Nível ESAF

Professor
Paulo Najar

INFORMÁTICA

PARA CONCURSOS PÚBLICOS

CAPÍTULO:

Redes de Computadores

REDES DE COMPUTADORES

O que são Redes de Computadores

Redes de computadores são estruturas físicas (equipamentos) e lógicas (programas, protocolos) que permitem que dois ou mais computadores possam compartilhar suas informações entre si.

Uma Rede de Computadores é formada por um conjunto de módulos processadores de comunicação (MPs) capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação.

Definição

Dois ou mais computadores conectados um ao outro por um meio de transmissão.

Objetivo

- Facilitar o compartilhamento de informações.
- Compartilhamento de recursos caros (discos/impressoras).
- Centralização Administração
- Aumentar Eficiência

Classificação da Rede quanto à Distância

Rede de Área Pessoal PAN (Personal Area Network - Rede de Área Pessoal)

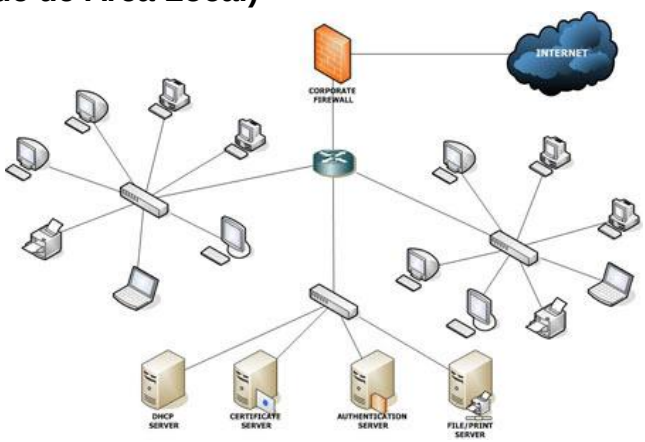
É uma rede de computadores pessoais, formadas por nós (dispositivos conectados à rede) muito próximos ao usuário (geralmente em metros). Estes dispositivos podem ser pertencentes ao usuário ou não. Como exemplo podemos imaginar um computador portátil conectando-se a um outro e este a uma impressora. Tecnologicamente é o mesmo que uma LAN, diferindo-se desta apenas pela pouca possibilidade de crescimento e pela utilização doméstica.

Rede Local LAN (Local Area Network – Rede de Área Local)

Permite a interconexão de equipamentos de comunicação de dados em uma pequena região, geralmente salas, prédios.

Características:

- Geralmente de propriedade privada;
- Alta taxa de transmissão;
- Baixa taxa de erro.
- Dois a alguns computadores conectados
- Area de abrangência: 10m a 1 km
- Um mesmo prédio ou em prédios adjacentes

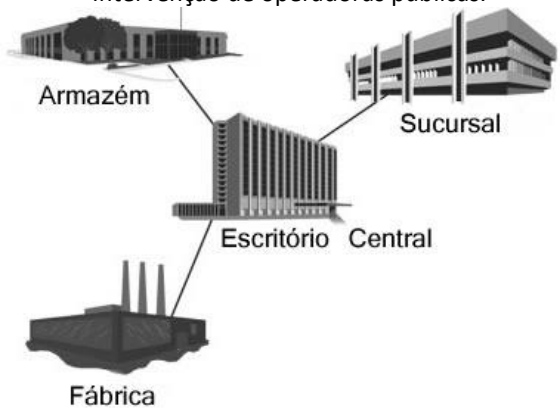


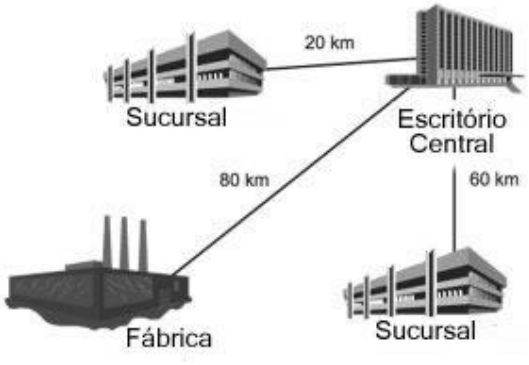
Rede Metropolitana MAN (*Metropolitan Area Network* - Rede de Área Metropolitana)

Permite interconexão de equipamentos de comunicação de dados em uma área metropolitana.

Características:

- Alta taxa de transmissão;
- Utilizam-se principalmente de fibras opticas e eventualmente de enlaces de rádio ou enlaces metálico;
- Cobrem uma cidade;
- Distancias inferiores a 200km e maiores que 1Km;
- Intervenção de operadoras públicas.

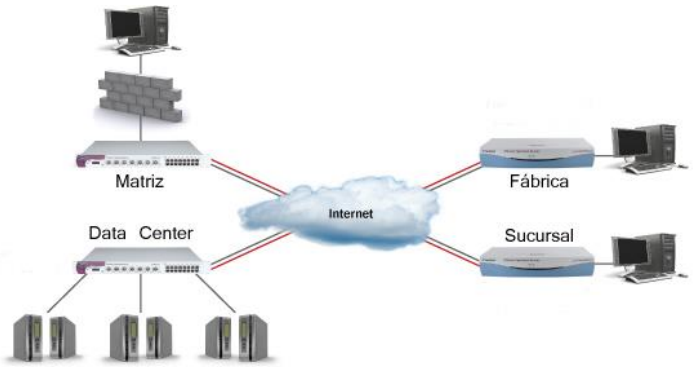




Rede de Longa Distância WAN (*Wide Area Network* - Rede de Área Abrangente)

Também chamada de Rede Geograficamente Distribuída.
Permite interconexão de equipamentos de comunicação de dados entre cidades, países ou continentes.
Em geral, as redes geograficamente distribuídas contém conjuntos de servidores, que formam sub-redes. Essas sub-redes têm a função de transportar os dados entre os computadores ou dispositivos de rede
Características:

- É geralmente um serviço público (apesar de poder ser administrado por uma entidade privada);
- Custo muito elevado devido a distância;
- Utilizam-se de satélites, microondas, cabos de cobre ou cabos submarinos e fibra ótica;
- Baixa taxa de transmissão, geralmente de 64 Kbps a 2 Mbps. Atualmente podendo chegar a Gbps (em enlaces óticos);
- Alta taxa de erros;
- Alta latência;



- Redundância: por necessidade de confiabilidade é importante a existência de caminhos alternativos
- Conexão de duas ou mais redes locais
- Intervenção de operadoras publicas.

Topologia de Redes

A topologia pode ser analisada sob dois aspectos:
Temos uma divisão entre topologias físicas de rede (a forma como os micros são interligados) e as topologias lógicas (a forma como os dados são transmitidos).

Topologia física

- Define o arranjo topológico físico.
- De acordo a forma que os enlaces físicos estão dispostos.

Topologia lógica

- Define o arranjo topológico lógico
- De acordo com o comportamento do arranjo dos enlaces.

Topologia Física

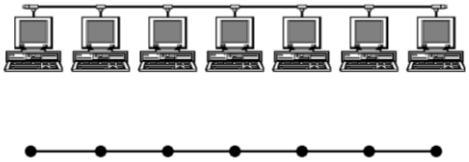
A topologia de uma rede é um diagrama que descreve como seus elementos estão conectados. Esses elementos são chamados de **NÓS**, e podem ser computadores, impressoras e outros equipamentos.
Podemos representar a rede através de um diagrama simplificado chamado GRAFO. Um grafo é formado por **NÓS** e **RAMOS**. Os nós são os equipamentos (micros, por exemplo), e os ramos são os cabos.

Topologias comuns

- Barramento
- Estrela
- Anel
- Árvore

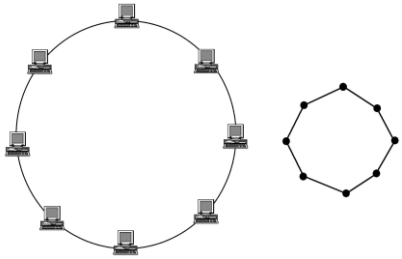
Barramento (Bus)

Este tipo de topologia foi muito utilizado nas redes durante os anos 80 e até meados dos anos 90. Uma grande desvantagem era a dificuldade para expansões. Cada vez que um novo equipamento era adicionado à rede, era preciso fazer um remanejamento de cabos para manter a seqüência, o que nem sempre era fácil. Outra grande desvantagem era que, ao desconectar um cabo qualquer, a rede inteira ficava inoperante.



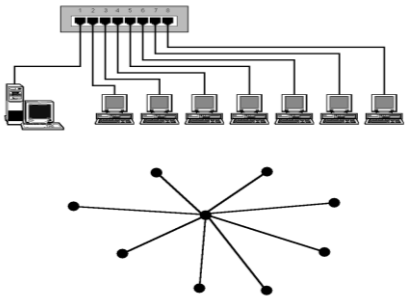
Anel

Esta topologia é empregada pelas redes "Token Ring", da IBM. Foi muito popular nos anos 80, mas hoje sua utilização é mais restrita.



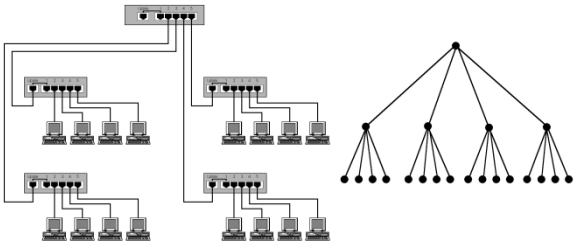
Estrela

Esta topologia é usada pela maioria das redes modernas, quando o número de computadores é pequeno. É usado um equipamento central chamado concentrador, e nele ficam ligados os demais equipamentos. Os concentradores mais comuns são o HUB e o SWITCH.



Árvore

Podemos dizer que este tipo de rede é formado por estrelas conectadas entre si. É bastante comum nas redes modernas que possuam um número grande de equipamentos.



PADRÕES

IEEE (Institute of Electrical and Electronic Engineers)

O Instituto de Engenheiros Eletricistas e Eletrônicos ou IEEE (pronuncia-se I-3-E) é uma organização profissional sem fins lucrativos, fundada nos Estados Unidos. É a maior (em número de sócios) organização profissional do mundo. O IEEE foi formado em 1963 pela fusão do Instituto de Engenheiros de Rádio (IRE) com o Instituto Americano de Engenheiros Elétricistas (AIEE). O IEEE tem filiais em muitas partes do mundo, sendo seus sócios engenheiros eletricistas, engenheiros da computação, cientistas da computação, profissionais de telecomunicações etc. Sua meta é promover conhecimento no campo da engenharia elétrica, eletrônica e computação. Um de seus papéis mais importantes é o estabelecimento de padrões para formatos de computadores e dispositivos.

Projeto 802

O Projeto 802 tem este nome por ter sido criado em Fevereiro de 1980. É o comitê responsável pela definição dos padrões e métodos de acesso.

A cada nova tecnologia emergente é criado uma novo sub- comitê para que se faça uma padronização.

Tecnologias atuais:

- 802.1 MAC layer Bridges and Bridge Management
- 802.1q standard for running Token Ring with Fast Ethernet
- 802.1b standard for network management
- 802.1d standard for Inter-LAN bridges between 802.3; 802.4 and 802.5
- 802.2 Logical Link Control
- 802.3 CSMA/CD (Ethernet)
- 802.3u Fast Ethernet em 100BaseT, 100BaseT4 e 100BaseFX
- 802.3z Gigabit Ethernet
- 802.4 Token Bus (MAP/TOP)
- 802.5 Token Ring (IBM 4 or 16 Mbps) physical layer
- 802.6 Metropolitan Area Network 1,5 Mbps to 155 Mbps
- 802.7 Broadband Local Area Network (cable television)
- 802.8 Fiber Optic CSMA/CD
- 802.9 Integrated Voice and Data Systems
- 802.10 Standard for Interoperable LAN Security (SILS)
- 802.11 Wireless - Radio, Spread Spectrum Radio and Infrared
- 802.12 Ethernet 100VG-Anylan

Protocolos de Comunicação

O que é protocolo

- Um conjunto de regras que serve como base para a execução de uma tarefa qualquer.
- No caso de redes, o protocolo define como duas máquinas irão se comunicar

Para que serve

Computadores só podem comunicar-se entre si se utilizarem o mesmo protocolo. Se o protocolo usado por um computador não for compatível pelo usado em outro, eles não podem trocar informações

- Para garantir que duas máquinas conseguirão estabelecer um diálogo coerente e efetivo, independentemente de suas especificidades.

Quais protocolos temos

- RM-OSI (Reference Model for Open Systems Interconnection)
- IEEE 802 (família de protocolos)
- TCP/IP (implementação)
- ATM (é mais um padrão)
- SNA (implementação, já morta)

Camadas

- A especificação de protocolos se dá sempre em camadas, permitindo uma grande flexibilidade para a inclusão de novas tecnologias.

ISO/OSI

Para facilitar o processo de padronização e obter interconectividade entre máquinas de diferentes sistemas operativos, a Organização Internacional de Padronização (ISO - International Organization for Standardization) aprovou, no início dos anos 80, um modelo de referência para permitir a comunicação entre máquinas heterogêneas, denominado *OSI* (Open Systems Interconnection). Esse modelo serve de base para qualquer tipo de rede, seja de curta, média ou longa distância

7	Aplicação
6	Apresentação
5	Sessão
4	Transporte
3	Rede
2	Enlace
1	Física

Os aspectos gerais da rede estão divididos em 7 camadas funcionais, facilitando a compreensão de questões fundamentais sobre a rede.

As regras que orientam a conversação entre as camadas são chamadas de "protocolos da camada". Esta conversação é processada entre as respectivas camadas de cada sistema comunicante, porém para que esta comunicação seja efetivada ela tem que "descer" até a camada mais baixa (Física) onde efetivamente as informações são transmitidas.

Os limites entre cada camada adjacente são chamados de interfaces, portanto a arquitetura de rede é formada de camadas, interfaces e protocolos.

Cada camada oferece um conjunto de serviços à camada superior, usando funções realizadas na própria camada e serviços disponíveis nas camadas inferiores.

Tipos de protocolos

Dois tipos de protocolos existem hoje: abertos e específicos.

Protocolos Abertos

Protocolos abertos são protocolos feitos para o padrão da indústria. Eles se comunicam com outros protocolos que utilizam o mesmo padrão. Um protocolo aberto não possui dono e todos os sistemas podem fazer implementações livremente. Um ótimo exemplo do que é um protocolo aberto é o TCP/IP (Transfer Control Protocol / Internet Protocol). Ele é composto por muitos outros protocolos e está implementado em muitos sistemas (como Macintosh, Windows, Linux, Unix, etc...). O TCP/IP é o protocolo padrão da Internet.

Protocolos Específicos

Protocolos específicos são feitos para ambientes de redes fechados e possuem donos. Como é o caso do IPX / SPX que foi desenvolvido especificamente para a estrutura Novell Netware e o NetBEUI da Microsoft.

Arquitetura de Redes TCP/IP

Introdução

No mundo de hoje, não se pode falar de redes sem falar do TCP/IP. O conjunto de protocolos originalmente desenvolvido pela Universidade da Califórnia em Berkeley, sob contrato para o Departamento de Defesa dos EUA, se tornou o conjunto de protocolos padrão das redes locais e remotas, suplantando conjuntos de protocolos bancados por pesos pesados da indústria, como a IBM (SNA), Microsoft (NetBIOS/NetBEUI) e Novell (IPX/SPX).

O grande motivo de todo este sucesso foi justamente o fato do TCP/IP não ter nenhuma grande empresa associada ao seu desenvolvimento. Isto possibilitou a sua implementação e utilização por diversas aplicações em praticamente todos os tipos de hardware e sistemas operacionais existentes.

Mesmo antes do “boom” da Internet o TCP/IP já era o protocolo obrigatório para grandes redes, formadas por produtos de muitos fornecedores diferentes, e havia sido escolhido pela Microsoft como o protocolo preferencial para o Windows NT, devido às limitações técnicas do seu próprio conjunto de protocolos, o NetBEUI.

Entretanto, ao contrário dos protocolos proprietários para redes locais da Microsoft e da Novell, que foram desenhados para serem praticamente "plug and play", as necessidades que orientaram o desenvolvimento do TCP/IP obrigaram ao estabelecimento de uma série de parametrizações e configurações que devem ser conhecidas pelo profissional envolvido com instalação, administração e suporte de redes.

As Pilhas de Protocolos

Todos os softwares de redes são baseados em alguma arquitetura de camadas, e normalmente nos referimos a um grupo de protocolos criado para funcionar em conjunto como uma pilha de protocolos. O termo "pilha" é utilizado porque os protocolos de uma dada camada normalmente interagem somente com os protocolos das camadas imediatamente superior e inferior.

O modelo de pilha traz a vantagem de modularizar naturalmente o software de redes, permitindo a sua expansão com novos recursos, novas tecnologias ou aperfeiçoamentos sobre a estrutura existente, de forma gradual.

Entretanto, o Modelo OSI é uma modelo conceitual, e não a arquitetura de uma implementação real de protocolos de rede. Mesmo os protocolos definidos como padrão oficial pelo ISO - International Standards Organization - a entidade criadora do modelo OSI, não foram projetados e construídos segundo este modelo.

O importante é entender o conceito de pilhas de protocolos, pelo qual cada camada realiza uma das funções necessárias para a comunicação em rede, tornando possível a comunicação em redes de computadores utilizando várias tecnologias diferentes.

O modelo de pilha de 4 camadas do TCP/IP

O TCP/IP foi desenhado segundo uma arquitetura de pilha, onde diversas camadas de software interagem somente com as camadas acima e abaixo. Há diversas semelhanças com o modelo conceitual OSI da ISO, mas o TCP/IP é anterior à formalização deste modelo e, portanto, possui algumas diferenças.

O nome TCP/IP vem dos nomes dos protocolos mais utilizados desta pilha, o IP (Internet Protocol) e o TCP (Transmission Control Protocol). Mas a pilha TCP/IP possui ainda alguns outros protocolos, dos quais veremos apenas os mais importantes, vários deles necessários para que o TCP e o IP desempenhem corretamente as suas funções.

Visto superficialmente, o TCP/IP possui 4 camadas, desde as aplicações de rede até o meio físico que carrega os sinais elétricos até o seu destino:

4. Aplicação (Serviço)	FTP, TELNET, HTTP, SMTP, POP3, IMAP, WHOIS, ...
3. Transporte	TCP, UDP
2. Rede	IP
1. Enlace	Ethernet, PPP, ...

Vamos apresentar agora uma descrição da função de cada camada do TCP/IP:

1. O protocolo de enlace tem a função de fazer com que informações sejam transmitidas de um computador para outro em uma mesma mídia de acesso compartilhado (também chamada de rede local) ou em uma ligação ponto-a-ponto (ex: modem). Nada mais do que isso. A preocupação destes protocolos é permitir o uso do meio físico que conecta os computadores na rede e fazer com que os bytes enviados por um computador cheguem a um outro computador diretamente desde que haja uma conexão direta entre eles.

2. O protocolo de rede, o Internet Protocol (IP), é responsável por fazer com que as informações enviadas por um computador cheguem a outros computadores mesmo que eles estejam em redes fisicamente distintas, ou seja, não existe conexão direta entre eles. Como o próprio nome (Inter-net) diz, o IP realiza a conexão entre redes. E é ele quem traz a capacidade da rede TCP/IP se "reconfigurar" quando uma parte da rede está fora do ar, procurando um caminho (rota) alternativo para a comunicação.

3. O protocolo de transporte muda o objetivo, que era conectar dois equipamentos, para conectar dois programas. Você pode ter em um mesmo computador vários programas trabalhando com a rede simultaneamente, por exemplo, um browser Web e um leitor de e-mail. Da mesma forma, um mesmo computador pode estar rodando ao mesmo tempo um servidor Web e um servidor POP3. Os protocolos de transporte (UDP e TCP) atribuem a cada programa um número de porta, que é anexado a cada pacote de modo que o TCP/IP saiba para qual programa entregar cada mensagem recebida pela rede.

4. Os protocolos de aplicação são específicos para cada programa que faz uso da rede. Desta forma existe um protocolo para a conversação entre um servidor web e um browser web (HTTP), um protocolo para a conversação entre um cliente Telnet e um servidor (daemon) Telnet, e assim em diante. Cada aplicação de rede tem o seu próprio protocolo de comunicação, que utiliza os protocolos das camadas mais baixas para poder atingir o seu destino.

Endereçamento

Em uma rede TCP/IP, cada computador (ou melhor, cada placa de rede, caso o computador possua mais do que uma) possui um endereço numérico formado por 4 octetos (4 bytes), geralmente escritos na forma w.x.y.z.

Decimal	Binário
255.255.0.0	11111111.11111111.00000000.00000000
255.255.7.0	11111111.11111111.00000111.00000000

Serviços de nomeação

Até agora nós estamos vendo a comunicação em rede utilizando apenas os endereços IP. Imagine o seu cartão de visitas, indicando a sua home-page como: "164.85.31.230". Imagine-se ainda com uma lista contendo dezenas de números como esse pendurada na parede junto ao seu computador, para quando você precisar se conectar a um dos servidores da sua empresa.

No início do desenvolvimento do TCP/IP, cada computador tinha um arquivo de hosts que listava os nomes dos computadores e os endereços IP correspondentes. Na Internet, certamente seria inviável manter estes arquivos, não só pelo tamanho que eles teriam mas também pela dificuldade em se manter milhões de cópias atualizadas.

Logo foi desenvolvido o DNS, pelo qual, diversos servidores mantém um banco de dados distribuído com este mapeamento de nomes lógicos para endereços IP.

O DNS funciona de forma hierárquica. Vejam um endereço Internet típico, como www.petrobras.com.br. Inicialmente, separamos o primeiro nome (até o primeiro ponto), "www", que é o nome de um computador ou host, e o restante do endereço, "petrobras.com.br", que é o nome da organização, ou o nome do domínio. Por favor, não confundam o conceito de domínios em endereços Internet com o conceito de domínios em uma Rede Microsoft. Não existe nenhuma relação entre eles.

O domínio petrobras.com.br possui o seu servidor DNS, que contém os nomes dos computadores (e endereços IP correspondentes) sob a sua autoridade. E ele sabe o endereço IP do servidor DNS do domínio que está acima dele, .com.br. Os computadores na Petrobras fazem todas as consultas por endereços IP ao servidor do seu domínio, e ele repassa as consultas a outros servidores DNS quando necessário. Os clientes necessitam saber apenas sobre o servidor do seu domínio, e mais nada.

Já o servidor DNS do domínio .com.br sabe os endereços IP de todos os servidores dos domínios a ele subordinados (por exemplo, texaco.com.br, mantel.com.br, etc) e o endereço IP do servidor acima dele (domínio .br, o domínio que engloba todo o Brasil). Por fim, o servidor DNS do domínio br sabe os endereços de todos os servidores dos domínios a ele subordinados (.com.br, .gov.br, etc) e o endereço do servidor DNS do InterNIC, que é o servidor DNS raiz de toda a Internet.

Uma consulta de uma aplicação por um endereço IP sobe por toda a hierarquia de servidores DNS, até o domínio comum de nível mais baixo que seja comum a origem e destino, ou até chegar ao servidor do InterNIC, e depois desce na hierarquia até o domínio onde está o computador destino. A resposta volta pelo caminho inverso, porém cada servidor DNS mantém um cache das respostas recebidas, de modo que uma nova requisição pelo mesmo nome não necessitará percorrer novamente todos os servidores DNS.

Pode parecer que é realizado um trabalho muito grande somente para obter um endereço IP, mas o processo como um todo é rápido (quem navega na Web sabe bem disso), e ele possibilita que milhares de organizações integrem suas redes a um custo aceitável e com grande autonomia. Quando você acrescenta uma máquina no seu domínio, você não precisa comunicar ao InterNIC e às redes vizinhas, basta registrar o novo computador no seu servidor DNS.

Outros Protocolos de Rede

SMTP

O Simple Mail Transfer Protocol é o protocolo responsável por entregar mensagens de e-mail a um destinatário. Toda vez que seus e-mails são enviados, um servidor smtp se encarrega de levá-los ao seu destino. Esse servidor geralmente se aloja na porta 25. O interessante do SMTP é que ao contrário do POP3 (visto a seguir), não é necessário senha para enviar um e-mail. Eu posso abrir o Microsoft Outlook e mandar e-mails como se fosse George Bush ou Tom Cruise. A falta de segurança no envio de mensagens é o ponto de partida para a facilidade de se enviar e-mails anônimos (como visto em anonimidade). O SMTP ainda permite anexar à uma mensagem de texto conteúdos binários (programas por exemplo), utilizando o MIME.
Simple Mail Transfer Protocol (SMTP) é o padrão de facto para envio de e-mail através da Internet.
SMTP é um protocolo relativamente simples, baseado em texto simples, em que um ou vários destinatários de uma mensagem são especificados (e, na maioria dos casos, validados), sendo depois a mensagem transferida. É bastante fácil testar um servidor SMTP usando o programa telnet. Este protocolo corre sobre a porta 25 numa rede TCP. A resolução DNS de um servidor SMTP de um dado domínio é possibilitada pela entrada MX (*Mail eXchange*).
O SMTP é um protocolo de envio apenas, ie, não permite que um utilizador descarregue as mensagens de um servidor. Para isso é necessário um cliente de email que suporte POP3 ou IMAP, que é o caso da maioria dos clientes atuais

POP3

Outro protocolo de mensagens, só que agora é o responsável por o recebimento dessas mensagens. O POP3 já necessita de senhas para poder habilitar o acesso dos usuários às suas caixas postais, além de saber "re-montar" os arquivos enviados em formato MIME com o SMTP. O POP3 geralmente se localiza na porta 113. Uma grande desvantagem dele é que fica muito fácil fazer um ataque de bruteforce para tentar descobrir as senhas, já que a maioria dos servidores possui falhas que possibilitam softwares maliciosos de serem rodados.
O Post Office Protocol (POP3) 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 numa caixa de correio eletrônico possam ser transferidas sequencialmente para um computador local. Aí, o utilizador pode ler as mensagens recebidas, apagá-las, responder-lhes, armazena-las, etc.

TELNET

Telnet, ou terminal remoto é um modo de se acessar remotamente sistemas como se você os estivesse operando localmente. Por exemplo: usando o telnet (e um trojan instalado) podemos ter acesso ao MS-DOS de qualquer um. Do mesmo modo que poderíamos digitar comandos para listar, copiar e apagar dados, conectados a outro computador também podemos. Na verdade, todos os trojans são clientes telnet. Apenas são disfarçados com botõezinhos bonitinhos pois geralmente quem precisa de trojans para invadir sistemas são pessoas que não possuem um bom conhecimento de segurança. Se você encontrar alguma porta ativa em algum sistema (qualquer uma, seja de trojan, SMTP, POP3, etc...), pode se conectar a ela por telnet.

Resumindo, se você souber usar bem telnet não precisa mais de outros programas no computador. Ele acessa servidores utilizados pelos browsers (como Netscape e Internet Explorer), clientes de E-mail, IRC, absolutamente tudo. Leia sobre o cliente telnet do Windows no capítulo seguinte.
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.
Antes de existirem os chats em IRC o telnet já permitia este género de funções.
O protocolo Telnet também permite obter um acesso remoto a um computador.

FTP File Transfer Protocol (Protocolo de Transferência de Arquivos)

FTP significa *File Transfer Protocol* (Protocolo de Transferência de Arquivos), e é uma forma bastante rápida e versátil de transferir arquivos (também conhecidos como ficheiros), sendo uma das mais usadas na internet.
Pode referir-se tanto ao protocolo quanto ao programa que implementa este protocolo (neste caso, tradicionalmente aparece em letras minúsculas, por influência do programa de transferência de arquivos do Unix).

A transferência de dados em redes de computadores envolve normalmente transferência de ficheiros e acesso a sistemas de ficheiros remotos (com a mesma interface usada nos ficheiros locais). O FTP (RFC 959) é baseado no TCP, mas é anterior à pilha de protocolos TCP/IP, sendo posteriormente adaptado para o TCP/IP. É o standard da pilha TCP/IP para transferir ficheiros, é um protocolo genérico independente de hardware e do sistema operativo e transfere ficheiros por livre arbítrio, tendo em conta restrições de acesso e propriedades dos ficheiros.

HTTP

Esse sem dúvida é conhecido por muitos. Afinal, quem nunca viu na frente do endereço de uma homepage esse nome? http://www.altavista.com/. O Hyper Text Transfer Protocol é o protocolo responsável de transmitir textos, imagens e multimídia na Internet. Sempre que você abre uma homepage (mesmo que ele só contenha textos), você está usando esse protocolo. Achei interessante comentar sobre ele para que se entenda melhor como a Internet não funciona isolada com um só protocolo. HTTP, FTP, TELNET e os outros muitas vezes trabalham em conjunto e nem percebemos. Quando você for baixar um arquivo, preste atenção no link. É muito provável que de uma página navegada por HTTP, se envie a um servidor FTP.

HTTP significa *HyperText Transfer Protocol* (Protocolo de Transferência de Hipertexto) e é um protocolo da camada de "Aplicação" do modelo OSI, utilizado para transferência de dados na World Wide Web. Esse é o protocolo da World Wide Web (www). O mesmo transfere dados de hiper-midia (imagens, sons e textos). Algumas de suas características são: geralmente este protocolo, utiliza a porta 80 e é usado para a comunicação de "sites". Este comunica na linguagem HTML (Hipertext Markup Language), contudo para haver comunicação, com o servidor do "site", teremos de utilizar comandos proprios do mesmo, os quais não são em HTML.

Para acessarmos outro documento a partir do documento atual, podemos utilizar os chamados links ou âncoras. Estes documentos encontram-se num "site" e para acessá-los devemos digitar o respectivo endereço, denominado URI (Universal Resource Indentifier), mas não confundir URI com URL(Universal Resource Locator), que é um tipo de URI que pode ser diretamente localizada.

WHOIS

WHOIS é um protocolo UDP específico para consultar informações de contato e DNS sobre entidades na internet.

Uma entidade na internet pode ser um nome de domínio, um endereço IP ou um AS (Sistema Autônomo).

O protocolo WHOIS apresenta três tipos de contato para uma entidade: Contato Administrativo (*Admin Contact*), Contato Técnico (*Technical Contact*) e Contato de Cobrança (*Registrant Contact*). Estes contatos são informações de responsabilidade do provedor de internet, que as nomeia de acordo com as políticas internas de sua rede.

SNMP

O protocolo SNMP (*Simple Network Management Protocol* - Protocolo de Gerência Simples de Rede) é um protocolo de gerência típica de redes TCP/IP, da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede. O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver problemas de rede, e planejar o crescimento desta.

O software de gerência de redes segue o modelo cliente-servidor convencional: uma aplicação 'cliente' na máquina do gerente e uma aplicação 'servidora' no dispositivo de rede a ser analisado ou monitorado. Para evitar confusão com outras aplicações de rede, os sistema de gerência de redes evitam os termos 'cliente' e 'servidor'. Em vez disso, usam "Gerente" para a aplicação cliente e "Agente" para a aplicação servidora que corre no dispositivo de rede.

SSH

Em informática o SSH (Secure Shell) é, ao mesmo tempo, um programa de computador e um protocolo de rede que permitem a conexão com outro computador na rede de forma a permitir execução de comandos de uma unidade remota. Ele possui as mesmas funcionalidades do TELNET, com a vantagem da criptografia na conexão entre o cliente e o servidor. Uma de suas mais conhecidas aplicações é o tunnelling, que oferece a capacidade de redirecionar pacotes de dados. Por exemplo, se alguém se encontra dentro de uma instituição cuja conexão à Internet é protegida por um firewall que bloqueia determinadas portas de conexão, não será possível, por exemplo, acessar e-mails via POP3 (via porta 110) ou enviá-los via SMTP (via porta 25 ou 587). As duas portas essenciais são a 80 para HTTP e a 443 para HTTPS. Não há necessidade de o administrador da rede deixar várias portas abertas, uma vez que conexões indesejadas e que comprometam a segurança da instituição possam ser estabelecidas pelas mesmas.

Para quebrar essa imposição rígida, o SSH oferece o recurso do Túnel. O processo se caracteriza por duas máquinas ligadas ao mesmo servidor SSH, que faz apenas o redirecionamento das requisições do computador que está sob firewall. O usuário envia para o servidor um pedido de acesso ao servidor pop.google.com pela porta 443 (HTTPS), por exemplo. Então, o servidor acessa o computador remoto e requisita a ele o acesso ao protocolo, retornando um conjunto de pacotes referentes à aquisição. O servidor codifica a informação e a retorna ao usuário via porta 443.

Sendo assim, o usuário tem acesso a toda a informação de que necessita. Tal prática não é ilegal caso o fluxo de conteúdo esteja de acordo com as normas da instituição.
O SSH faz parte da suíte de protocolos TCP/IP que torna segura a administração remota de um servidor Unix.

SIP

O Protocolo de Iniciação de Sessão (Session Initiation Protocol - SIP) é um protocolo de aplicação, que utiliza o modelo "requisição-resposta", similar ao HTTP, para iniciar sessões de comunicação interativa entre utilizadores. É um padrão da Internet Engineering Task Force (IETF) (RFC 2543, 1999.).
SIP é um protocolo de sinal para estabelecer chamadas e conferências através de redes via Protocolo IP. O estabelecimento, mudança ou término da sessão é independente do tipo de mídia ou aplicação que será usada na chamada; uma chamada pode utilizar diferentes tipos de dados, incluindo áudio e vídeo.
SIP teve origem em meados da década de 1990 (naquele tempo o H.323 estava a começar a ser finalizado como um padrão) para que fosse possível adicionar ou remover participantes dinamicamente numa sessão multicast. O desenvolvimento do SIP concentrou-se em ter um impacto tão significativo quanto o protocolo HTTP, a tecnologia por trás das páginas da web que permitem que uma página com links clicáveis conecte com textos, áudio, vídeo e outras páginas da web. Enquanto o HTTP efetua essa integração através de uma página web, o SIP integra diversos conteúdos a sessões de administração. O SIP recebeu uma adoção rápida como padrão para comunicações integradas e aplicações que usam presença. (Presença significa a aplicação estar consciente da sua localização e disponibilidade).
SIP foi moldado, inspirado em outros protocolos de Internet baseados em texto como o SMTP (email) e o HTTP (páginas da web) e foi desenvolvido para estabelecer, mudar e terminar chamadas num ou mais utilizadores numa rede IP de uma maneira totalmente independente do conteúdo de dados da chamada. Como o HTTP, o SIP leva os controles da aplicação para o terminal, eliminando a necessidade de uma central de comutação.
O protocolo SIP possui as seguintes características:

- Simplicidade e possui apenas seis métodos.
- Independência do protocolo de transporte.
- Baseado em texto.

RDP

Remote Desktop Protocol (ou somente RDP) é um protocolo multi-canal que permite que um usuário se conecte a um computador rodando o Microsoft Terminal Services. Existem clientes para a maioria das versões do Windows, e outros sistemas operacionais como o Linux. O servidor escuta por padrão a porta TCP 3389.
Baseado no protocolo da ITU T.share (conhecido como T.128), a primeira versão do RDP (chamada versão 4.0) foi introduzida com o Terminal Services no Windows NT 4.0 Server, Terminal Server Edition. A versão 5.0 introduzida com o Windows 2000 Server adicionou suporte para alguns recursos incluindo impressão em impressoras locais e foi voltado para melhorar o uso da banda. A versão 5.1, lançada com o Windows XP inclui vários recursos como suporte a cor em 24-bits e som.

IRC

Internet Relay Chat (IRC) é um protocolo de comunicação utilizado na Internet. Ele é utilizado basicamente como bate-papo (chat) e troca de arquivos, permitindo a conversa em grupo ou privada.

NNTP

NNTP ou Network News Transfer Protocol é um protocolo da Internet para grupos de discussão da chamada usenet. Foi definido inicialmente pela RFC 977; 20 anos depois, em Outubro de 2006 a RFC 3977 substituiu e tornou obsoleta a RFC original.
Especifica o modo de distribuição, busca, recuperação e postagem de artigos usando um sistema de transmissão confiável. Para clientes de leitura de noticias, o NNTP habilita a recuperação de artigos armazenados em um banco de dados centralizado, permitindo aos assinantes a opção de selecionar somente os artigos nos quais estão interessados.

BitTorrent

BitTorrent é um protocolo de rede que permite ao utilizador realizar downloads (descarga) de arquivos, em geral indexados em websites. Esse protocolo introduziu o conceito de partilhar o que já foi descarregado, maximizando o desempenho e possibilitando altas taxas de transferência, mesmo com um enorme número de usuários realizando descargas (downloads) de um mesmo arquivo simultaneamente. Foi criado por Bram Cohen em abril de 2001 e teve sua primeira implementação liberada no dia 2 de Julho de 2001.1 Desde de então tem sido alvo de empresas que lutam em defesa da propriedade intelectual, devido a alegações de violação de copyright (autoria) de alguns arquivos

transmitidos pela rede. No ano de 2005 o protocolo BitTorrent foi responsável por 35% dos dados transferidos na Internet em todo o mundo.
Na rede BitTorrent os arquivos são quebrados em pedaços de geralmente 256Kb. Ao contrário de outras redes, os utilizadores da rede BitTorrent partilham pedaços em ordem aleatória, que podem ser reconstituídos mais tarde para formar o arquivo final. O sistema de partilha otimiza o desempenho geral de rede, uma vez que não existem filas de espera e todos partilham pedaços entre si, não sobrecarregando um servidor central, como acontece com sites e portais de downloads, por exemplo. Assim, quanto mais utilizadores entram para descarregar um determinado arquivo, mais largura de banda se torna disponível.

PING

Ping ou latência como podemos chamar, é um utilitário que usa o protocolo ICMP para testar a conectividade entre equipamentos. Seu funcionamento consiste no envio de pacotes para o equipamento de destino e na "escuta" das respostas. Se o equipamento de destino estiver ativo, uma "resposta" (o "pong", uma analogia ao famoso jogo de ping-pong) é devolvida ao computador solicitante.
O autor da ferramenta, Mike Muuss, deu a ele este nome pois lembrava o som que o sonar emitia.1 (Depois Dave Mills arrumou um significado para a sigla, "Packet Internet Grouper (Groper)", algo como "Procurador de Pacotes da Internet")
A utilidade do ping para ajudar a diagnosticar problemas de conectividade na Internet foi enfraquecida no final de 2003, quando muitos Provedores de Internet ativaram filtros para o ICMP Tipo 8 (echo request) nos seus roteadores. Esses filtros foram ativados para proteger os computadores de Worms como o Welchia, que inundaram a Internet com requisições de ping, com o objetivo de localizar novos equipamentos para infectar, causando problemas em roteadores ao redor do mundo todo.
Outra ferramenta de rede que utiliza o ICMP de maneira semelhante ao ping é o Traceroute.
A saída do ping, e seus primos, geralmente consiste no tamanho do pacote utilizado, o nome do equipamento "pingado", o número de seqüência do pacote ICMP, o tempo de vida e a latência, com todos os tempos dados em milissegundos.

Servidores e Clientes

Servidores
São computadores ou equipamentos que disponibilizam seus recursos para outros computadores.
Exemplos:
a) Servidor de arquivos: Seus discos rígidos podem ser acessados por outros computadores.
b) Servidor de impressão: Suas impressoras podem ser usadas por outros computadores.
c) Servidor de backup: Suas unidades de fita magnética, discos ou outros dispositivos de armazenamento podem ser usados por outros computadores.
d) Servidor Web: Hospedagem de sites
e) Servidor de Email: Envia e recebe mensagens eletrônicas
f) Servidor de DNS: Serviço de nomeação
g) Servidor Proxy: Trabalha com cache e Firewall em uma rede
Clientes
São os computadores que usam os recursos dos servidores. Também é correto chamar esses computadores de *estação de trabalho* (workstation).
- Um computador pode operar somente como cliente.
- Um computador pode operar somente como servidor. Nesse caso é chamado de *servidor dedicado*.
- Um computador pode operar simultaneamente como cliente e como servidor. Isso é comum em redes muito pequenas. Nesse caso é chamado de *servidor não dedicado*.

Servidor não dedicado

Servidores não dedicados são muito comuns em redes pequenas.

- Normalmente os PC's estão num mesmo ambiente de trabalho (escritório);
- Não existe administrador de rede;
- Não existem "servidores";
- A rede terá problemas ao crescer de tamanho;

Servidor dedicado

Em redes de porte médio e grande, os servidores são dedicados. Não são usados para tarafes convencionais, como edição de texto, programas gráficos, etc. Ficam disponíveis o tempo todo para permitir que seus recursos sejam usados por outros computadores. Na pequena rede ao lado temos um servidor e 7 estações de trabalho.

HOST

Em informática, **host** é qualquer máquina ou computador conectado a uma rede. Os hosts variam de computadores pessoais a supercomputadores, dentre outros equipamentos, como roteadores.
Todo **host** na internet precisa obrigatóriamente apontar (representar) um endereço IP.

IPv6

IPv6 é a versão mais atual do Protocolo de Internet. Originalmente oficializada em 6 de junho de 2012, é fruto do esforço do IETF para criar a "nova geração do IP" (IPng: Internet Protocol next generation), cujas linhas mestras foram descritas por Scott Bradner e Allison Marken, em 1994, na RFC 1752.1 Sua principal especificação encontra-se na RFC 2460.2
O protocolo está sendo implantado gradativamente na Internet e deve funcionar lado a lado com o IPv4, numa situação tecnicamente chamada de "pilha dupla" ou "dual stack", por algum tempo. A longo prazo, o IPv6 tem como objetivo substituir o IPv4, que só suporta cerca de 4 bilhões (4x109) de endereços IP, contra cerca de 3,4x1038 endereços do novo protocolo.

Motivações para a implantação do IPv6

O esgotamento do IPv4 e a necessidade de mais endereços na Internet[editar]
O principal motivo para a implantação do IPv6 na Internet é a necessidade de mais endereços, porque os endereços livres IPv4 acabaram.
Para entender as razões desse esgotamento, é importante considerar que a Internet não foi projetada para uso comercial. No início da década de 1980, ela poderia ser considerada uma rede predominantemente acadêmica, com poucas centenas de computadores interligados. Apesar disso, pode-se dizer que o espaço de endereçamento do IP versão 4, de 32 bits, não é pequeno: 4.294.967.296 endereços.
Ainda assim, já no início de sua utilização comercial, em 1993, acreditava-se que o espaço de endereçamento da Internet poderia se esgotar num prazo de 2 ou 3 anos. Isso não ocorreu por conta da quantidade de endereços, mas sim por conta da política de alocação inicial, que não foi favorável a uma utilização racional desses recursos.
O DHCP (Dynamic Host Configuration Protocol), descrito pela RFC 2131. Esse protocolo trouxe a possibilidade aos provedores de reutilizarem endereços Internet fornecidos a seus clientes para conexões não permanentes.
O conjunto dessas tecnologias reduziu a demanda por novos números IP, de forma que o esgotamento previsto para a década de 1990, ainda não ocorreu.

Outros fatores motivantes

O principal fator que impulsiona a implantação do IPv6 é a necessidade. Ele é necessário na infraestrutura da Internet. É uma questão de continuidade de negócios, para provedores e uma série de outras empresas e instituições.
Contudo, há outros fatores que motivam sua implantação:

Internet das Coisas: A tecnologia estará presente em vários dispositivos hoje não inteligentes, que serão capazes de interagir autonomamente entre si - computadores invisíveis interligados à Internet, embutidos nos objetos usados no dia a dia - tornando a vida ainda mais líquida. Pode-se imaginar eletrodomésticos conectados, automóveis, edifícios inteligentes, equipamentos de monitoramento médico, etc. Dezenas, talvez mesmo centenas ou milhares de equipamentos estarão conectados em cada residência e escritório... O IPv6, com endereços abundantes, fixos, válidos, é necessário para fazer desse futuro uma realidade.

Expansão das redes: Vários fatores motivam uma expansão cada vez mais acelerada da Internet: a inclusão digital, as redes 3G, etc. São necessários mais IPs.

Qualidade de serviço: A convergência das redes de telecomunicações futuras para a camada de rede comum, o IPv6, favorecerá o amadurecimento de serviços hoje incipientes, como VoIP, streaming de vídeo em tempo real, etc, e fará aparecerem outros, novos. O IPv6 tem um suporte melhorado a classes de serviço diferenciadas, em função das exigências e prioridades do serviço em causa.

Mobilidade: A mobilidade está a tornar-se um fator muito importante na sociedade de hoje em dia. O IPv6 suporta a mobilidade dos utilizadores, estes poderão ser contados em qualquer rede através do seu endereço IPv6 de origem.

Novidades nas especificações do IPv6

- Espaço de Endereçamento. Os endereços IPv6 têm um tamanho de 128 bits.
- Autoconfiguração de endereço. Suporte para atribuição automática de endereços numa rede IPv6, podendo ser omitido o servidor de DHCP a que estamos habituados no IPv4.

- Endereçamento hierárquico. Simplifica as tabelas de encaminhamento dos roteadores da rede, diminuindo assim a carga de processamento dos mesmos.
- Formato do cabeçalho. Totalmente remodelados em relação ao IPv4.
- Cabeçalhos de extensão. Opção para guardar informação adicional.
- Suporte a qualidade diferenciada. Aplicações de áudio e vídeo passam a estabelecer conexões apropriadas tendo em conta as suas exigências em termos de qualidade de serviço (QoS).
- Capacidade de extensão. Permite adicionar novas especificações de forma simples.
- Encriptação. Diversas extensões no IPv6 permitem, à partida, o suporte para opções de segurança como autenticação, integridade e confidencialidade dos dados.

Endereçamento]
O endereçamento no IPv6 é de 128 bits, e inclui prefixo de rede e sufixo de host. No entanto, não existem classes de endereços, como acontece no IPv4. Assim, a fronteira do prefixo e do sufixo pode ser em qualquer posição do endereço.
Um endereço padrão IPv6 deve ser formado por um campo provider ID, subscribe ID, subnet ID e node ID. O node ID (ou identificador de interface) deve ter 64bits, e pode ser formado a partir do endereço físico (MAC) no formato EUI 64.
Os endereços IPv6 são normalmente escritos como oito grupos de 4 dígitos hexadecimais. Por exemplo,
2001:0db8:85a3:08d3:1319:8a2e:0370:7344
Se um grupo de vários dígitos seguidos for 0000, pode ser omitido. Por exemplo,
2001:0db8:85a3:0000:0000:0000:0000:7344
é o mesmo endereço IPv6 que:
2001:0db8:85a3::7344