Sumário

1. INTRODUÇÃO

Conjunto de computadores **autônomos interconectados** por uma única tecnologia [Tanenbaum].

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

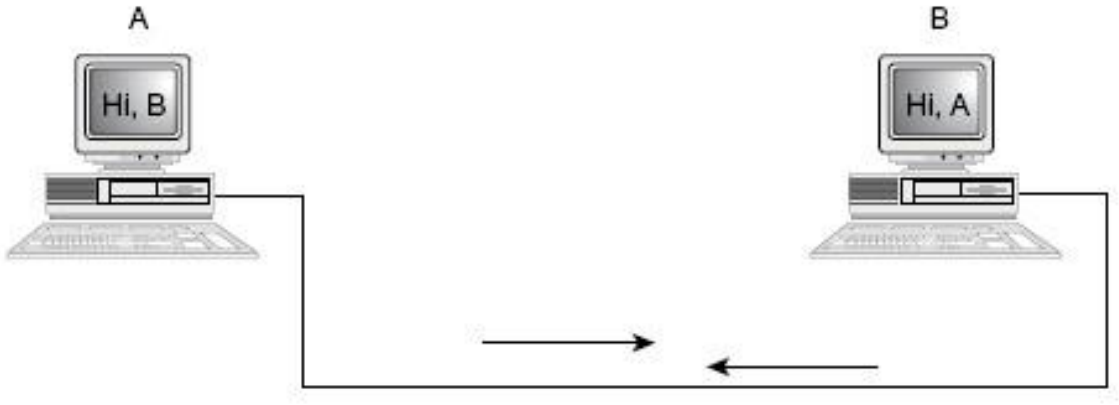


Figura 1.1 – Uma rede de dois computadores.

Os computadores que fazem parte de uma rede podem compartilhar:

- ➔ Dados,
- ➔ Mensagens,
- ➔ Gráficos,
- ➔ Impressoras,
- ➔ Aparelhos de fax,
- ➔ Modems,
- ➔ Outros recursos de hardwares.

2. USO DAS REDES DE COMPUTADORES

2.1 Aplicações comerciais

Compartilhamento de recursos físicos: (impressoras, scanners, gravadores de cds.)

Compartilhamento de informações (registros de clientes, estoques, contas a receber, extratos financeiros, informações sobre impostos e muitas outras informações on-line).

Comunicação entre usuários (email, videoconferência).

Comércio eletrônico (realizar negócios eletronicamente com outras empresas, em especial fornecedores e clientes).

- Realizar negócios com consumidores pela Internet. Empresas aéreas, livrarias descobriram que muitos clientes apreciam a conveniência de fazer compras em casa. Conseqüentemente, muitas empresas fornecem catálogos de suas mercadorias e serviços on-line e emitem pedidos on-line.

2.2 Aplicações domésticas

Acesso a informações remotas: Ele pode significar navegar na World Wide Web para obter informações ou apenas por diversão.

As informações disponíveis incluem artes, negócios, culinária, governo, saúde, história, passatempos, recreação, ciência, esportes, viagens e muitos outros.

Muitos jornais são publicados on-line e podem ser personalizados.

Comunicação entre pessoas: O correio eletrônico (e-mail) já é usado diariamente por milhões de pessoas em todo o mundo e seu uso está crescendo rapidamente.

Em geral, ele já contém áudio e vídeo, além de texto e imagens.

Hoje em dia, qualquer adolescente é fanático pela troca de mensagens instantâneas.

Uma versão dessa ideia para várias pessoas é a sala de bate-papo (ou chat room).

Entretenimento interativo: uma indústria enorme e que cresce mais e mais a cada dia.

A aplicação fundamental nesse caso (aquela que deverá orientar todas as outras) é o vídeo por demanda.

Dentro de aproximadamente uma década talvez seja possível selecionar qualquer filme ou programa de televisão, qualquer que seja a época ou país em que tenha sido produzido, e exibi-lo em sua tela no mesmo instante.

Novos filmes poderão se tornar interativos e ocasionalmente o usuário poderá ser solicitado a interferir no roteiro, com cenários alternativos para todas as hipóteses.

Comércio eletrônico: A atividade de fazer compras em casa já é popular e permite ao usuário examinar catálogos on-line de milhares de empresas.

Outra área em que o comércio eletrônico já é uma realidade é o acesso a instituições financeiras. Muitas pessoas já pagam suas contas, administram contas bancárias e manipulam seus investimentos eletronicamente.

2.3 Usuários Móveis

Computadores móveis, como notebooks e PDAs (personal digital assistants), constituem um dos segmentos de mais rápido crescimento da indústria de informática.

3 HISTÓRICO

3.1 ARPANET em 1969

Projeto desenvolvido pela *ARPA(Agência de Pesquisas em Projetos Avançados*). No auge da Gerra Fria – Rede Militar.

3.2 NSFNET final da década 70

Estimulada pela *NFS(Fundação Nacional de Ciência*) .

Rede universitária.

3.3 Janeiro de 1983

Junção da NFSNET com a ARPANET.

Conexão com redes de outros países.

Nascimento da Internet.

3.4 1987 FAPESP/LNCC

Laboratório Nacional de Computação Científica.

3.5 1990 RNP

Rede Nacional de Pesquisa.

3.6 2008 UESC/ILHÉUS

Entrada da Uesc/Ilhéus na RNP.

4 MODELOS DE COMPUTAÇÃO

O processamento de informações nas redes podem se dar de duas formas: centralizada e distribuída.

4.1 Centralizada

No passado antes do surgimento dos PCs, existiam computadores centrais com alto poder de processamento que eram responsáveis pelo processamento de informações. Esses computadores também conhecidos por mainframes, liam as informações contidas em um cartão e as processava de forma sequencial.

A única forma de entrar com dados em um mainframe era com cartões que eram inseridos nas leitoras.Com o surgimento das redes, outras opções foram criadas para colocar e retirar informações no sistema. Através de terminais que eram nada mais do que dispositivos de entrada e saída, e impressoras, o usuário poderia ter uma interação maior com o mainframe.

Esses terminais eram conhecidos como terminais burros devido ao fato de não haver qualquer poder de processamento neles.

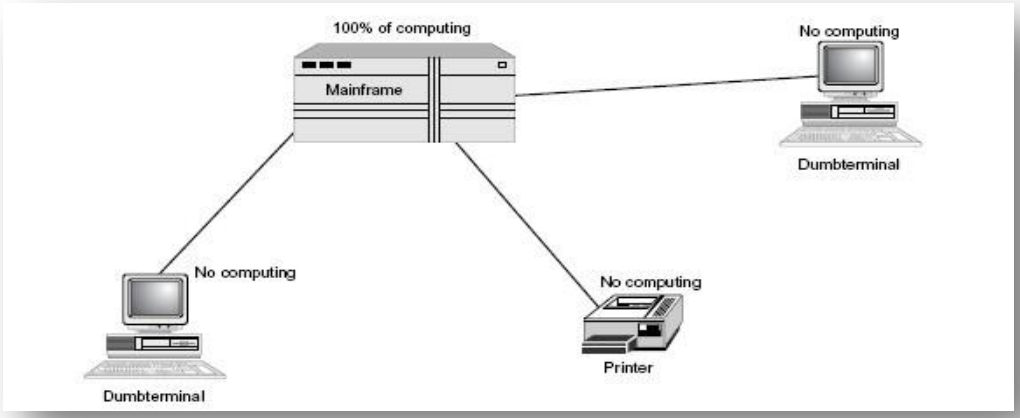


Fig 1.2 – Modelo de computação centralizada

4.2 Distribuída

Como o mainframe era restrito a grandes corporações e órgãos do governo devido a seu alto custo e tamanho, pequenas e médias empresas não tinham como usufruir dos benefícios da computação centralizada.

Com o passar dos anos e o surgimento dos PCs, o processamento das informações deixou de estar centralizado a passou a ser distribuído entre os “terminais”, que agora não eram mais burros, eram PCs.

É importante lembrar que o poder de processamento de um PC é muito inferior a de um mainframe, mas é inegável que isso se tornou em uma ótima opção de baixo custo para pequenas e médias empresas.

Os PCs passaram então a dividir uma parcela do processamento de informações com o computador central, conforme ilustrado na figura 1.3.

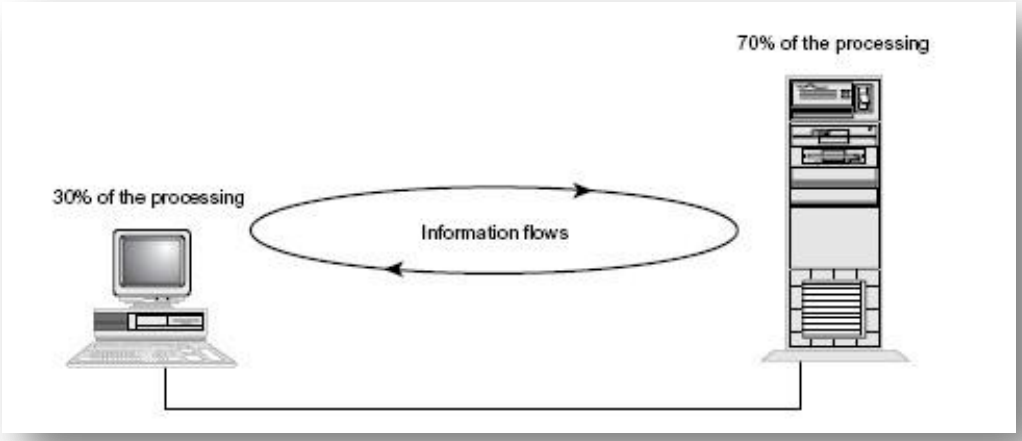


Fig 1.3 – Modelo de computação distribuída

4.3 Downsizing

Processo pelo qual as empresas migram de um ambiente mainframe (arquitetura centralizada, grande porte) para um ambiente de microcomputadores (arquitetura distribuída), a fim de obterem maior produtividade, agilidade e redução de custos.

Pode também ser definido como processo pelo qual, em certos casos, pode-se substituir aplicações mantidas em ambiente de grande porte (arquitetura centralizada) por uma equivalente em ambiente de microcomputadores (arquitetura distribuída) com vantagens.

Vantagens principais:

a) Segurança:

Evita a redundância de equipamentos críticos;

b) Disponibilidade:

Existe sempre uma estação de trabalho disponível em caso de alguma ou a principal apresentar algum problema;

c) Escalabilidade:

Crescimento conforme a demanda. Pode se crescer lentamente apenas trocando os equipamentos que estão em situação crítica. Pode-se dizer também flexibilidade lógica e física para expansão;

d) Custo:

Economia em equipamentos, instalação, manutenção e em investimentos futuros, tendo um custo / desempenho baixo para soluções que exigem muitos recursos;

e) Produtividade:

Como cada estação de trabalho é um microcomputador, nele podem estar instalados software e recursos que aumentam a qualidade e a velocidade dos trabalhos realizados, melhorando a produtividade de pessoas e grupos de trabalho;

Outras Vantagens:

Comunicação e intercâmbio de informações entre usuários (correios principalmente), aumentando a interação entre departamentos e usuário de toda a organização;

Racionalização do uso de periféricos;

Acesso rápido a informações em arquivos compartilhados;

Banco de dados distribuídos, já que nesse caso existe diminuição real de trafego na rede;

5 CONFIGURAÇÃO DA REDE

No que tange as formas de configuração as redes podem ser classificadas em ponto a ponto e baseada em servidor. Nenhuma configuração é melhor que a outra.

Elas são adequadas para determinadas necessidades e possuem vantagens e desvantagens.

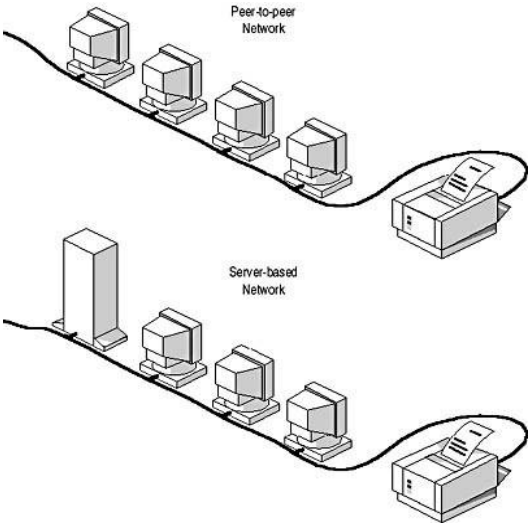


Figura 1.4 – Redes ponto a ponto e baseada em servidor

O tipo de configuração escolhido vai depender de determinados fatores tais como:

» Tamanho da organização

» Nível de segurança necessário

» Tipo do negócio

» Nível de suporte administrativo disponível

» Tráfego da rede

» Necessidades dos usuários

» Orçamento

5.1 Redes Ponto a Ponto

Redes ponto a ponto são mais adequadas para redes com no máximo 10 computadores. Não há servidores dedicados nem hierarquia entre os computadores.

Todos podem compartilhar e utilizar recursos, operam de forma igual, atuando como cliente e servidor ao mesmo tempo e são chamados de pontos ou nós da rede.

A figura de um administrador não é necessária ficando essa tarefa a cargo de cada usuário. Eles determinam quais dados do seu computador serão compartilhados na rede.

Poderíamos destacar os seguintes pontos em redes ponto a ponto:

» Não há servidor dedicado.

» Os nós da rede são ao mesmo tempo cliente e servidor.

» Não há a figura de um administrador responsável pela rede.

» Fácil implantação.

» Treinamento dos usuários é necessário.

» O controle de acesso a rede não é centralizado.

» A segurança não é uma preocupação.

» Pouca possibilidade de crescimento.

» A medida que a rede cresce, a performance diminui.

5.2 Redes baseada em servidor

Redes baseadas em servidor são voltadas para redes acima de 10 computadores.

Possui um ou mais servidores dedicados. Por dedicado entende-se que eles não são clientes e são otimizados para atender aos pedidos da rede rapidamente e, além disso, garantem a segurança de arquivos e diretórios.

Os recursos compartilhados estão centralizados e há um maior controle do nível de acesso sobre os mesmos. Há um controle de acesso do usuário e o que ele pode fazer na rede. A figura de um administrador de rede é necessária. Treinamento dos usuários não é necessário.

Existem vários tipos de servidores :

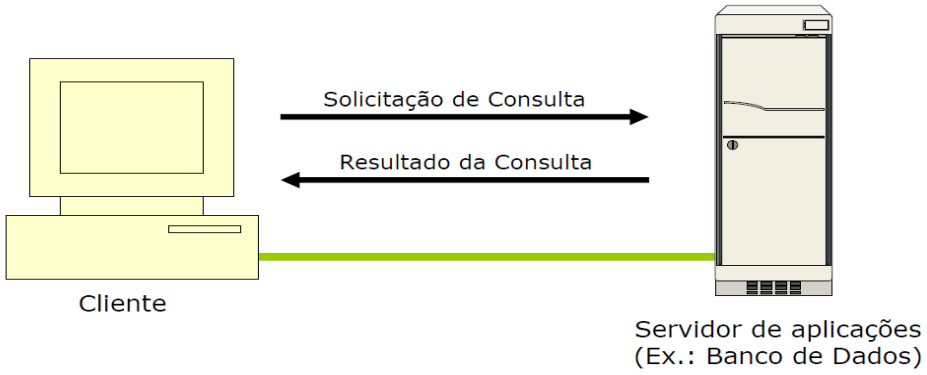
» Servidores de aplicação.

» Servidores de arquivo e impressão.

» Servidores de comunicação.

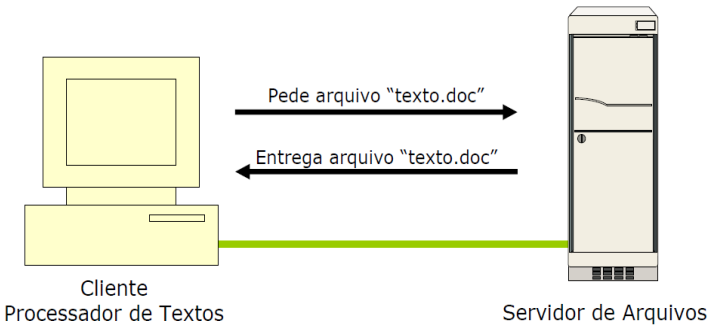
» Servidores de correio eletrônico.

a) Servidores de aplicação: Possuem uma porção servidora responsável por processar os pedidos enviados pela porção cliente que fica na estação. Diferentemente do servidor de arquivos, somente o que é requisitado é passado para a estação e não a massa de dados inteira. Um bom exemplo seria a pesquisa em um banco de dados.

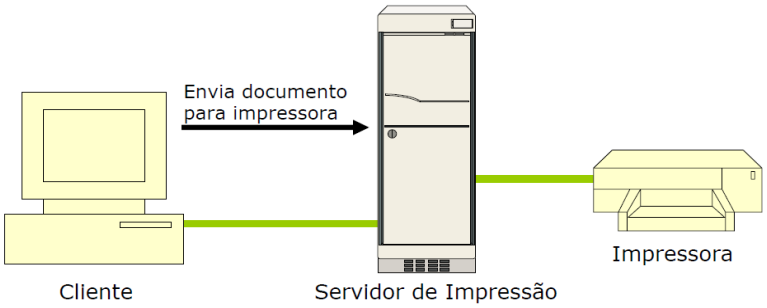


Servidor de Aplicações

b) Servidores de arquivo e impressão: Os dados ficam armazenados no servidor e quando precisam ser utilizados por uma estação, esses dados são transferidos para a memória da estação e usados localmente.

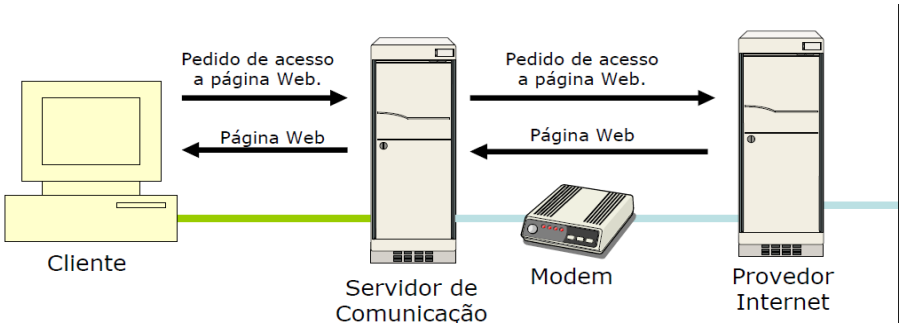


Servidor de Arquivos



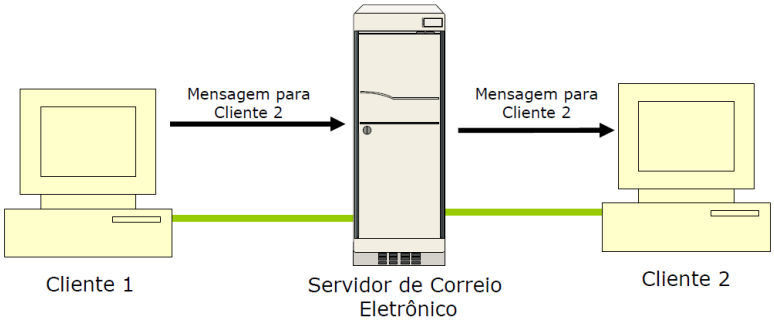
Servidor de Impressão

c) Servidor de comunicação: Controla o acesso de usuários externos aos recursos da rede. Um exemplo desse servidor é o que compartilha a conexão da internet em uma rede.



Servidor de Comunicação

d) Servidores de correio eletrônico: Um tipo de servidor de aplicação. O principio é o mesmo o que muda é o tipo da aplicação. Ex: servidores de email. (postfix, sendmail, etc)



Postfix - Sendmail

Servidor de Correio Eletrônico

Como todos os dados importantes da rede agora estão centralizados, um backup é fundamental, já que uma vez que os dados são importantes, eles não podem ser perdidos devido a falhas de hadware.

Há meios de agendar backups periódicos e que são executados automaticamente.

Nunca é demais lembrar que esses backups devem ser agendados para serem realizados em horários em que a rede estiver praticamente sem utilização.

Redundância também é um importante. Se o servidor principal falhar, todos os recursos e dados importantes não poderão ser acessados.

Existe uma forma de duplicar os dados do servidor e mantê-los online.

Se o esquema de armazenamento primário falhar, o secundário será utilizado no lugar deste, sem causar qualquer interrupção na rede.

Poderíamos destacar os seguintes pontos em redes baseadas em servidor:

» Há um ou mais servidores dedicados

» Segurança é fundamental

» A figura de um administrador é muitas vezes imprescindível

» Possui controle maior do usuário e do que é permitido a ele fazer na rede.

» Meios de restringir o acesso do usuário a rede a determinados períodos

» Crescimento da rede só depende do hardware do servidor

» Recursos compartilhados estão centralizados

» Instalação não é tão simples

6 ELEMENTOS FÍSICOS DE UMA REDE

- Estações ou sistemas finais - Hosts
- Subsistemas de comunicação - Roteadores
- Linhas de enlace de comunicação - Links

6.1 Estações ou sistemas finais - Hosts

- ❖ Computadores de usuários conectados em uma rede
- ❖ Laptops conectados via conexão 3G wireless
- ❖ Celulares
- ❖ Câmera de vigilância

- Podem ser dividir em clientes e servidores:
  - ❖ Clientes
    - Computadores domésticos, PDAs.
    - Procuram ter uma interface amigável.
    - Podem possuir recursos multimídia.
    - São ferramentas do dia a dia dos usuários.
  - ❖ Servidores
    - São de capacidade de processamento e armazenamento maior que os clientes.
    - Funcionam em tempo integral 24 horas por dia.
    - Hospedam serviços que são utilizados pelos clientes.

6.2 Estações ou sistemas finais - Roteadores

- Decidem pela melhor rota ou caminho a ser tomado por uma mensagem.
- O destinatário pode estar diretamente ligado ao roteador ou não.
- Cada roteador possuem portas onde se conectam os **enlaces** ou **linhas de comunicação.**
- Como são os roteadores fisicamente?
  - ❖ Computador rodando um software específico de roteamento.
    - As portas são as placas adicionadas ao seu barramento.
  - ❖ Hardware específico (computador dedicado).
    - Fabricado por empresas como Cisco, Cyclades, IBM, 3Com

6.3 Enlaces de Comunicação - Links

- Propagam as mensagens entre as estações.
- Os enlaces são formados por meios de transmissão de sinais **ópticos** ou **eletromagnéticos.**

  - Ar (rádio freqüência, canais de satélite, etc).
  - Fios metálicos(cobre, etc).
  - Fibra ótica.

6.4 Transmissão de Sinal

- Duas técnicas podem ser usadas para transmitir sinais codificados sobre um cabo:
  - Transmissão banda base;
  - Transmissão banda larga.

6.4.1 Transmissão Banda Base

- Usa sinalização digital sobre um simples canal. Sinais digitais fluem na forma discreta de pulsos de eletricidade ou luz.
- Neste método de transmissão todo a capacidade de comunicação do canal é usada para transmitir um único sinal de dados.
- A largura de banda do canal refere-se a capacidade de transmissão de dados ou velocidade de transmissão de um sistema de comunicação digital.
- É expressa em bps (bits por segundo).
- A medida que o sinal viaja ao longo do meio ele sofre redução na sua amplitude e pode se tornar distorcido.

- Se o comprimento do abo é muito longo, o sinal recebido pode estar até mesmo irreconhecível.

6.4.2 Transmissão Banda Larga

- Usa sinalização analógica e uma faixa de frequências.
- Os sinais não são discretos e são contínuos. Sinais fluem na forma de ondas eletromagnéticas ou óticas. Seu fluxo é unidirecional.
- Se toda a largura de banda está disponível, vários sistemas de transmissão podem ser suportados simultaneamente no mesmo cabo, por exemplo, tv a cabo e transmissões de rede.
- A cada sistema de transmissão é alocada uma fatia da largura de banda total.
- Sistemas banda base usam repetidores para fortalecer o sinal;
- Sistemas banda larga usam amplificadores para a mesma finalidade.

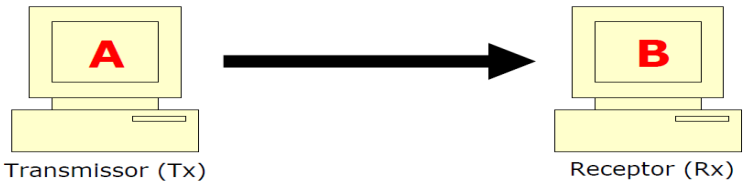
6.5 Formas de transmitir informação

- Aumentar a velocidade da transmissão de dados é uma necessidade a medida que uma rede cresce em seu tamanho e na quantidade de tráfego.
- Maximizando o uso do canal, podemos trocar mais dados em menos tempo. Existem três formas de transmitir informação :

  - Simplex.
  - Half-duplex.
  - Full-duplex.

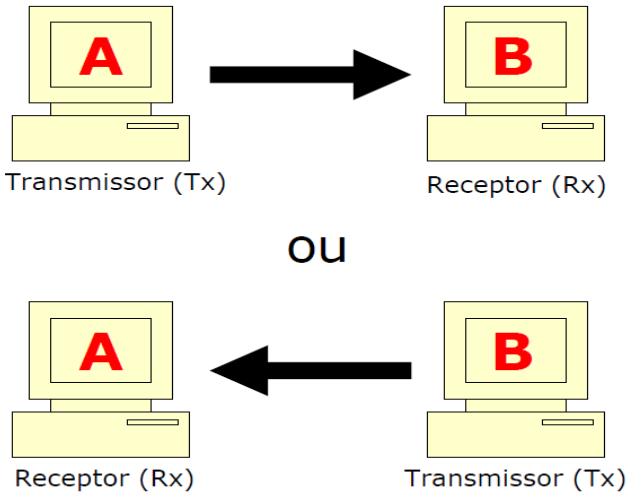
6.5.1 Simplex

- Forma mais básica de transmissão.
- Nela a transmissão pode ocorrer apenas em uma direção.
- O transmissor envia os dados, mas não tem certeza se o receptor os recebeu.
- Não há meios de verificar a recepção dos dados.
- Problemas encontrados durante a transmissão não são detectados e corrigidos.
- Um bom exemplo de transmissão simplex é a transmissão de TV aberta.



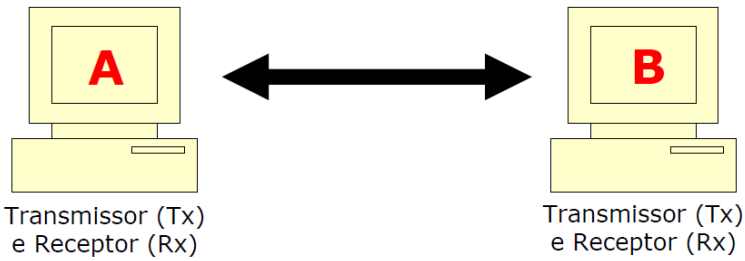
6.5.2 Half-Duplex

- A transmissão pode ocorrer em ambos as direções mas não ao mesmo tempo.
- Detecção de erro é possível.
- Um bom exemplo é a comunicação com rádios comunicadores. Modems usam half-duplex.



6.5.3 Full-Duplex

- A melhor forma de transmissão.
- Os dados podem transmitidos e recebidos simultaneamente.
- Um bom exemplo é uma conexão de TV a cabo, em que você pode ver TV e navegar na internet ao mesmo tempo.



7 CLASSIFICAÇÃO DE REDES

7.1 Extensão Geográfica

- Redes pessoais (Personal Area Networks – PANs)
- Redes locais (Local Area Networks – LANs)
- Redes metropolitanas (Metropolitan Area Networks – MANs)
- Redes de longa distância (Wide Area Networks – WANs)

Distância entre processadores	Exemplo	Classificação
1 m	Metro quadrado	Rede pessoal (PAN)
10 m	Sala	Rede local (LAN)
100 m	Edifício	
1 km	Campus	
10 km	Cidade	Rede metropolitana (MAN)
100 km	País	Rede geograficamente distribuida (WAN)
> 1.000 km	Continente/Planeta	

7.2 Redes Pessoais (PAN)

- Cobrem distâncias muito pequenas
- Destinadas a uma única pessoa

  Ex: Seu celular e o fone de ouvido bluetooth, é um exemplo de rede PAN;

7.3 Redes Locais (LAN)

- Cobrem pequenas distâncias
  - Um prédio ou um conjunto de prédios
- Geralmente pertencentes a uma mesma organização
- Taxa de transmissão da ordem de Mbps

  Ex: Vários computadores de uma sala ou prédio

7.4 Redes Metropolitanas (MAN)

- Cobrem grandes distâncias
  - Uma cidade

    Ex: Duas filiais de uma empresa, na mesma cidade, se comunicando.

7.5 Redes de Longa Distância (WAN)

- Cobrem distâncias muito grandes
  - Um país, um continente
- De um modo geral possuem taxas de transmissão menores que as das LANs

Ex: Comunicação entre Países ou planetas, como por exemplo a comunicação entre a NASA e um foguete ou uma sonda.

8 TOPOLOGIAS DE REDES

8.1 Definição

O termo topologia ou mais especificamente topologia da rede, diz respeito ao layout físico da rede, ou seja, como computadores, cabos e outros componentes estão ligados na rede.

Topologia é o termo padrão que muitos profissionais usam quando se referem ao design básico da rede.

A escolha de uma determinada topologia terá impacto nos seguintes fatores:

» Tipo de equipamento de rede necessário.

» Capacidades do equipamento.

» Crescimento da rede.

» Forma como a rede será gerenciada.

» Custo.

» Confiabilidade.

» Alcance.

Para trabalhar bem uma topologia deve levar em conta o planejamento.

Não somente o tipo de cabo deverá ser levado em consideração , mas também, a forma como ele será passado através de pisos, tetos e paredes.

As topologias padrão são as seguintes:

» Barramento

» Estrela

» Anel

» Malha

» Híbrida (Estrela-Barramento; Estrela-Anel)

8.2 Barramento

Nesta topologia os computadores são ligados em série por meio de um único cabo coaxial. Esse cabo também é chamado de backbone ou segmento.

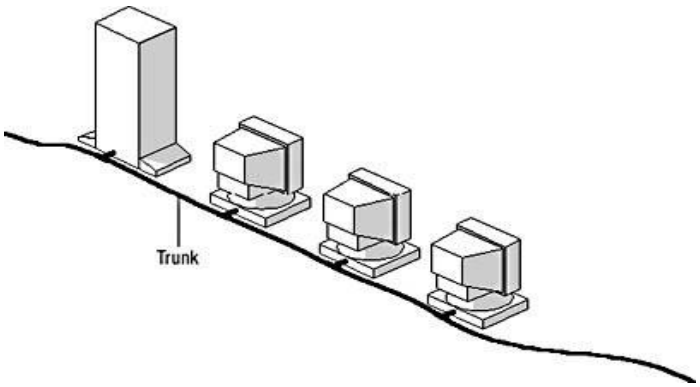


Figura 1.7 – Rede em topologia barramento

É a mais rudimentar de todas as topologias e já caiu em desuso.

Comunicação

Dados enviados do computador A para o computador B, são recebidos por todos, mas somente o computador B processa esses dados, os demais rejeitam.

Somente um computador por vez pode transmitir dados.

Aumentar o número de computadores impactará na performance da rede, porque teremos mais computadores compartilhando o meio e esperando para colocar dados no barramento.

Quando um computador transmite dado ele consequentemente estará utilizando o meio e nenhum outro computador poderá fazer o mesmo, até que o meio esteja novamente disponível.

Os computadores ficam constantemente monitorando o meio para saber se ele está livre ou não.

Terminadores (normalmente de 50 ohms) são usados em ambas as extremidades do cabo para evitar que haja reflexão do sinal transmitido

Sem eles o sinal seria refletido e o meio estaria constantemente ocupado, ou seja, nenhuma estação conseguiria transmitir dados.

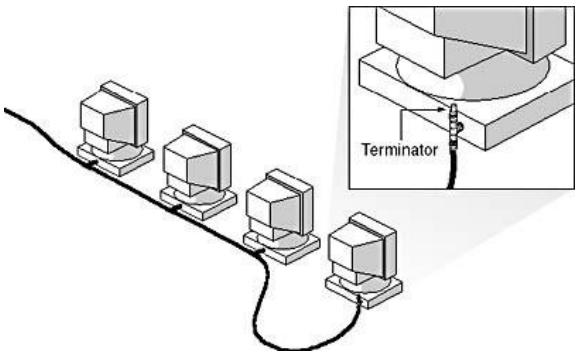


Figura 1.8 – Terminador em destaque

Interrupção na comunicação

Embora seja de fácil implementação essa topologia tem um inconveniente.

Se houver uma ruptura no cabo em um determinado ponto, ou houver algum conector em curto ou ainda, um terminador apresentar qualquer tipo de problema, toda a rede pára.

Nenhum computador conseguirá se comunicar com qualquer outro enquanto a falha não for sanada.

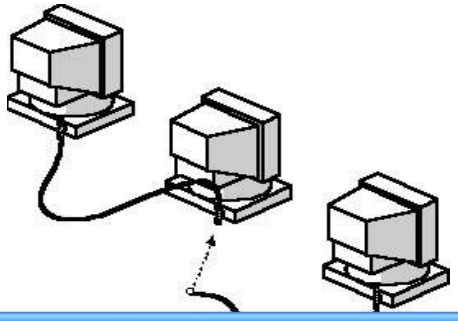


Figura 1.9 – Uma ruptura o cabo paralisará toda a rede.

Expansão da rede

A medida que a rede cresce, o barramento pode ser expandido através dos seguintes formas:

- Um conector BNC fêmea, que serve para unir dois segmentos de cabo pode ser utilizado.

- Mas conectores enfraquecem o sinal e devem ser usados de forma criteriosa.

É preferível ter um único cabo continuo do que vários segmentos ligados por conectores.

Um segmento teoricamente, pode se estender até 385 metros, sem o uso de repetidores.

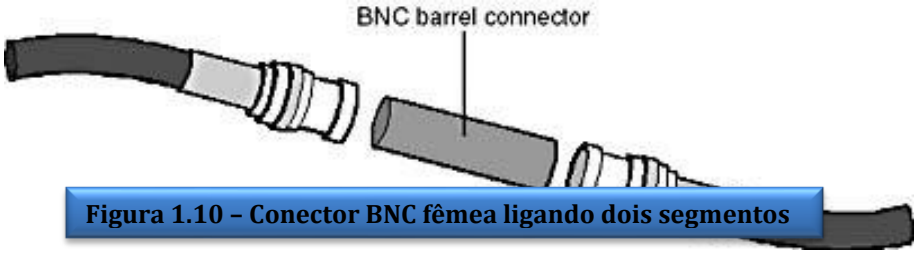


Figura 1.10 – Conector BNC fêmea ligando dois segmentos

A medida que o sinal viaja pelo cabo, ele tem a sua amplitude reduzida, repetidores são usados para aumentar o nível do sinal.

Um repetidor é preferível em comparação ao conector BNC.

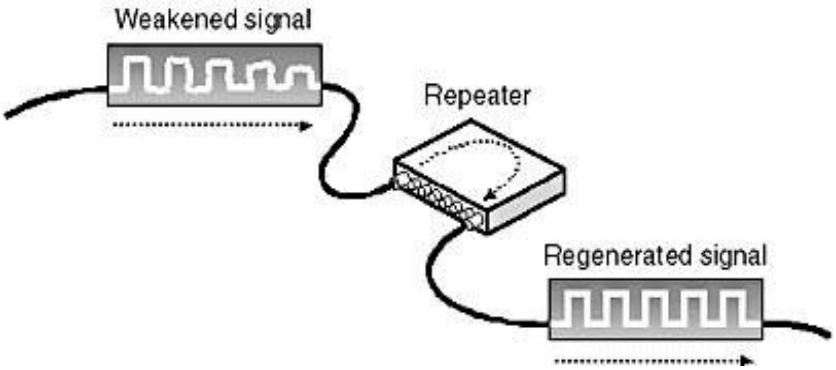


Figura 1.11 – Repetidores ligando dois segmentos

8.3 Estrela

Nessa topologia não há mais um único segmento ligando todos os computadores na rede.

Eles estão ligados por meio de vários cabos a um único dispositivo de comunicação central, que pode ser um hub ou um switch.

Este dispositivo possui várias portas onde os computadores são ligados individualmente, e é para onde converge todo o tráfego.

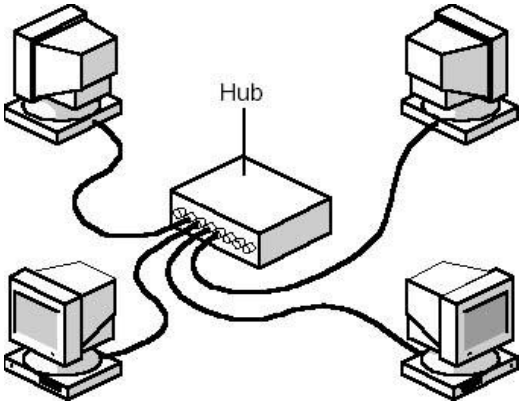


Figura 1.12 – Topologia estrela simples

<u>Comunicação</u>

Quando uma estação A deseja se comunicar com uma estação B, esta comunicação não é feita diretamente, mas é intermediada pelo dispositivo central, que a replica para a toda a rede, novamente somente a estação B processa os dados enviados, as demais descartam.

Hubs e switches intermedeiam esta comunicação entre as estações de formas diferentes.

Por exemplo, se um hub replica todo o tráfego que recebe para todas as suas portas, o mesmo não ocorre com o switch.

O Switch envia apenas para a máquina de destino.

Interrupção na Comunicação

A grande vantagem da topologia estrela em relação a de barramento, é que agora uma falha no cabo não paralisará toda a rede.

Somente aquele segmento onde está a falha será afetado.

Por outro lado, a rede poderá ser paralisada se houver uma falha no dispositivo central.

Os cabos utilizados se assemelham aos cabos utilizados na telefonia, porém com maior quantidade de pares. São cabos par-trançados, vulgarmente chamados de UTP.

Possuem conectores nas extremidades chamados de RJ-45.

8.4 Anel

Nessa topologia, as estações estão conectadas por um único cabo como na de barramento, porém na forma de circulo. Portanto não há extremidades.

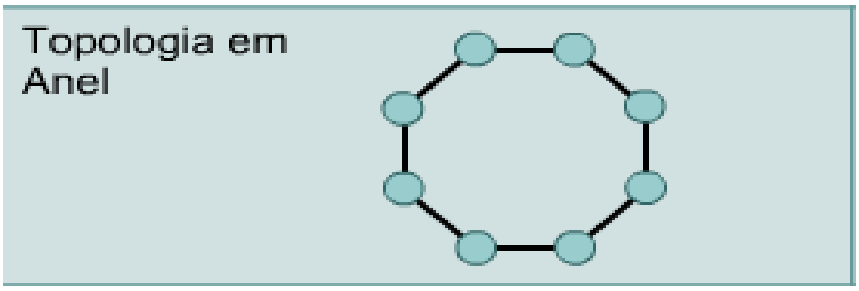


Figura 1.13 – Topologia em Anel

O sinal viaja em loop por toda a rede e cada estação pode ter um repetidor para amplificar o sinal.

A falha em um computador impactará a rede inteira.

Comunicação

Diferentemente das duas topologias descritas anteriormente, uma estação que deseja transmitir não compete com as demais.

Ela tem autorização para fazê-lo.

Existe um token que é como se fosse um cartão de autorização que circula na rede. Quando uma estação quer transmitir ele pega o token.

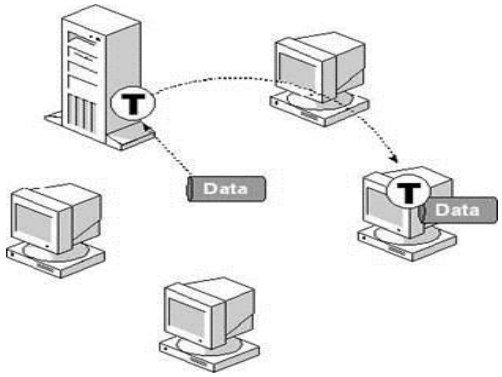


Figura 1.14 – Passagem do token

8.5 Malha

Nessa topologia os computadores são ligados uns aos outros por vários segmentos de cabos.

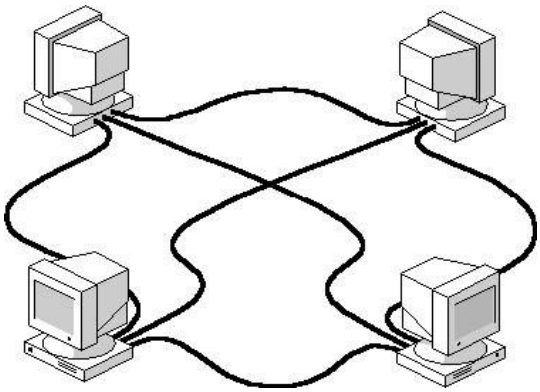


Figura 1.15 – Topologia em malha

Comunicação

Essa configuração oferece redundância e confiabilidade. Se um dos cabos falhar, o tráfego fluirá por outro cabo. Porém essas redes possuem instalação dispendiosa, devido ao uso de grande quantidade de cabeamento. Por vezes essa topologia será usada juntamente com as outras descritas, para formar uma topologia híbrida.

8.6 Estrela – Barramento

É uma combinação das topologias barramento e estrela.

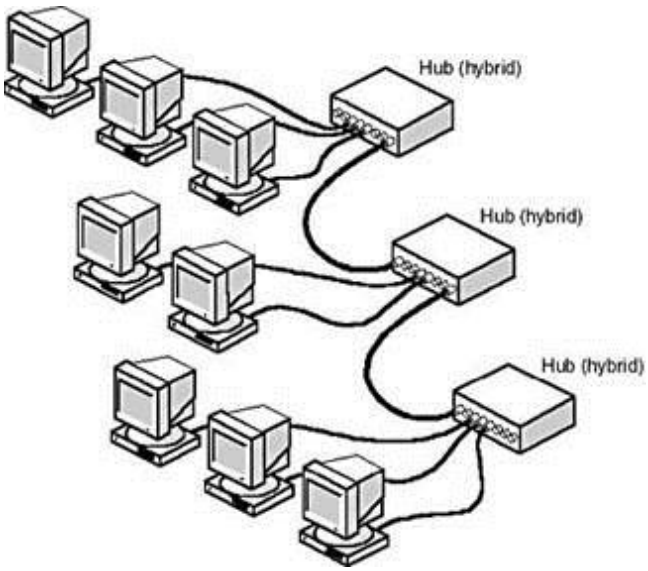


Figura 1.16 – Topologia Estrela-Barramento

Interrupção na Comunicação

Se um computador falhar a rede não será impactada por essa falha.

Se um hub falhar, os computadores ligados a esse hub serão incapazes de se comunicar e de se comunicar com o restante da rede.

Se o hub estiver ligado a outro hub, a comunicação entre os dois também será afetada.

8.7 Estrela – Anel

Essa topologia é similar a anterior.

Ambas as topologias possuem um hub central que contem o anel ou o barramento.

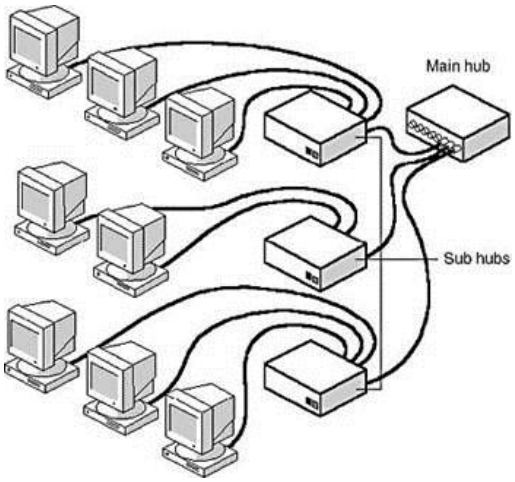


Figura 1.17 – Topologia Estrela-Anel

8.8 Selecionando uma topologia

Existem muitos fatores que devem ser levados em consideração quando da escolha de qual tecnologia melhor se adequa as necessidades de uma organização.

A tabela mostra um resumo com as vantagens e desvantagens de cada topologia.

Topologia	*Vantagens*	*Desvantagens*
Barramento	▪ Uso do cabo é econômico. ▪ Mídia é barata e fácil de trabalhar e instalar. ▪ Simples e relativamente confiável. ▪ Fácil expansão.	▪ Rede pode ficar extremamente lenta em situações de tráfego pesado. ▪ Problemas são dificieis de isolar. ▪ Falha no cabo paralisa a rede inteira.
Estrela	▪ Modificação e adição de novos computadores é simples. ▪ Gerenciamento centralizado. ▪ Falha de um computador não afeta o restante da rede.	▪ Uma falha no dispositivo. central paralisa a rede inteira.
Anel	▪ Todos os computadores acessam a rede igualmente. ▪ Performance não é impactada com o aumento de usuários.	▪ Falha de um computador pode afetar o restante da rede. ▪ Problemas são dificieis de isolar.
Malha	▪ Maior redundância e confiabilidade. ▪ Facilidade de diagnóstico.	▪ Instalação dispendiosa.

9 ELEMENTOS LÓGICOS DE UMA REDE

- Regras de comunicação (Protocolos)
- Serviços oferecidos pela rede

9.1 Regras de comunicação (Protocolos)

É a padronização de procedimentos que são dispostos a execução de determinada tarefa. Em redes protocolo é um padrão que especifica o formato de dados e as regras a serem seguidas. Sem protocolos, uma rede não funciona.

A maioria das transmissões de dados em redes locais é do tipo half-duplex. Todos os computadores em uma rede compartilham o mesmo cabo e recebem as mesmas informações ao mesmo tempo.

Se uma transmissão está sendo feita entre dois dispositivos, nenhuma outra transmissão poderá ocorrer ao mesmo tempo. Se um arquivo muito grande tiver de ser transmitido, os demais dispositivos da rede terão de esperar muito tempo para começarem a transmitir. Poderão ocorrer interferências no caminho e o dado não chegar corretamente ao seu destino.

9.1.1 Pacotes

Os protocolos são a solução para este problema:

- Divide o dado a ser transmitido em pequenos *pacotes ou quadros.*

- Exemplo: arquivo de 100KB e tamanho do pacote de 1KB = arquivo será dividido em 100 pacotes de 1 KB.

Dentro do pacote temos:

- Informação de origem.

- Informação de destino.

- Usada pelos dispositivos para saber se o dado é destinado a eles.

Placas de rede tem um endereço fixo, gravado em hardware.

Pacotes pequenos geram várias transmissões pequenas em vez de uma única grande.

- Estatisticamente: maior probabilidade de um computador encontrar o cabo livre para transmissão.

Assim vários dispositivos podem se comunicar ao mesmo tempo, intercalando as transmissões.

9.2 Velocidade da rede X Número de transmissões

A velocidade da rede depende diretamente do número de transmissões simultâneas.

- Exemplo: rede de 100Mbps (limitada pelo meio de transmissão):

  - 1 transmissão: 100Mbps

  - 2 transmissões: 50Mbps

  - 4 transmissões: 25Mbps

Conclusão: quanto mais máquinas em uma rede, mais lenta ela será.

9.3 CRC

Ao colocar um pacote na rede a placa adiciona um *checksumou CRC (CyclicalRedundancyCheck).*

Campo com a soma de todos os bytes do pacote armazenado no próprio pacote.

Receptor refaz a conta e verifica se o resultado confere.

- Valores iguais = pacote OK.

- Valores diferentes = pacote corrompido, pedido de retransmissão.

9.4 Pacote de Dados

Exemplo hipotético de um pacote de dados

9.5 Serviços oferecidos pela rede

Exemplos.

- Recuperação de conteúdo

  - FTP, HTTP

- Acesso remoto

  - Telnet, SSH

- Comunicação entre usuário

  - SMTP, POP3

10 MEIOS DE TRANSMISSÃO

10.1 Transmissão de sinal

Propagação de ondas através de um meio físico.

- Ar, fios metálicos, fibra de vidro.

Podem ter suas características (amplitude, freqüência, fase) alteradas no tempo para refletir a codificação da informação transmitida.

10.2 Banda passante de um sinal

Intervalo de freqüências que compõe o sinal.

- Exemplo:

  - banda passante do ouvido humano: 20 Hz a 20 kHz.

10.3 Largura de banda

Tamanho da banda passante (diferença entre a maior e a menor freqüência).

- Exemplo:
  - largura de banda do ouvido humano: 20.000 - 20 = 19.980 Hz

10.4 Meios físicos de transmissão de sinais

Os mais comuns:

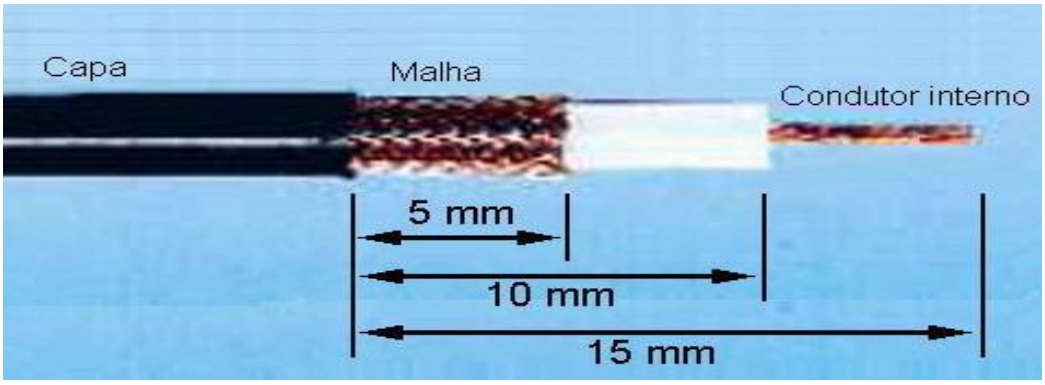
- cabo de pares trançados;
- cabo coaxial;
- fibra ótica.

Sob circunstâncias especiais podem ser usados:

- radiodifusão;
- infravermelho;
- enlaces de satélites;
- enlaces de microondas

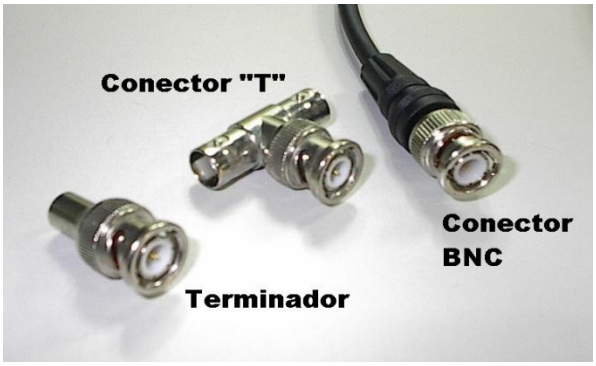
10.4.1 Cabo coaxial

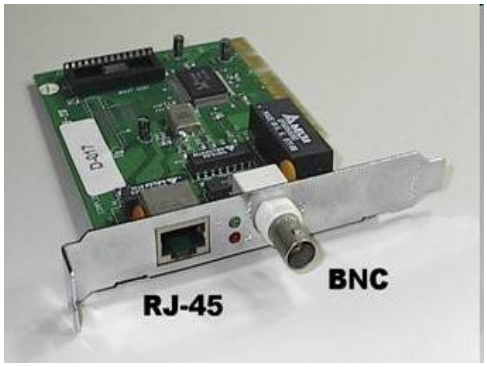
Os cabos coaxiais são cabos constituídos de 4 camadas:

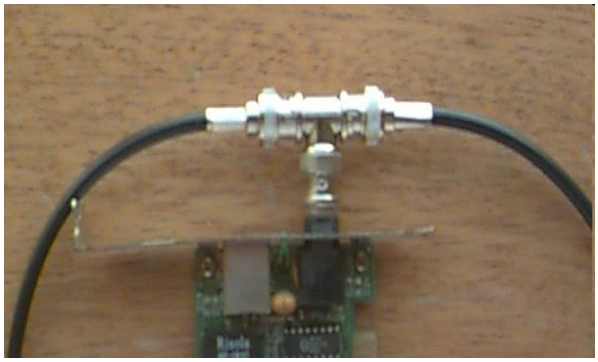


10.4.1.1 Cabo coaxial conector BNC

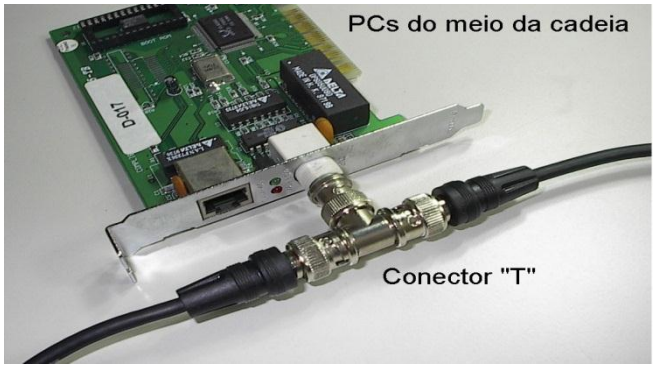
Os cabos coaxiais utilizam também conectores BNC tipo “T” e o terminador. Cada placa de rede é ligada aos cabos através de um conector “T”. O último nó da rede deve ter um terminador, como mostraremos adiante.



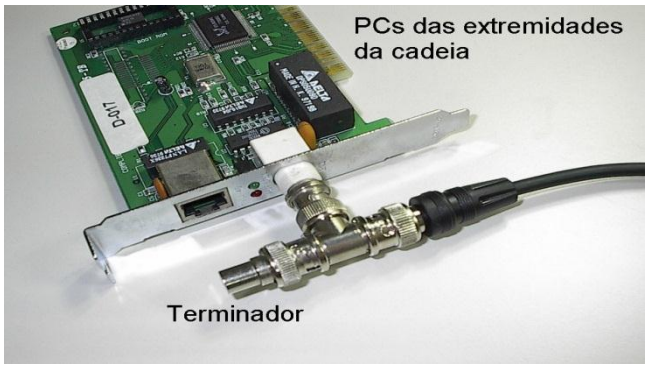




A) Conectores “T” são ligados em cada placa de rede. As duas extremidades laterais desses conectores são ligadas aos cabos coaxiais.



B) A última placa de rede, ou o último dispositivo do cabo, deve ter ligado no seu conector “T”, um terminador.



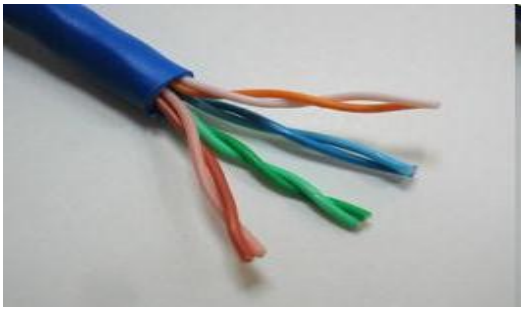
10.4.1.2 Cabo de pares trançados

No cabo de pares trançados, um, dois ou quatro pares de fios são enrolados em espiral dois a dois de forma a reduzir o ruído e manter constante as propriedades elétricas do meio ao longo de todo o seu comprimento.

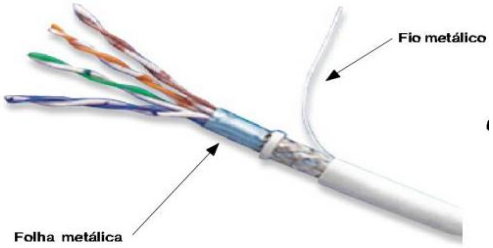
Suporta transmissão analógica e digital

Tem largura de banda relativamente alta (10/100/1000 Mbps, dependendo da distância, técnica de transmissão e qualidade do cabo).

- Não blindado: (*Unshielded Twisted Pair* - UTP): quando seus pares são envolvidos unicamente por uma cobertura plástica (são mais baratos, mas mais sujeitos à interferências).

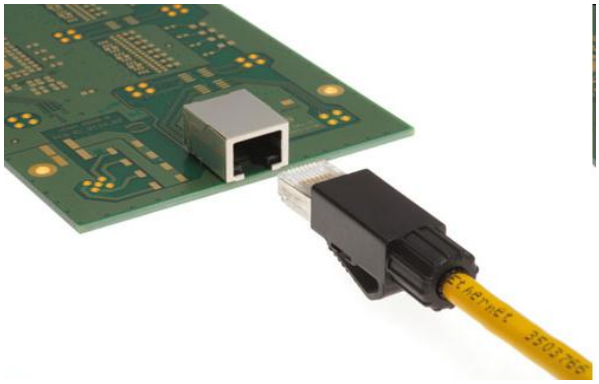


- Blindado: (Shielded Twisted Pair - STP): quando seus pares são envolvidos por uma capa metálica (blindagem) e uma cobertura plástica. A malha metálica confere uma imunidade bastante boa em relação ao ruído.



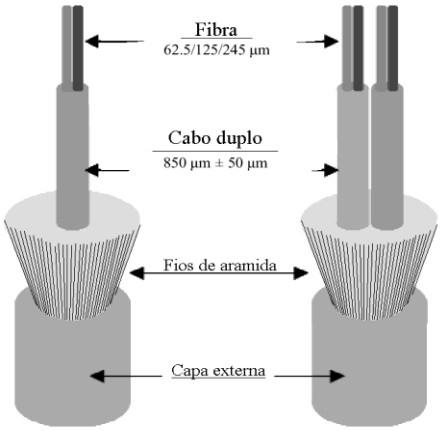
Hoje em dia, os cabos de pares trançados mais usados são os não blindados, nas seguintes classificações e características:

CATEGORIA	CARACTERÍSTICAS
3	16 MHz, utilizado em ligações de até 10 Mbps
4	20 MHz, utilizado em ligações de até 16 Mbps
5	125 MHz, utilizado em ligações de até 100 Mbps
6	250 MHz, utilizado em ligações de até 155 Mbps
7	600 MHz, utilizado em ligações de até 1000 Mbps



10.4.1.3 Fibra ótica

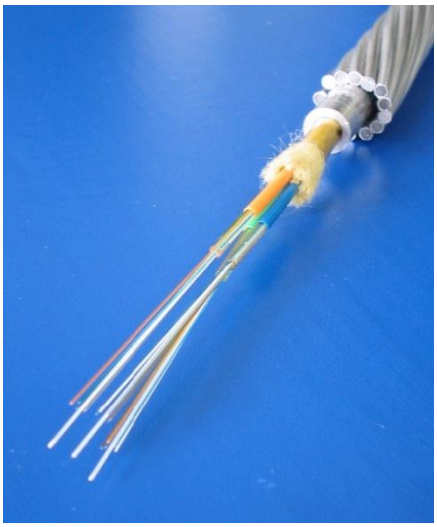
A transmissão em fibra ótica é realizada pelo envio de um sinal de luz codificado, dentro de um domínio de frequência do infravermelho, através de um cabo ótico que consiste de um filamento de sílica ou plástico.



A transmissão da luz dentro da fibra é possível graças a uma diferença de índice de refração entre o revestimento e o núcleo.

O núcleo possui sempre um índice de refração mais elevado. O vidro é mais utilizado porque absorve menos as ondas eletromagnéticas. As ondas eletromagnéticas mais utilizadas são as correspondentes à gama da luz infravermelha.

Os fabricantes de fibras ópticas produzem cabos com pares. Uma conexão de fibra óptica sempre exige um par, sendo uma fibra para transmissão e outra para recepção. Existem cabos com até 96 pares.



As fibras ópticas podem ser basicamente de dois modos: Monomodo e Multimodo.

- Monomodo:

- Permite o uso de apenas um sinal de luz pela fibra.
- Maior banda passante por ter menor dispersão.
- Geralmente é usado laser como fonte de geração de sinal.

- Multimodo:

- Permite o uso de fontes luminosas de baixa ocorrência tais como LEDs (mais baratas).

- Diâmetros grandes facilitam o acoplamento de fontes luminosas e requerem pouca precisão nos conectores.

- Muito usado para curtas distâncias pelo preço e facilidade de implementação.

- Conectores

- Existem vários tipos de conectores de fibra óptica.

- O conector tem uma função importante, já que a fibra deve ficar perfeitamente alinhada para que o sinal luminoso possa ser transmitido sem grandes perdas.

- Os quatro tipos de conector mais comuns são os LC, SC, ST e MT-RJ.

- Conector LC

- O LC (Lucent Connector) é um conector miniaturizado que, como o nome sugere, foi originalmente desenvolvido pela Lucent.

- Ele vem crescendo bastante em popularidade, sobretudo para uso em fibras monomodo.

- Conector ST

- O ST (Straight Tip) é um conector mais antigo, muito popular para uso com fibras multímodo.

- Ele foi o conector predominante durante a década de 1990, mas vem perdendo espaço para o LC e outros conectores mais recentes.

- Ele é um conector estilo baioneta, que lembra os conectores BNC usados em cabos coaxiais.

- Embora os ST sejam maiores que os conectores LC, a diferença não é muito grande.

- Conector SC

- O SC, que foi um dos conectores mais populares até a virada do milênio. Ele é um conector simples e eficiente, que usa um sistema simples de encaixe e oferece pouca perda de sinal.

- Ele é bastante popular em redes Gigabit, tanto com cabos multimodo quanto monomodo, mas vem perdendo espaço para o LC.

- Uma das desvantagens do SC é seu tamanho avantajado; cada conector tem aproximadamente o tamanho de dois conectores RJ-45 colocados em fila indiana, quase duas vezes maior que o LC.

- Conector MT-RJ (Mechanical Transfer Registered Jack)

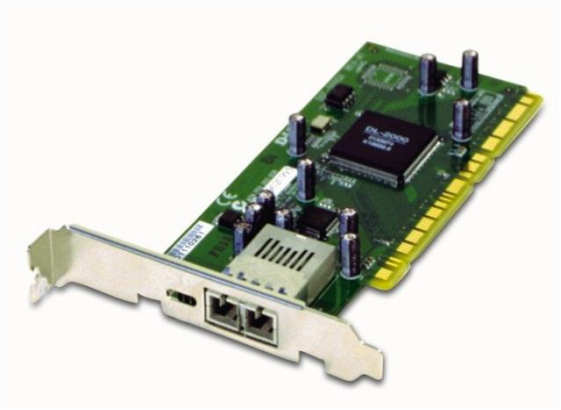
- É um novo padrão, que utiliza um ferrolho quadrado, com dois orifícios (em vez de apenas um) para combinar as duas fibras em um único conector.

- Pouco maior que um conector telefônico. Ele vem crescendo em popularidade, substituindo os conectores SC e ST em cabos de fibra multimodo, mas ele não é muito adequado para fibra monomodo.

Exemplo de uma placa de rede de fibra ótica

Vemos ao lado o exemplo de uma placa de rede para fibras ópticas. Essas placas operam com velocidade de 1000 Mbits/s e 10.000 Mbits/s (1 GB/s e 10 GB/s), dependendo do modelo.

A placa do exemplo ao lado usa conectores SC.



Exemplo de um conversor de fibra ótica

Na maioria dos casos não é necessário fazer o cabeamento de uma rede totalmente óptico. Podemos usar cabos UTP, que são mais baratos, na maior parte da rede, e apenas em pontos críticos, instalar conversores de mídia. São aparelhos que convertem sinais elétricos (RJ-45) para sinais ópticos (fibra). Por exemplo, para interligar dois prédios separados por uma distância acima de 100 metros (o máximo que os cabos UTP suportam), colocamos em cada prédio, conversores de mídia e fazemos a ligação entre os prédios usando fibras ópticas.

10.5 Vantagens

A transmissão de dados em uma rede através de fibras ópticas tem como principais vantagens:

- **Maior velocidade**: Redes do tipo Gigabit Ethernet (1.000 Mbits/s) podem operar com cabos UTP ou com fibras ópticas. Redes do tipo 10-Gigabit Ethernet (10.000 Mbits/s) operam com fibras ópticas.

- **Maior alcance**: Cabos UTP são limitados a 100 metros de alcance. Com fibras ópticas podemos ter alcances bem maiores, na faixa de 1 km ou mais.

- **Isolamento elétrico**: Na ligação entre prédios diferentes, muitas vezes existem problemas de aterramento. Quando existem áreas abertas, raios podem induzir tensões nos cabos de rede.

- Fibras ópticas não têm esses problemas, pois não transportam eletricidade.

10.6 Desvantagens

Como tudo na vida, as fibras ópticas têm vantagens e desvantagens. As desvantagens são relacionadas ao maior custo e à dificuldade de confecção dos cabos:

- As fibras ópticas são mais caras que os cabos UTP
- Conectores para fibras ópticas também são mais caros
- Placas de rede, hubs e switches para fibras ópticas são mais caros
- A montagem de cabos é uma operação muito especializada, que requer treinamento e equipamentos sofisticados.

10.7 Outros meios de transmissão

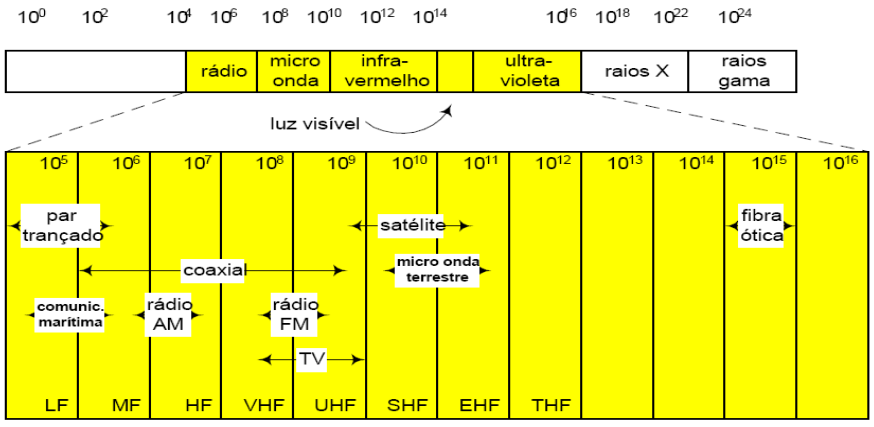
Radiodifusão (*wireless networks*)

Adequada para ligações ponto a ponto e para ligações multiponto. É uma alternativa viável onde é difícil, ou mesmo impossível, instalar cabos metálicos ou de fibra ótica.

Radiação infravermelha, microondas e satélites.

Também podem ser usados como meios de transmissão em redes de computadores.

10.8 Expectro de Frequências



O gerenciamento do espectro eletromagnético é normalmente realizado por organismos internacionais (ITU-R) e nacionais (Dentel - Departamento Nacional de Telecomunicações).

Legenda:

LF	Low Frequency
MF	Medium Frequency
HF	High Frequency
VHF	Very High Frequency
UHF	Ultra High Frequency
SHF	Super High Frequency
EHF	Extremely High Frequency
THF	Tremendously High Frequency

Transmissão de Rádio

Espectro vai de LF a VHF;

Viaja a longa distância e é multidirecional;

VLF, LF e MF atravessa obstáculos (p. ex. prédios), perde potência muito rapidamente e tende a seguir a curvatura da Terra;

HF, UHF e VHF

Viaja em linha reta .

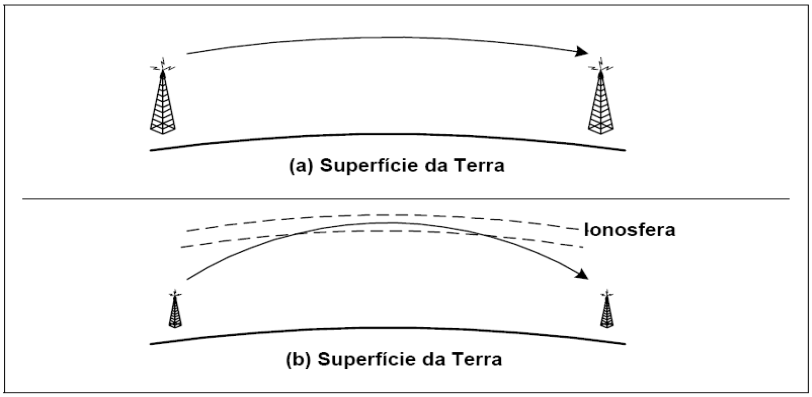
Reflete em obstáculos

Pode ser absorvida pela chuva

É sujeitas a interferências de motores

É absorvida pela Terra e refletida pela ionosfera;

Governo controla o uso através do Departamento Nacional de Telecomunicação (DENTEL);



Propagação de ondas: (a) VLF, LF e MF, (b) HF e VHF

Transmissão em Microondas

Acima de 100 MHz, as ondas viajam em linha reta, sendo necessário um alinhamento perfeito entre o emissor e o receptor;

Até o surgimento da fibra ótica, por décadas formaram o coração do sistema de transmissão das operadoras de telecomunicação.

Como sua propagação é em linha reta o seu alcance é curto (devido à curvatura da Terra).

Com torres de 100 metros de altura, são necessários repetidores a cada 80 Km aproximadamente.

É muito usada na comunicação de longa distância (telefonia fixa, telefonia móvel, distribuidoras de TV);

A faixa de 2,400 a 2,484 GHz é reservada para uso industrial / científico / médico, podendo ser usada sem autorização prévia do governo.

Ondas em Infravermelho

Usadas para comunicação de curta distância (controles remotos de TC, videocassete, aparelhos de som, redes locais);

Barato e fácil de construir;

Não atravessa objetos sólidos (não transparentes);

Transmissão em ondas de luz (laser)

Emissão de feixe de luz de alta frequência com alto poder de propagação.

Bastante usada para interligação de prédios não muito distantes, sem obstáculos interpostos.

Bluetooth

É uma especificação industrial para redes pessoais sem fio (Wireless personal area networks - PANs).

É um protocolo padrão de comunicação primariamente projetado para baixo consumo de energia com baixo alcance.

O Bluetooth provê uma maneira de conectar e trocar informações entre dispositivos como telefones celulares, notebooks, computadores, impressoras, câmeras digitais e consoles de videogames digitais através de uma freqüência de rádio de curto alcance globalmente não licenciada e segura.

Primariamente projetado para baixo consumo de energia com baixo alcance variando de acordo a sua potencia em:

- ~1 metro
- ~10 metros

- ~100 metros

RDIS ou ISDN

Rede Digital de Serviços Integrados, traduções alternativas do inglês ISDN (Integrated Service Digital Network).

Conhecida popularmente como Linha Dedicada é uma tecnologia que usa o sistema telefônico comum.

O ISDN já existe há algum tempo, sendo consolidado nos anos de 1984 e 1986, sendo umas das pioneiras na tecnologia xDSL.

10.9 Tipos de Cabeamento

Usada para tecnologia LAN com algumas aplicações WAN

- 10Base5 (Ethernet grossa)

- O cabo coaxial 10Base5 é também conhecido como cabo coaxial grosso, e é utilizado em redes de telecomunicação.

- Normalizada em 1980

- Suporta uma velocidade de 10Mbps para transmissão de dados.

- Usada para tecnologia LAN com algumas aplicações WAN

- 10Base5 (Ethernet grossa) (Cont...)

- Topologia em barramento

- Possui um alcance de 500 metros por segmento (isto é, sem a adoção de repetidores).

- Máximo de 30 estações por segmento

- Pouca flexibilidade do cabo

- 10Base2 (Ethernet fina)

- Utiliza cabo coaxial fino o cabo transmite sinais a 10 Mbps a uma distância máxima de 185 metros por segmento.

- Normalizada em 1987

- Topologia em barramento

- Máximo de 30 estações por segmento

- Cabo de 0,5 cm de diâmetro

- Conectores BNC padrão

10Base-T

- É uma implementação de Ethernet de 10 Mbps que permite que estações sejam ligadas por cabos de par trançado.
- Normalizada em 1990
- Par trançado como meio de transmissão
- Estação conectada a um hub através de dois pares trançados
- Topologia em estrela
- Alcance de 100 a 200 m (do hub a uma estação)
- Esse alcance depende da qualidade do cabo

11 ENTIDADES DE PADRONIZAÇÃO

11.1 ISO (International Standards Organization)

É uma organização voluntária e independente, fundada em 1946, responsável por todos os tipos de padrões.

A ISO publica padrões sobre uma vasta gama de assuntos, que vão desde parafusos e porcas ao revestimento usado nos postes de telecomunicações.

11.2 ANSI (American National Standards)

Desenvolve e publica padrões internacionais, incluindo a área de comunicação digital.

A ANSI faz contribuições para a ISO. Temos como exemplo de padronização o padrão ANSI X3T9.5 (FDDI), que especifica redes de fibras ópticas operando a 100 Mbps na topologia anel.

11.3 IEEE (Institute of Electrical and Eletronics Engineers)

O IEEE possui um grupo de padronização que desenvolve padrões nas áreas de Engenharia Elétrica e de Informática.

Temos como exemplo o famoso padrão 802 do IEEE para as redes Ethernet.

11.4 ITU-T (International Telecommunications Union)

Antigo CCITT (Comitê Consultivo International de Telegrafia e Telefonia).

Foi criado 1992 e tem como objetivo formular e propor recomendações para telecomunicações.

11.5 TIA (Telecommunications Industry Association)

O comitê EIA/TIA especifica o sistema de cabeamento estruturado utilizado nas redes de computadores.

12 ENTIDADES DE PADRONIZAÇÃO DIRECIONADAS A INTERNET

Internet é uma rede pública mundial e autônoma baseada em padrões abertos. Não existe nenhuma autoridade central que controle o funcionamento da internet. Para permitir a interoperabilidade das diversas redes que compõem a Internet, várias organizações colaboram no estabelecimento de padrões e políticas gerais de operação da rede.

12.1 IAB (Internet Architecture Board)

Responsável por coordenar os trabalhos de pesquisa e normalização relacionados à Internet.

Supervisiona atividades de dois grupos

- **IETF (Internet Engineering Task Force)**

  - Curto prazo

  - Os padrões propostos são publicados na Internet por meio de RFC (Request for Comments).

- **IRTF (Internet Research Task Force)**

  - Trabalha com assuntos estratégicos de longo prazo

  - Incluindo esquemas de endereçamento e novas tecnologias.

12.2 Internic (Internet Network Information Center)

A InterNIC, até a década de 1990, foi a responsável pela alocação de nomes de domínio e endereços IP; ou seja, até a década de 1990, os registros de domínios com extensão .com, .net e .org foram controlados pela InterNIC.

12.3 ARIN (American Registry for Internet Numbers)

O ARIN é quem cuida da distribuição de IPv4 e IPv6 para os países da América do norte.

12.4 LACNIC (Latin American and Caribbean Internet Addresses Registry)

Cuida da distribuição de de IPv4 e IPv6 para os países da América do Latina e Caribe.

12.5 IANA (The Internet Assigned Numbers Authority)

Organização internacional responsável por coordenar a distribuição de endereços IP entre as diversas redes de computadores que se conectam à Internet.

No Brasil, a distribuição de endereços IP e a atribuição de nomes de domínio br são feitos pela FAPESP.

13 MODELO DE REFERÊNCIA OSI

Quando as redes surgiram as soluções eram proprietárias, um único fabricante tinha que construir tudo na rede.

Para facilitar a interconexão de sistemas a ISO (International Standards Organization) criou o modelo OSI (Open System Interconnection), para que os fabricantes criassem seus dispositivos a partir desse modelo.

Primeiro passo à padronização internacional dos protocolos utilizados nas diversas camadas. Modelo em sete camadas: Física, enlace, rede, transporte, sessão, apresentação e aplicação.

13.1 Princípios:

Um nível de abstração por camada.

Camadas com funções bem definidas.

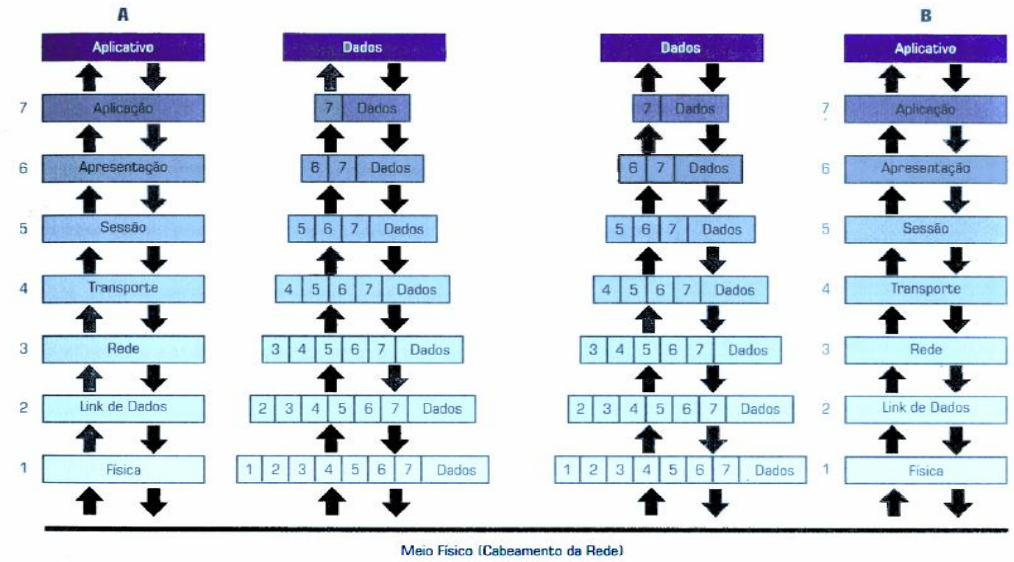
Em cada camada devem ser usados protocolos padronizados internacionalmente

O número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar.

13.2 Encapsulamento

Na transmissão cada camada pega as informações passada pela camada superior, acrescenta suas informações e passa os dados para a camada abaixo. Na recepção ocorre o processo inverso.

13.3 Comunicação entre as camadas OSI



Na prática não nos preocupamos com os detalhes da comunicação, não precisamos nos preocupar com a camada inferior aquela em que estamos trabalhando.

- Exemplo: ao enviar um e-mail sabemos que nosso programa de e-mail vai se conectar ao servidor, mas não precisamos saber os detalhes de como isso será feito.

13.4 Quadros e Pacotes

Quadro: conjunto de dados enviado através da rede (baixo nível).

– Endereçamento físico (Exemplo: MAC).

– Nível 1 e 2 do modelo OSI.

Pacote: informação proveniente de vários quadros (nível mais alto).

– Endereçamento virtual (Exemplo: IP).

– Nível 3 e 4 do modelo OSI.

13.5 Camada 7 - Aplicação

Faz interface entre o protocolo de comunicação e o aplicativo que pediu ou receberá informação através da rede

– Exemplo: baixar o e-mail com o aplicativo de e-mail

13.6 Camada 6 - Apresentação

Também chamada Tradução converte o formato do dado recebido da camada de aplicação em um formato comum, a ser usado na transmissão desse dado

– Exemplos:

• conversão do padrão de caracteres (código de página)

• Compressão de dados

• Criptografia

13.7 Camada 5 - Sessão

Permite que duas aplicações em computadores diferentes estabeleçam uma sessão de comunicação.

– Definem inicialmente como será feita a transmissão e a partir daí usam marcadores.

– Se a transmissão falhar, reiniciam a partir da última marcação.

– Exemplos:

• Você está baixando e-mails e a rede falha, quando ela voltar o programa de e-mails continua baixando de onde parou.

13.8 Camada 4 - Transporte

Responsável por pegar os dados enviados pela camada de Sessão e dividí-los em pacotes que serão transmitidos pela rede (repassados para a camada de rede).

No receptor a Camada de Transporte pega os pacotes recebidos da rede e remonta o dado original para enviá-lo a camada de Sessão.

• Essa camada inclui:

– Controle de fluxo: reordena pacotes fora de ordem

– Correção de erros: aviso se pacote chegou OK

13.9 Camada 3 – Rede

Responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos, de forma que os pacotes consigam chegar corretamente ao destino, baseada em fatores como condições de tráfego de rede e prioridades.

Essa camada também é responsável por escolher a rota quando há diversos caminhos para um pacote trafegar até o destino.

13.10 Camada 2 – Link de Dados

Também chamada de Enlace

Pega os pacotes de dados recebidos da camada de Rede e os transforma em quadros que serão trafegados pela rede, adicionando informações:

- endereço da placa de rede de origem.
- endereço da placa de rede de destino.
- dados de controle
  - os dados em si
  - CRC

O receptor confere o CRC e manda uma confirmação de recebimento (acknowledge ou ack). Se essa confirmação não for recebida a camada reenvia o quadro.

13.11 Camada 1 – Física

Pega os quadros enviados pela camada Link de Dados e os transforma em sinais compatíveis com o meio onde os dados deverão ser transmitidos (elétrico, óptico, etc...)

- A camada Física:
  – Não sabe o significado dos dados que está transmitindo.
  – Não inclui o meio onde os dados circulam (cabo de rede), apenas precisa saber qual o meio e tipo de conector para fazer a conversão correta.

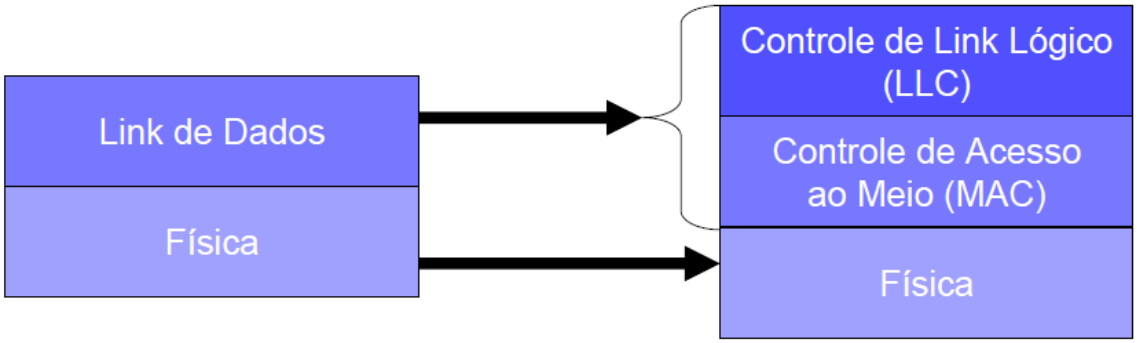
14 PADRÃO IEEE 802

IEEE (Institute of Electrical and Electronic Engineers) criou uma série de padrões de protocolos. 802 é a série mais importante: conjunto de protocolos usados no acesso à rede.

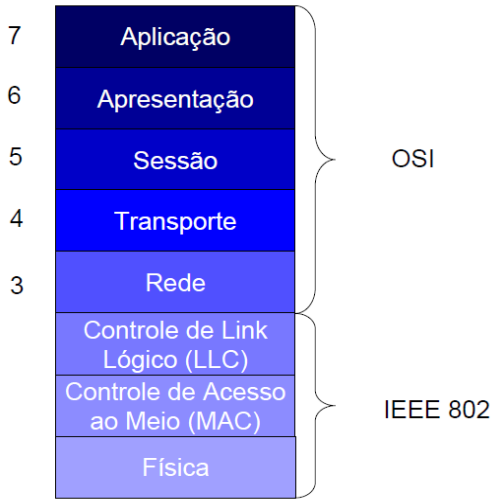
Três camadas que equivalem as duas primeiras do modelo OSI. Camada 2 do modelo OSI é dividida em duas:

- Controle do Link Lógico (LLC, Logic Link Control).
- Controle de Acesso ao meio (MAC, Media Access Control).

14.1 Camadas do protocolo IEEE 802



14.2 Modelo de protocolo usado por dispositivos que usam o protocolo IEEE 802



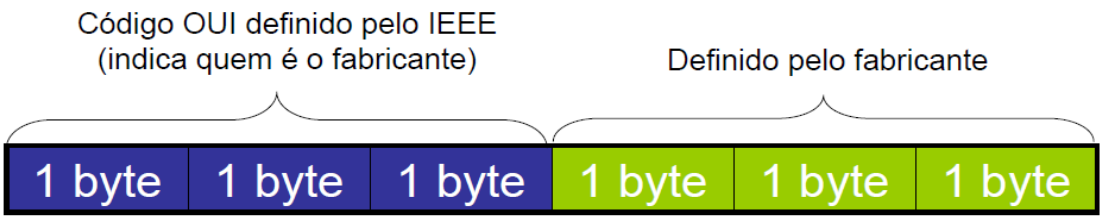
14.3 Controle de Acesso ao Meio (MAC)

Cada placa tem seu endereço MAC único gravado em hardware (teoricamente não pode ser alterado).Um endereço MAC tem 6 bytes. Exemplo: 02-60-8C-42-81-97

Estrutura do Endereço (MAC)

• OUI (OrganizationUniqueIdentifier)

• Cada fabricante deve se cadastrar no IEEE para obter seu OUI



Cada fabricante é responsável por controlar sua numeração. Um mesmo fabricante pode ter mais de um OUI. No quadro enviado a rede, a camada MAC irá incluir o endereço MAC de origem e de destino. A placa de rede cujo MAC é o receptor receberá o pacote e as outras permanecerão inativas.

Controle de uso do cabo

A camada MAC verifica se o cabo estásendo usado naquele momento:

– Se o cabo estiver ocupado o quadro não é enviado

– Caso duas máquinas enviem quadros ao mesmo tempo há uma colisão que é detectada pelas camadas MAC de cada dispositivo.

Elas esperam o cabo ficar livre para tentar uma retransmissão, esperando um tempo aleatório para que não ocorra uma nova colisão. A camada MAC usa um driver que ensina como lidar com o modelo de placa de rede instalado no micro.

Estrutura de um quadro MAC

Preambulo (7 bytes)	SFD (1 byte)	MAC Destino (6 bytes)	MAC Origem (6 bytes)	Comprimento (2 bytes)	Dados e Pad (De 46 a 1500 bytes)	FCS (4 bytes)

Preâmbulo: marca o início do quadro. São sete bytes 10101010. Junto com SFD forma um padrão de sincronismo. (sinal de clock).

SFD (Startof Frame Delimiter): um byte 10101011.

Comprimento: indica quantos bytes serão transmitidos no campo de dados.

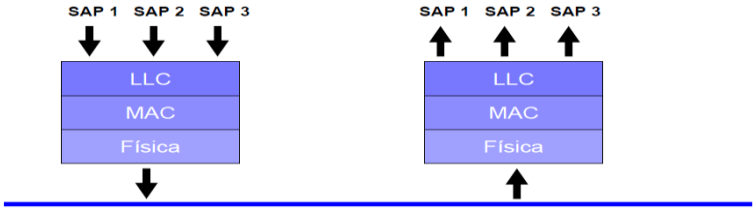
Dados: enviados pela camada de Controle de Link Lógico, tem tamanho variável.

PAD: caso os dados sejam menos que 46 bytes, serão inseridos dados pad até que se atinja o limite mínimo.

FCS (Frame Check Sequence): informações para controle de correção de erro (CRC).

14.4 Controle do Link Lógico (LLC)

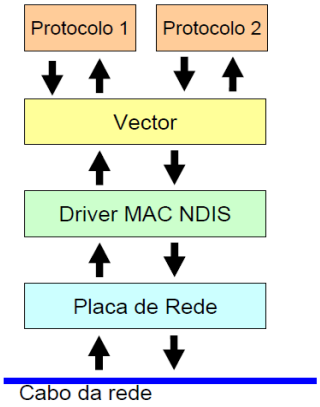
Permite que mais de um protocolo seja usado acima dela (protocolos da camada 3 do modelo OSI). Define pontos de comunicação entre transmissor e receptor chamado SAP (Service Access Point).



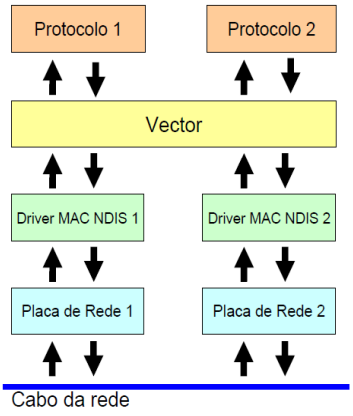
Adiciona ao dado recebido informações de quem enviou esta informação (o protocolo que passou essa informação). Sem essa camada não seria possível usar mais de um protocolo no nível 3.

14.5 NDIS – Network Driver Interface Specification

Criado pela Microsoft e pela 3Com. Permite que uma única placa de rede possa utilizar mais de um protocolo de rede ao mesmo tempo.

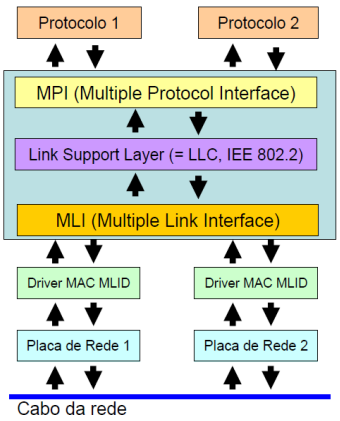


Permite a existência de mais de uma placa de rede em um mesmo micro. Compartilha uma única pilha de protocolos (tudo que estiver do nível 3 do modelo OSI para cima) para as duas placas. Mesma função da LLC.



14.6 ODI – Open Datalink Interface

Driver com mesmo objetivo do NDIS criado pela Novelle pela Apple. Funcionamento um pouco mais complexo e mais completo. Adiciona uma interface entre a LLC e os vários protocolos e outra interface entre o LLC e as várias placas de rede.



15 MODELO DE REFERÊNCIA TCP/IP

15.1 Princípios

Atualmente é o protocolo mais usado em redes locais.

– Principal responsável: Popularização da Internet

– Mesmo SOs que antigamente só suportavam seu protocolo proprietário hoje suportam TCP/IP.

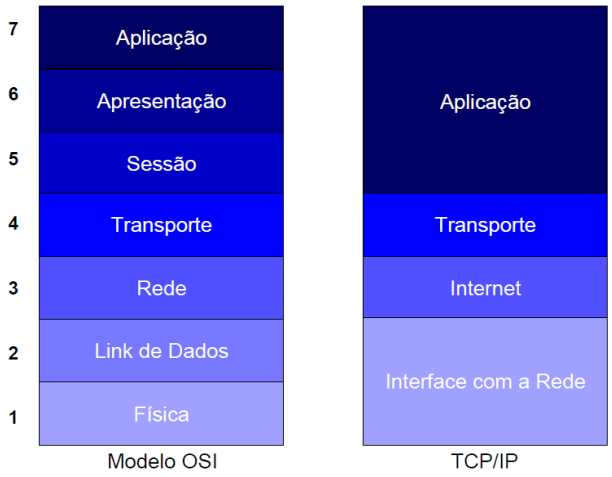
- Windows NT com seu NETBEUI
- Netware com seu IPX/SPX

É roteável, foi criado pensando em redes grandes e de longa distância, onde pode haver vários caminhos para chegar ao destino. Composto por 4 camadas ao contrário de 7 do modelo OSI.

Arquitetura aberta.

– Qualquer fabricante pode adotar sua própria versão do TCP/IP em seu SO sem pagar direitos autorais.

- Todos os fabricantes acabaram adotando TCP/IP .
- Protocolo Universal.



TCP/IP é na realidade um conjunto de protocolos:

– TCP: Transmission Control Protocol.

– IP (Internet Protocol).

• Operam nas camadas de Transporte e Internet respectivamente.

• Não são os únicos.

15.2 Camada de Aplicação

Equivale às camadas 5, 6 e 7 do modelo OSI. Faz a comunicação entre aplicativos e a camada de transporte. Os protocolos mais conhecidos:

• HTTP (HyperText Transfer Protocol).

• SMTP (Simple Mail Transfer Protocol).

• FTP (File Transfer Protocol).

• SNMP (Simple Network Management Protocol).

• DNS (Domain Name System).

• Telnet.

Comunica-se com a camada de transporte através de uma *porta(ou porto)*. Portas são numeradas e as aplicações padrão usam sempre a mesma porta.

–Exemplos:

• SMTP utiliza a porta 25

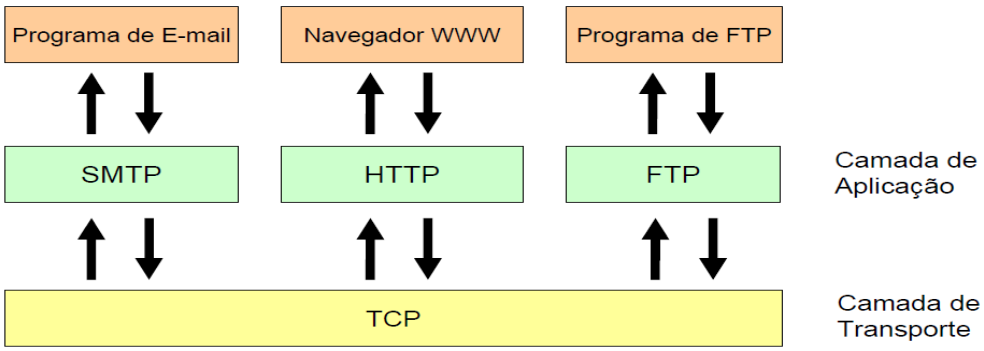
• HTTP utiliza a porta 80

• FTP as portas 20 (dados) e 21 (informações de controle)

Uso de portas: permite ao protocolo de transporte (tipicamente o TCP) saber qual éo tipo de conteúdo do pacote de dados.

No receptor, ao receber um pacote na porta 25 irá entregá-lo ao protocolo conectado a essa porta (tipicamente SMTP), que por sua vez irá repassá-lo para a aplicação (programa de e-mail).

Funcionamento da camada de aplicação



15.3 Camada de Transporte

A camada de transporte do TCP/IP é um equivalente direto da camada de transporte (4) do modelo OSI. Responsável por pegar dados enviados pela aplicação e transformá-los em pacote para serem repassados para a camada de Internet.

Nesta camada operam dois protocolos:

–TCP (Transmission Control Protocol).

- Mais utilizado na transmissão de dados.

–UDP (User Datagram Protocol).

- Não verifica se o dado chegou ou não ao destino.
- Mais usado na transmissão de informações de controle.

Recepção:

– Pega os pacotes passados pela camada Internet.

– Coloca os pacotes em ordem e verifica se todos chegaram corretamente.

Quadros podem seguir caminhos diferentes e chegarem fora de ordem.O protocolo IP (camada de Internet) não verifica se o pacote de dados chegou ao destino; ficando o TCP com essa tarefa (eventualmente pedindo uma retransmissão).

15.4 Camada de Internet

Equivale a Camada de Rede (3) do modelo OSI. Todas as explicações dadas sobre essa camada no modelo OSI são 100% válidas para a camada de Internet do TCP/IP.

Vários protocolos podem operar nessa camada:

– IP (Internet Protocol).

– ICMP (Internet Control Message Protocol).

– ARP (Address Resolution Protocol)

– RARP (Reverse Address Resolution Protocol)

Pacote de dados recebido da camada TCP é dividido em pacotes chamados *datagramas.*

– Datagramas são enviados para a camada de interface com a rede, onde são transmitidos pelo cabeamento de rede através de quadros.

Não verifica se os dados chegaram ao destino, isso éfeito pelo TCP.

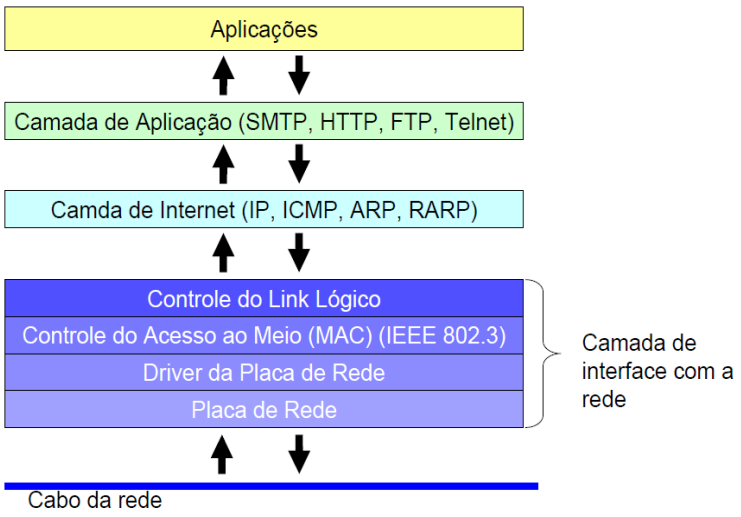
Responsável pelo roteamento de pacotes.

– Adiciona informações ao datagrama sobre o caminho que ele deverá percorrer.

15.5 Camada de Interface de Rede

Equivale as camadas 1 e 2 do modelo OSI. Responsável por enviar o datagrama recebido pela camada de Internet em forma de um quadro através da rede.

15.6 Funcionamento do TCP - IP



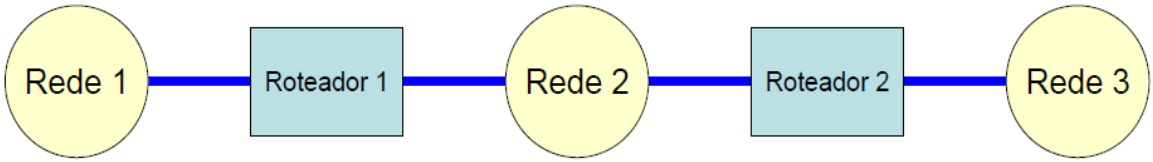
15.7 Endereçamento IP

TCP/IP é roteável, foi criado pensando na interligação de diversas redes (podem haver vários caminhos entre o transmissor e o receptor). Cada dispositivo conectado em rede necessita usar pelo menos um endereço IP. Endereço IP permite identificar o dispositivo e a qual rede ele pertence.

As redes são interligadas através de dispositivos chamados *roteadores.*

– Quando um computador da rede 1 quer enviar um pacote de dados para um computador da rede 3, ele envia o pacote para o roteador 1, que então repassa esse pacote

diretamente ao roteador 2, que se encarrega de fazer a entrega ao computador de destino na rede 3.



A entrega é feita facilmente pelo roteador, pois os pacotes possuem o endereço IP do computador de destino.

– Nesse endereço há informação de em qual rede o pacote deve ser entregue.

– O roteador 1 sabe que o destinatário não está na rede 2 e portanto o envia diretamente para o roteador 2.

Redes TCP/IP tem um ponto de saída chamado *gateway*. Todos os pacotes de dados recebidos que não são para aquela rede vão para o gateway. As redes subseqüentes vão enviando os pacotes a seus respectivos gateways até que cheguem ao destino. Isso é possível porque o endereço IP possui duas partes (próximo slide).

Campo de um endereço IP

O endereço IP é um número de 32 bits, representado em decimal em forma de 4 números de 8 bits separados por um ponto no formato a.b.c.d.

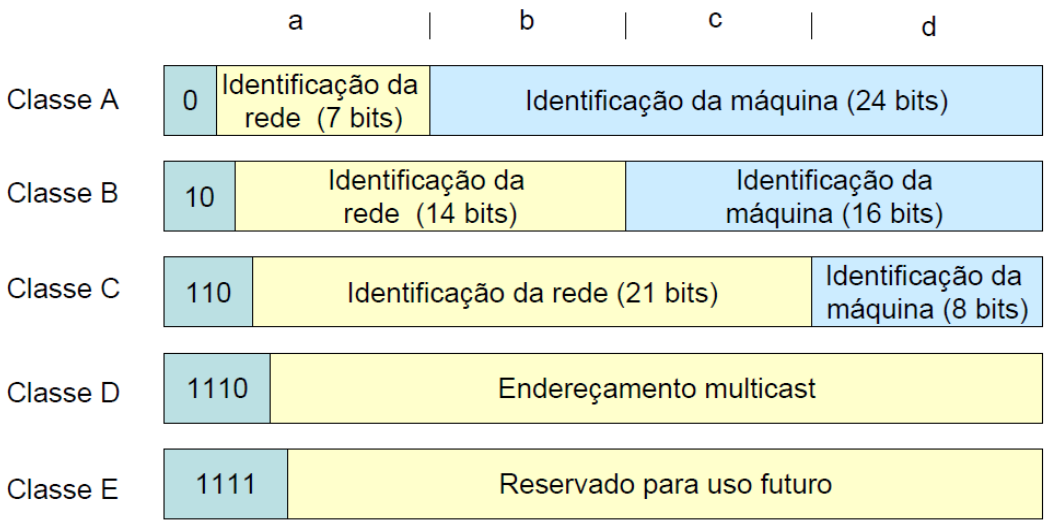
– Menor endereço possível: 0.0.0.0

– Maior endereço possível: 255.255.255.25

Teoricamente um endereço TCP/IP pode ter até 4.294.967.296 endereços IP (256^4). Porém alguns endereços são reservados e não podem ser usados. Logo esse limite máximo será atingido, por isso já foi padronizado o endereçamento usando 128 bits em vez de 32, chamado IPv6. Também chamado IP Next Generation (IPng) ou Simple Internet Protocol Plus(SIPP). Ainda não usado comercialmente.

É possível endereçar 340.282.366.920.938.463.463.374.607.431.770.000.000 dispositivos diferentes. Daria para ter 1.564 endereços IP por metro quadrado da superfície do planeta Terra. Cada dispositivo de uma rede TCP/IP precisa ter um endereço IP único, para que o pacote de dados consiga ser entregue corretamente. Você terá que obrigatoriamente usar endereços que não estejam sendo usados por nenhum outro computador da rede.

Classes de endereço IP



Classe	Endereço mais baixo	Endereço mais alto
A	1.0.0.0	126.0.0.0
B	128.1.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.254

* alguns endereços não constam na tabela por serem de uso reservado

Em rede usamos somente as classes A, B e C

Classe	Números para Identificação da Rede	Números para Identificação da máquina	Quantidade de máquinas na rede
A	1	3	16.777.216
B	2	2	65.536
C	3	1	256

Os endereços 0 e 255 são reservados, então na prática o número de máquinas por rede é menor.

– Exemplo: Classe C: 254 máquinas.

A escolha da classe da rede depende de seu tamanho. Grande maioria usa classe C.

O sistema de redes que forma a estrutura básica da Internet é chamado *backbone*, e para estar na internet você deve estar ligado a ele de alguma forma (diretamente ou indiretamente).

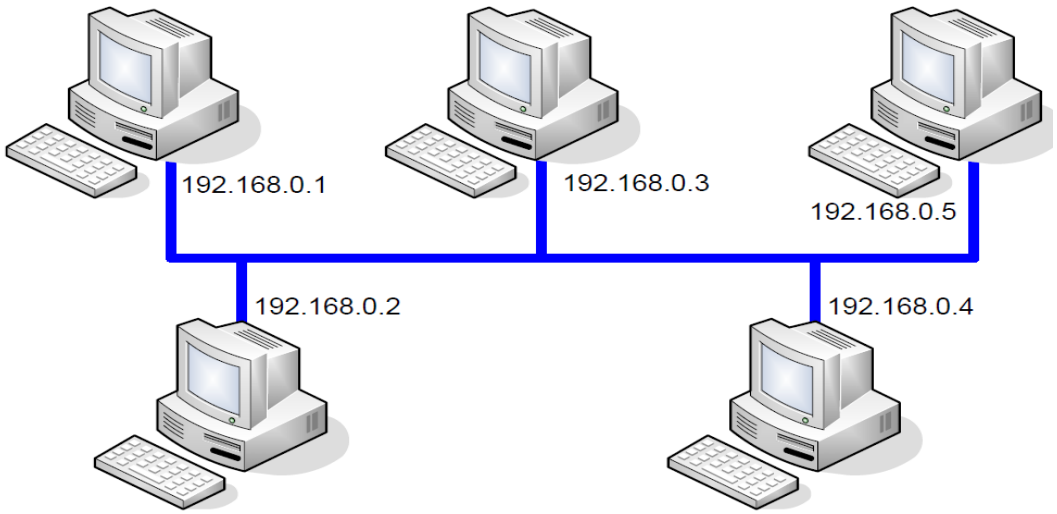
A Internet possui uma estrutura hierárquica. Responsável pelo backbone é responsável pelo controle e fornecimento de endereços Ips a seus subordinados. Por sua vez, os Ips de um backbone foram atribuídos pelo backbone hierarquicamente superior a ele.

Alguns endereços Ips são reservados para redes privadas. Roteadores reconhecem esses endereços como sendo de redes particulares e não os repassam para o resto da Internet. Mesmo que um roteador esteja configurado errado e passe o pacote adiante, outro roteador configurado corretamente irá barrá-lo.

Endereços especiais reservados para redes privadas:

- Classe A: 10.0.0.0 a 10.255.255.255
- Classe B: 172.16.0.0 a 172.31.255.255
- Classe C: 192.168.0.0 a 192.168.255.255

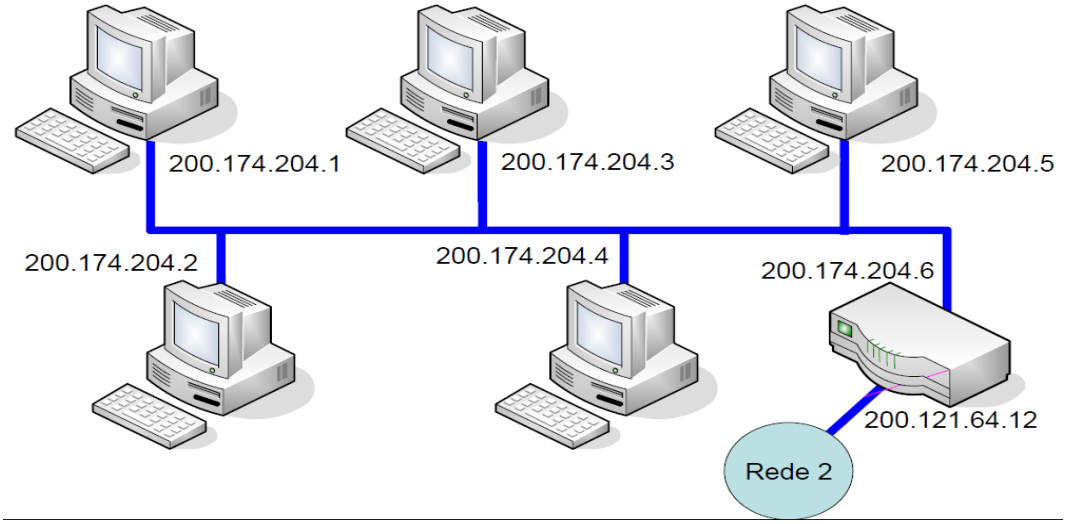
Exemplo de uma rede TCP-IP



O endereço 255 é reservado para broadcast(enviar um pacote de dados para todas as máquinas da rede ao mesmo tempo). Para conectar essa rede a Internet existem duas soluções:

– A primeira seria obter um endereço classe C público e atribuir um IP único na Internet e válido dentro da rede.

Exemplo de uma rede TCP-IP conectada a internet



Outra solução para conectar a rede à Internet é criar uma tabela de tradução no roteador, que pega os pacotes vindos com endereços Ips válidos na Internet e converte esses endereços em endereços privados, aceitos somente na rede local.

Essa tradução pode ser estática ou dinâmica.

– **Estática:** um determinado endereço privado sempre é convertido em um mesmo endereço público.

– **Dinâmica:** é usada por clientes que não precisam prestar serviço para a rede. Assim mais de um endereço privado pode estar usando um mesmo IP público.

DCHP (Dynamic Host Configuration Protocol)

Permite atribuição automática ou manual de endereços Ips para computadores da rede. Quanto um cliente solicita um endereço IP o servidor DHCP atribui um IP a ele por um certo período (que deverá ser renovado quando o prazo estiver expirando).

Máscara de rede

É formada por 32 bits no mesmo formato que o endereço IP e cada bit 1 da máscara informa a parte do endereço IP que é usada para o endereçamento da rede e cada bit 0 informa a parte do endereço IP que é usada para o endereçamento das máquinas.

Dessa forma as máscaras padrões são:

– Classe A: 255.0.0.0

– Classe B: 255.255.0.0

– Classe C: 255.255.255.0

Valores fora do padrão podem ser usados quando houver necessidade de segmentar a rede.

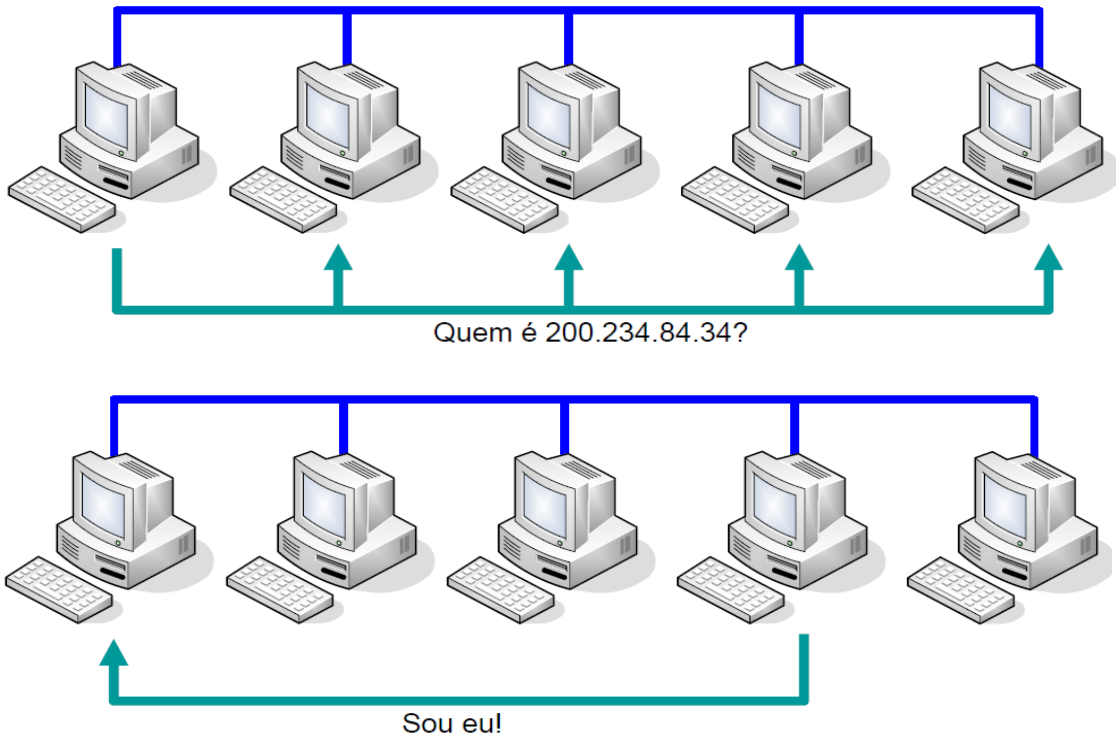
ARP (Address Resolution Protocol)

As redes TCP/IP baseiam-se em um endereçamento virtual (IP), mas as placas de rede utilizam endereçamento MAC. O protocolo ARP é responsável por fazer a conversão entre endereços Ips e os endereços MAC da rede.

Em uma grande rede, os pacotes TCP/IP são enviados até a rede de destino através dos roteadores. Atingindo a rede de destino o protocolo ARP entra em ação para detectar o endereço da placa de rede para qual o pacote deve ser entregue, já que no pacote há somente o endereço IP.

Funciona primeiramente enviando uma mensagem de broadcast para a rede perguntando a todas as máquinas qual responde pelo IP destinatário do pacote que chegou. A máquina responsável por tal IP responde, identificando-se e informando seu endereço MAC para que a transmissão possa ser feita.

O dispositivo armazena os endereços Ips recentemente usados e seus endereços MACs correspondentes em uma tabela na memória.



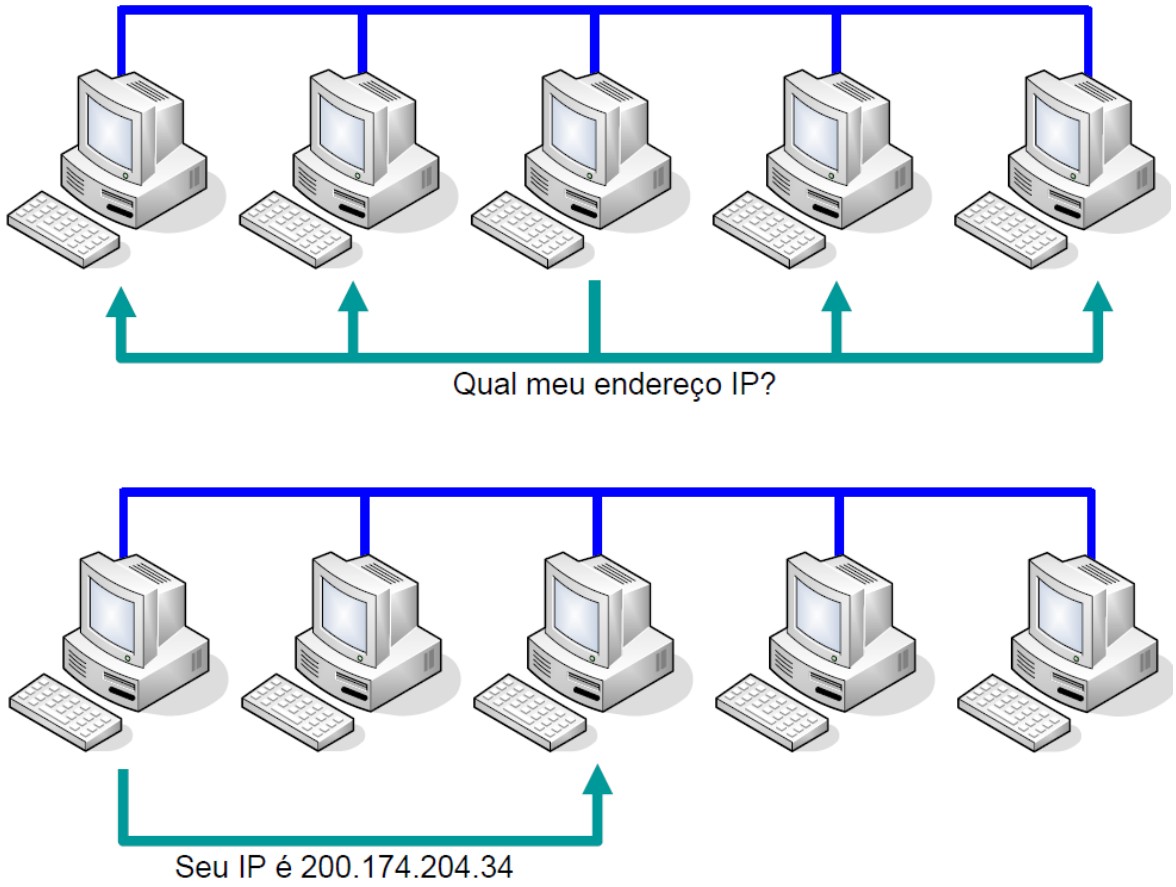
RARP (Reverse Address Resolution Protocol)

Permite que uma máquina descubra um endereço IP através de um endereço MAC, fazendo o inverso do que o protocolo ARP faz.

Quando ligamos um computador ele não sabe seu endereço IP. Essa informação estará gravada no disco rígido ou alguma memória não volátil. Estações com boot remoto não tem como saber seu endereço IP, e portanto não tem como usar TCP/IP. Nesses casos utilizamos

um servidor RARP, que armazena uma tabela com os endereços MACs das máquinas da rede e seus respectivos Ips.

Uma máquina que precisa saber seu próprio endereço IP envia um pedido para todas as máquinas, mas somente o servidor RARP responde, informando seu IP. A partir daí, o endereço IP ficará na memória RAM da máquina.



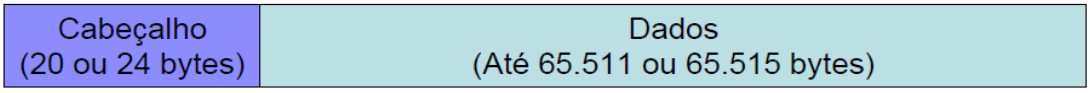
15.8 IP - Internet Protocol

Pega os dados enviados pela camada de transporte (TCP ou UDP) e envia para a camada física. Na camada física os datagramas serão empacotados em quadros (como já vimos anteriormente). IP não é orientado a conexão. Não verifica se o datagrama chegou ao destino.

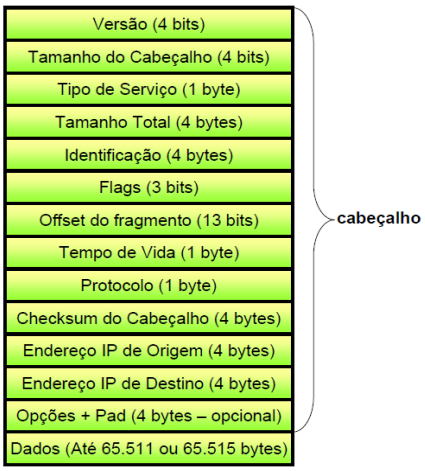
Isso é feito pelo TCP, que pega os dados que estão chegando e os coloca em ordem, pedindo uma retransmissão caso algum dado esteja faltando. Principal função: roteamento.

Adicionar mecanismos para que o datagrama chegue o mais rápido possível ao destino. Feito com auxílio dos roteadores de rede. Escolhem o caminho mais rápido entre a origem e o destino.

Estrutura do Datagrama IP



Estrutura simplificada



O campo Opções+Pad pode não existir, reduzindo o tamanho do cabeçalho para 20 bytes.

A área de dados não tem tamanho fixo, portanto o tamanho do datagrama IP é variável.

O tamanho máximo é 65.535 (incluindo o cabeçalho).

Versão: indica a versão do protocolo IP que está sendo usado. O protocolo IP que estamos descrevendo é o IPv4. Portanto encontraremos o valor 4 nesse campo.

Tamanho do cabeçalho (IHL, Internet HeaderLength): indica o comprimento do cabeçalho do datagrama, dado em número de palavras de 32 bits.

Tipo de Serviço: informa a qualidade desejada para entrega do datagrama, falaremos dele mais adiante.

Tamanho Total: número total de bytes que compõem o datagrama. Esse campo possui 16 bits, portanto o tamanho máximo do datagrama é 65.535 bytes (21^6). Quanto maior o datagrama, mais a estação ocupa a rede (deixando-a mais lenta), portanto normalmente utiliza-se valores bem menores que 65.535 bytes, um valor comum é 576 bytes.

Identificação: quando um datagrama é criado recebe um número de identificação que será usado para identificá-lo caso ele seja fragmentado no caminho até o destino.

Flags: usado para controlar a fragmentação de datagramas, será estudo mais adiante.

Offset do Fragmento: usado para controle da fragmentação de datagramas, também explicado mais adiante.

Tempo de Vida (TTL): tempo máximo de vida do datagrama, cada vez que o datagrama passa por um gateway (um roteador, por exemplo) esse número é decrementado.

– Quando chega a zero o datagrama é descartado, não atingindo o destino.

– No receptor o protocolo IP percebe que está faltando um datagrama e pede retransmissão.

Objetivo: eliminar datagramas que demorem muito para chegar ao destino (rota muito longa ou mesmo errada devido a roteador mal configurado no caminho).

Protocolo: indica o protocolo que pediu o envio do datagrama, através de um código numérico. Exemplo: número 6 indica TCP, 17 indica UDP.

Checksum do Cabeçalho: cálculo do checksum somente do cabeçalho (não usa os dados no cálculo).

– Conta menor e mais rápida de ser feita.

– Os roteadores analisam esse campo e refazem o checksum para saber se o cabeçalho está ou não corrompido.

Endereço IP de origem: endereço IP de onde está partindo o datagrama.

Endereço IP de destino: endereço IP de destino do datagrama.

Opções + Pad: campo opcional. Se não for usado, o cabeçalho passa a ter 20 bytes. Como seu tamanho é variável ele é preenchido com zeros até completar 32 bits (que são conhecidos como *padou padding)*. Usado em testes e verificações de erro na rede.

Dados: são os dados que o datagrama está carregando.

– Tamanho máximo de 65.515 bytes ou 65.511 bytes

– Normalmente utiliza-se valores em torno de 556 bytes

Fragmentação de Datagrama

Quando os datagramas são enviados à rede através da camada Física, seu tamanho fica limitado ao da área de dados do protocolo usado nessa camada.

– Por exemplo: em uma rede Ethernet o tamanho máximo é 1500 bytes.

Essa característica é chamada MTU (Maximum Transfer Unit).

– O pacote passa por vários roteadores antes de chegar a seu destino, e pode encontrar roteadores com diferentes MTU.

– A solução é a fragmentação de datagramas.

15.9 ICMP (Internet Control Message Protocol)

Mecanismo utilizado pelos roteadores para informar que um problema ocorreu.

– Congestionamento.

– TTL de datagrama zerado.

Ele apenas informa a máquina transmissora que um erro ocorreu. Não se importa em corrigi-lo. Parte integrante do IP. Dividi-los em 2 ou mais quadros menores e depois juntá-los novamente.

Eco: utilizado para saber se o caminho entre o transmissor e o receptor está bom. Exemplo: Comando Ping.

Destino Inalcançável: enviada quando o roteador não consegue entregar o datagrama.

Congestionamento: se o roteador está recebendo mais datagramas do que consegue processar, ele começa a descartá-los, e informa a maquina transmissora para diminuir a velocidade.

Redirecionamento: o roteador pode verificar que há uma rota melhor para ser usada, e avisa o transmissor.

Tempo de Vida excedido: se o TTL do datagrama é zerado, o roteador informa o transmissor.

Problema nos Parâmetros: quando o roteador não consegue processar o datagrama e não há outra mensagem ICMP que cubra o problema encontrado, essa mensagem é enviada.

Solicitação de Horário: uma máquina pode pedir o horário do relógio de outra. Pode ser usado para sincronizar o relógio de duas máquinas, mas o atraso da rede impede que a sincronia fique perfeita.

15.10 UDP (User Data Protocol)

Não orientado a conexão. Não verifica se os dados chegaram ao destino. O protocolo de aplicação deve implementar essa verificação se for necessário. Vantagem: transmissão de dados mais rápida. Cabeçalho menor que o TCP, Não precisa esperar mensagens de confirmação.

Viável em redes locais confiáveis. Na Internet usado apenas quando a taxa de perda de pacotes não seja um problema. Streaming de audio e vídeo.

15.11 TCP (Transmission Control Protocol)

Recebe datagramas IP, os coloca em ordem e verifica se todos chegaram corretamente. Aplicativos enviam e recebem dados pela rede TCP através de canais virtuais de comunicação (http –80, telnet–23, etc..). TCP empacota os dados adicionando informações de porta de

origem e destino, entre outras, passando o pacote de dados ao protocolo IP. Se o transmissor não recebe uma confirmação de recebimento dentro de um determinado tempo o pacote é enviado novamente.

Conexão

Comunicação entre duas aplicações em duas máquinas diferentes. O protocolo TCP é responsável por abri-las, mantê-las e fechá-las. A abertura é feita através de um processo chamado *handshake*.

A conexão é mantida através do envio de pacotes do transmissor ao receptor. Se tudo correr bem a transmissão será encerrada quando não houverem mais dados a ser transmitidos.

Protocolos de Comunicação

DNS (Domain Name System): usado para identificar máquinas através de nomes em vez de endereços IP.

Telnet: usado para comunicar-se remotamente com uma máquina.

FTP (File Transfer Protocol): usado na transferência de arquivos.

SMTP (Simple Mail Transfer Protocol): usado no envio e recebimento de e-mails.

HTTP (Hyper Text Transfer Protocol): usado na transferência de documentos hipermídia (WWW, World Wide Web).

16 COMPARAÇÃO ENTRE OS MODELOS DE REFERÊNCIA OSI E TCP/IP

16.1 Fundamentos

Os modelos de referencia OSI e TCP/IP têm muito em comum. Os dois se baseiam no conceito de uma pilha de protocolos independentes. Além disso, as camadas têm praticamente as mesmas funções. Apesar dessas semelhanças fundamentais, os dois modelos também tem muitas diferenças.

O modelo OSI tem três conceitos fundamentais:

- Serviços
- Interfaces
- Protocolos

Originalmente, o modelo TCP/IP não distinguia com clareza a diferença entre serviço, interface e protocolo, embora as pessoas tenham tentado adaptá-lo ao modelo OSI.

16.2 Uma crítica aos protocolos e ao modelo OSI

Momento Ruim: Quando os padrões OSI foram lançados, a indústria já tinha investido no TCP/IP, e não queria investir novamente em outra pilha de protocolos;

Tecnologia Ruim: A camada de sessão com pouco uso, e camada de apresentação quase vazia. Em oposição, as camadas de enlace e rede extremamente cheias, a ponto de ter que dividi-las em subcamadas.

Implementação Ruim: Devido à complexidade do modelo, as implementações OSI vieram repletas de bugs, e o mercado começou a associar "OSI" com "baixa qualidade".

Política Ruim: TCP/IP ficou associado a Unix, sendo adorado no meio acadêmico de 1980. O OSI, entretanto, parecia um padrão a ser "enfiado goela abaixo" pelos burocratas europeus.

16.3 Uma crítica ao modelo de referência TCP/IP

Ele não consegue descrever outras pilhas de protocolos (só TCP/IP). Coloca os níveis de enlace e físico na mesma camada (Host/Rede). Isso faz com que o modelo TCP/IP não seja o melhor para estruturar novas redes.

16.4 Modelo Híbrido

Está sugerido em [TANEMBAUM] um modelo híbrido, com 5 camadas, que retira o excesso do modelo OSI e melhora o modelo TCP/IP.

Modelo híbrido

5	Aplicação
4	Transporte
3	Rede
2	Enlace
1	Físico