado.

Entre as principais características da arquitetura APPN temos:

- Um melhor controle distribuído de rede; isto devido à organização ser peer-to-peer em lugar de hierárquica, falhas nos terminais podem ser isolados.
- Intercambio de informação dinâmica sobre a topologia da rede, o que possibilita conexões, reconfigurações de rede e roteamento mais fáceis.
- Automação e definição dinâmica dos recursos de rede disponíveis.
- Flexibilidade, o que permite que a APPN possa ser utilizada em qualquer topologia de rede.

SNA Em Relação Ao Modelo OSI

Conforme citado anteriormente a SNA não é somente uma pilha de protocolos e sim um arquitetura completa; é possível mapear seus níveis para o modelo OSI relativamente bem.



As camadas da SNA são:

- **Controle Físico** – Essa camada executa as funções que dizem respeito a características elétricas, mecânicas e de controle da mídia física e inclusive estabelece as interfaces com essa mídia. Ela é muito similar à camada Física da OSI. A SNA não faz a definição explícita de protocolos específicos para essa camada. Ela pode ser inclusive implementada com Token Ring e outros padrões internacionais.
- **Data Link Control** – Essa camada é bem similar à camada de Enlace da OSI (Data Link). A SNA utiliza o SDLC para criar os links de comunicação em que os máster (primários) efetuam a comunicação com os slaves (secundários) e inclusive do Token Ring (IBM) em rede peer-to-peer.
- **Controle de Caminho** – Essa camada efetua várias das funções que estão descritas na camada de rede do modelo OSI. Essas funções são, por exemplo, roteamento, fragmentação e reconstrução de datagramas. Ela também executa algumas das funções da camada de enlace do modelo OSI, como controle de fluxo.
- **Controle de Transmissão** – Essa camada fornece o serviço de transporte confiável dos dados da origem ao destino e é similar à camada de transporte do modelo OSI. Essa camada também dispõe de serviços de criptografia e descriptografia (isso quem faz no modelo OSI é a camada de Apresentação). Então podemos considerar que ela executa essa função atribuída a camada de Apresentação da OSI.
- **Controle de fluxo de dados** – Essa camada é equivalente à camada de Sessão do modelo OSI. Ela efetua as funções de controle de fluxo de dados e controla o processamento de solicitações e respostas, determinando quem conversa, agrupa mensagens e interrompe o fluxo de dados conforme solicitado.
- **Serviços de Apresentação** – Essa camada especifica algoritmos de conversão de dados (essa função equivale a efetuada pela camada Apresentação do modelo OSI). Ela também controla o compartilhamento de recursos e efetua o sincronismo de operações.

- **Serviços NAU** – Essa camada tem funções similares à camada de Aplicação do modelo OSI. Ela fornece os serviços de aplicativo na forma de programas que possibilitam o processamento distribuído ou serviços de gerenciamento. O SNADS (SNA Distribution Services) é um bom exemplo de serviço de transação utilizado pelos aplicativos SNA.

Componentes Básicos Da Arquitetura

A arquitetura SNA utiliza produtos e equipamentos IBM e compatíveis e se baseia na estrutura de nós, como mainframes e sistemas de faixa média.

Essas redes podem incluir vários nós de computadores e possibilitam que um terminal de um domínio possa acessar aplicativos de outro domínio.

A SNA utiliza as seguintes unidades para interconectar os nós:

- **Unidade Física** – Que é a combinação de hardware, firmware e software que efetua o gerenciamento e monitoramento de um nó.
- **Unidades Lógicas** – É o que fornece meios para estabelecer conexões em uma unidade lógica e que possibilita trocar informações. Elas permitem o acesso à rede e as funções permitidas pelo VTAM.
- **Pontos de Controle** – São utilizados para gerenciar e controlar o fluxo de dados na rede. E se utilizam do SSCP principalmente.

Protocolos SNA E Termos Principais

- **Token Ring** – Essa especificação foi desenvolvida pela IBM para ser utilizada como modelo para IEEE 802.5. Ela faz a especificação de uma topologia de rede em forma de estrela física. O Token Ring especifica um método de acesso que permite a

transmissão de dados a 4 e 16Mbps. Inclusive cabos e conectores específicos estão definidos nessa especificação.

- **SLDC (Synchronous Data Link Control)** – Essa tecnologia faz o emprego de hardware específico para estabelecer uma interface específica com linhas de telefones dedicadas e de dial-up. Ela suporta conexão ponto-a-ponto ou multiponto, Half-duplex ou Full-duplex. O SDLC faz uso de mensagens de controle específicas, além de também adicionar cabeçalhos de nível de Data Link aos pacotes que são recebidos das camadas superiores.
- **NCP (Network Control Program)** – Faz o controle de recursos conectados em um controle de comunicação. Ele foi desenvolvido para operar processadores de front-end e executar as funções de data link e outras função limitadas a camada de Rede. Na atualidade o NCP dispõe das funções de roteamento e gateway em redes SNA.
- **VTMA (Virtual Telecommunications Acess Method)** – Ele efetua o controle de comunicação e fluxo de dados na rede SNA. Ele proporciona um único domínio, vários domínios e o recurso de rede interconectada. O VTAM pode utilizar o NCP para efetuar o controle de recursos de rede. O SSCP e o VTAM são considerados como termos sinônimos. Porem o VTAM é o produto do programa e o SSCP é o programa de software principal no VTAM.
- **APPN (Advanced Peer-to-Peer Networking)** – Esta em nível de rede permite a descoberta de rota, serviços de diretório e controle de fluxo de janela. Inclusive pode fornecer redes que operem somente por intermédio das Pus do tipo 2.1 (sem mainframe).
- **CICS (Customer Information Control System)** - Faz o suporte de aplicativos que efetuam o processamento de transação e faz a generalização dos comandos de entrada e saída para serem utilizados em uma rede. Os desenvolvedores de software podem utilizar o CICS para construir aplicativos que fazem transações em sistemas locais e remotos. Ele possibilita a comunicação do terminal com o aplicativo, o acesso a arquivos distribuídos, segurança, várias tarefas, gerenciamento de armazenamento

e recuperação de transações, reversão de transações e o recurso de reinicio com tolerância.

- **IMS (Information Management System)** – Ele é composto por dois produtos: O Gerenciador de Transações IMS e o Gerenciador de Banco de Dados IMS. Ele permite que vários aplicativos compartilhem BDs do Gerenciador de Bancos de Dados IMS e inclusive fornece recurso de comutação de mensagens e facilita o agendamento de transações de prioridade.
- **APPC (Advanced Program-to-Program Communication)** – Essa versão de SNA foi a primeira que possibilitou comunicações peer-to-peer entre unidades lógicas que não envolviam um host de mainframe.
- **DDM (Distributed Data Management)** – Possibilita o acesso aos arquivos remotos transparentes para os solicitantes de serviços SAN. Ele recebe solicitações e as executa através do SO local ou de um servidor DDM na rede (isso vai depender da localização física do arquivo).
- **SNADS (SNA Distribution Services)** – Esse é um serviço que esta no nível de aplicativo que possibilita as transferências de armazenamento e reencaminhamento (distribuição) de mensagens e documentos.
- **DIA (Document Interchange Architecture)** – Ele executa as funções que permitem a troca de documentos entre diferentes sistemas de computadores. Ele faz o gerenciamento de serviços de arquivo que incluem o armazenamento e recuperação de documentos e a transferência de arquivos.

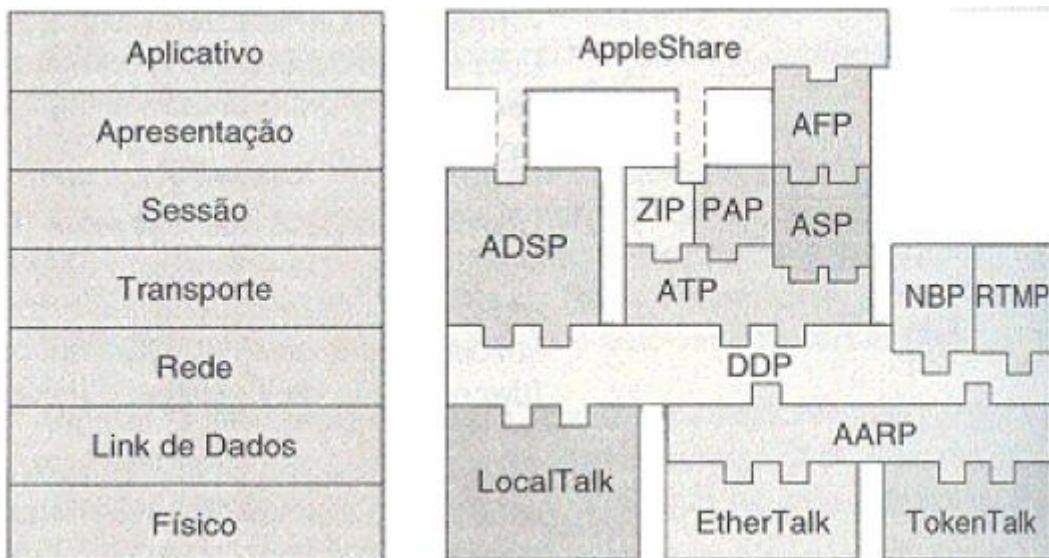
UNIDADE 30

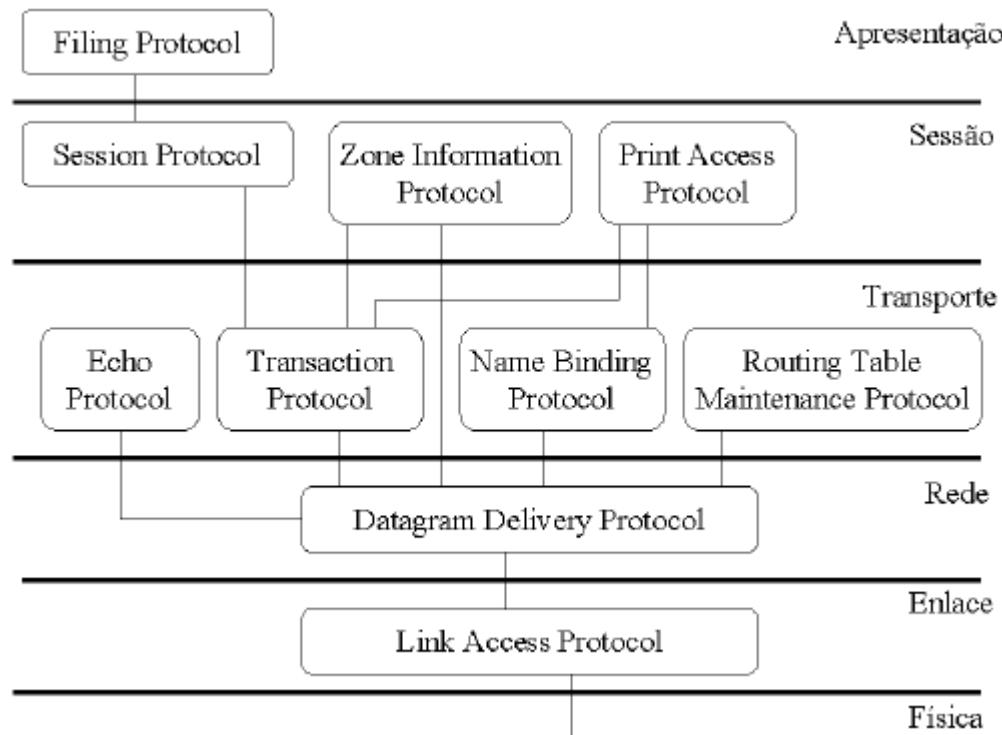
Objetivo: Conhecer os protocolos dos computadores Macintosh e suas funcionalidades e as principais tecnologias MAN e WAN..

Pilha De Protocolos Appletalk, SMDS & SONET/SDH

AppleTalk é uma série de protocolos de comunicações projetados pela empresa Apple Computer. É um sistema de rede que está disponível em todos os computadores Macintosh e outros periféricos, particularmente impressoras LaserWriter operando a 230 Kbps, além de muitos sistemas UNIX.

Os pacotes AppleTalk relacionados ao Macintosh e ao UNIX foram desenvolvidos dentro, ou são mantidos pelo Departamento de Informática de Tecnologia de Programação na Universidade de Melbourne.





Acima outra representação da Apple Talk em relação a OSI.

Principais Protocolos AppleTalk

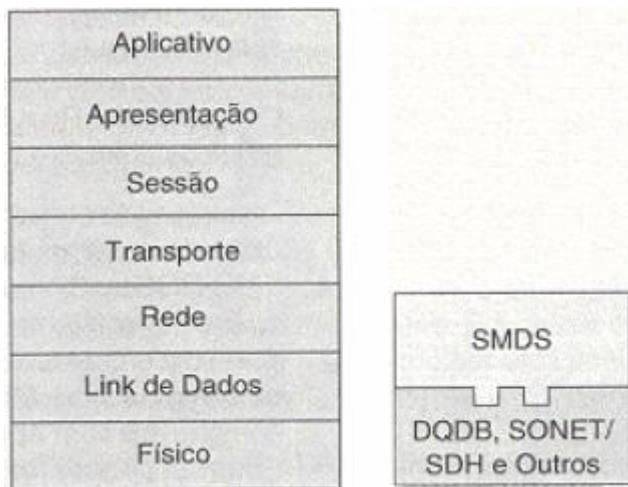
- **ALAP - Apple Talk Link Access Protocol:** Este protocolo provê serviços de baixo nível para o Apple Talk, através do controle de acesso à rede. Cada dispositivo de rede é denominado nodo, sendo identificado por um ID de 8 bits, único e dinâmico. O ALAP provê comunicação ponto-a-ponto, juntamente com facilidades de broadcast. O frame pode conter de 0 até 600 bytes de dados, além de um header e um tail. O header é composto por 3 bytes que indicam, respectivamente, o ID do nodo destino, o ID do nodo emissor e o tipo de protocolo, usado para identificar o processo cliente dentro de um nodo. Se o endereço de destino for 255, então a transmissão é realizada via broadcast. O tail contém um FCS (Frame Control Sequence) de 16 bits, usado para detecção de erros de transmissão. Este protocolo somente detecta erros; não implementa nenhum tipo de retransmissão (best-effort protocol).

- **DDP - Datagram Delivery Protocol:** Este protocolo executa como um cliente ALAP, provendo comunicação ponto-a-ponto através de sockets em redes locais Apple Talk (que podem possuir bridges). A comunicação é feita por datagramas, com até 586 bytes de dados.
- **RTMP - Routing Table Maintenance Protocol:** Este protocolo serve para o estabelecimento e gerenciamento de tabelas de roteamento para redes Apple Talk. Os nodos "não-bridges" utilizam este protocolo para descobrir o número da rede a qual estão conectados e o ID de um nodo bridge dentro dessa rede. Estes nodos executam uma parte do protocolo denominada RTMP stub, executando como cliente DDP e utilizando o socket 1 (estático).
- **NBP - Name Binding Protocol:** Protocolo para o gerenciamento de tabelas de nomes em cada nodo Apple Talk. Um nome é composto por um par nome, endereço de rede, conhecido como tupla. O conjunto de tabelas de nomes é denominado diretório de nomes. Este protocolo implementa duas operações básicas: permite que um nodo adicione entradas na tabela de nomes e procure por endereços de rede para nomes dentro dessa tabela. Neste último caso, o NBP executa como cliente DDP e faz broadcast de pacotes lookup para todos os nodos da rede, recebidos através do socket 2 em cada nodo.
- **ATP - Apple Talk Transaction Protocol:** Este protocolo provê transmissão confiável, livre de erros. Está baseado no conceito de transações, onde cada transação consiste em uma requisição e uma resposta. Cada requisição possui um identificador de 16 bits (único no sistema) e é repetida até que uma resposta válida seja recebida. O intervalo de retransmissão pode ser configurado pela aplicação cliente. Uma requisição é geralmente bastante pequena, ocupando somente um datagrama. Já as respostas podem ocupar até 8 datagramas, numerados de 0 a 7, para garantir a ordenação. O ATP executa como cliente DDP, com duas semânticas de funcionamento: at-least-once e exactly once.

- **EP - Echo Protocol:** Este é um protocolo interno da arquitetura Apple Talk, ou seja, não é acessível via Apple Talk Manager. Provê um serviço de eco através do socket 4 (estático), conhecido como "socket ecoador". Através desse socket, pacotes são recebidos e enviados de volta ao transmissor. O EP é utilizado para duas funções básicas dentro da arquitetura Apple Talk: para permitir que clientes DDP possam determinar se um nodo é atingível dentro da rede; para determinar o tempo médio de tráfego de um pacote dentro da rede, partindo de um emissor até um receptor remoto. Este serviço é utilizado para determinar timeouts dentro dos protocolos ASP e ATP. O EP executa como um cliente DDP, utilizando o socket 4.
- **ASP - Apple Talk Session Protocol:** Este protocolo provê funcionalidades para o estabelecimento e gerenciamento de sessões dentro de uma rede Apple Talk. É implementado com base no modelo Cliente/Servidor, com diferentes serviços em cada lado. Suas principais características compreendem a garantia de coerência e participação de ambos os nodos durante a sessão. Para tanto, implementa entrega ordenada e não replicada de datagramas entre clientes e servidores.
- **AFP - Apple Talk Filing Protocol:** Protocolo da camada de apresentação que permite a um cliente acessar arquivos em um servidor AFP. Este protocolo implementa toda a autenticação de usuários, bem como controle de acesso no nível de volumes e diretórios compartilhados. Executa como um cliente ASP.
- **Apple Share:** Adicionalmente, existe o protocolo Apple Share, que permite o compartilhamento de arquivos, impressoras e acesso a Internet via a adaptação do protocolo ATP para a utilização de TCP/IP.

SMDS

O SMDS (Switched Megabit Data Service) é um tipo de serviço de dados público de alta velocidade baseado em comutação de pacotes que permite performance do tipo das LANs em MANs ou WANs não teria limite de distância. Ele pode ser considerado um antecessor do ATM (Asynchronous Transfer Mode).



Acima esta representado o SMDS em relação a camada OSI.

Esse padrão efetua suporte para a camada de enlace assim como para vários padrões da camada Física. O SMDS funciona como serviço que atua na camada de enlace sem conexão que pode ser utilizado com DQDB e SONET. Ele faz comutação de célula (tamanho fixo) à taxa de 1,544 Mbps a 45 Mbps.

Embora utilizando padrões DQDB, o SMDS também pode ser utilizado sobre ATM. Oferece um tamanho variável de pacote, redes privadas virtuais (Virtual Private Network) e grupos fechados de usuários (Closed User Group) com velocidades de 34 Mbps a 150 Mbps.

O protocolo DQDB (Distributed Queue Dual Bus) foi definido pelo IEEE (802.6) para redes de área metropolitana, que opera como um duplo barramento (dual bus) cada um dos quais transporta dados em ambos os sentidos utilizando um método de acesso ao meio do tipo determinístico. Um sistema de fila mantém a ordem na transmissão. Oferecendo altas

velocidades (entre 2 e 300 Mbps), possui uma grande tolerância a falhas e um alto desempenho. Nunca foi muito popular tendo vindo a ser substituído pelo SMDS e pelo ATM com o qual possui algumas semelhanças.

SONET/SDH

SONET (Synchronous Optical Network) e SDH (Synchronous Digital Network) são padrões que são regionalizados para comportar as diferenças internacionais.

Disso resultam os padrões:

- SDH-Europa (que comporta CEPT)
- SDH-Japão
- SDH-SONET (que incorpora estruturas da América do Norte)



Tanto o SONET e SDH são usados como padrões para redes WAN, eles podem ser utilizados com base nas especificações da camada Física e são bastante confiáveis. Os documentos abaixo descrevem esses tipos de tecnologia:

- ITU G.707-709 – Taxas e formatos SDH
- ITU G.781-784 – Funções de equipamentos
- ITU G.957 – Interfaces óticas
- ITU G.958 – Sistemas de linha
- ITU G.803 – Arquitetura de rede
- ITU G.831 – Recursos de gerenciamento
- ITU G.774 – Modelo de informações sobre gerenciamento
- ANSI T1.105 – Taxas e formatos SONET
- ANSI T1.117 – Curto alcance de parâmetros óticos
- ANSI T1.118 – Comunicações OAM&P

O padrão SDH possui como principais características:

- Padronizar a interconexão de equipamentos ópticos de diversos fornecedores;
- Arquitetura flexível, capaz de se adaptar a futuras aplicações (como RDSI-FL) com taxas variáveis;
- Padronização da multiplexagem utilizando uma taxa de 51,84 Mbps;
- Incluem no padrão funções de extensão, operação e manutenção (OAM - Operation & Maintenance);
- Simplificação da interface com comutadores e multiplexadores devido à sua estrutura síncrona.

O SDH possui capacidade de transmitir:

- 2/ 34/ 140 Mbps;
- DS1/ DS2/ DS3 (EUA);
- FDDI;
- ATM;
- DQDB.

Foi definida uma hierarquia de taxas padronizadas para o SDH, portanto, existem as seguintes capacidades:

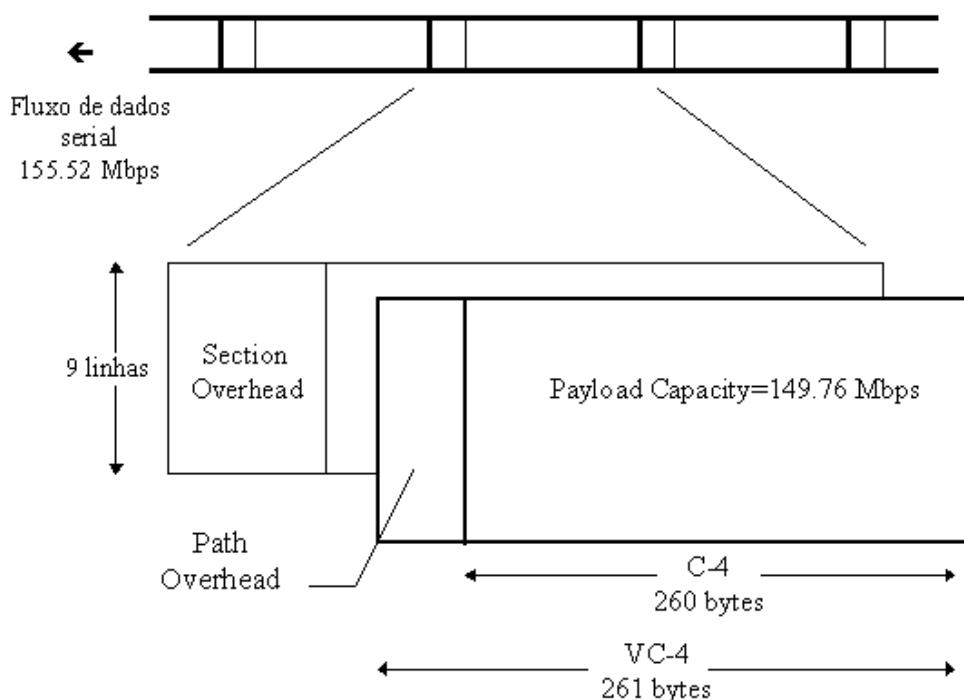
SONET/SDH	Taxa (Mbps)
STS-1/OC-1	51,84
STS-3/OC-3 STM-1	155,52
STS-4/OC-4 STM-3	466,56
STS-12/OC-12 STM-4	622,08
STS-18/OC-18 STM-6	933,12
STS-24/OC-24 STM-8	1244,16
STS-36/OC-36 STM-12	1866,24
STS-48/OC-48 STM-16	2488,32

Onde, **STS** = Synchronous Transport Signal Level, **OC** = Optical Carrier Level e **STM** = Synchronous Transfer Mode Level.

Estrutura De Um Quadro SDH

O quadro básico SDH é o quadro STM-1 (tabela anterior). Ele possui 2430 bytes transmitidos a cada 125 us, resultando em uma taxa de 155,52 Mbps (2430 bytes/quadro x 8 bits/quadro x 8000 quadros/seg. = 155,52 Mbps). Logicamente, o quadro pode ser considerado uma matriz de 9 filas de 270 bytes cada, sendo que cada fila é transmitida por vez.

Como já vimos anteriormente, em um sistema telefônico convencional, para se incluir ou retirar um tributário, há todo um processo de demultiplexação. Para facilitar isso, o SDH faz uso de apontadores para acessar, remover e inserir informações em um canal. Esses ponteiros estão contidos no cabeçalho do quadro (porém não fazem parte deste) e possuem referências à estrutura de multiplexação dos canais neste quadro. Na figura pode-se observar a estrutura de um quadro STM-1. O Virtual Container (VC) é utilizado para o transporte dos tributários.



O quadro é transmitido fim-a-fim na rede, sendo montado e desmontado apenas uma vez. O Virtual Container é formado pelo Container (C-4) e pelo Path Overhead. O Container (C-4)

possui uma capacidade de 149,76 Mbps (para o caso do transporte de um tributário de 140 Mbps) e pode conter também Path Overheads de mais baixa ordem (caso transmita outros tipos de tributários diferentes). O Path Overhead (de alta ordem) provê serviços de monitoração de alarme e monitoração de performance. O Section Overhead é um cabeçalho que provê facilidades para suportar e manter o transporte de um VC na rede, sendo que pode sofrer alterações ao longo do percurso.

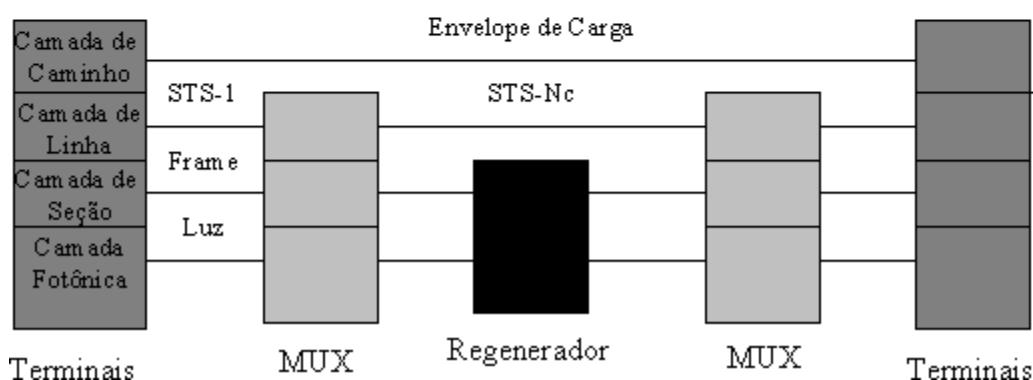
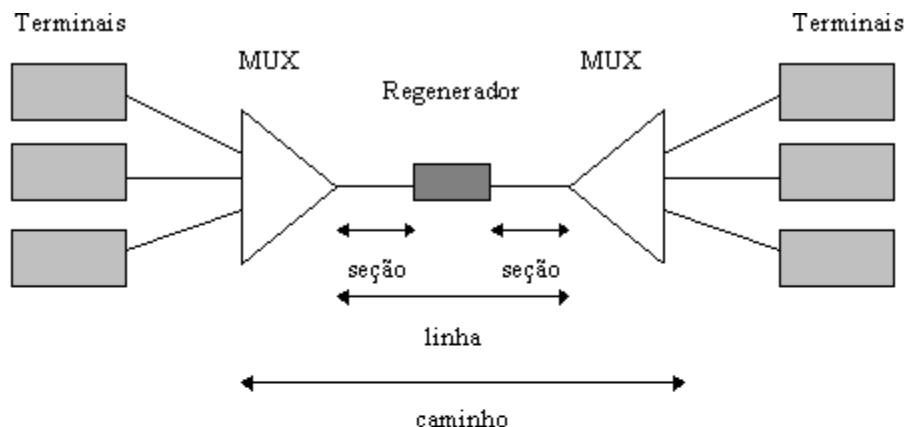
Arquitetura SDH

A arquitetura SDH é composta de uma hierarquia de quatro níveis:

1. **Camada Fotônica:** Esta no nível físico e inclui especificações sobre o tipo da fibra óptica utilizada, detalhes sobre a potência mínima necessária, características de dispersão dos lasers transmissores e a sensibilidade necessária dos receptores. É responsável, ainda, pela conversão eletro-óptica dos sinais.
2. **Camada de Seção:** É a responsável pela criação dos quadros SDH, embaralhamento e controle de erro. É processada por todos os equipamentos, inclusive os regeneradores.
3. **Camada de Linha:** Cuida da sincronização, multiplexação dos quadros e comutação. É responsável, ainda, pela delimitação de estruturas internas ao envelope de carga. Seu processamento ocorre em todos os equipamentos, exceto os regeneradores.
4. **Camada de Caminho:** Responsável pelo transporte de dados fim-a-fim e da sinalização apropriada. Processada apenas nos terminais.

A figura abaixo mostra as camadas fisicamente. Uma sessão representa, como no SNA, um link estabelecido entre dois receptores/transmissores (porém aqui esses links são ópticos). Para distâncias pequenas, a fibra pode ser ligada diretamente entre os usuários, mas se a distância for maior, há a necessidade da utilização de regeneradores. Uma linha é composta

de uma ou mais sessões (de modo que a estrutura do canal permanece a mesma), e o path (caminho) é o circuito completo, Fim-a-Fim.



Atividades

Antes de dar início à sua Prova Online é fundamental que você acesse sua SALA DE AULA e faça a Atividade 3 no “link” ATIVIDADES.



GLOSSÁRIO

1Base5 - Ethernet de Par Trançado sem blindagem; velocidade de 1 Mbps; a distância máxima entre estações de trabalho e o conector é de 500 metros. Não muito utilizado.

10Base2 - Cheapernet, ThinNet ou Thin Ethernet; velocidade de 10 Mbps; o segmento máximo de cabo é de 200 metros.

10Base5 - Ethernet espesso, o sistema de cabo especificado pela Dec e Xerox; velocidade de 10 Mbps; o segmento máximo de cabo é de 500 metros.

10Base-F - Ethernet de Fibra; utilizado entre estações de trabalho e um concentrador; velocidade de 10 Mbps; a distância estimada é de 2,2 quilômetros.

10BaseT - Ethernet de par trançado; velocidade de 10 Mbps. Muito popular.

Agente - Um programa de computador ou processo que opera sobre uma aplicação cliente ou servidor e realiza uma função específica, como uma troca de informações.

Alias - Significa segundo nome ou apelido. Pode referenciar um endereço eletrônico alternativo de uma pessoa ou grupo de pessoas, ou um segundo nome de uma máquina. É também um dos comandos básicos do UNIX.

ANSI - Acrônimo de American National Standards Institute, uma organização afiliada à ISO e que é a principal organização norte-americana envolvida na definição de padrões (normas técnicas) básicos como o ASCII.

Anatel - A Agência Nacional de Telecomunicações (Anatel) é uma autarquia brasileira, administrativamente independente, financeiramente autônoma, não subordinada hierarquicamente a nenhum órgão de governo brasileiro. Por ser uma Autarquia, é uma entidade auxiliar da administração pública descentralizada, tutelada pelo estado Brasileiro, e fiscalizada pela população.

Aplicação - Programa que faz uso de serviços de rede tais como transferência de arquivos, login remoto e correio eletrônico.

Archie - Um serviço de busca de arquivos armazenados em FTP anônimo. Pouco disseminado no Brasil.

ARPANET - Advanced Research Projects Agency Network. Rede de longa distância criada em 1969 pela Advanced Research Projects Agency (ARPA, atualmente Defense Advanced Projects Research Agency, ou DARPA) em consórcio com as principais universidades e centros de pesquisa dos EUA, com o objetivo específico de investigar a utilidade da comunicação de dados em alta velocidade para fins militares. É conhecida como a rede-mãe da Internet de hoje e foi colocada fora de operação em 1990, posto que estruturas alternativas de redes já cumpriam seu papel nos EUA.

ASCII – É a sigla da American Standard Code for Information Interchange. Trata-se de um esquema de codificação que atribui valores numéricos às letras do alfabeto, números, sinais de pontuação e alguns símbolos especiais para ser usado em computadores e dispositivos de armazenamento eletrônico de dados.

Assinatura - 1. Um arquivo (tipicamente de três ou quatro linhas) que as pessoas inserem no fim de suas mensagens; 2. Ato de subscrever uma lista de discussão ou newsgroup; 3. Informação que autentica uma mensagem.

ATM Protocolo de Modo de Transmissão Assíncrona de Dados em blocos de 53 bits, atingindo velocidades a partir de 155 MB/s até 1,7Gb/s. Corresponde à futura tecnologia para redes de dados e permitirá, entre outras coisas, videoconferência em tempo real.

B2B - Business-to-Business expressão utilizada para definir as relações que acontecem entre empresas. Muitas vezes aparece como qualificativo de determinadas ações de marketing, geralmente o direto, cujo público alvo são empresas. As vendas para empresas são orientadas por estratégias bastante diversas daquelas que são usadas para atrair o consumidor. As chamadas para empresas geralmente são atendidas, mas nem sempre chegam até as pessoas que efetivamente respondem pelas decisões de compra. Discadores

preditivos raramente são usados para vendas telefônicas nas iniciativas Business-to-Business.

Backbone - A interconexão central de uma rede Internet. Pode ser entendido como uma espinha dorsal de conexões que interliga pontos distribuídos de uma rede, formando uma grande via por onde trafegam informações.

Baud rate - Medida de taxa de transmissão elétrica de dados em uma linha de comunicação. Mede o número de sinais elétricos transmitidos por unidade de tempo.

BBS - Bulletin Board System é um sistema que, tipicamente, oferece serviços de correio eletrônico, repositório de arquivos (de programas, dados ou imagens) e outros serviços tais como conversação on-line. Seus assinantes, usualmente, obtém acesso através de linhas telefônicas (isto é, de voz) utilizadas via computador pessoal e modem.

BER – (Bit Error Rate) é um teste para determinar o percentual de bits errados em relação ao total de bits enviados, por exemplo, são transmitidos 1 milhão de bits por um canal e só um bit foi recebido com erro, então o nosso BER nesse canal de comunicações é de 10^{-6} . Uma fibra óptica tem um BER = 10^{-11} ou menor.

B-ISDN [RDSI-FL] – A B-ISDN (Broadband-Integrated Service Digital Network), ou seja, a Rede Digital de Serviços Integrados de Faixa-Larga é uma rede digital que integra serviços de diversas naturezas como voz, dados, imagens, etc. que deve substituir gradualmente a infra-estrutura física atual das redes de telecomunicações, em que cada serviço tende a trafegar por segmentos independentes.

BIT – É a menor unidade de informação em um sistema binário, um estado zero ou um. O bit é a menor unidade de informação que um computador pode processar (usualmente indicado por 1 ou 0). 8 bits equivalem a um Byte (ou octeto). A palavra BIT resulta da contração das palavras em inglês **BInary digiT** (BIT).

BITNET - Because It's Time Network. Rede de computadores formada em maio de 1981 para interconectar instituições educacionais e de pesquisa, fazendo uso de um protocolo chamado RSCS (Remote Spooling Communication System). Teve seu tráfego encerrado em 1996.

BNC - Vem de Baionet Nipple Conector, que poderia ser traduzido para "conector em forma de baioneta". É o conector usado em cabos de rede coaxiais, onde existe apenas um cabo de cobre, coberto por camadas de isolamento e blindagem.

BNC (2) - Um tipo de conector de vídeo encontrado em alguns monitores profissionais, onde existem cinco cabos separados, três para os sinais de cor (verde, azul e vermelho) e dois para os sinais de sincronismo horizontal e vertical. O objetivo de usar cabos separados é diminuir o nível de interferência, obtendo a melhor qualidade de imagem possível.

Bps - Uma medida da taxa de transferência real de dados de uma linha de comunicação. É dada em bits por segundo. Variantes ou derivativos importantes incluem Kbps (= 1.000 bps) e Mbps (= 1.000.000 bps).

BR Código ISO de identificação do Brasil na Rede, tipo de sufixo de um endereço na Internet. Um endereço brasileiro na Internet, registrado no órgão de gerenciamento da rede por aqui, sempre tem esta sigla.

Bridge - Um dispositivo que conecta duas ou mais redes de computadores transferindo, seletivamente, dados entre ambas.

Browser - Programa para visualizar, folhear páginas na Internet. Navegador, software para navegação da Internet. Os mais utilizado são o Netscape Navigator e o Internet Explorer.

Cabeamento estruturado - Técnica de disposição de cabos em um edifício caracterizada por uma configuração topológica flexível, facilitando a instalação e o remanejamento de redes locais.

Cabo UTP - Tipo de cabo mais utilizado nas topologias de redes de computadores atuais. É composto por quatro pares de cabos trançados entre si atingindo a velocidade de 155 milhões de bytes por segundo (155MBp/s). Pode alcançar até 100 metros entre duas conexões dentro da Categoria 5.

Categoria 5 - Categoria máxima homologada para redes de dados que estejam dentro das normas-padrão EIA/TIA (Associações das Indústrias Elétricas e Telefônicas dos E.U.A). Garantia de uma rede atual e com funcionamento perfeito.

CCITT - Acrônimo de Comitê Consultatif Internationale de Telegraphie et Telephonie, um órgão da International Telecommunications Union (ITU) das Nações Unidas que define padrões de telecomunicações. (Em 1993, foi extinto e suas atribuições passaram para o ITU-TSS, Telecommunications Standards Section da ITU.)

CERN - Trata-se do European Laboratory for Particle Physics, possivelmente o mais importante centro para pesquisas avançadas em física nuclear e de partículas, localizado em Genebra, Suíça. O nome CERN relaciona-se ao seu nome anterior, Conseil Europeen pour la Recherche Nucleaire. Para os usuários Internet, o CERN é conhecido como o local onde foi desenvolvido a Web.

Cliente - É um processo ou programa que requisita serviços a um servidor.

Ciberespaço - Espaço virtual onde a informação circula através de computadores. Espaço cibernético.

Conexão - Ligação entre computadores feita à distância que permite a comunicação de dados entre ambos.

Correio Eletrônico - Sistema de troca de mensagens através de redes de computadores. As mensagens podem conter textos e outros tipos de arquivos em anexo (attachment). Ver e-mail.

CPA - Central por programa armazenado. Centrais telefônicas com sistemas digitais controlados por computadores de alta capacidade de processamento, cujos terminais são os telefones.

Crosstalk - Tendência do sinal de um par de fios ser induzido em um par adjacente. D.G. Sigla para Distribuidor Geral. É um quadro que contém as conexões e organiza a distribuição de cabos de telefonia ou dados.

Domínio - É uma parte da hierarquia de nomes da Internet – DNS -, que permite identificar as instituições ou conjunto de instituições na rede. Sintaticamente, um nome de domínio da Internet consiste de uma seqüência de nomes separados por pontos (.). Por exemplo, ci.rnp.br. Neste caso, dentro do domínio ci.rnp.br, o administrador do sistema pode criar diferentes grupos como info.ci.rnp.br ou staff.ci.rnp.br, conforme a necessidade.

Domínio público, (software de) - Programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso. Em geral, o software pode ser utilizado sem custos para fins estritamente educacionais e não tem garantia de manutenção ou atualização. Um dos grandes trunfos da Internet é a quantidade praticamente inesgotável de software de domínio público, de excelente qualidade, que circula pela rede.

Download - Ato de "baixar" e carregar um programa, ou seja, fazer a transferência de arquivos de um computador remoto para seu computador através da rede.

DNS - O Domain Name System (DNS) é um serviço e protocolo da família TCP/IP para o armazenamento e consulta a informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes Internet em seus números IPs correspondentes.

EDVAC - (Electronic Discrete Variable Automatic Computer) foi um dos primeiros computadores eletrônicos. Diferentemente de seu predecessor ENIAC, utilizava o sistema binário e possuía arquitetura de von Neumann.

ENIAC - (Electrical Numerical Integrator and Calculator) foi o primeiro computador digital eletrônico de grande escala. Criado em fevereiro de 1946 pelos cientistas norte-americanos John Eckert e John Mauchly, da Electronic Control Company. O ENIAC começou a ser desenvolvido em 1943 durante a II Guerra Mundial para computar trajetórias táticas que exigissem conhecimento substancial em matemática, mas só se tornou operacional após o final da guerra. O computador pesava 30 toneladas, media 5,50 m de altura e 25 m de comprimento e ocupava 180 m² de área construída. Foi construído sobre estruturas metálicas com 2,75 m de altura e contava com 70 mil resistores e 17.468 válvulas a vácuo ocupando a área de um ginásio desportivo. Segundo Tom Forester, quando acionado pela

primeira vez, o ENIAC consumiu tanta energia que as luzes de Filadélfia piscaram. Esta máquina não tinha sistema operacional e seu funcionamento era parecido com uma calculadora simples de hoje. O ENIAC, assim como uma calculadora, tinha de ser operado manualmente. A calculadora efetua os cálculos a partir das teclas pressionadas, fazendo interação direta com o hardware, como no ENIAC, no qual era preciso conectar fios, relés e seqüências de chaves para que se determinasse a tarefa a ser executada. A cada tarefa diferente o processo deveria ser refeito. A resposta era dada por uma seqüência de lâmpadas.

EIA/TIA - Sigla para União das Associações das Indústrias de Telefonia e Associação das Indústrias de Elétrica dos Estados Unidos. Criaram as normas que regulam a instalação de redes de dados com o uso de cabos de par trançado (cabos UTP).

e-Accessibility - Basicamente o conceito de e-Accessibility é abrir a sociedade da informação para todos. Para se ter um sucesso real na Internet, os benefícios de uma sociedade da informação devem ser compartilhados com a sociedade toda, principalmente com aquelas pessoas que tem dificuldade no uso das novas tecnologias, tais como pessoas discapacitadas e as pessoas mais velhas ou idosas. Toda a sociedade deve ter as mesmas chances de poder usufruir os benefícios que traz a Internet, mas para isso as pessoas idosas e discapacitadas devem ter as ferramentas e as pessoas certas para lhes ensinarem o uso da acessibilidade a Internet.

e-Competences - As mudanças, na sociedade da informação, vêm muito rápido: Novas tecnologias e serviços aparecendo a diário significam que os usuários devem estar preparados para atualizar suas habilidades e competências, aqueles que não o fizerem, devido a uma falta de oportunidade ou motivação, correm o sério risco de ficarem para traz. Portanto, é fundamental estar preparados para poder fazer uso destas novas ferramentas, isto se conhece como o e-Competences, isto é fundamental para ter as habilidades corretas, o conhecimento e a atitude para assim poder obter o melhor da atual sociedade da tecnologia e da informação. As novas tecnologias as quais podem fazer as nossas vidas e o nosso trabalho muito mais simples e fáceis estão sempre aparecendo no mercado, mas se as

pessoas não podem fazer um uso apropriado delas, correm o risco de ficar para traz na era da informação globalizada.

e-Mail - Do inglês, electronic mail ou correio eletrônico. Endereço eletrônico para envio de mensagens na Internet. Exemplo: joaodasilva@embratel.com.br. Basicamente esta nomenclatura indica que o usuário João da Silva está (ou tem) uma caixa de correio eletrônico no servidor da Embratel, a letra @ (arroba) é o comando “at” (dos sistemas UNIX) que traduzido significa algo assim como “em” ou “aonde”, portanto, João da Silva se encontra em (at) um servidor da Embratel.

Ethernet - Padrão de rede (IEEE 802.3) local amplamente utilizado na década de 90, quando passaram a ser instalados em cabos UTP. É um sistema flexível, barato e com velocidade de transmissão de dados entre 4 e 10 MBp/s.

FAQ - Frequently Asked Questions, ou Perguntas Mais Freqüentes. Perguntas e respostas das questões e dúvidas mais freqüentes sobre um assunto.

FastEthernet - Padrão de rede local (IEEE 802.3u) do tipo Ethernet que atinge velocidades superiores daquelas encontradas nas velhas redes Ethernet (entre 80 e 100Mb/s).

FCS – O campo FCS (Frame Check Sequence), que traduzido do inglês seria algo assim como a seqüência de verificação (checagem) do quadro, é extremamente útil para verificar que os dados enviados foram recebidos sem alterações durante a viagem desde o computador transmissor ao receptor que poderia estar na própria rede local ou uma rede remota. Nos quadros Ethernet o FCS é um campo de 4 Bytes que basicamente contém um algoritmo de controle de erros a nível de bit (Checksum) que permite revisar a integridade do quadro recebido, desta forma se o quadro está correto ele é entregue às camadas superiores, caso contrário será descartado.

FDDI – O padrão FDDI (Fiber Distributed Data Interface) foi desenvolvido pelo ASC X3T9.5 da ANSI nos EUA e adotado pela ISO como padrão internacional (ISO 9314/1/2/3) em 1987. Inicialmente foi proposto para redes de comutação de pacotes, sendo mais tarde melhorado, onde a rede é dotada de capacidade de comutação de circuitos de modo a expandir o campo

de aplicações para a integração de voz, imagem e dados em tempo real. Este abrange o nível físico e de ligação de dados (as primeiras duas camadas do modelo OSI). A expansão de redes de âmbito mais estendido, ou seja, redes do tipo MAN (Metropolitan Area Network), são algumas das possibilidades do FDDI, tal como pode servir de base à interligação de redes locais, como em campus universitários. As redes FDDI adotam uma tecnologia de transmissão idêntica às das redes Token-Ring, mas utilizando cabos de fibra óptica, o que lhes concede capacidades de transmissão muito elevadas (na casa dos 100 Mbps ou mais) e a oportunidade de se alargarem a distâncias desde 100 até 200 Km, conectando entre 500 até 1000 estações de trabalho. Todas estas particularidades fazem do padrão FDDI altamente indicado para a interligação de redes LAN através de um backbone, neste caso, o backbone é a própria rede FDDI. Não existe requisito de configuração mínima. A rede FDDI fica altamente tolerante a falhas, devido à configuração de um anel duplo e por um mecanismo de isolamento de falhas implementado nas estações.

FDMA – Os sistemas FDMA (Frequency Division Multiple Access) conhecidos como sistemas de acesso múltiplo por divisão de freqüência são utilizados geralmente em sistemas de transmissão analógicos utilizando a multicanalização (ou multiplexação) em freqüência. O funcionamento básico é o seguinte: Cada canal de voz (de vários), que originalmente ocupa o mesmo espectro de freqüências com todos os outros canais, é alocado (através da multiplexação) a uma única banda de freqüências, porém ocupando diferentes posições um atrás do outro (como um trem) e assim todo esse grupo de canais serializados podem ser enviados de forma simultânea por um único meio de transmissão. Desta forma podem se transmitir muitos canais de banda relativamente estreita, como por exemplo, canais de voz cada um com uma largura de 4 kHz, por um único sistema de transmissão de banda larga.

Fibra Óptica - Tipo de cabo feito de cristal de quartzo muito fino que permite o tráfego de grandes pacotes de informações em altíssima velocidade (2 bilhões de bits por segundo- 2GBp/s) por meio de luz de 850 nanômetros de comprimento de onda, (multimodo) e que em geral é utilizado para a troca de pulsos informações entre grandes distâncias (aproximadamente 2.5 Km).

Frame-Relay - Protocolo que permite a conexão (com largura de banda ajustável de acordo com a demanda) entre duas redes locais através de uma rede pública utilizando comutação por pacotes.

Freqüência - Medida pela qual uma corrente elétrica é alternada, em hertz.

FTP - File Transfer Protocol - Protocolo de transferência de arquivos, usado para enviar e receber arquivos via Internet.

Gateway - 1. Sistema que possibilita o intercâmbio de serviços entre redes com tecnologias completamente distintas, como FidoNet e Internet; 2. Sistema e convenções de interconexão entre duas redes de mesmo nível e idêntica tecnologia, mas sob administrações distintas. 3 Roteador (terminologia TCP/IP).

GIF - Graphic Interchange Format - Formato gráfico utilizado em imagens e com grande capacidade de compressão. A maioria das imagens animadas na Internet é feita nesse formato.

GNU - acrônimo recursivo de: GNU is Not Unix (em português: GNU não é Unix).

GPL - General Public License (Licença Pública Geral), GNU GPL ou simplesmente GPL, é a designação da licença para software livre idealizada por Richard Stallman no final da década de 1980, no âmbito do projecto GNU da Free Software Foundation (FSF). A GPL é a licença com maior utilização por parte de projectos de software livre, em grande parte devido à sua adoção para o Linux.

GUI – O termo corresponde à Interface Gráfica do Usuário, ou em inglês Graphic User Interface, é a consola gráfica que todo programa visual tem, onde é disponibilizada a interface para que o usuário possa interagir com um determinado aplicativo ou hardware do computador, tais como, botões, janelas, menus, etc.

Hacker - Indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas. Originário do inglês, o termo é comumente utilizado no português sem modificação. Os Hackers utilizam toda a sua

inteligência para melhorar softwares de forma legal. Os Hackers geralmente são pessoas com alta capacidade mental e com pouca atividade social. Eles geralmente são de classe média e alta, com idade de 16 a 28 anos. A maioria dos Hackers são usuários avançados de Software Livre como o sistema operacional Linux. A verdadeira expressão para invasores de computadores é denominada Cracker e o termo designa programadores maliciosos e Ciberpiratas que agem com o intuito de violar ilegal ou imoralmente sistemas cibernéticos.

Hertz - Unidade de medida para definir freqüência, em ciclos por segundo.

Hipertexto - Destaque de palavras, geralmente sublinhadas, em um texto que remete a outros locais (texto ou imagem ou site) permitindo uma leitura não linear.

Home Page - Primeira página de um site na Internet. Tornou-se sinônimo de endereço Web.

Host - Em português, hospedeiro. Computador que hospeda, guarda as informações para uma rede, no caso, a Internet.

HTML - HyperText Markup Language, linguagem de programação básica da Internet. Permite ao browser exibir textos e outros recursos multimídia de um site.

HTTP - HyperText Transfer Protocol - Protocolo ou padrão de transferência de arquivos HTML através da Internet.

HUB - Dispositivo de conexão eletrônica entre o servidor e os outros micros de uma rede do tipo Estrela. Podem ser passivos, apenas distribuindo o sinal; ativos, que possuem um repetidor que regenera o sinal, inteligentes, que permitem monitoração dos micros, ou chaveados que funcionam fechando conexões não utilizadas e acelerando a velocidade de transmissão.

Impedância - Oposição ao fluxo dinâmico corrente em um meio de transmissão.

Internet - Significa a "rede das redes". Originalmente criada nos EUA, que se tornou uma associação mundial de redes interligadas, que utilizam protocolos da família TCP/IP. A Internet provê transferência de arquivos, login remoto, correio eletrônico, news e outros

serviços. Uma coleção de redes locais e/ou de longa distância, interligadas numa rede virtual pelo uso de um protocolo que provê um espaço de endereçamento comum e roteamento.

Intranet - Rede particular usada em empresas e instituições. Utiliza a tecnologia do ambiente Web da Internet, porém com acesso restrito aos usuários desta rede privada.

IP - O Internet Protocol é o protocolo responsável pelo roteamento de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP, desenvolvida e usada na Internet. É considerado o mais importante dos protocolos em que a Internet é baseada.

IRC - Acrônimo de Internet Relay Chat, serviço que possibilita a comunicação escrita on-line entre vários usuários pela Internet. É a forma mais próxima do que seria uma “conversa escrita” na rede.

ISO - International Organization for Standardization (ISO), uma organização internacional formada por órgãos de diversos países que discute, especifica e propõe padrões para protocolos de redes. Muito conhecida por ter estabelecido um modelo de sete camadas que descreve a organização conceitual de protocolos, o OSI.

ITU - International Telecommunications Union. Órgão da ONU responsável pelo estabelecimento de normas e padrões em telecomunicações.

JAVA - Linguagem de programação criada pela Sun Microsystems. Permite baixar pequenos programas (Applets) que são ativados na própria máquina do usuário. Foi criada para poder ser utilizada em qualquer tipo de computador.

Jitter – É uma variação estatística do retardo na entrega de dados em uma rede, ou seja, pode ser definida como a medida de variação do atraso entre os pacotes sucessivos de dados. Observa-se ainda que, uma variação de atraso elevada produz uma recepção não regular dos pacotes. Logo, uma das formas de minimizar a variação de atraso é a utilização de buffer (memória), aonde esse buffer vai armazenando os dados à medida que eles chegam e os encaminham para a aplicação a uma mesma cadência. Minimizar o Jitter é de extrema importância nos serviços de Voz sobre IP (VoIP), por exemplo.

JPEG - Joint Photographic Experts Group - Formato de arquivo de imagens comprimidas.

kHz – Kilo-Hertz significa mil Hertz. O Hertz é a unidade de medida básica dos sinais periódicos em sistemas de telecomunicações por radio freqüência. Lembrar que um 1 Hertz = 1 ciclo por segundo, como os sinais são periódicos, por exemplo, um sinal de 10 kHz significa que ele cumpre 10 mil vezes seu período (ciclo) a cada segundo, em outras palavras, esse sinal gira a 10 mil ciclos por segundo. Outras medidas importantes nos sistemas de radio freqüência são os MHZ (Mega-Hertz), GHz (Giga-Hertz), THz (Tera-Hertz), etc.

LAN - Sigla para Rede de Área Local (Local Area Network), definida por uma rede de computadores restrita à uma mesma área, como por exemplo, um edifício comercial ou uma fábrica.

Largura de Banda - Capacidade de um determinado canal (fibra ótica, fio de cobre) de transmitir informações. No Brasil as linhas telefônicas convencionais utilizadas para transmissão de dados da Internet normalmente permitem uma largura de banda de 56 Kbps.

LINK - Ligação. Na Internet, uma palavra ou imagem em destaque que faz ligação com outra informação. Os links permitem a leitura não-sequencial de um documento e são indicados nas páginas WEB pelo símbolo da mãozinha no lugar do cursor do mouse.

Login remoto - Acesso a um computador via rede para execução de comandos. Para todos os efeitos, o computador local, usado pelo usuário para “logar” no computador remoto, passa a operar como se fosse um terminal deste último.

Leased Line - Linha privada de telefonia utilizada por empresas para aumentar a segurança e velocidade de transmissão de dados.

MAN - Rede metropolitana é o acrônimo de Metropolitan Area Network, uma rede com tecnologia que opera a alta velocidade (de centenas de megabits por segundo a alguns gigabits por segundo) e que tem abrangência metropolitana.

MAU - Sigla para Unidade de Acesso de Mídia (Media Access Unit), dispositivo que serve como transceiver em uma rede do tipo Ethernet.

Mbps - Acrônimo para Mega bits por segundo, que é a medida da velocidade de transmissão de dados em um sistema, equivalente ao envio de um milhão de bits por segundo.

MHz (Mega Hertz) - Medida da freqüência de um sinal periódico que gira 1 milhão de ciclos por segundo. $1 \text{ MHz} = 10^6 \text{ Hertz}$, ou seja, 1 milhão de Hertz. Normalmente utilizado para sinais de rádio freqüência em telecomunicações ou na área de informática é utilizado como unidade de medida da freqüência de trabalho de um dispositivo de Hardware, por exemplo, para indicar a velocidade de processamento de um microprocessador.

MIMO - É o acrônimo em inglês para Multiple-Input Multiple-Output, ou seja, Múltiple Entrada Múltiple Saída. Esta sigla foi dada às antenas que fazem uso desta tecnologia em ambiente Wireless (sem fio). A tecnologia MIMO se refere especificamente à forma como são processadas (manejadas) as ondas de RF para transmissão e recepção nas antenas dos dispositivos Wireless como, por exemplo, nos roteadores em redes WLAN (Wireless LAN). A tecnologia MIMO aproveita os fenômenos físicos tais como a propagação multitrajeto (do sinal) para incrementar a taxa de transmissão e reduzir a taxa de erro. Em poucas palavras, a técnica MIMO aumenta a eficiência espectral de um sistema de comunicações Wireless através da utilização do domínio espacial, ou seja, muitas mais antenas e todas elas funcionando ao mesmo tempo. Com esta tecnologia é possível conseguir que cada uma das antenas possa receber ou transmitir de forma simultânea, para melhorar o desempenho do sistema. Além disso, pode corrigir de maneira muito mais eficiente as interferências, e consequentemente, a qualidade do sinal recebido. Esta tecnologia foi implementada primeiramente em produtos com o padrão 802.11g, mas seu verdadeiro potencial foi atingido com os equipamentos utilizando o padrão 802.11n.

Modem - Sigla para Modulador/Demodulador (**Modulator/demodulator**). Dispositivo que converte a informação digital em informação analógica para ser transmitida por uma linha telefônica da rede de comutação pública, e vice-versa.

Mosaic - Um programa cliente de fácil utilização projetado para procura de informações disponíveis na Web. Distribuído como freeware, o Mosaic foi criado pelo National Center for Supercomputing Applications (NCSA) dos EUA e tem capacidade multimídia.

Multicast - Um endereço Internet Classe D para um grupo específico de computadores em uma rede LAN, ou uma mensagem enviada a um grupo específico de computadores em rede. Um endereço Multicast é útil para aplicações como teleconferência.

NAT - Network Address Translation, é a técnica utilizada em redes de computadores, também conhecida como enmascaramento (masquerading) e consiste em reescrever os endereços IP de origem de um pacote que passam por um router ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior (rede pública).

Navegação - Ato de conectar-se a diferentes computadores da rede distribuídos pelo mundo, usando as facilidades providas por ferramentas como browsers Web. O navegante da rede realiza uma “viagem” virtual explorando o ciberespaço, da mesma forma que o astronauta explora o espaço sideral. Cunhado por analogia ao termo usado em Astronáutica.

Net - The Net ou a rede, normalmente é assim que se conhece atualmente a Internet.

Netiqueta - Um conjunto de regras de etiqueta para o uso socialmente responsável da Internet, ou seja, o modo como os usuários devem proceder na rede, especialmente na utilização de correio eletrônico.

Netnews - Usenet News, Usenet ou News. Serviço de discussão eletrônica sobre vasta gama de assuntos, cada qual ancorado por um grupo de discussão.

Newsgroup - Grupo temático de discussão do netnews.

NFS - O Network File System, desenvolvido pela Sun Microsystems Inc., é um protocolo que usa IP para permitir o compartilhamento de arquivos entre computadores.

NIC [CI] - Network Informations Center, centro de informação e assistência ao usuário da Internet que disponibiliza documentos, como RFCs, FAQs e FYIs, realiza treinamentos, etc.

NIS - Acrônimo para Network Information System (NIS), é um sistema distribuído de bases de dados que troca cópias de arquivos de configuração unindo a conveniência da replicação à facilidade de gerência centralizada. Servidores NIS gerenciam as cópias de arquivos de bases de dados, e clientes NIS requerem informação dos servidores ao invés de usar suas cópias locais destes arquivos. É muito usado por administradores UNIX para gerenciar bases de dados distribuídas através de uma rede.

NIS+ - Versão atualizada do NIS de propriedade da Sun Microsystems Inc. que provê mais recursos ao serviço e uma maior segurança.

Nó - Qualquer dispositivo, inclusive servidores e estações de trabalho, ligado a uma rede.

NOC [CO] - Network Operations Center. Um centro administrativo e técnico que é responsável por gerenciar os aspectos operacionais da rede, como o controle de acesso a mesma, roteamento, etc.

On Line - Em linha. Você está on line quando seu computador estiver conectado a outro computador ou a uma rede, permitindo a troca de informações através dessa conexão.

OSI - O Open Systems Interconnection (OSI) é um modelo conceitual de protocolo com sete camadas definido pela ISO, para a compreensão e o projeto de redes de computadores. Trata-se de uma padronização internacional para facilitar a comunicação entre computadores de diferentes fabricantes.

Pacote - Dado encapsulado para transmissão na rede. Um conjunto de bits compreendendo informação de controle, endereço fonte e destino dos nós envolvidos na transmissão.

Paridade - Método de checagem de erros na transmissão de informação por meio de bits.

Patch Panel - Dispositivo de conexão manual que permite uma fácil organização, e remanejamento dos pontos de um cabeamento estruturado, alterando a posição do ponto sem modificação física do cabo UTP.

Ping - O ping (Packet Internet Groper) é um programa usado para testar o alcance de uma rede, enviando a nós remotos uma requisição e esperando por uma resposta.

PIR [Ponto de Interconexão de Redes] - Locais previstos para a inter-conexão de redes de mesmo nível (peer networks), visando assegurar que o roteamento entre redes seja eficiente e organizado. No Brasil, os três principais PIR's estão previstos em Brasília, Rio de Janeiro e São Paulo.

Plug-In - Programa adicional instalado em seu browser para ampliar seus recursos. Exemplos: Shockwave Flash, Real Audio, VDO e outros.

POP3 - O Post Office Protocol (versão 3) é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico. O POP3 está definido no RFC 1225 e permite que todas as mensagens contidas na caixa de correio eletrônico remota possam ser transferidas sequencialmente para o computador local. Desta forma, o usuário pode ler as mensagens recebidas, apagá-las, responde-las, armazena-las, etc. Tudo localmente e Off-line.

Porta - Uma abstração usada pelo protocolo TCP/IP para distinguir entre conexões simultâneas para um único host destino. O termo também é usado para denominar um canal físico de entrada ou de um dispositivo.

PostMaster - E-mail do responsável pelo correio eletrônico de uma instituição.

PPP - Um dos protocolos mais conhecidos para acesso via interface serial, permite que um computador faça uso do TCP/IP através de uma linha telefônica convencional e um modem de alta velocidade. É considerado o sucessor do SLIP por ser mais confiável e eficiente.

PPPoE - (Point-to-Point Protocol over Ethernet) protocolo para conexão de usuários de uma rede Ethernet para a Internet. Seu uso é típico nas conexões de um ou múltiplos usuários em uma rede LAN à Internet através de uma linha DSL, de um dispositivo Wireless (sem fio) ou de um modem de cabo broadband comum. O protocolo PPPoE deriva do protocolo PPP. O PPPoE estabelece a sessão e realiza a autenticação com o provedor de acesso a Internet.

Protocolo - Uma descrição formal de formatos de mensagem e das regras que dois computadores devem obedecer ao trocar mensagens. Um conjunto de regras padronizado que especifica o formato, a sincronização, o seqüenciamento e a verificação de erros em comunicação de dados. O protocolo básico utilizado na Internet é o TCP/IP.

Provedor de Acesso - Instituição que se liga à Internet, via um ponto de presença ou outro provedor, para obter conectividade IP e repassá-la a outros indivíduos e instituições, em caráter comercial ou não.

Provedor de Informação - Instituição cuja finalidade principal é coletar, manter e/ou organizar informações on-line para acesso, através da Internet, por parte de assinantes da rede. Essas informações podem ser de acesso público incondicional, caracterizando assim um provedor não-comercial ou, no outro extremo, constituir um serviço comercial onde existem tarifas ou assinaturas cobradas pelo provedor.

Provedor de Serviço - Pode ser tanto o provedor de acesso quanto o de informação.

RACK - Equipamento em forma de armário que armazena os diversos dispositivos de controle de rede (como Hubs, patch panels e D.I.O.s) que são encaixados como gavetas.

Rede - Conjunto de computadores interligados entre si e a um computador principal, o servidor. No caso da Internet, são vários servidores interligados em todo o mundo.

Repetidor - Um dispositivo que propaga (regenera e amplifica) sinais elétricos em uma conexão de dados, para estender o alcance da transmissão, sem fazer decisões de roteamento ou de seleção de pacotes.

RFC - Acrônimo para Request For Comments. RFCs constituem uma série de documentos editados desde 1969 e que descrevem aspectos relacionados com a Internet, como padrões, protocolos, serviços, recomendações operacionais, etc. Uma RFC é, em geral, muito densa do ponto de vista técnico.

Reply - Resposta dada a um e-mail recebido.

RJ-11 - Tipo de conector para telefonia em cabos UTP, de fácil manuseio e instalação.

RJ-45 - Tipo de conector para dados em cabos UTP de fácil manuseio e instalação.

Roteador - Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes. Tipicamente, uma instituição, ao se conectar à Internet, deverá

adquirir um roteador para conectar sua Rede Local (LAN) ao ponto de presença mais próximo.

Search - Busca, procura. Mecanismo de busca de informações na Internet. Cadê, Google e Yahoo são muito populares.

Servidor - Micro designado para gerenciar uma rede, organizando a transmissão de dados entre os computadores de uma empresa e para fora dela, além de armazenar bancos de dados e controlar o acesso de informações confidenciais. Uma rede pode ter mais de um servidor.

Shareware - Software distribuído gratuitamente por determinado período. Depois de um período inicial de testes, espera-se que o usuário envie um pagamento aos autores do programa para continuar a utilizá-lo.

Site - Espaço ou local de uma empresa ou instituição na Internet. Um site é composto de uma Home Page e várias outras páginas.

SLDD - Serviço por Linha Dedicada para Sinais Digitais, para interligação de dois até cinco equipamentos de comunicação de dados.

SLIP - Serial Line IP é um protocolo Internet bastante popular usado via interfaces seriais.

Smiley - Uma "carinha" construída com caracteres ASCII e muito usada em mensagens eletrônicas para dar idéia de sentimentos ou emoções. Por exemplo, a mais comum é :-), que significa humor e ironia. Você deve girar o smiley 90 graus para a direita para entendê-lo.

SMTP - O Simple Mail Transfer Protocol é o protocolo TCP/IP usado para troca de mensagens via correio eletrônico na Internet.

SNMP - O Simple Network Management Protocol é um protocolo usado para monitorar e controlar serviços e dispositivos de uma rede TCP/IP. É o padrão adotado pela RNP para a gerência de sua rede.

Store-and-Forward - É o termo em inglês que significa Armazenar e Encaminhar (ou enviar) este método é muito utilizado nos sistemas por comutação de mensagens, onde toda a mensagem enviada pelo transmissor deve ser temporariamente armazenada em cada nó intermediário da rede, uma vez que a mensagem completa chegou para o primeiro nó de rede, esse nó deve enviá-la (ou encaminhá-la) para o seguinte nó e assim sucessivamente até a mensagem atingir seu destino final.

Switch - Dispositivo de rede que funciona como um distribuidor central da LAN e serve para segmentar uma rede em diferentes domínios de difusão (ou domínios de colisão). O Switch escuta em todos seus portos e constrói tabelas nas quais mapeia os endereços (físicos) MAC com o porto através do qual (um dado endereço MAC) pode ser alcançado. Desta maneira quando um computador (em um segmento da LAN) envia uma mensagem para outro computador (em outro segmento da LAN), a mensagem será lida pelo Switch e será encaminhada unicamente ao porto que contém o endereço MAC do computador destino assim limitando ao mínimo as colisões na rede LAN. Portanto, o Switch trabalha no nível 2 do modelo OSI.

TCP/IP - Transmission Control Protocol - Internet Protocol - Protocolo que define o processo de comunicação entre os computadores na Internet.

TDMA - Os sistemas TDMA (Time Division Multiple Access) conhecidos como sistemas de acesso múltiplo por divisão de tempo, são os sistemas de multiplexação (ou multicanalização) mais utilizados na atualidade, especialmente nos sistemas de transmissão digital. Nestes sistemas a largura de banda total do meio de transmissão é designada a cada canal durante uma fração do tempo total (intervalo de tempo).

Telnet - Serviço que permite login remoto segundo o jargão e a vertente técnica Internet.

Token-Ring - as redes Token-Ring (IEEE 802.5) utilizam uma topologia lógica de anel. Quanto à topologia física, é utilizado um sistema de estrela parecido com o 10BaseT, onde temos Hubs inteligentes com 8 portas cada ligados entre si. Tanto os Hubs quanto as placas de rede e até mesmo os conectores dos cabos têm que ser próprios para redes Token-Ring.

Existem alguns Hubs combo, que podem ser utilizados tanto em redes Token-Ring quanto em redes Ethernet. A taxa de transferência de uma rede Token-Ring ia desde 4 até 16 Mbps.

Transceiver - Dispositivo que transmite e recebe informação de um computador para uma conexão de rede.

Transceiver Óptico - Dispositivo eletrônico que transforma sinais digitais provenientes de uma fibra óptica em sinais balanceados de 8 vias (RJ 45) para acoplamento de Hubs.

UNIX - É um sistema operacional portável, multitarefa e multiusuário originalmente criado por Ken Thompson, que trabalhava nos Laboratórios Bell (Bell Labs) da AT&T. A marca UNIX é uma propriedade do The Open Group, um consórcio formado por empresas de informática. Atualmente existem várias versões de sistemas UNIX que depende da arquitetura da máquina em questão, por exemplo, alguns dos Sistemas Operativos derivados do Unix são: BSD (FreeBSD, OpenBSD e NetBSD), Solaris anteriormente conhecido por SunOS (da Sun), IRIX (da Silicon Graphics), AIX (da IBM), HP-UX (da Hewlett-Packard), Tru64 (da Digital Equipment Corporation), Linux (nas suas centenas de distros para plataforma Intel x86/x64), e até o Mac OS X (baseado em um kernel Mach BSD chamado Darwin). Existem mais de quarenta sistemas operacionais *nix, rodando desde celulares a supercomputadores, de relógios de pulso a sistemas de grande porte.

Upgrade - Atualização de um software (versão mais recente) ou de um computador (configuração).

Upload - Transferência de arquivos de um computador para outro.

UDP - Acrônimo para User Datagram Protocol, o protocolo de transporte sem conexão da família TCP/IP, usado com aplicações como o de gerenciamento de redes (SNMP) e de serviço de nomes (DNS).

URL - Uniform Resource Locator - Sistema de endereçamento usado em toda a WWW.
Exemplo: <http://www.usp.br/>

Vírus - Programa de computador feito para destruir outros programas ou arquivos específicos. Pode causar um prejuízo irreparável. O Anti-vírus é um programa que detecta e elimina os vírus.

VPN - É a sigla em inglês para denominar uma rede virtual privada (Virtual Private Network). Basicamente é uma conexão onde o acesso e a troca de dados somente é permitido a usuários e/ou redes que façam parte de uma mesma comunidade de interesse, por exemplo, uma empresa. Utilizando a técnica chamada de tunelamento, pacotes são transmitidos na rede pública, como por exemplo, pela Internet através de um túnel privado que simula uma conexão Ponto-a-Ponto.

Waffle - Um programa que possibilita a um BBS tornar-se um site Usenet.

WAIS - Acrônimo para Wide Area Information Server, é um serviço de bases de dados distribuídas acessíveis via Internet, cuja principal peculiaridade é a conversão automática de formatos para visualização remota de documentos e dados.

WAN - Sigla para Rede de Grande Área(Wide Area Network), definida por uma rede de computadores ligada por meios de comunicação de longa distância, como por exemplo, sinais de rádio, L.P.s (linhas privadas) e até mesmo satélites.

Webmail - Interface via web que permite ao usuário ler e processar seus e-mails diretamente de uma página na internet. Ele tem todas as características de um programa de e-mail, possibilitando que você leia uma nova mensagem, envie e/ou encaminhe mensagens, envie e/ou veja anexos, podendo, inclusive, usar pastas para organizá-las.

Webtrends - Solução de Análise e Gerenciamento Web que fornece dados estatísticos de todos os elementos sobre a atividade do visitante no site, possibilitando, assim, melhorias sobre performance, disponibilidade e resultados esperados.

WHOIS - Banco de dados de informações sobre domínios, redes, hosts e pessoas, fornecendo um serviço de diretório de usuários da Internet.

Wi-Fi - Wireless Fidelity. É a tecnologia de interconectividade entre dispositivos sem o uso de fios. É disponibilizado através de um determinado ponto (Hotspot) que cobre uma faixa de freqüência e estabelece dentro desta faixa o acesso para uma conexão de Internet.

WiMAX - (Worldwide Interoperability for Microwave Access/Interoperabilidade Mundial para Acesso de Micro-ondas) Especifica uma interface sem fio para redes metropolitanas (WMAN) de conexão de banda larga (last mile) oferecendo conectividade para uso doméstico, empresarial e em hotspots. O benefício crucial do padrão WiMAX é a oferta de conexão internet banda larga em regiões onde não existe infra-estrutura de cabeamento telefônico ou de TV a cabo.

Wireless - A tecnologia Wireless (sem fios) permite a conexão entre diferentes pontos sem a necessidade do uso de cabos telefônico, coaxial ou ótico, por meio de equipamentos que usam rádio freqüência (comunicação via ondas de rádio) ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA. Wireless é uma tecnologia capaz de unir terminais eletrônicos, geralmente computadores, entre si devido às ondas de rádio ou infravermelho, sem necessidade de utilizar cabos de conexão entre eles. O uso da tecnologia Wireless vai desde transceptores de rádio como walkie-talkies até satélites artificiais no espaço. Seu uso mais comum é em redes de computadores, onde a grande maioria dos usuários utiliza-se da mesma para navegar pela Internet no escritório, em um bar, um aeroporto, um parque, em casa, etc. Uma rede de computadores sem fios são redes que utilizam ondas eletromagnéticas ao invés de cabos, tendo sua classificação baseada na área de abrangência delas: redes pessoais ou curta distância (WPAN), redes locais (WLAN), redes metropolitanas (WMAN) e redes geograficamente distribuídas ou de longa distância (WWAN).

WORM - Acrônimo de Write Once Read Many. 1. Ferramenta de busca na rede Web; 2. Verme, programa que, explorando deficiências de segurança de hosts, logrou propagar-se de forma autônoma na Internet na década de 80.

WWW - World Wide Web. É a área multimídia da Internet. Por ser a mais popular é confundida com a própria Internet. Além da WWW existem outras áreas da Internet, como: FTP, Gopher, Usenet e Telnet.

BIBLIOGRAFIA

SCRIMGER, Rob / LASALLE, Paul / PARIHAR, Mridula / GUPTA, Meeta.

TCP/IP A Bíblia. Rio de Janeiro. Campus, 2002.

TORRES, Gabriel. Hardware Curso Completo, ed. 4. Axcel Books. 2001.

GALLO, Michael A. Hancock, WILLIAN, M. Comunicação entre Computadores e Tecnologia de Redes. São Paulo. Thompson, 2003.

KUROSE, James F. Ross / KEITH W. Ross - Redes de Computadores e a Internet. São Paulo. Addison Wesley, 2003.

FALBRIARD, Claude. Protocolos e Aplicações para Redes de Computadores. São Paulo. Érica, 2002.

LAMMLE, Tood. CCNA – Cisco Certified Network Associate: Guia de

Estudos. Rio de Janeiro. Campos, 2003.

LINKS

Dicas de protocolos:

<http://www.protocols.com>

Camada OSI e protocolos:

<http://penta2.ufrgs.br/homeosi.html>

Lista de Portas TCP/UDP

<http://www.iana.org/assignments/port-numbers>

Apostilas de Rede e de protocolos:

<http://www.apostilando.com/sessao.php?cod=17>

Tutoriais:

<http://www.teleco.com.br/tutoriais.asp>

Cálculo de Sub-redes:

<http://www.abusar.org/subredes-retry.html>

MARCAS REGISTRADAS

APPLE e Quicktime – marcas registradas da Apple Computer, Inc.

CISCO Systems – marca registrada da CISCO Systems, Inc.

IBM – marca registrada da IBM Corporation.

LUCENT e Bell Labas – marcas registradas da Lucent Technologies.

MICROSOFT e WINDOWS – marcas registradas da Microsoft Corporation.

NEC – marca registrada da NEC Corporation.

NETWARE - marca registrada da Novell, Inc.

MACINTOSH E APPLETALK- são marcas registradas da Apple Computers.

Todos os demais nomes registrados, marcas registradas ou direitos de uso citados nessa apostila pertencem aos seus respectivos fabricantes e foram utilizados exclusivamente para fins didáticos.