

TCP/IP

Rede

Conceitos

Topologias

Endereços da Internet

Endereços IP

Estrutura de Acesso à Internet

Nomes de Domínios (Domain Names)

DNS – Domain Name Server

Registro de Domínios

TCP/IP

Introdução

Modelo de Camadas

Exemplos de Protocolos TCP/IP por Camada

Exemplos de Protocolos TCP/IP por Função

Camada Física

Hardware

Placas de Rede e Cabos

HUBs

MAC – Medium Access Control

Camada de Enlace

LAN (Intranet)

Ethernet

CSMA/CD

Hardware

Repetidores

Bridges e Switches

WAN (Extranet/Internet)

PPP

HDLC

Camada de Internet

IP

Hardware

Roteadores

Camada de Transporte

UDP

TCP

Camada de Aplicação

HTTP

SMTP

POP3/IMAP4

FTP

Endereços

URLs

Compartilhamento de Endereços: Proxy, NAT e Socks

Exemplos de aplicação de redes com arquitetura TCP/IP

Bibliografia

[KUR03] KUROSE, James F. e ROSS, Keith. W. Redes de Computadores e a Internet. São Paulo, Addison Wesley, 2005.

[TAN03] TANENBAUM, Andrew S. Redes de Computadores. São Paulo, Editora Campus, 2003.

Rede

Conceitos

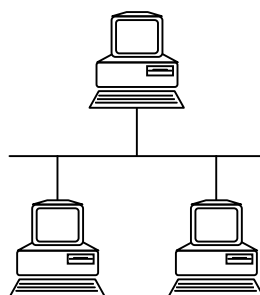
A rede para fins do nosso estudo é compreendida como um conjunto de computadores e periféricos conectados entre si, com o objetivo de compartilhar recursos, como discos ou impressoras, e serviços.

A rede pode ser local, como, por exemplo, a rede dentro de uma mesma empresa ou remota, como, por exemplo, entre filiais de uma mesma empresa. A rede local é conhecida como LAN (Local Area Network) e a rede remota como WAN (Wide Area Network). Atualmente, com a popularização da Internet, o termo Intranet é muitas vezes usado como sinônimo de LAN, e o termo Extranet como sinônimo de WAN. Isto não é muito correto pois os termos LAN e WAN se referem a infra-estrutura de rede e os termos Intranet e Extranet se referem a uma LAN/WAN com recursos de Internet. Apesar disso utilizaremos os termos Intranet e Extranet, por melhor se enquadrarem em uma disciplina voltada para estudo da Internet.

Topologias

A forma de conectar os diversos computadores e periféricos de uma Intranet é conhecida como Topologia de Rede. Historicamente existem 2 topologias principais: Barramento e Estrela.

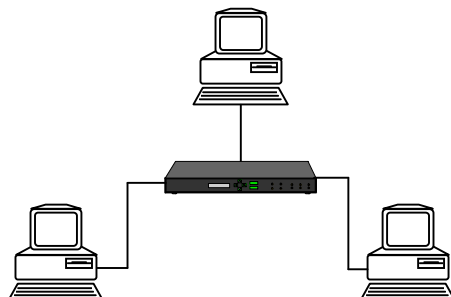
A Topologia em Barramento conecta os computadores a um cabo segmentado, usualmente um cabo coaxial de 50 Ohms ligados ao computador através de um conector BNC em formato de "T", com 2 terminadores nas pontas da rede. Esta topologia foi muito utilizada nas décadas de 80 e 90 por ser simples e fácil de implantar.



[Topologia em Barramento]

A Topologia em Estrela conecta os computadores através de um cabo com 4 pares de fios trançados e conectores RJ 45, muito parecidos com os conectores RJ 11 utilizados em telefones, utilizando 1 cabo para cada computador,

conectados a um dispositivo central chamado HUB. A Topologia em Estrela se tornou muito popular na década de 90, pois, apesar do custo adicional do HUB, tinha-se uma rede muito mais confiável, pois se um cabo rompesse ou abrisse, apenas 1 computador sairia da rede e não todos como no caso da Topologia em Barramento.



[Topologia em Estrela]

Além disso, a Topologia em Estrela abriu caminho para o desenvolvimento dos Switches, que por sua vez permitiram a comunicação Full-Duplex, ou seja, envio e recebimento simultâneo entre 2 pontos da rede. Além disso o uso de pares trançados na rede permitiu integrar redes de voz e dados usando os mesmos cabos, aumentando a flexibilidade das redes.

Endereços da Internet

Endereços IP

Endereços são usados para localizar computadores. O sistema de endereçamento atualmente utilizado é o IPv4, Protocolo de Internet versão 4 (Internet Protocol version 4). O endereço IP é representado por 4 bytes (32 bits), sendo representado por 4 números, com valor entre 0 e 255, existindo assim cerca de 4.294.967.295 possibilidades de endereços. Usualmente, o primeiro ou o primeiro e o segundo números indicam a rede, o terceiro indica a sub-rede e o quarto indica o computador. Por definição, o computador nunca pode ser 0 ou 255, nenhum dos números pode ser 255 e o primeiro número não pode ser 0. Isto porque existe um modo de transmissão de pacotes chamado "broadcasting" (difusão), endereçado a todos os computadores da rede, feito usando o valor 255. O endereço 0.0.0.0 não pode ser usado pois é utilizado pela máquina ao ligar, enquanto não recebe o endereço definitivo. A parte do endereço IP que representa a rede é chamada de "network ID" e parte que representa o computador é chamada de "host ID".

Os endereços IP são separados em classes, utilizando para isso o conceito de máscara de rede. A operação AND binária deve ser aplicada entre o endereço e a máscara de rede para definir a parte do endereço que corresponde a rede e a parte que corresponde ao computador. O valor 255 é representado por 11111111 em notação binária, assim, a operação AND preserva todos os bits do endereço. O valor 0 é representado 00000000 em notação binária, assim, a operação AND zera os bits da parte referente ao computador.

Classe	1º BYTE	Máscara	Observação
A	1 a 127	255.0.0.0	
B	128 a 191	255.255.0.0	
C	192 a 233	255.255.255.0	
D	234 a 239	-	multicast
E	240 a 255	-	testes e pesquisa de TCP/IP

Exemplo:

endereço	200.210.100.97
máscara	255.255.255.0

rede	200.210.100.0
computador	97

Os endereços IP servem não apenas para identificar computadores na Internet, mas também podem ser usados para identificar computadores de Intranets. Os computadores de uma rede interna não podem ter os mesmos endereços de computadores ligados na Internet, pois se o usuário tentasse acessar um computador da Internet cujo mesmo endereço estivesse sendo usado por um computador da rede interna, quem responderia seria o computador da rede interna e não o computador da Internet.

As seguintes faixas de endereços estão reservadas para redes internas:

Classe

A	10.0.0.0	a	10.255.255.255
B	172.16.0.0	a	172.31.255.255
C	192.168.0.0	a	192.168.255.255

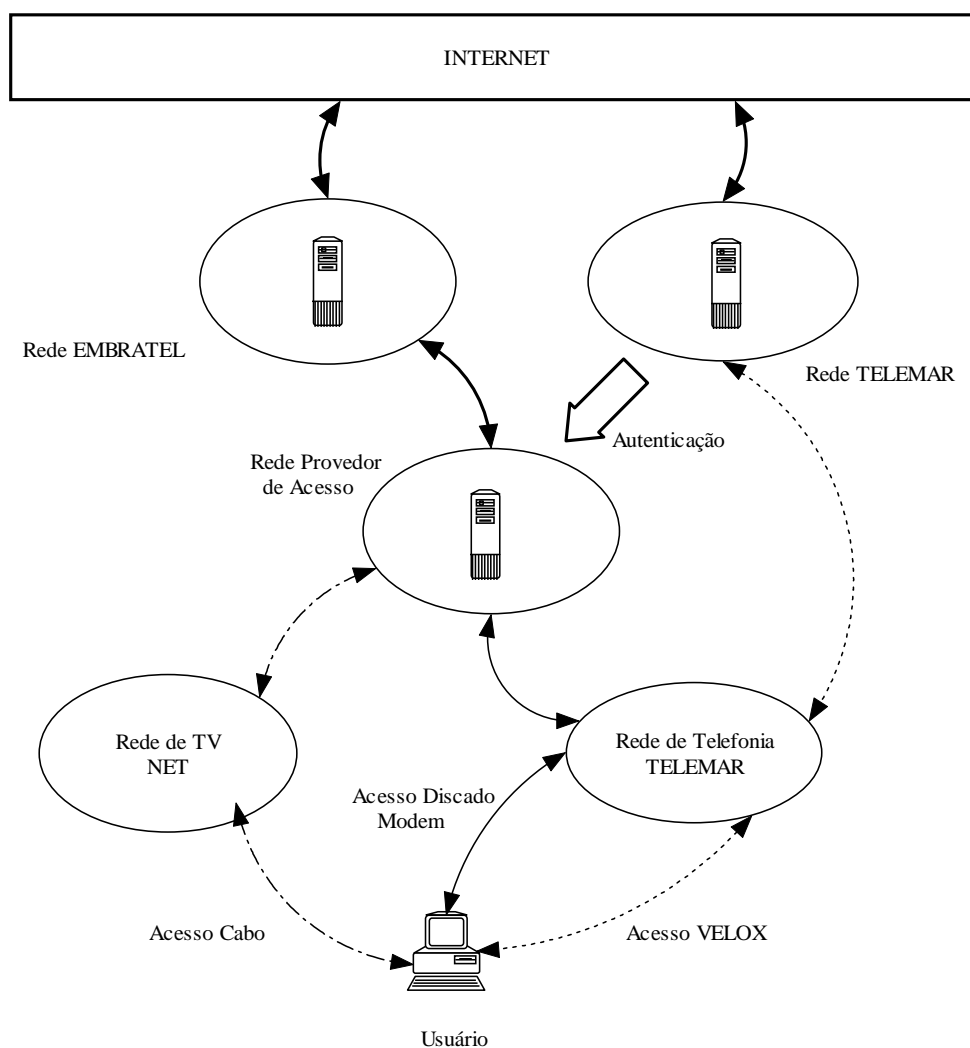
Com o crescimento da Internet começou a preocupação de aumentar o tamanho do endereço IP de modo a atender a expansão futura da Internet. O IPv6 é um sistema de endereçamento com 128 bits ao invés de 32. Se fosse utilizada a forma de representação do IPv4 teríamos um endereço como, por exemplo:

194.153.11.222.128.17.135.44.240.36.97.66.205.221.52.4

Infelizmente isto seria muito difícil de memorizar, assim foi criada uma representação baseada em números hexadecimais como, por exemplo:

DEAD:BEEF:0000:0000:0000:0073:FEED:F00D

Estrutura de Acesso à Internet



A estrutura de acesso acima mostra a estrutura de acesso a Internet. Ela considera um Provedor de Acesso com conexão via EMBRATEL, acesso via cabo através da NET e acesso ADSL via TELEMAR (VELOX).

1. Acesso Discado via Modem

O Acesso Discado é realizado utilizando um Modem conectado a rede de telefonia da TELEMAR, que por sua vez se conecta a outro Modem no Provedor.

2. Acesso via Cabo

O Acesso via Cabo é realizado através a rede de cabos de TV da NET, que por sua vez se conecta ao Provedor, usualmente através de fibra óptica.

3. Acesso via VELOX (ADSL)

O Acesso via VELOX (ADSL) é realizado através da rede de telefonia da TELEMAR, que está conectada diretamente a TELEMAR. Em função de

restrições da Lei da Telecomunicações, as empresas de Telefonia ainda não podem prover acesso pleno, assim é necessário um processo de autenticação entre a TELEMAR e o Provedor, para garantir que o usuário tem como ser cobrado, neste caso, através de algum Provedor de Acesso.

Nome de Domínios (Domain Names)

Pelo fato dos endereços IP serem compostos apenas de números, e serem de difícil memorização, a Universidade de Wisconsin desenvolveu em 1983 um Servidor de Nomes de Domínios (DNS – Domain Name Server) que foi introduzido na Internet no ano seguinte. O DNS , de forma automática e invisível, traduz endereços compostos de palavras em endereços compostos de números, o que torna a Internet muito mais amigável. Por exemplo, o endereço 200.181.15.9 representa o domínio www.planalto.gov.br.

Não há uma fórmula de cálculo possível para transformar um endereço de nomes em um endereço de números, assim a única forma possível de trabalhar com nomes é consultando uma tabela.

Os nomes de domínios consistem de 2 ou mais partes separadas por pontos, sendo a parte da esquerda a mais específica e a parte de direita a mais geral. A parte mais a esquerda define usualmente o propósito, como “www” para servidores web e “smtp” para servidores de e-mail. A parte mais a direita usualmente define o tipo de site, sendo chamado usualmente de extensão, como:

.com – comercial
.org. – organização (sem fins lucrativos)
.gov – governo
.mil – militar
.net – provedores de serviços de comunicação de redes

Finalmente seguem 2 letras indicando o país de registro, como:

.br – Brasil
.de – Alemanha
.fr – França

Exemplos de domínios:

www.google.com
www.terra.com.br
www.planalto.gov.br

DNS – Domain Name Server

O protocolo DNS é responsável pela resolução de domínios, ou seja, pela transformação de um nome de domínio (www.planalto.gov.br) em um endereço IP (200.181.15.9). O DNS é um serviço hierárquico e distribuído entre inúmeros servidores ao redor do mundo. Existem instituições (ver abaixo), que centralizam a administração do processo de registro de domínios, porém a implementação do DNS é feita de forma distribuída para permitir que cada país, instituição ou empresa decida onde será feita a resolução de seus próprios domínios.

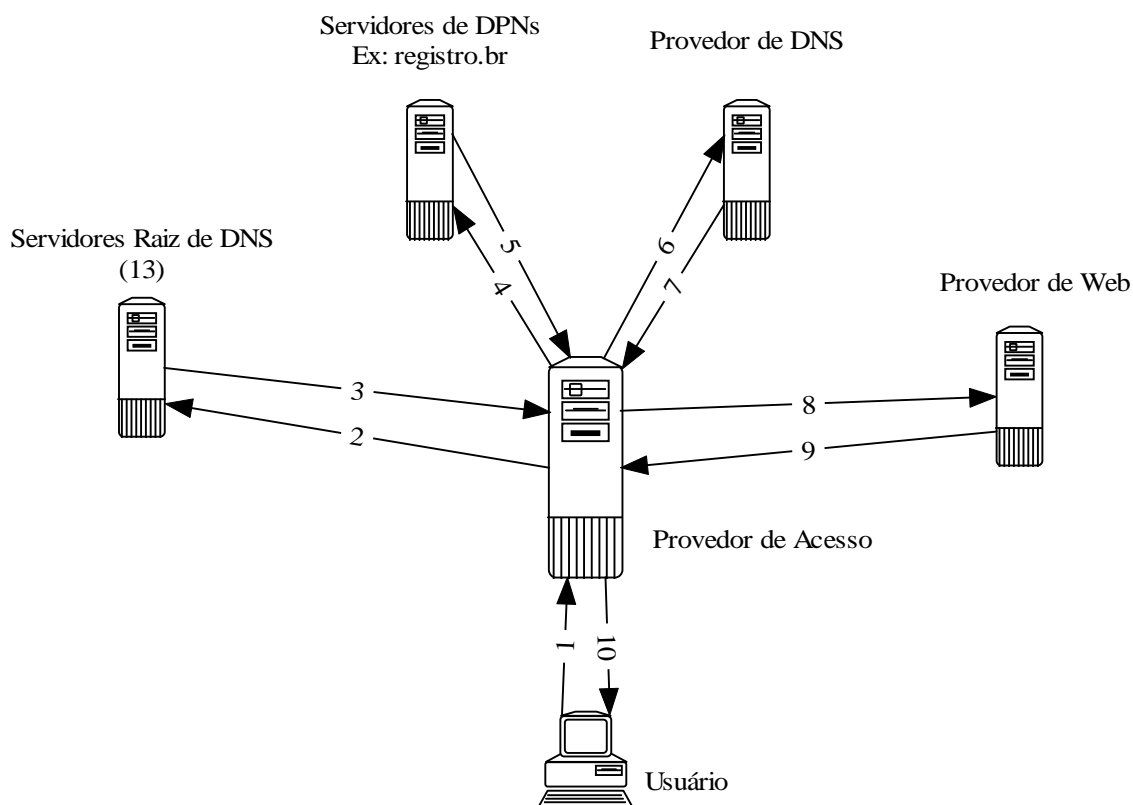
Um processo de resolução de domínio começa, por exemplo, quando o usuário digita <http://www.planalto.gov.br> em seu navegador (browser) de web. Ao receber este endereço o navegador entra em contato com o servidor de DNS do seu Provedor de acesso a Internet. Se alguém tiver acessado recentemente este mesmo endereço, o provedor terá guardado em uma tabela, chamada cache, o respectivo IP, senão o Servidor de DNS contacta um dos 13 servidores da lista de "Root Servers", ou, Servidores Raiz, espalhados pelo mundo. Estes por sua vez tem uma lista de servidores que respondem por determinados domínios, que são informados para o servidor DNS do Provedor. O ".br" é responsabilidade da FAPESP, através do "registro.br". O servidor de DNS da FAPESP ao receber a consulta do domínio www.planalto.gov.br verifica se este realmente existe, consulta qual o servidor de DNS que efetivamente responde por ele, e informa novamente o servidor DNS do Provedor. Este, último, servidor finalmente resolve o domínio e fornece o número do IP que corresponde a ele. Quando a requisição de resolução de domínio volta ao navegador web, este finalmente entra em contato diretamente com o IP e carrega as páginas do site.

Se o servidor de DNS do registro.br não encontrar o domínio www.planalto.gov.br na sua lista de domínios, ele retorna uma mensagem de domínio inexistente. Se o servidor de DNS que efetivamente resolve o domínio (o último da seqüência acima) não estiver funcionando, o domínio não é resolvido e o navegador não consegue abrir a página, mesmo que a máquina com IP 200.181.15.9 esteja funcionando corretamente. Porém se o usuário digitar <http://200.181.15.9> ele consegue carregar, pois o endereço IP foi fornecido diretamente, não sendo necessária a resolução de domínio.

Os servidores de DNS responsáveis por determinados domínios normalmente trabalham no mínimo em 2, ou mesmo, 3 servidores diferentes, em lugares diferentes, utilizando diferentes links com a Internet. Isto porque se algum deles sair do ar, quer por problemas no computador ou no link, existem pelo menos mais 1 ou 2 que podem responder pelos domínios, evitando que as pessoas parem de acessar o site.

Ao alterar o endereço IP que atende por determinado domínio, decorre um certo tempo antes deste novo IP se propagar por todos os Servidores de DNS.

Isto ocorre porque cada entrada da tabela de cache tem associado um tempo de duração, que normalmente é horas. Ou seja, antes de passar este tempo, o Servidor de DNS irá utilizar este IP, toda vez que alguém consultar o domínio, sem fazer uma nova consulta como explicada acima.



[Processo de Resolução de Domínios]

Registro de Domínios

A IANA (Internet Assigned Numbers Authority) é a entidade da Internet responsável por gerenciar a atribuição de endereços e domínios. Usuários recebem os IPs de seus Provedores de Internet (ISP – Internet Service Provider). Os Provedores de Internet recebem endereços das LIRs (Local Internet Registry) ou NIRs (National Internet Registry), que por sua vez recebem os endereços das 4 RIRs (Regional Internet Registry) existentes.

IANA

Internet Assigned Numbers Authority

<http://www.iana.org>

APNIC

Asia Pacific Network Information Centre

Ásia e Pacífico

<http://www.apnic.net>

ARIN

American Registry for Internet Numbers

América do norte e África sub-Sahara

<http://www.arin.net>

LACNIC

Latin American and Caribbean IP address Regional Registry

América Latina e alguma ilhas do Caribe

<http://lacnic.net>

RIPE NCC

Réseaux IP Européens Network Coordination Centre

Europa, Oriente Médio, Ásia Central e países Africanos acima do Equador

<http://www.ripe.net>

A consulta de endereços e/ou domínios pode ser feita em vários sites na internet, abrangendo apenas os domínios do país ou todos os domínios do mundo. Este serviço é oferecido por entidades relacionadas à Internet ou por empresas que oferecem serviços de registro, no intuito de hospedar os domínios registrados.

<http://registro.br>

Brasil, em português

<http://100br.com/whois.completo.php>

Mundo, em português

<http://ww.allwhois.com>

Mundo em inglês

Registro de Domínios - Brasil

O registro de domínios “.br” é feito através do site <http://registro.br>. O processo de registro é feito totalmente via Internet, bastando ao final pagar o Taxa de Manutenção anual.

Inicialmente é preciso ter a certeza de que o nome não esteja registrado, reservado pelo Comitê Gestor, ou se é uma marca notória do INPI, verificando no sistema de Pesquisa. Se a pesquisa resultar em "Domínio Inexistente" ou em informações sobre tickets ativos (com pendências), significa que o domínio poderá ser registrado. Caso contrário, não poderá ser registrado.

Para qualquer operação no sistema de registro, é necessário que o usuário seja previamente cadastrado e esteja IDentificado no sistema. Para isto, caso você ainda não tenha feito o cadastro siga o tutorial Cadastrando-se como usuário do sistema de registro.

Pelas atuais regras, para que o registro de um domínio seja efetivado, são necessários ao menos dois servidores DNS conectados à Internet e já configurados para o domínio que está sendo solicitado. Certifique-se disto através do sistema de verificação.

Para registrar um domínio, é necessário ser uma entidade legalmente representada ou estabelecida no Brasil como pessoa jurídica (Instituições que possuam CNPJ) ou física (CPF) que possua um contato em território nacional.

Uma entidade poderá registrar, sob um DPN (Domínio de Primeiro Nível), quantos domínios quiser. Porém, não é permitido registrar o mesmo nome em diferentes DPNs genéricos. A restrição de homonímia não se aplica aos DPNs com restrições. Todos os DPNs disponíveis, excetuando-se os restritos, são classificados como genéricos.

Uma entidade poderá registrar quantos domínios quiser sob COM.BR, ou sob IND.BR, mas, se possuir o domínio XXX.COM.BR, não poderá registrá-lo também em IND.BR. Ou seja, se tiver XXX.COM.BR não poderá registrar XXX.IND.BR, por ser tratar de domínios genéricos. Já nada impede que, caso essa entidade preencha os requisitos para registrar sob TV.BR, registre também o XXX.TV.BR, porque TV.BR é um domínio com restrições próprias, às quais não se adicionam as restrições de homonímia.

O DPN NOM.BR é uma exceção à regra da homonímia. Por exemplo: pessoas físicas podem registrar XXX.ADV.BR, ZZZ.ENG.BR e XXX.ZZZ.NOM.BR, mas não podem registrar XXX.ADV.BR e XXX.ENG.BR.

Regras Sintáticas de Nomes de Domínios

- Tamanho mínimo de 2 e máximo de 26 caracteres, não incluindo a categoria, por exemplo: no domínio XXXX.COM.BR, esta limitação se refere ao XXXX;
- Caracteres válidos são [A-Z;0-9] e o hífen;
- Nenhum tipo de acentuação é válido;
- Não pode conter somente números;
- O hífen vale como separador sintático interno de palavras, sendo que domínios já registrados com ou sem o mesmo, só poderão ser registrados com esta diferença pelo detentor do primeiro registro.

Observação: Especificamente para o domínio .NOM.BR é necessário a escolha de 2 nomes, ou seja: NOME1.NOME2.NOM.BR.

Um nome de domínio não contém www, ou seja, não pode ser pedido o registro de www.xyz.com.br, o correto será apenas xyz.com.br.

Para o registro de um domínio existe um valor a ser retribuído referente a manutenção pelo período de 1 ano. Atualmente o valor é de R\$ 30,00. As instruções para o pagamento são enviadas no email de confirmação do registro do domínio. O valor é o mesmo para todos os DPNs, sejam para pessoas jurídicas, profissionais liberais ou pessoas físicas.

DPNs para Pessoas Jurídicas	
AGR.BR	Empresas agrícolas, fazendas
AM.BR	Empresas de radiodifusão sonora
ART.BR	Artes: música, pintura, folclore
EDU.BR	Entidades de ensino superior
COM.BR	Comércio em geral
COOP.BR	Cooperativas
ESP.BR	Esporte em geral
FAR.BR	Farmácias e drogarias
FM.BR	Empresas de radiodifusão sonora
G12.BR	Entidades de ensino de primeiro e segundo grau
GOV.BR	Entidades do governo federal
IMB.BR	Imobiliárias
IND.BR	Indústrias
INF.BR	Meios de informação (rádios, jornais, bibliotecas, etc..)
MIL.BR	Forças Armadas Brasileiras
NET.BR	Detentores de autorização para o serviço de Rede e Circuito Especializado da Anatel e/ou detentores de um Sistema Autônomo conectado a Internet conforme o RFC1930
ORG.BR	Entidades não governamentais sem fins lucrativos
PSI.BR	Provedores de serviço Internet
REC.BR	Atividades de entretenimento, diversão, jogos, etc...
SRV.BR	Empresas prestadoras de serviços
TMP.BR	Eventos temporários, como feiras e exposições
TUR.BR	Entidades da área de turismo
TV.BR	Empresas de radiodifusão de sons e imagens
ETC.BR	Entidades que não se enquadram nas outras categorias

DPNs para Profissionais Liberais

ADM.BR	Administradores
ADV.BR	Advogados
ARQ.BR	Arquitetos
ATO.BR	Atores
BIO.BR	Biólogos
BMD.BR	Biomédicos
CIM.BR	Corretores
CNG.BR	Cenógrafos
CNT.BR	Contadores
ECN.BR	Economistas
ENG.BR	Engenheiros
ETI.BR	Especialista em Tecnologia da Informação
FND.BR	Fonoaudiólogos
FOT.BR	Fotógrafos
FST.BR	Fisioterapeutas
GGF.BR	Geógrafos
JOR.BR	Jornalistas
LEL.BR	Leiloeiros
MAT.BR	Matemáticos e Estatísticos
MED.BR	Médicos
MUS.BR	Músicos
NOT.BR	Notários
NTR.BR	Nutricionistas
ODO.BR	Dentistas
PPG.BR	Publicitários e profissionais da área de propaganda e marketing
PRO.BR	Professores
PSC.BR	Psicólogos
QSL.BR	Rádio amadores
SLG.BR	Sociólogos
TRD.BR	Tradutores
VET.BR	Veterinários
ZLG.BR	Zoólogos

DPNs para Pessoas Físicas

NOM.BR Pessoas Físicas

TCP/IP

Introdução

O TCP/IP representa um conjunto de protocolos de comunicação entre computadores, cujos 2 principais protocolos são o TCP (Transmission Control Protocol), ou Protocolo de Controle de Transmissão e o IP (Internet Protocol), ou Protocolo Internet.

O TCP/IP começou a ser desenvolvido em 1973 por Vinton Cerf da Universidade de Stanford e Bob Kahn do DARPA (Defense Advanced Research Projects Agency). Em 1974 foi publicado o trabalho “Um protocolo para interconexão de redes de pacotes”, onde, pela primeira vez de usou a palavra “Internet”, significando “Interconnected Networks”, ou , Redes Interconectadas. Em 1º de janeiro de 1983 o uso do TCP/IP se tornou obrigatório em todas a máquinas conectadas a então ARPANET.

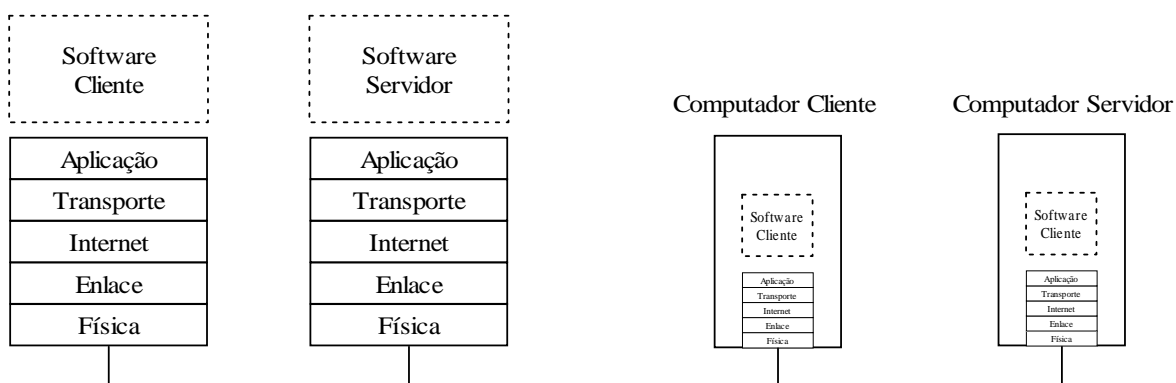
O TCP/IP pode ser usado na Internet, em Intranets e em Extranets. Com a adoção em larga escala do TCP/IP, diferentes computadores em diferentes redes podem se comunicar entre si desde que possuam um módulo TCP/IP, criando os chamados “Sistemas Abertos”.

Uma mesma conexão TCP/IP pode ser compartilhada por vários serviços simultâneos, sendo que cada um utiliza um “Porta” diferente. Abaixo é mostrada uma lista com os principais protocolos TCP/IP e respectivas portas:

Porta	Protocolo	Utilização
20/21	FTP	transferência de arquivos
22	Telnet	acesso remoto
25	SMTP	remessa de e-mails
80	HTTP	Web
110	POP3	recebimento de e-mails

Modelo de Camadas

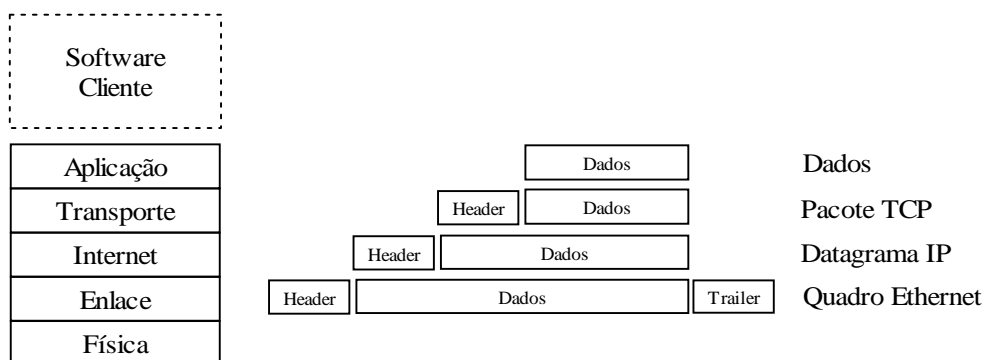
O protocolo TCP/IP é estruturado em um modelo de 5 camadas: Física, Enlace, Internet, Transporte e Aplicação.



[Modelo de Camadas TCP/IP]

Os dados a serem transmitidos são passados, para baixo, de camada para camada, até serem transmitidos pela rede na Camada Física. Na outra ponta, os dados são passados para cima, de camada para camada, até a Camada de Aplicação. Cada camada não precisa saber como as Camadas adjacentes funcionam, ela apenas precisa saber como passar os dados para as outras. Cada camada da pilha emissora conversa com a camada da pilha receptora.

Cada camada da pilha adiciona informações de controle, como, por exemplo, endereço de destino, controles de roteamento e checagem de erros, para garantir que os dados sejam entregues corretamente. Estes controles são chamados de "header", se foram colocados no início e "trailer" se forma colocados no final. Cada camada trata as informações que recebe da camada de cima como dados e inclui nela o "header" e o "trailer". Este processo é conhecido como Encapsulamento de Dados.



[Encapsulamento de Dados TCP/IP]

Exemplos de Protocolos TCP/IP por Camada

Exemplos de Protocolos da Camada de Enlace

Ethernet

Ethernet não é realmente um protocolo. Além disso existem vários tipos de Ethernet. A Ethernet mais comum é a 802.3, utilizada para manipular os dados na camada mais baixa da rede. A Ethernet 802.3 prevê meios de encapsular pacotes (frames) de dados e enviá-los entre computadores. Ela especifica de que forma deve-se lidar com colisão de pacotes e como manipular o endereçamento MAC de cartão de rede.

Exemplo: Ethernet é utilizado em praticamente todas as Intranets

PPP – Point to Point Protocol – Protocolo Ponto a Ponto

É uma forma de encapsulamento de dados em linhas seriais que representa uma melhoria em relação ao SLIP pois permite comunicação bidirecional. Em muito se parece ao SLIP, mas permite dá suporte aos protocolos AppleTalk, IPX, TCP/IP e NetBEUI além do TCP/IP. Ele é capaz de negociar parâmetros de autenticação como, por exemplo, velocidade, bem como suporte a autenticação de usuário PAP e CHAP.

Exemplo: PPP é utilizado na conexão entre Usuário de Internet e Provedor de Internet via Modem e Linha Telefônica

SLIP – Serial Line Internet Protocol – Protocolo Internet de Linha Serial

Este protocolo coloca dados em pacotes preparando-o para transporte através do hardware de rede. Este protocolo é utilizado para envio de dados através de linhas seriais. Não existe correção de erro, endereçamento ou identificação de pacotes. Não existem capacidades de autenticação ou negociação no SLIP. SLIP apenas suporta a transmissão de pacotes IP.

Exemplos de Protocolos da Camada de Internet

ARP – Address Resolution Protocol

O ARP é um protocolo de sistema e mensagens utilizado para encontrar o endereço Ethernet, ou endereço MAC da placa de rede, relacionado a determinado IP. Sem este protocolo um pacote Ethernet não poderia ser gerado a partir de um pacote IP, pois o endereço Ethernet não poderia ser determinado.

IP – Internet Protocol – Protocolo Internet

Exceto pelo ARP e RARP, todos os outros pacotes de protocolos serão trocados utilizando o IP. O IP prevê um mecanismo que permite o endereçamento e gerenciamento de pacotes de dados via software.

RARP – Reverse Address Resolution Protocol

O RARP é utilizado por um computador sem disco, e assim sem capacidade de armazenamento local, para determinar seu endereço IP a partir de seu endereço Ethernet.

Exemplos de Protocolos da Camada de Transporte**ICMP** – Internet Control Message Protocol – Protocolo de Controle de Mensagens Internet

O ICMP provê uma forma de gerenciamento e aviso de erros para auxiliar a remessa de pacotes entre computadores. Este protocolo é utilizado para retornar informações de status de conexão entre computadores que estão tentando se conectar. Ele pode reportar, por exemplo, que o computador de destino não foi encontrado.

Exemplo: Comunicação entre Roteadores

TCP – Transmission Control Protocol – Protocolo de Controle de Transmissão

TCP é um protocolo confiável orientado a conexões utilizado para gerenciar o controle de transporte de pacotes para serviços da camada de aplicações.

Exemplo: Protocolo HTTP de Web utiliza TCP

UDP – User Datagram Protocol – Protocolo de Datagrama de Usuário

UDP é um protocolo não confiável e não orientado a conexões utilizado para gerenciar o transporte de pacotes para serviços da camada de aplicações. Aplicações que fazem uso do UDP devem cuidar por si mesmas do controle da transmissão.

Exemplo: Protocolo SNMP utiliza UDP

Exemplos de Protocolos da Camada de Aplicação**BOOTP** – Boot Protocol – Protocolo de Boot

Utilizado para atribuir um endereço IP para computadores sem disco e informar qual servidor e arquivo deve ser acessado para obter o sistema operacional a ser executado.

DHCP – Dynamic Host Configuration Protocol – Protocolo de Configuração Dinâmica de Computadores

Protocolo de atribuição e controle de endereços IP de computadores em determinada rede. É um serviço baseado em um servidor que automaticamente atribui um endereço IP quando o computador inicia, assim, o endereço IP deste computador não precisa ser definido manualmente, o que torna muito mais simples gerenciar alterações na rede. O protocolo DHCP pode executar todas as funções do BOOTP.

FTP – File Transport Protocol – Protocolo de Transporte de Arquivos
Permite a transferência de arquivos entre computadores utilizando senhas de acesso.

HTTP – Hypertext Transfer Protocol – Protocolo de Transferência de Hipertexto
Utilizado para enviar páginas HTML dos servidores web para os browsers web.

IMAP4 – Internet Mail Access Protocol/4 – Protocolo de Acesso de Correio Internet

É uma evolução do protocolo POP3, permitindo trabalhar com e-mails no modo “on-line” e modo “desconectado” além do modo “off-line” do POP3.

NFS – Network File System – Sistema de Arquivos de Rede

POP3 - Post Office Protocol/3 – Protocolo de Agência de Correios
Utilizado por clientes para acessar um servidor de correio Internet para buscar os e-mails.

RIP – Routing Information Protocol – Protocolo de Informações de Roteamento
Utilizado para atualizar dinamicamente as tabelas de roteamento na Internet e em Extranets.

SNMP – Simple Network Management Protocol – Protocolo Simples de Gerenciamento de Rede
Utilizado no gerenciamento de componentes de uma rede.

Telnet

Utilizado para abrir uma sessão remota em outro computador.

Exemplos de Protocolos TCP/IP por Função

Empacotamento e Baixo Nível

Ethernet
IP
PPP
SLIP

Transporte e Funções Básicas

TCP
UDP

Gerenciamento de Rede

SNMP
ICMP
ARP

Gerenciamento de Computadores

BOOTP
DHCP
RARP

Correio

IMAP4
POP3
SMTP

Roteamento

RIP

Camada Física

A Camada Física é composta pelo hardware, especificações técnicas e características dos equipamentos, conectores, interfaces mecânicas e elétricas, níveis de tensão, e demais características físicas da rede.

Hardware

Placas de Rede e Cabos

Um computador para ser ligado em rede utiliza uma placa de rede conectada a outros computadores via cabos ou via rádio. Inicialmente se utilizavam cabos coaxiais de 50 Ohms, conectados utilizando uma Topologia em Barramento. Hoje são utilizados cabos de Par Trançado, em Topologia Estrela.

Além disso existe a possibilidade de utilizar fibras óticas em ambientes de grande interferência elétrica ou com grande necessidade de largura de banda. Nos últimos anos ocorreu um grande desenvolvimento da tecnologia "Wireless" (Sem Fio), que permite conectar equipamentos via sinal de rádio. Este tipo de equipamento pode ser utilizado tanto para WANs, quanto para LANs, evoluindo a cada dia.

HUBs

Em Topologias Estrela é necessária a utilização de um equipamento central, onde se conectam todos os computadores. Este equipamento é conhecido como HUB. Sua função é fazer a conexão de sinal entre os computadores, e eventualmente sinalizar eventuais colisões da rede Ethernet, podendo transmitir informações sobre a situação da rede através do protocolo SNMP, isto em modelos mais sofisticados. Os HUBs vem perdendo espaço a cada dia para os Switches, capazes de estruturar uma rede mais rápida e eficiente.

MAC – Media Access Control

As Placas de Rede trazem dentro delas um endereço fixo de 6 bytes, denod 3 reservados para o código do fabricante da placa de rede e 3 para um número serial desta placa. Assim, cmo cerca de mais de 16 milhões de números possíveis (apenas considerando 1 fabricante) , temos a garantia de ter um endereço único para cada placa em uma mesma rede.

Camada de Enlace

A Camada de Enlace é responsável por transmitir os dados através de determinado tipo de rede física. As funções exercidas por esta camada incluem o encapsulamento de datagramas em quadros a serem transmitidos pela rede. Ela também é responsável pela associação de um endereço IP com um endereço físico MAC. Ao contrário das camadas superiores, a Camada de Enlace deve conhecer o tipo de rede que irá transmitir os dados, o que irá influenciar, por exemplo, na estrutura dos quadros a serem transmitidos e esquema de endereçamento físico utilizado.

LAN (Intranet)

As redes locais, ou LANs, são utilizadas para conectar computadores em uma mesma sala ou prédio, ou seja, geograficamente próximos. A tecnologia mais utilizada nestas redes é a Ethernet.

Ethernet

Em 1973 no Centro de Pesquisas da XEROX em Palo Alto, Califórnia, Bob Metcalfe projetou e testou a primeira rede Ethernet. Ao tentar conectar um computador e uma impressora, Metcalfe desenvolveu uma forma de cabeamento físico que conectava os dispositivos além de definir a forma de comunicação no cabo. Hoje a Ethernet se tornou o mais popular e largamente implementada tecnologia de rede do mundo.

A Ethernet original descrevia a comunicação sobre um cabo simples compartilhado por todos os dispositivos na rede. Uma vez que um dispositivo se conectava a este cabo, ele tinha a capacidade de se comunicar com qualquer outro dispositivo conectado ao cabo. Isto permitiria que rede fosse expandida para acomodar novos dispositivos sem que fossem necessárias alterações nos dispositivos já conectados na rede.

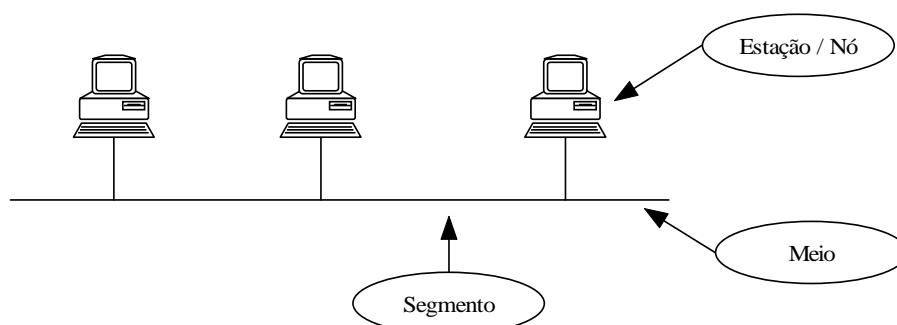
A terminologia da Ethernet é composta de 4 elementos básicos: meio, segmento, nó e pacote.

Meio: Os dispositivos Ethernet se conectam a um meio comum que provê um caminho ao longo do qual os sinais eletrônicos irão trafegar. Antigamente este meio era encontrado na forma de cabos coaxiais e hoje são cabos com pares trançados ou fibras óticas.

Segmento: Um meio compartilhado único é chamado de segmento.

Nó: Os dispositivos conectados ao segmento são chamados de Nós ou Estações.

Pacotes: Os Nós se comunicam através de mensagens curtas chamadas de Pacotes, que são pedaços de informação de tamanho variável.



[Elementos da Ethernet]

Pacotes são o equivalente a sentenças na linguagem humana. O Protocolo Ethernet especifica as regras para construção de pacotes. Existe um comprimento mínimo e máximo explícito para os pacotes, bem como pedaços de informações que necessariamente devem aparecer e, cada pacote. Cada pacote deve incluir o endereço de destino e o endereço de origem, que identificam aquele que receberá a mensagem e aquele que a enviou. O endereço identifica de forma única cada Nó, assim, nunca dois dispositivos Ethernet tem o mesmo endereço. Como o sinal elétrico da Ethernet atinge todos os Nós, o endereço de destino é crucial para identificar quem vai receber o pacote.

Uma característica interessante sobre endereçamento Ethernet é o Endereço de Broadcasting (Difusão). Ao utilizar o Endereço de Broadcasting, todos os Nós da rede receberão e processarão o pacote.

CSMA/CD

CSMA/CD significa Carrier-Sense Multiple Access with Collision Detection (Múltiplo Acesso via Detecção de Portadora com Detecção de Colisão) e descreve como a Ethernet transmite os pacotes entre os Nós. A compreensão deste processo é essencial para compreensão de algumas das razões que levaram ao desenvolvimento de switches e roteadores, e da necessidade de separar as redes em sub-redes.

Imagine o segmento Ethernet como uma mesa de jantar, com várias pessoas sentadas, tentando manter uma conversa educada, que representam os nós. O termo "Múltiplo Acesso" significa que quando uma Estação transmite as outras Estações escutam, da mesma forma que quando uma pessoa na mesa fala, as outras escutam.

Imagine-se agora sentado na mesa tentando falar algo. Porém neste momento outra pessoa está falando. Como a conversa deve ser educada, você vai esperar a pessoa parar de falar para você mesmo começar a falar. Este é o conceito chamado de "Detecção de Portadora", mencionado pela Ethernet. Antes de uma Estação começar a transmitir ela "escuta" o Meio para saber se alguém está falando. Se o Meio estiver "quieto" ela sabe que pode falar.

O protocolo CSMA é um bom começo para definir uma forma de "conversação" na rede, porém existe um problema a resolver. Imagine que existe um determinado momento de silêncio na mesa e que você e outra pessoa percebem isso e começam a conversar na mesma hora. Na terminologia da Ethernet o que ocorre é uma colisão..

Nós podemos gerenciar isso de forma educado parando de falar e dando a vez a outra pessoa. A Ethernet também "escuta" o Meio para saber se alguém começou a falar. Se eles receberem a própria transmissão "embaralhada" é sinal de que outra estação também está transmitindo e assim sabem que a colisão ocorreu. Quando isto ocorre, as estações param de transmitir e esperam um intervalo de tempo aleatório para recomençar a transmitir, desde que o Meio esteja em "silêncio".

A Ethernet começou com a velocidade de 2 Mbps (Mega bits por segundo), popularizou-se com 10 Mbps, atualmente está em 100 Mbps, estando em desenvolvimento a "Gigabit Ethernet" de 1000 Mbps ou 1 Gbps.

Hardware

A Ethernet tem sérias limitações quanto ao comprimento dos Segmentos de Rede. Em cabos coaxiais esse limite era de 185 metros e em cabos com par trançado era de 100 metros. Além disso, considerando o protocolo de CSMA/CD onde apenas existe uma estação transmitindo, aparecem limites práticos para o número de estações em rede.

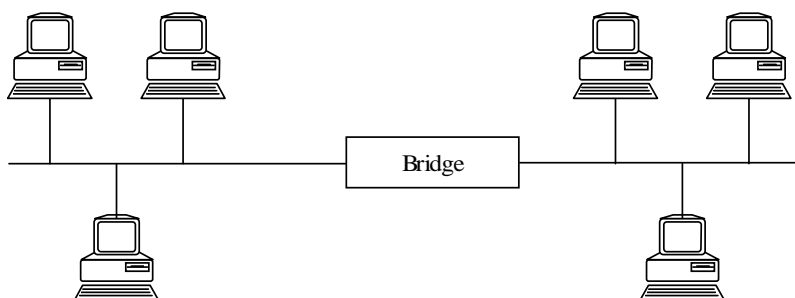
Foram desenvolvidos vários dispositivos de Rede para tentar resolver estes problemas. Em especial existem três: Repetidores, Bridges (Pontes) e Roteadores. Os Repetidores, bem como os HUBs, operam na Camada Física do TCP/IP. Os Bridges operam na Camada de Enlace e os Roteadores operam na Camada de Internet, separando a rede Logicamente ao invés de Fisicamente como os Bridges.

Repetidores

Os Repetidores são amplificadores de sinal que são conectados ao Meio e permitem aumentar a distância que os cabos alcançam.

Bridges e Switches

Os Bridges permitem segmentar uma rede, separando-a em vários pedaços. Em nossa mesa de jantar isto equivaleria a separar a mesa em alguns grupos. O Bridge verifica o endereço de destino e só passa adiante pacotes que se destinam para outro segmento. Isto ajuda em muito a diminuir o tráfego desnecessário.



[Bridges]

Os Switches são a implementação moderna dos Bridges, permitindo criar Segmentos Dedicados entre duas Estações de Rede. Além disso, permitiram que a Ethernet se torna Full-Duplex, ao invés de Half-Duplex, ou seja, uma Estação pode transmitir e receber ao mesmo tempo, pois passa a falar apenas com o Switch.

Este conceito é conhecido como Rede Chaveada (Switched Network), pois permite criar canais dedicados para transmissão entre Estações. As Redes Chaveadas substituem o cabo simples da Ethernet por segmentos dedicados para cada Estação. Este segmentos são conectados a um Switch, que age de forma similar a um Bridge, mas permite conectar vários segmentos de Estações, chegando as centenas em Switches modernos. Como os dispositivos no segmento são a Estação e o Switch, este pega todos os pacotes antes deles chegarem ao destino. O switch então transmite o pacote para o segmento ao qual está conectado apenas o Destinatário do pacote. Isto permite que várias conversas ocorram ao mesmo tempo na Rede, ao contrário da Ethernet com o cabo simples.

As redes chaveadas permitiram também transformar o protocolo Ethernet em Full-Duplex ao invés de Half-Duplex. O termo Full-Duplex diz respeito a capacidade de transmitir e receber dados ao mesmo tempo. A Ethernet original é Half-Duplex, permitindo apenas transmissão ou recebimento. Além disso hoje são utilizados cabos de pares trançados e fibras ópticas que transmitem e recebem dados por diferentes condutores. Assim as Estações não precisam se preocupar mais com colisões, pois elas e o Switch são os únicos dispositivos na Rede.

Uma característica importante dos Bridges é que eles permitem a passagem de pacotes Ethernet de "Broadcast" para todos os segmentos conectados. Este comportamento é necessário, mas se torna um problema quando a rede e o número de segmentos crescem. Assim, ao crescer a rede torna-se necessário utilizar roteadores.

WAN (Extranet/Internet)

A Ethernet é o protocolo utilizado em Redes Locais, ou LANs. Entretanto em Redes Remotas, ou WANs, são necessários outros protocolos, em função das limitações da Ethernet discutidas acima. Exemplos bem conhecidos de protocolos de WAN são o PPP (Point-To-Point Protocol) e HDLC (High Level Data Link Control).

PPP - Point-To-Point Protocol

O protocolo PPP é normalmente utilizado em nas conexões discadas entre Usuários domésticos e seus Provedores de Internet. Além dele existe o protocolo SLIP, mas este permite apenas a utilização de TCP/IP, enquanto o PPP permite transmitir usando AppleTalk, IPX, Microsoft NetBEUI e outros.

HDLC - High Level Data Link Control

O protocolo HDLC é um protocolo muito utilizado pa conexão entre roteadores, transportando dados IP. Ele é utilizado em redes do tipo X.25 ou Frame-Relay.

Camada de Internet

A Camada de Enlace é responsável por rotear as mensagens através de redes. Existem 2 tipos de dispositivos responsáveis pelo roteamento de mensagens entre redes: Gateways e Roteadores. O Gateway é um computador com 2 placas de rede. Ele recebe mensagens de uma rede através da primeira placa de rede e roteia para segunda rede através da segunda placa. O Roteador é um equipamento dedicado que executa a mesma função.

Esta camada trabalha com Datagramas de dados. Os Datagramas são pacotes de informação com informações de controle associadas, contendo, por exemplo, endereço de destino, endereço de origem e valores de checagem de erros. A Camada de Internet não suporta qualquer conceito de sessão ou conexão. Uma vez enviados os dados não existe nenhum controle sobre o que foi transmitido. Quando os protocolos desta camada recebem um Datagrama com erros eles simplesmente o desprezam, sem notificar as camadas superiores.

IP

O Protocolo IP (Internet Protocol) é o mais conhecido protocolo desta camada. Ele é um protocolo sem conexão, ou seja, não é estabelecido nenhum tipo de conversação entre o transmissor e o receptor antes de iniciar a transmissão. Além disso é um protocolo não confiável, ou seja, ele depende de outros protocolos para executar correção e recuperação de erros.

Hardware

Roteadores

Os Roteadores são equipamentos destinados a conectar 2 ou mais redes, utilizando-se do Endereçamento IP para executar suas funções. Os Roteadores utilizam-se de uma Tabela de Configuração para executar o roteamento que contém informações como:

- Conexões do Roteador que levam a um grupo particular de endereços IP;
- Prioridade das Conexões a serem utilizadas;
- Regras para gerenciar o tráfego de Rede.

O Roteador é responsável essencialmente por 2 tarefas:

- Garantir que a informação não vá para onde não é necessária, o que é crucial para que a rede seja "entupida" com grandes quantidades de dados inúteis;
- Garantir que a informação chegue a seu destino.

O Roteador permite unir 2 ou mais redes, passando informações entre elas, e em alguns casos fazendo a tradução entre diferentes protocolos de rede. Ele protege as redes umas das outras, impedindo que dados desnecessários trafeguem nelas.

Ao utilizar a rede de telefonia, uma pessoa faz uma conexão permanente através do sistema de telefonia entre 2 pontos. A conexão é permanente e disponível enquanto um dos lados não a terminar. Entretanto, se durante a conversação algum ponto desta grande rede que conecta os 2 pontos falhar a ligação cai .

A Internet utiliza um sistema de Chaveamento de Pacotes, que “quebra” a informação a ser transmitida, não importa de um arquivo de música, uma página web ou um e-mail, em pequenos pacotes. Estes pacotes são então enviados pela rede, um por vez. Uma rede baseada em Chaveamento de Pacotes tem 2 grandes vantagens sobre uma rede de Telefonia convencional:

- Pode balancear a carga através das diversas redes conectadas a cada milissegundo;
- Pode alterar a rota de transmissão do pacote caso algum equipamento falhe no caminho atual, de forma a não parar a transmissão.

Os Roteadores são capazes de alterar o caminho que determinado pacote deve seguir pois eles consultam as informações de controle, como, endereço de origem e destino, que o pacote contém. Além disso, eles trocam informações entre si, através do protocolo ICMP (Internet Configuration Management Protocol), sobre atrasos no recebimento e envio de mensagens além de tráfego em diversas partes da rede.

Dependendo do dia da semana, alguns trechos da grande rede pública de chaveamento de pacotes podem estar mais carregados que outros. Quando isso acontece os Roteadores, após se comunicarem entre si, desviam o tráfego para segmentos menos carregados da rede.

Os ataques do tipo “Denial of Service, ou, Negação de Serviço, são tentativas de parar determinados servidores pelo excesso de requisições de serviços. Quando isso, acontece, como por exemplo, no caso do vírus “MyDoom”, que atacariam os sites das empresas MICROSOFT e SCO, vários Roteadores podem ser “entupidos” de tráfego, um após o outro.

Camada de Transporte

A Camada de Transporte é responsável por prover a integridade dos dados através de uma comunicação confiável entre 2 pontos da rede. Além das funções usuais de transmissão e recepção de dados, são utilizados comandos de abertura (open) e fechamento (close) de sessão, que permitem iniciar e terminar uma conexão destinada a troca de dados. É criado assim o conceito de Conexão ou Circuito Virtual. Uma Conexão é o estado que existe entre o momento em que um comando de abertura de sessão foi aceito pelo receptor e o momento que o comando de fechamento de sessão.

TCP

O Protocolo TCP (Transmission Control Protocol) é um protocolo confiável e orientado a conexões. A confiabilidade deste protocolo vem dos controles exercidos sobre os Datagramas transmitidos durante uma Conexão. O Protocolo TCP oferece comunicação Full-Duplex e controles que garantem que os dados serão retransmitidos caso a transmissão resulte em erro. Além disso ele permite que um computador mantenha múltiplas conexões ao mesmo tempo.

UDP

O Protocolo UDP (User Datagram Protocol) oferece acesso direto aos Datagramas, da mesma forma que o IP. Ele é utilizado quando a correção de erros, através do conceito de Conexão, oferecido pelo TCP/IP não é necessário. É uma forma de oferecer a possibilidade de transmissões com um mínimo de sobrecarga em relação ao que o Protocolo IP já executa. Aplicações que trabalham com consultas-respostas, como, por exemplo, o sistema de mensagens ICQ, são excelentes usos para o UDP. A resposta à determinada consulta pode ser considerada como controle de sucesso no envio. Caso não haja nenhuma resposta, o usuário pode mandar os dados novamente.

Camada de Aplicação

HTTP

O protocolo HTTP (Hypertext Transfer Protocol) ou Protocolo de Transferência de Hipertexto

clientes e servidores Web trocam arquivos de texto, imagens, áudio, vídeo, etc. Os clientes HTTP são os Navegadores (Browsers) Web que solicitam informações, as chamadas páginas Web, armazenadas em servidores Web. Exemplos de Clientes Web são o Internet Explorer, Netscape, Mozilla e Opera. Exemplos de Servidores Web são o Apache e o Internet Information Server.

Em essência o protocolo HTTP é composto de uma Requisição do Cliente e de uma Resposta do Servidor. A Resposta do Servidor normalmente vem na forma de um arquivo texto codificado utilizando a linguagem HTML (Hypertext Markup Language) ou Linguagem de Marcação de Hipertexto. O intervalo de tempo Requisição/Resposta é conhecido como Conexão. O Cliente inicia uma Conexão, envia a Requisição, recebe a Resposta e fecha a Conexão. Desta forma, o protocolo HTTP é um protocolo, a priori, sem manutenção de estado, ou seja, uma segunda Conexão aberta não lembra nada a respeito da primeira, cabendo ao software que utiliza este protocolo, criar alguma forma de armazenar o estado.

Quando uma página é requisitada pelo cliente ao servidor, não é enviada apenas a URL do arquivo mas várias informações extras. O mesmo vale para resposta do servidor, que além da página solicitada, contém várias informações extras enviadas pelo servidor. As informações extras são geradas automaticamente pelo cliente ou pelo servidor Web sendo transparentes para o usuário final.

As mensagens HTTP tem o mesmo formato, independentemente de serem Requisições ou Respostas, sendo separadas em 3 seções:

- Linha de Requisição/Resposta;
- Cabeçalho (Header) HTTP;
- Corpo (Body) HTTP.

Requisição HTTP

A Requisição HTTP é enviada pelo Cliente Web para o Servidor Web requisitando uma página identificada através de uma URL.

Linha de Requisição

A primeira linha de cada Requisição HTTP contém uma Linha de REquisição com 3 informações:

- Um comando HTTP conhecido como método;
- O caminho no servidor (URL) para encontrar o recurso que o Cliente deseja;
- A número da versão do HTTP.

O método é utilizado para informar ao servidor como manipular a requisição. Os 3 métodos mais comuns que aparecem são: GET, HEAD e POST.

Método	Descrição
GET	A maioria das Requisições HTTP usam o método GET. A URL pode conter parâmetros para a página requisitada, enviados no final da URL.
HEAD	O mesmo que o método GET, exceto que indica uma requisição para um Cabeçalho HTTP apenas sem dados
POST	Este comando indica que parâmetros serão enviados como parte do Corpo HTTP ao invés de serem enviados ao final da URL como acontece no método GET

Existem vários outros métodos HTTP, como, por exemplo, PUT, DELETE, TRACE, CONNECT e OPTIONS, porém são bem menos comuns.

Cabeçalho HTTP

O Cabeçalho HTTP contém informações sobre quais tipos de documentos o Cliente irá aceitar, que tipo de Browser solicitou as informações, a data e informações gerais de configuração.

Corpo HTTP

O Corpo HTTP contém qualquer informação adicional que o Cliente deseja mandar para o Servidor, assim como parâmetros do método GET ou Cookies, que são pequenas porções de informação usadas para manter o estado entre as conexões HTTP.

Resposta HTTP

A Resposta HTTP é enviada pelo Servidor de volta para o Cliente, usualmente devolvendo uma página HTML requisitada por uma Requisição HTTP.

Linha de Resposta

A Linha de Resposta contém apenas 2 informações:

- O número da versão HTTP;
- Um código de requisição HTTP que indica o sucesso ou erro da requisição.

O código 200, por exemplo, representa "sucesso", e o código 4040 representa "página não encontrada". Códigos de erro são números de 3 dígitos, onde o primeiro dígito representa a classe de resposta.

Classe	
100-199	Estes códigos são informativos – eles indicam que a requisição está sendo processada
200-299	Estes códigos indicam sucesso – eles indicam que o servidor processou a requisição.
300-399	Estes códigos indicam que a requisição não foi processada porque a informação solicitada mudou de lugar.
400-499	Estes códigos indicam um erro do cliente – a requisição estava incompleta, incorreta ou impossível de avaliar.
500-599	Estes códigos indicam um erro do servidor – a requisição estava aparentemente correta, mas foi impossível executá-la.

Cabeçalho HTTP

O Cabeçalho HTTP da Resposta é similar ao Cabeçalho HTTP da Requisição, porém agora as informações são relativas ao Servidor e não ao Cliente.

Corpo HTTP

O Corpo HTTP da Resposta contém a página HTML requisitada ou gerada pelo Servidor, juntamente com qualquer script que venha a ser executada pelo Cliente.

Requisição	GET http://www.google.com/HTTP/1.0
Cabeçalho	Accept: image/jpg, appication/schockwave-flash Accept-Language:pt-br Cookie=PREF=ID=0bd019283901823120938: TM=12371927391782: LM=120938190283:S=1289371982738yYUtd User-Agent: Moxilla/4.0 (compatible; MSIE 6.0; Wndows NT 5.0) Host: www.google.com Connection: Close
Corpo	

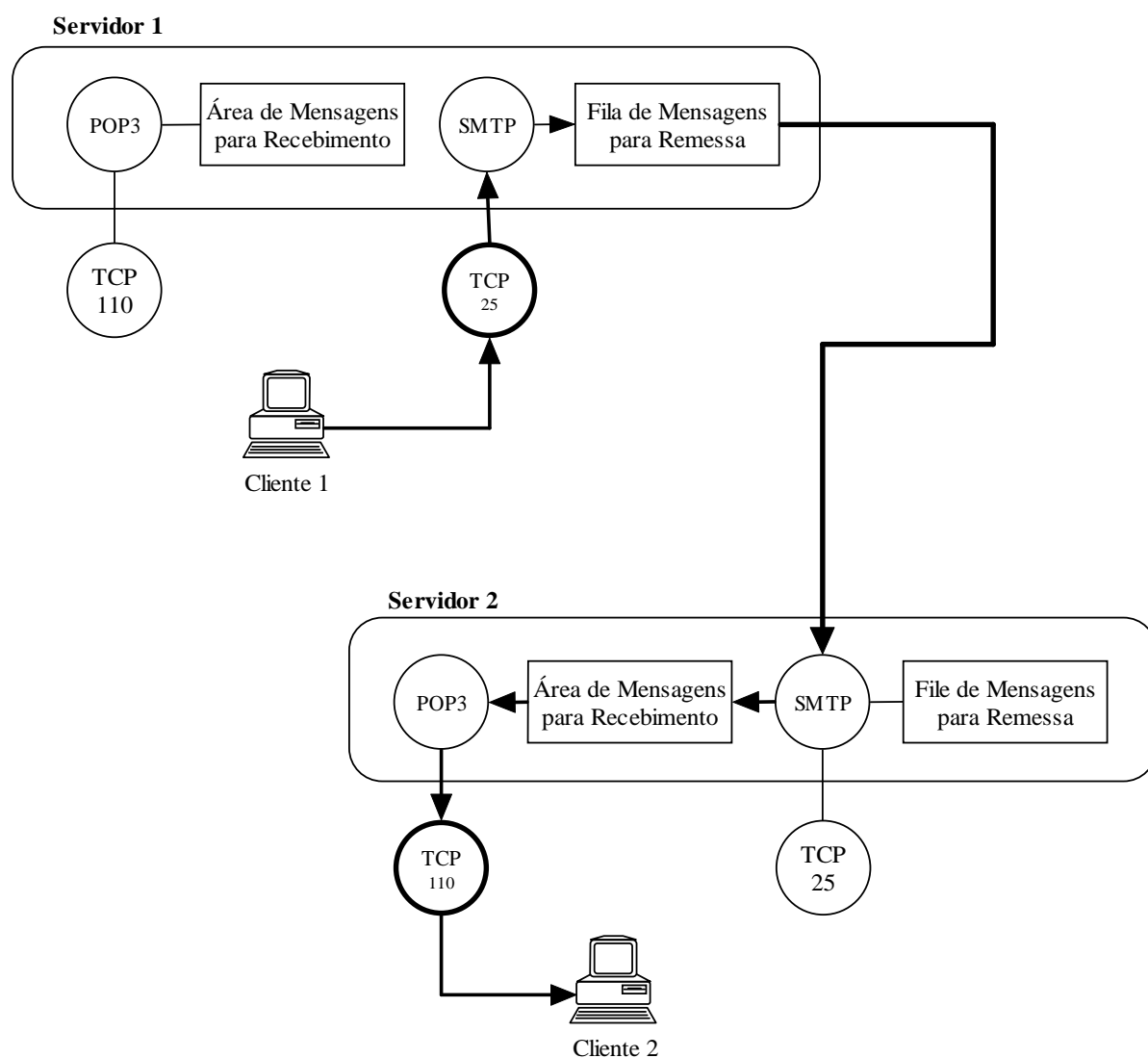
Requisição HTTP de <http://www.google.com>

Resposta	HTTP/1.0 200 OK
Cabeçalho	Cache-control: private Content-Type: text/html Server: GWS/2.1 Content-length: 3074 Date: Mon, 8 Aug 2007 14:26:45 GMT Connection: Keep-Alive
Corpo	<html> <head> ... </head> <body> ... </body> </html>

Resposta HTTP de <http://www.google.com>

SMTP – Simple Message Transfer Protocol
POP3 – Post Office Transfer Protocol
IMAP4 – Internet Message Access Protocol

O protocolo SMTP (Simple Message Transfer Protocol) é responsável pela remessa de e-mails, respondendo na porta TCP 25. O protocolo POP3 (Post Office Protocol) é responsável pelo recebimento de e-mails, respondendo na porta TCP 110. O protocolo IMAP (Internet Message Access Protocol) é uma evolução do protocolo POP3 para recebimento de e-mails, respondendo na porta TCP 143.



[Remessa e Recebimento de e-mails]

Os clientes SMTP/POP3/IMAP4 são os programas de e-mail que conversam com servidores SMTP/POP3/IMAP4. Exemplos de Clientes Web são o Outlook Express, Mozilla e Eudora. Quando um computador cliente 1 deseja mandar um e-mail para um computador cliente 2, ele inicialmente entra em contato com o servidor SMTP 1 via porta 25, enviando sua mensagem, que será colocada em uma fila de remessa de mensagens. O servidor SMTP 1 entra em contato com o servidor SMTP 2 e envia a mensagem. Isto pode levar algum tempo, se a fila de remessa de mensagens estiver grande. O servidor SMTP 2 salva a mensagem em uma área de mensagens do usuário, onde ficam até o usuário de conectar a próxima vez. Quando o usuário se conecta, usando o protocolo SMTP, via porta TCP 110, ele transfere as mensagens da sua área de mensagens para seu computador, e as mensagens são apagadas da área do servidor 2.

O protocolo POP/3 permite armazenar as mensagens no servidor, de onde, ao serem transferidas, serão apagadas. Esta forma de trabalhar com o e-mail se chama "offline" (fora de linha). Existem entretanto 2 outras formas de trabalhar com o e-mail: "online", ou seja, os e-mails permanecem no servidor e não são apagados a não ser que o usuário ordene, e "desconectado", onde os e-mails são transferidos para uma máquina local, lidos, eventualmente respondidos e depois transferidos integralmente de volta para o servidor, que sempre mantém uma cópia completa dos e-mails. O protocolo POP/3 permite apenas o trabalhar no modo "offline", enquanto o IMAP/4 permite trabalhar com os modos "offline" e "desconectado".

Um exemplo muito comum de utilização do protocolo IMAP/4 são os sistemas de "Web Mail", disponíveis em vários provedores de acesso, principalmente os gratuitos. O usuário tem acesso a uma página Web que mostra seus e-mails, e eles são apagados apenas se o usuário assim o solicitar. Estes e-mails ficam armazenados no servidor (ocupando espaço em disco) e nunca são transferidos para uma máquina cliente do usuário, como acontece no caso da utilização de programas como o Outlook Express.

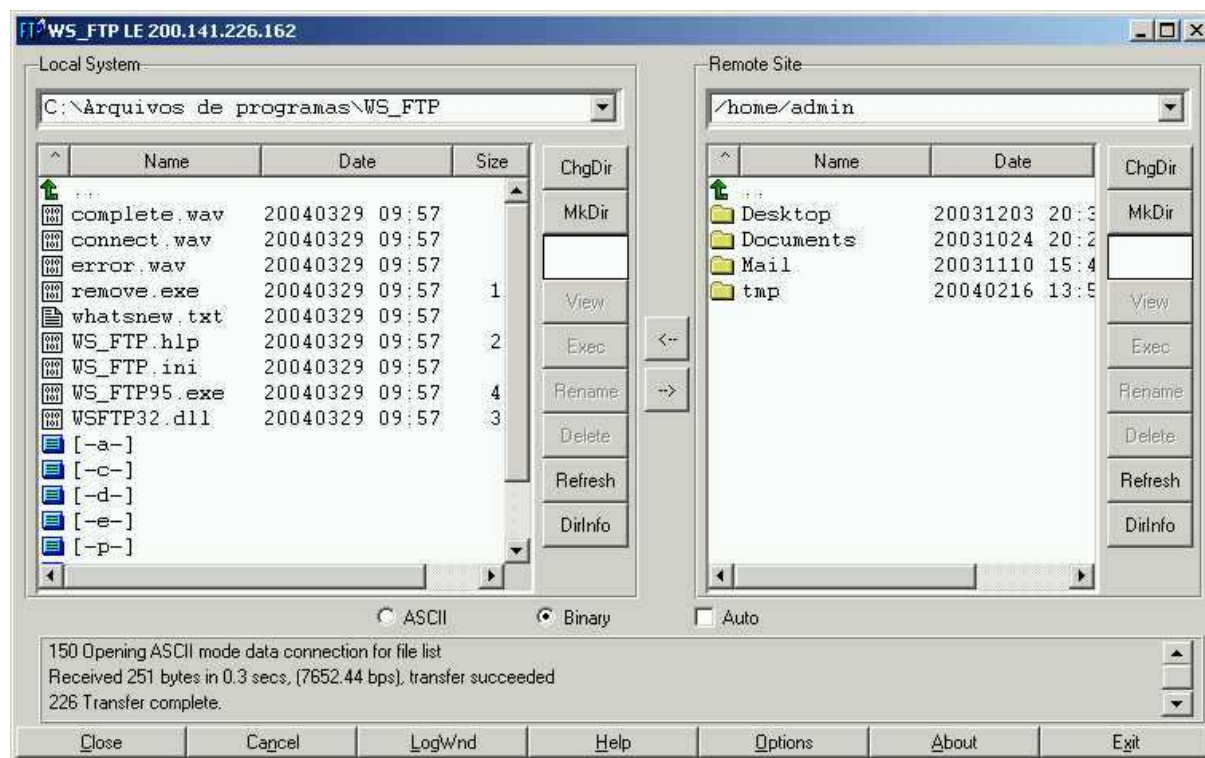
FTP – File Transfer Protocol

O protocolo FTP (File Transfer Protocol) ou Protocolo de Transferência de Arquivos é uma forma clássica de transferência de arquivos via Internet. Em essência ele permite conectar em um servidor e transferir arquivos de e para este servidor utilizando um conjunto de comandos de uma forma muito similar que utilizamos para navegar em uma estrutura de diretórios do disco local de nosso computador. O protocolo FTP responde por padrão na porta 21.

Existem inúmeros clientes FTP, desde os mais simples que abrem apenas uma linha de comando onde são digitados os comandos FTP até sofisticados programas gráficos com uma interface muito parecida com o Windows Explorer.

O interessante na utilização do protocolo FTP, é que o mesmo pode ser usado por 2 computadores para, automaticamente, trocar arquivos entre si. Isto porque é baseado em comandos, que podem ser executados por um script ou programa que esteja sendo executado. Hoje o HTTP está substituindo em muito o FTP para cópia de arquivos da Internet. Porém em aplicações mais rebuscadas o FTP ainda é imbatível.

Utiliza-se o termo “Download” para indicar a cópia de arquivos do servidor para o cliente local e “Upload” para indicar a cópia de arquivos do computador local para o servidor.



Os servidores FTP tem usualmente a opção de conectar usando um usuário “anônimo”. Isto é particularmente comum em sites de download de software. Assim, ao conectar é necessário informar o nome do usuário como “anonymous”. A senha não é obrigatória, mas, segundo as regras de etiqueta da Internet, deve-se colocar o e-mail pessoal do usuário que está se conectando.

Comandos de FTP

Comando FTP	Descrição
? ou help	exibe lista de comandos disponíveis
Cd	muda de diretório
dir ou ls	mostra arquivos e diretórios
user	identifica o usuário
get	executa download de arquivos
pwd	mostra diretório corrente
quit	desconecta do servidor
send	Executa upload de arquivos

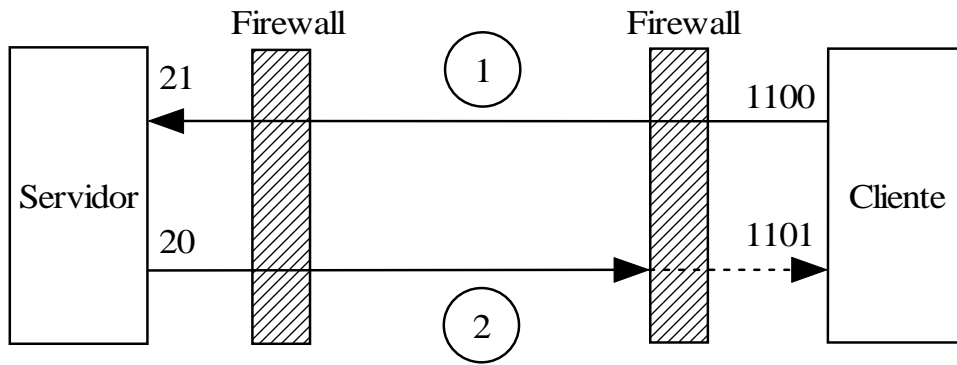
[Comandos Básicos FTP]

FTP Ativo X FTP Passivo

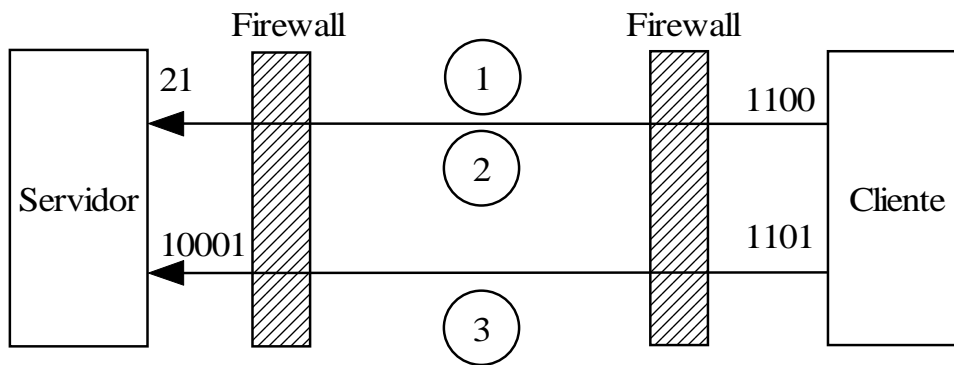
Existe uma confusão muito comum quanto à configuração do protocolo FTP Ativo e Passivo, em função do FTP utilizar 2 portas para comunicação: Porta de Comandos (21) e Porta de Dados (20).

O **FTP Ativo** abre uma conexão a partir de uma porta qualquer acima de 1024 (1100, no exemplo) do Cliente para porta 21 (Porta de Comandos) do Servidor. Em seguida o Servidor abre uma conexão da porta 20 (Porta de Dados) para porta do Cliente seguinte a porta da conexão anterior (1101, no exemplo) com mostra a figura. O problema com este tipo de conexão é que se existir um Firewall na máquina Cliente ele muito provavelmente não irá permitir a conexão.

O **FTP Passivo** abre uma conexão a partir de uma porta qualquer acima de 1024 (1100, no exemplo) do Cliente para porta 21 (Porta de Comandos) do Servidor (1). O Servidor retorna para o Cliente o número de uma porta do Servidor que será liberada para conexão (10001, no exemplo) (2). Em seguida o Cliente abre uma conexão na porta seguinte a porta da conexão anterior (1001, no exemplo) com a porta informada pelo Servidor (10001, no exemplo) como mostra a figura. O Firewall do Servidor é configurado para receber conexão em uma faixa de portas para FTP Passivo apenas, permitindo assim a conexão.



FTP ATIVO



FTP PASSIVO

Endereços

URLs

Uma URL (Uniform Resource Locator), ou, Localizador Uniforme de Recursos é uma forma de especificar a localização de recursos disponíveis eletronicamente. URLs tornam possível a pessoas e/ou programas acessar uma grande variedade de informações disponibilizada através de diferentes protocolos da Internet. Usualmente utilizam-se URLs em navegadores da Web, pois ela utiliza URLs para ligar diferentes páginas de informações.

A URL funciona de forma similar a endereçamento postal, contendo toda as indicações necessárias para obter determinada informação. Porém ele contém mais, pois podem acessar indicar informações disponíveis em diferentes fontes, acessadas de diferentes formas.

A sintaxe geral da URL, definida pela RFC 1738, é:

<esquema>:<informação dependente do esquema>

O “esquema” serve para informar a aplicação qual o tipo de informação será acessada e/ou qual mecanismo será utilizado para acessá-la. Exemplos de “esquemas” seriam http, ftp e news.

HTTP – Hypertext Transfer Protocol

O protocolo HTTP é utilizado para a acesso a Web, sendo a utilização mais comum de URLs.

<http://<host>:<porta>/<caminho>?<parâmetros>>

O “host” indica o computador, referenciado através de um domínio ou de um endereço IP onde está o servidor Web. A “porta” indica o número da porta TCP onde o servidor está respondendo. A porta TCP 80 é a padrão do protocolo HTTP, podendo ser omitida quando usada. O “caminho” indica a página que desejamos acessar, que, se omitida, retorna a página padrão, ou “home page”. Os parâmetros são utilizados para passar parâmetros para página a ser chamada, podendo não ter nenhum ou vários parâmetros, separados por “?” seguindo a seguinte sintaxe:

parâmetro1=valor1&parâmetro2=valor2&...

Outro símbolo que pode ser encontrado frequentemente em URLs é o “#” que indica uma âncora HTML dentro da página solicitada como em:

<http://www.netxpto.com/users/dwb/url-guide.html#document>

As âncoras HTML servem para indicar uma parte específica do documento solicitado.

FTP – File Transfer Protocol

O protocolo FTP é uma forma muito conhecida de troca de arquivos pela Internet.

<ftp://<usuário>:<senha>@<host>:<porta>/<comando1>/<comando2>/...>

O "host" é o endereço IP onde se encontra o servidor FTP, que pode ser acessado por um "usuário" através de uma "senha". A porta TCP 21 é a padrão do protocolo FTP, podendo ser omitida quando usada. A série "comandoN" é um conjunto de comandos FTP válidos como "GET" ou "PUT" que podem ser executados automaticamente no servidor.

e-mail

A URL de e-mail é diferente das anteriores pois não indica um arquivo disponível na Internet, mas sim um usuário de e-mail.

<mailto:<usuário@host>>

O usuário@host é um endereço de e-mail válido, como, por exemplo, siegmar@acessa.com. Usualmente ao clicar em uma URL de e-mail, será aberto o programa cliente de e-mail, como, por exemplo, o Outlook Express.

Arquivos

Uma URL de arquivo indica um arquivo local ou de rede. Ela não utiliza um protocolo de Internet, mas sim acesso direto, se o arquivo estiver na máquina local, ou acesso via rede, se o arquivo estiver em uma máquina em rede.

<file://<host>/<caminho>>

Compartilhamento de Endereços: Proxy, NAT e Socks

O Compartilhamento ou Tradução de Endereços Internet é um método utilizado para conectar múltiplos computadores a Internet utilizando apenas um endereço IP. Este método permite que redes de computadores se conectem a Internet de forma barata e eficiente.

A utilização do Compartilhamento de Endereços se dá em função de 3 fatores:

- escassez de endereços IP;
- segurança;
- flexibilidade de administração de redes.

Os endereços IP, usando o modelo IPv4 de 4 números, são recursos cada vez mais escassos. Assim, um IP válido ou fixo, não é barato, e nem largamente disponível. Se todos os computadores de todas as redes do mundo precisassem de um IP fixo não haveria números suficientes. Ao conectarmos em um Provedor de Internet através de uma linha discada utilizando um modem, recebemos um IP válido ou público, que permanece fixo até o final da conexão. Se voltarmos a nos conectar 5 minutos depois, podemos recebemos o mesmo IP ou outro, pois o primeiro pode estar sendo utilizado por outro usuário. Da mesma forma, a conexão via ADSL ou Cabo, nos fornece um IP válido ou público, mas dinâmico, ou seja, que pode ser alterado durante o dia pela empresa fornecedora do serviço.

O Compartilhamento de Endereços executa a tradução de endereços IP públicos para endereços IP privados (utilizados em alguma rede interna) utilizando uma das 3 tecnologias abaixo:

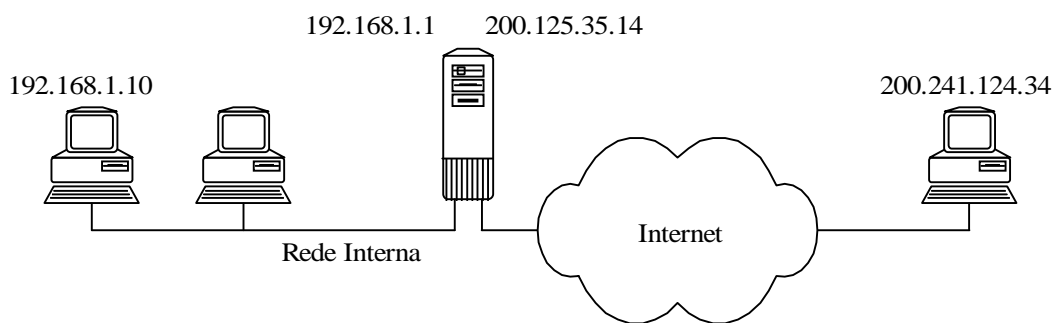
- Software Proxy;
- Protocolo Socks;
- NAT (Network Address Translation), ou, Tradução de Endereços de Rede, utilizado em roteadores.

Quando uma máquina da rede interna tenta acessar um recurso da Internet, são trocados pacotes TCP/IP que contém a endereço de origem e o endereço de destino do pacote. Em essência o Roteador ou Gateway tem acesso a rede interna e a rede externa ou Internet, no caso do Roteador através de suas portas de comunicação e no caso do Gateway através de 2 placas de rede. O endereço do computador da rede interna é trocado para o endereço público, utilizando uma outra porta, diferente da original para abrir a conexão com o destino.

Suponha que o computador 192.168.1.10 da rede interna queira abrir uma página na Internet no endereço 200.241.124.34, na porta 80, e que o Roteador ou Gateway tenha o endereço 210.125.35.14 obtido através de uma conexão ADSL. Se o Gateway tiver o endereço 192.168.1.1 e estiver

executando um software Proxy na porta 81, teríamos a seguinte tradução de endereços (Observação: Os números de porta 2000 e 3000 são aleatórios):

	rede interna		rede externa		
	computador cliente	gateway rede interna	gateway rede externa	computador servidor	
endereço	192.168.1.10 =>		192.168.1.1		=>
	200.125.35.14 =>		200.241.124.34		
porta	2000	81	3000	80	



[Compartilhamento de Endereços]

Software Proxy

Um "Proxy" é um software que trabalha em benefício de outro, sendo normalmente utilizado para o protocolo HTTP. Um Proxy HTTP age como um semi-servidor, ou seja, o cliente (Browser) se conecta ao Proxy que por sua vez se conecta ao servidor. Usualmente um Proxy permite o armazenamento de páginas em uma memória "cache", ou seja, uma memória temporária, de tal forma que se um segundo usuário tentar acessar a mesma página acessa por outro usuário a pouco ele já estará disponível. Usualmente um software Proxy oferece suporte a protocolos HTTP, HTTPS e FTP.

Os inconvenientes na utilização de um software Proxy, são a necessidade de suporte ao protocolo que queremos utilizar e o fato de não ser uma operação transparente, pois o software cliente deverá ser configurado para utilizar o Proxy.

Protocolo SOCKS

O Protocolo SOCKS foi desenvolvido inicialmente pela NEC, se tornando posteriormente um padrão da Internet para compartilhamento de endereços IP. O Protocolo SOCKS segue a mesma idéia do Software Proxy, ou seja, o Protocolo SOCKS, rodando no Gateway irá fazer uma conexão com o computador servidor na Internet "em nome" do computador cliente que está na rede interna.

A vantagem do Protocolo SOCKS é ser genérico, podendo, por exemplo, ser utilizado para HTTP ou FTP, desde que o software cliente a ser utilizado suporte SOCKS. Além disso ele permite comunicação bidirecional, ao contrário da maioria dos outros métodos de compartilhamento de endereços. Além disso com a versão SOCKS/5 foi disponibilizada a possibilidade de autenticação através de usuário/senha, o que permite maior segurança no acesso entre a rede interna e a externa.

NAT – Network Address Translation

O funcionamento básico do NAT é multiplexar o tráfego na rede interna, apresentando-o a Internet como se estivesse vindo de apenas 1 computador. A multiplexação de endereços é obtida através da utilização de portas TCP, porém, ao contrário dos métodos anteriores, isto é feito dinamicamente, dentro do Roteador. Desta forma, o NAT, é transparente as aplicações, não necessitando configurações.

O NAT é um método bastante sofisticado, ainda mais por funcionar dinamicamente. Os pacotes IP tem dentro deles informações de endereço de origem e de destino, além do próprio pacote de dados conter por vezes informações de endereços, como no caso do FTP Passivo. O NAT cuida de traduzir todos estes endereços, alterando também os dígitos de correção de erros de cada pacote alterado.

Segurança

Os métodos de Compartilhamento de Endereços trazem dentro de si um grande recurso de segurança. Como os endereços da rede interna são invisíveis para a Internet, estas máquinas jamais seriam visíveis para Internet, pois apenas as conexões originadas de dentro para fora são traduzidas, já que as máquinas da rede interna conseguem enxergar as máquinas da Internet. Entretanto pode-se criar uma ligação (link) no Gateway, transferindo as conexões da porta 89 no IP 200.125.35.14 com a porta 80 do computador 192.168.1.9. Assim, as máquinas da rede interna apenas serão visíveis, se o administrador de rede o permitir.

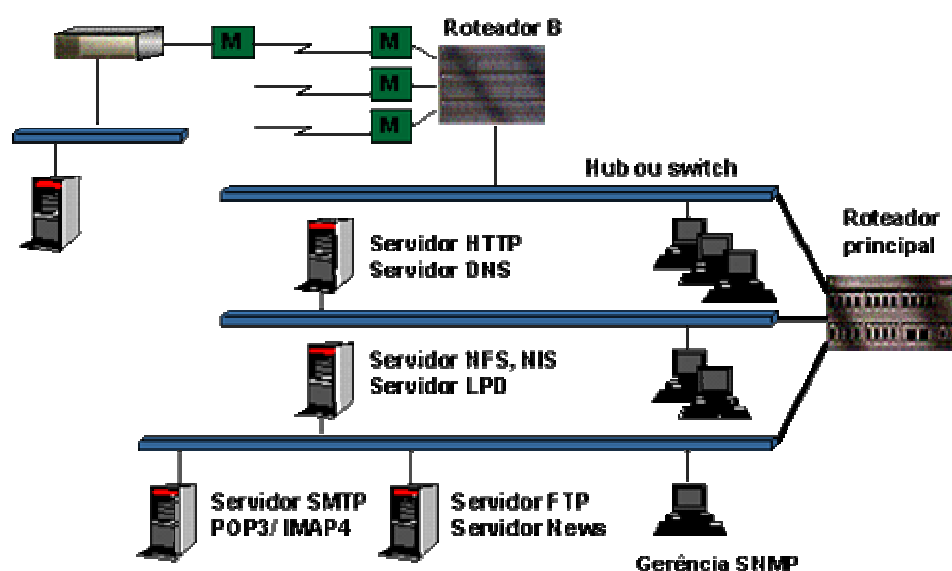
	rede interna		rede externa	
	computador servidor	gateway rede interna	gateway rede externa	computador cliente
endereço	192.168.1.9 200.125.35.14	<= =>	192.168.1.1 200.241.124.34	<=
porta	80	3000	89	2000

Exemplos de aplicação de redes com arquitetura TCP/IP

Seguem abaixo, alguns exemplos de aplicações de arquiteturas distintas de rede baseadas em TCP/IP, como por exemplo, redes internas de empresas baseadas em transporte TCP/IP, serviços de redes de empresas conectados à Internet, provedores de acesso à Internet.

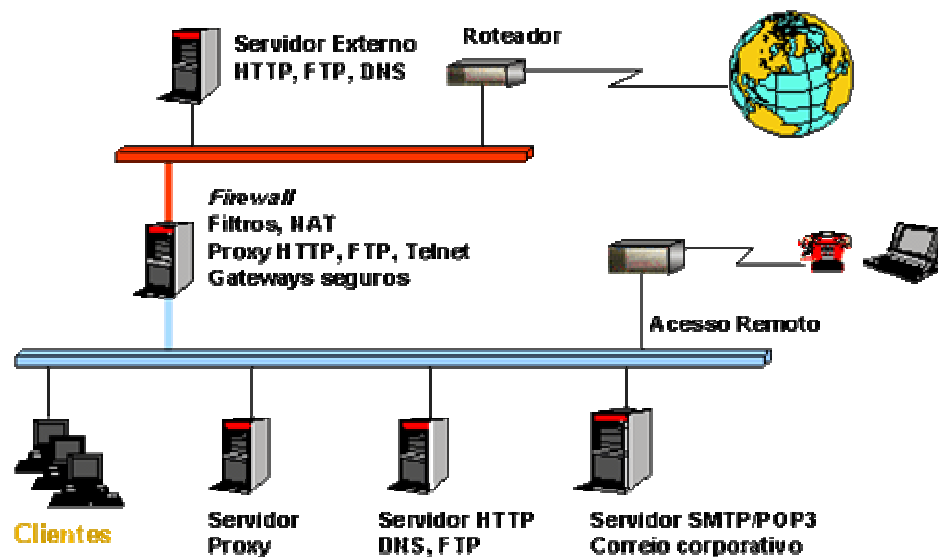
Exemplo 1

Redes internas à empresa utilizando protocolos TCP/IP para formar a estrutura de comunicação e a base das aplicações de rede (correio-eletrônico), compartilhamento de arquivos, distribuição de informação via hipertexto, etc... e chamadas de intranet:



Exemplo 2

Uma estrutura de rede TCP/IP conectada à Internet de forma segura, através da utilização de um firewall, que realiza o filtro de pacotes IP e o transporte de protocolo de aplicações por meio de um gateway (proxy):



Exemplo 3

Um provedor de acesso à Internet, fornecendo serviços de conexão a usuários discados e empresas por meio de ligação dedicada, além de oferecer os serviços básicos de Internet como HTTP, SMTP, POP3, FTP, etc...

