FACULDADES INTEGRADAS FACVEST
Curso de Ciência da Computação

APOSTILA DE REDES DE COMPUTADORES

APOSTILA DE REDES DE COMPUTADORES

Curso: Ciências da Computação

Professora: Madalena Pereira da Silva

Disciplina: Redes de Computadores

Turma: 6ª Fase – Período: Noturno – Ano: 2003

SUMÁRIO

1. INTRODUÇÃO A REDES DE COMPUTADORES

1.1. EVOLUÇÃO DOS SISTEMAS DE COMPUTAÇÃO

Nos últimos três séculos existiram o domínio de apenas uma tecnologia. O século XVIII foi à época dos grandes sistemas mecânicos, característica da Revolução Industrial. O Século XIX foi à era das máquinas a vapor e no século XX as conquistas tecnológicas voltaram-se para o campo da informação. Dentro outros desenvolvimentos destacam-se a instalação das redes de telefonia em escala mundial, a invenção do rádio e da televisão, o surgimento da indústria de computadores e lançamento dos satélites de comunicação.

Em função do crescente progresso tecnológico, as áreas citadas estão convergindo rapidamente e a cada dia nos deparamos com a evolução das tecnologias difundidas ao longo dos séculos. Atualmente, organizações com centenas de escritórios dispersos por uma extensa área geográfica, por intermédio do apertar de um botão podem analisar e controlar remotamente as suas filiais.

Inicialmente, os sistemas computacionais eram acondicionados em uma grande sala com paredes de vidro, onde os visitantes impressionados podiam contemplar o cérebro daquela maravilha eletrônica. Na época, uma Universidade ou uma empresa de médio porte possuíam um ou dois computadores, enquanto as grandes instituições possuíam algumas dezenas. Era pura fixação científica a idéia de que, em apenas alguns anos, haveria milhões de computadores com chips miniaturizados.

A fusão dos computadores e das comunicações foi influenciada através da forma com que os sistemas computacionais eram organizados. Está totalmente ultrapassado o conceito de um “centro de computadores”, como uma sala para onde os usuários levam os programas a serem processados. O velho modelo de um computador atendendo a todas as necessidades computacionais da organização foi substituído pelas redes de computadores.

1.2. HISTÓRICO DAS REDES DE COMPUTADORES

Na década de 50 ocorreu a evolução dos equipamentos para a realização do processamento e armazenamento de informações; evolução da microeletrônica e da informática; utilização de sistemas centralizados. Nesta década as máquinas ainda eram de grande porte; existia uma complexidade no processamento das informações, pois os

usuários enfileiravam-se para submeter suas leitoras de cartões ou fitas magnéticas que eram processados em lote. Não havia nenhuma forma de interação direta entre usuários e máquina.

Na década de 60 os sistemas eram compartilhados; existia um compartilhamento do tempo de processamento do computador central. Os usuários tinham acesso ao computador central por meio de linhas de comunicação. Em 69 houve a integração de computadores surgindo a primeira rede: a ARPANET. Rede mundial que interligava quatro universidades americanas. Inúmeras outras redes de caráter militar e científico surgiriam nos anos seguintes.

Na década de 70 surgiram os microcomputadores[1] com maior capacidade de processamento que os computadores até então desenvolvidos. Os microcomputadores ofereciam compartilhamento de recursos (discos, impressoras etc); trabalhavam com maior velocidade na transmissão de dados e com eles, houve uma maior facilidade para estender as redes.

1.3. CONCEITUAÇÃO E TERMINOLOGIAS

Nas **redes de computadores** os trabalhos são realizados por uma série de computadores autônomos interconectados. Dois computadores estão interconectados quando podem trocar informações. Quando exigimos que os computadores sejam autônomos, desejamos excluir os sistemas em que haja uma nítida relação mestre/escravo. Se um computador tiver o poder de iniciar, encerrar ou controlar outro computador haverá uma clara indicação de que não há autonomia entre eles. Um sistema com uma unidade de controle e muitos escravos não é uma rede, assim como não o é um grande computador com grandes terminais e impressoras remotas.

As **redes de computadores** são formadas por módulos processadores[2] capazes de trocar informações e compartilhar recursos físicos e lógicos e são interligados por um sistema de comunicação[3].

1.4. IMPORTÂNCIA DAS REDES DE COMPUTADORES

[1] Em 1976 foi lançado no mercado o primeiro microcomputador: APLLE I.
[2] Os módulos processadores são os componentes que formam uma rede: computadores, *hub*, *switch*, roteadores entre outros.
[3] Os sistemas de comunicação são constituídos pelo arranjo topológico, pelos meios físicos de transmissão e pelos protocolos.

6.2.1. Redes corporativas

- Compartilhamento de recursos;
- Confiabilidade (segurança, sistema nunca para de funcionar);
- Custo reduzido;
- Uso de modelos cliente / servidor;
- Escalabilidade (eficiência no processamento de grandes conjuntos de dados ou no ajuste de performance, quando mais processadores são disponibilizados para a aplicação);
- Acesso a informações remotas.

6.2.2. Redes Pessoais

- Acesso a informações remotas;
- Comunicação pessoa a pessoa;
- Diversão e interatividade.

2. ARQUITETURAS DE REDES DE COMPUTADORES

A forma como os equipamentos são interligados e interagem entre si é chamada de Arquitetura de redes. Existem diversas arquiteturas tanto de *hardware* como de *software*, as quais podem ser definidas pela forma de conexão física dos equipamentos, ou pelos componentes de *Software* ou programas que utilizam. Em nível de conexão física, temos definições de arquiteturas conforme segue: ponto a ponto; multiponto e topologia mista.

2.1. PONTO A PONTO

É a forma mais comum de conexão, na qual temos dois pontos (receptor e transmissor) interligando e trocando informações diretamente. Neste tipo de ligação, não existe o compartilhamento do meio com vários usuários, e sim dois pontos comunicando-se entre si [figura 1].

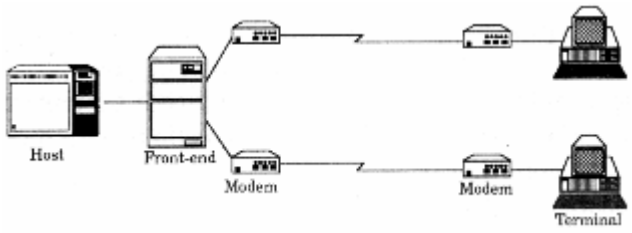


Figura 1 – Exemplo de Arquitetura Ponto a Ponto

2.2. MULTIPONTO OU PONTO-MULTIPONTO

Neste tipo de arquitetura um ponto central envia informações para vários outros pontos, utilizando um mesmo meio e fazendo derivações ao longo do meio. Esse tipo de ligação pode existir numa arquitetura de redes WAN (*Wide Area Network*) em que a informação parte de um computador central por um único meio de transmissão e é distribuída para vários pontos por meio de endereços lógicos diferentes [figura 2].

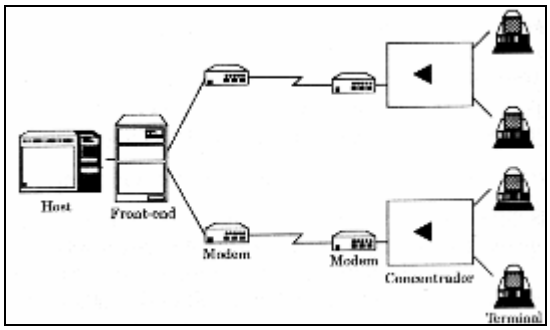


Figura 2 – Exemplo de Arquitetura Multi Ponto

2.3. TOPOLOGIA MISTA

As **Topologias Mistas** são tipos de redes que utilizam características dos dois tipos básicos de redes, a ligação ponto-a-ponto e multiponto, para obter redes mais complexas e com maiores recursos. As estruturas mistas podem ser do tipo Estrela, Barra, Anel, Hierárquica e Distribuídas. No entanto descreveremos apenas as três primeiras topologias.

2.4. BARRAMENTO

A topologia em barra [figura 3] se caracteriza pela ligação de estações (nós) ao mesmo meio de transmissão. Neste caso é utilizado um cabo disposto de forma linear ao qual são conectadas as estações e por ele todos os dados da rede trafegam. Ao contrário das outras topologias que são configurações ponto a ponto (isto é, cada enlace físico de transmissão conecta apenas dois dispositivos), a topologia em barra tem uma configuração multiponto (isto é, mais do que dois dispositivos estão conectados ao meio de comunicação).

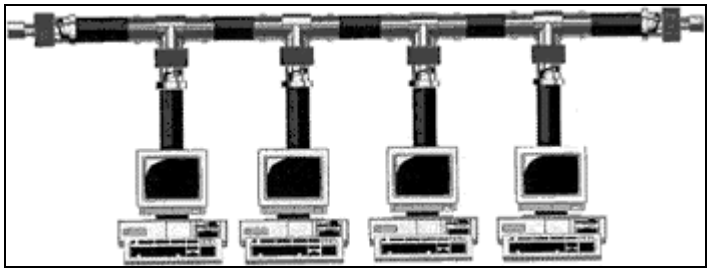


Figura 3 - Exemplo de Topologia em Barra

Nas redes em barra comum cada nó conectado à barra pode ouvir todas as informações transmitidas. A comunicação ocorre da seguinte forma:

- Cada computador da rede possui um endereço único (identificador único e individual para cada equipamento conectado a uma rede);
- Quando um computador necessita comunicar-se com outro computador da rede prepara a mensagem ou o dado a ser enviado e coloca o sinal eletrônico correspondente no cabeamento da rede. Um dos componentes desse sinal é o endereço do computador de destino;
- O sinal é disponibilizado para todos os computadores da rede, mas, somente aquele que possui o endereço de destino especificado na mensagem ou dado poderá lê-lo, interpretando seu conteúdo.Quando o sinal é colocado no

barramento da rede os outros computadores sabem que não devem enviar sinais. Para isso o sinal deve ficar num movimento contínuo de “bate e volta” até que a estação de destino receba os dados. Depois o sinal deve ser absorvido para ser descartado. Essa é a função de uma peça especial chamada terminador, que deve ser colocado em cada ponta do barramento.

Nessa topologia, a comunicação entre os computadores pode ser interrompida se houver uma falha no cabeamento entre um computador e outro ou se um dos terminadores estiver desconectado do barramento. Se isso ocorrer, os computadores da rede estarão *stand-alone*[4] e nenhuma função de rede estará disponível. Resolvido o problema à comunicação volta à normalidade.

2.5. ESTRELA

A arquitetura em estrela [figura 4] é aquela em que todos os pontos e equipamentos da rede convergem para um ponto central. Neste tipo de topologia cada nó é interligado a um nó central (*computador de grande porte, hub, switch, roteador*), através do qual todas as mensagens devem passar. Tal nó age, assim, como centro de controle da rede, interligando os demais nós (estações) que usualmente podem se comunicar apenas com um outro nó de cada vez. Isto não impede que haja comunicações simultâneas, desde que as estações envolvidas sejam diferentes.

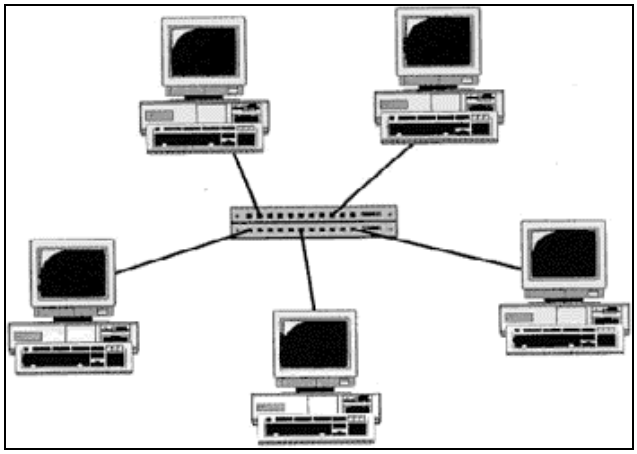


Figura 4 – Exemplo de Topologia em Estrela

[4] Quando os computadores não estão conectados em rede diz-se que estão em *stand-alone*.

Várias redes em estrela operam em configurações onde o nó central tem tanto a função de gerência de comunicação como facilidades de processamento de dados. Em outras redes o nó central tem como única função o gerenciamento das comunicações.

A configuração em estrela é em alguns aspectos parecida com os sistemas de barra comum centralizados os requisitos de comunicação são, entretanto menos limitados, uma vez que a estrela permite mais de uma comunicação simultânea. A confiabilidade das ligações também é maior, pois uma falha na barra de comunicação em uma estrela só colocaria a estação escrava correspondente fora de operação. Por outro lado, o nó central é mais complexo, uma vez que deve controlar vários caminhos de comunicação concorrentemente.

Confiabilidade é um problema nas redes em estrela. Falhas em um nó escravo apresentam um problema mínimo de confiabilidade, uma vez que o restante da rede ainda continua em funcionamento. Falhas no nó central, por outro lado, podem ocasionar a parada total do sistema. Redundâncias podem ser acrescentadas, porém a dificuldade de custo em tornar o nó central confiável pode mais do que mascarar o benefício obtido com a simplicidade das interfaces exigidas pelas estações secundárias.

Outro problema da rede em estrela é relativo a modularidade. A configuração pode ser expandida até um certo limite imposto pelo nó central; como por exemplo, o número total de nós que podem ser servidos.

O desempenho obtido em uma rede em estrela depende da quantidade de tempo requerido pelo nó central para processar e encaminhar uma mensagem, e da carga de tráfego na conexão, isto é, o desempenho é limitado pela capacidade de processamento do nó central. Um crescimento modular visando o aumento do desempenho torna-se a partir de certo ponto impossível, tendo como única solução à substituição do nó central.

Importante notar que o funcionamento da topologia em estrela depende do periférico concentrador utilizado, se for um *hub* ou um *switch*.

6.2.3. Se for utilizado um *hub*:

- A topologia fisicamente será em estrela [Figura 4], porém logicamente ela continua sendo uma rede de topologia linear. O hub é um periférico que repete para todas as suas portas os pacotes que chegam, assim como ocorre na topologia linear, ou seja, ao receber o dado de uma porta, o *hub* faz o *broadcasting* para todas simultaneamente.
- Em outras palavras, se a estação 1 enviar um pacote de dados para a estação 2, todas as demais estações recebem esse mesmo pacote. Portanto, continua

havendo problemas de colisão e disputa para ver qual estação utilizará o meio físico.

6.2.4. Se utilizar um *switch*:

- A rede será tanto fisicamente quanto logicamente em estrela [Figura 4]. Este periférico tem a capacidade de analisar o cabeçalho de endereçamento dos pacotes de dados, enviando os dados diretamente ao destino, sem replicá-lo desnecessariamente para todas as suas portas.
- Desta forma, se a estação 1 enviar um pacote de dados para a estação 2, somente esta recebe o pacote de dados. Isso faz com que a rede torne-se mais segura e muito mais rápida, pois praticamente elimina problemas de colisão. Além disso, duas ou mais transmissões podem ser efetuadas simultaneamente, desde que tenham origem e destinos diferentes, o que não é possível quando utilizamos topologia linear ou topologia em estrela com *hub*.

2.6. ANEL

Numa rede em anel [Figura 5] os dados circulam num cabo que conecta todas as estações da rede num formato circular. Os dados passam por todos os nós da rede, até encontrar o nó como endereço destino dos dados. O fluxo dos dados ao longo do anel é unidirecional, ou seja, ele é transmitido e caminha em apenas um sentido.

O meio pode ser um anel [Figura 5], ou então o anel pode ser simulado dentro de um *hub* central que concentra as conexões.

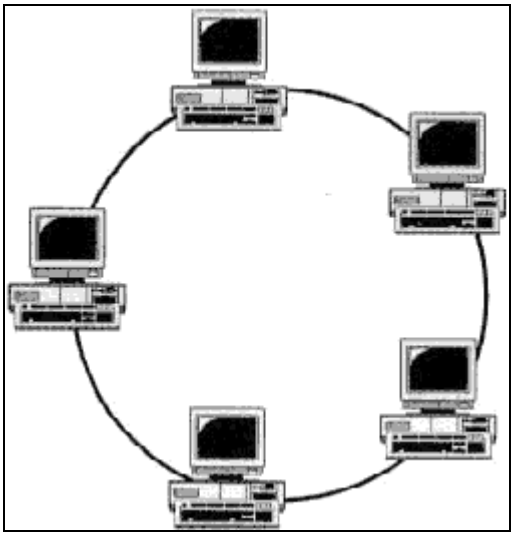


Figura 5 – Exemplo de Topologia em Estrela

Os dados, para alcançar o seu destino, devem obrigatoriamente passar pelos nós intermediários, os quais lêem o endereço. Caso o endereço não seja o do nó, ele repassa para o próximo nó. Caso um nó da rede pare, a transmissão dos dados pára, interrompendo o funcionamento da rede.

Caso um nó da rede pare de funcionar, a transmissão dos dados no anel também é interrompida, afetando toda a rede. Para evitar estes problemas, as estações podem ser conectadas num *hub* concentrador que simula internamente a ele o anel de conexão e a unidirecionalidade da arquitetura, e mantém a continuidade do anel no caso de falhas.

Na arquitetura de rede em anel, todos os nós estão interconectados, não existindo um nó central. O funcionamento global depende de cada nó e para acrescentar um novo nó (ponto ou computador) na rede, todo o seu funcionamento se altera em nível de endereçamento.

Embora as configurações mais usuais nas arquiteturas em redes em anel sejam unidirecionais, alguns autores publicaram que as redes em anel são capazes de transmitir e receber dados em qualquer direção. As configurações mais usuais, no entanto, são unidirecionais o projeto dos repetidores mais simples e tornar menos sofisticados os protocolos de comunicação que asseguram a entrega da mensagem corretamente e em seqüência ao destino, pois sendo unidirecionais evita o problema do roteamento. Os repetidores são em geral projetados de forma a transmitir e receber dados simultaneamente, diminuindo assim o retardo de transmissão e assegurando um funcionamento do tipo "*full-duplex*[5]".

A topologia em anel requer que cada nó seja capaz de remover seletivamente mensagens da rede ou passá-las à frente para o próximo nó. Isto vai requerer um repetidor ativo em cada nó e a rede não poderá ser mais confiável do que estes repetidores. Uma quebra em qualquer dos enlaces entre os repetidores irá parar toda a rede até que problema seja isolado e um novo cabo instalado. Falhas no repetidor ativo também podem causar a parada total do sistema.

Por serem geralmente unidirecionais, as redes com esta topologia são ideais para utilização de fibra ótica. Existem algumas redes que combinam seções de diferentes meios de transmissão sem nenhum problema, como é o caso do ANEL DE CAMBRIDGE.

[5] Os dados podem ser enviados e recebidos ao mesmo tempo, em ambos os sentidos num mesmo canal físico, porém por meio de dois canais simultâneos.

3. CLASSIFICAÇÃO DAS REDES DE COMPUTADORES

Segundo a abrangência geográfica as redes de computadores podem ser classificadas em: redes locais, redes metropolitanas e redes remotas.

3.1. REDES LOCAIS (*LOCAL AREA NETWORK - LANS*)

São redes privadas contidas em prédio ou em campus universitário que tem uma pequena extensão. São amplamente utilizadas para conectar computadores localizados numa mesma sala, num mesmo prédio ou num campus. Surgiram para viabilizar a troca de informações e o compartilhamento de informações e dispositivos periféricos (recursos físicos e lógicos), mantendo a independência das estações tanto no processamento quanto no armazenamento de dados, permitindo a integração em ambientes de trabalho cooperativo. Possuem características que as diferenciam das demais:

- Abrangência: faz a interconexão de equipamentos em uma pequena região, onde utilizando *hub* e/ou *switch* podem atingir distâncias que variam de 100m e 5Km.
- Tecnologia de transmissão: quase sempre consiste em um cabo ao qual todas as máquinas são conectadas;
- Velocidade: operam com altas taxas de transmissão, com variações de 10 a 100 Mbps (Lans tradicionais) podendo atingir alguns Gbps;
- Taxas de Erros: trabalham com baixas taxas de erros: 10^{-8} a 10^{-11} bits;
- Retardo: possuem baixo retardo (microssegundos / milissegundos).
- Topologias: geralmente são do tipo barra, estrela e anel.

3.2. REDES METROPOLITANAS (*METROPOLITAN AREA NETWORK - MANS*)

Uma MAN é uma versão ampliada de uma LAN, pois os tipos de redes utilizam tecnologias semelhantes. Uma MAN pode ser privada ou pública e pode abranger um grupo de escritórios vizinhos ou uma cidade inteira. Uma rede metropolitana pode ser constituída por uma única sub-rede ou por várias sub-redes ou redes independentes interligadas por meio de um canal de comunicação de alta velocidade, usualmente um *backbone* de cabo óptico. As principais características de uma MAN são:

- Abrangência: pode abranger uma cidade ou um conjunto de cidades próximas, num raio de aproximadamente 100km, realizando ligações entre instituições de uma metrópole.

- Tecnologias de transmissão: operam sobre um canal de comunicação de alta velocidade, geralmente um *backbone* de cabo óptico, ondas de rádio etc.
- Velocidade: como a banda total da MAN é dividida pelos diversos usuários, embora a velocidade total da MAN seja bem elevada, as velocidades para esses usuários são frações da velocidade total.
- Topologia: normalmente do tipo ponto a ponto.

3.3. REDES REMOTAS (*WIDE AREA NETWORK- WANS*)

Uma rede remota também chamada de rede geograficamente distribuída abrange uma ampla área geográfica, com freqüência um país ou continente. Contém um conjunto de máquinas conectadas por uma sub-rede[6] de comunicação. As WANs surgiram da necessidade de se compartilhar recursos especializados por uma maior comunidade de usuários geograficamente dispersos. Por terem um custo de comunicação bastante elevado (circuitos para satélites e enlaces de microondas), tais redes são, em geral, públicas, isto é, o sistema de comunicação chamado sub-rede de comunicação é mantido gerenciado e de propriedade pública. Em face de várias considerações em relação ao custo, a interligação entre os diversos módulos processadores nessa rede determinará a utilização de um arranjo topológico específico e diferente daqueles utilizados em redes locais. A constituição de WANs exige o uso de *bridges* e/ou *routers*, equipamentos capazes de interligar, filtrar tráfego e estabelecer rotas de acesso entre as redes envolvidas na comunicação.

As principais características de uma WAN são:

- Abrangência: abrange uma ampla área geográfica, país ou continente;
- Tecnologias de Transmissão: a forma de comunicação ocorre por meio de canais de comunicação alugados que operam por fibras óticas, satélites, microondas entre outras.
- Velocidade: os canais de comunicação operam numa velocidade que varia entre 1200 a 622Mps, expandindo-se a 2Gbps e 10Gbps sobre ATM. Mas isto irá depender do meio e da tecnologia utilizados, fornecidos pelas empresas de telecomunicações.
- Topologia: geralmente é do tipo ponto-a-ponto.

[6] A função da sub-rede é transportar mensagens de um *host* para outro.

4. MEIOS FÍSICOS DE TRANSMISSÃO

A informação que circula numa rede de computadores é constituída por **sinais** físicos (elétricos, ópticos, microondas, etc) que se propagam num dado **meio físico de transmissão**. Alguns dos meios de transmissão mais utilizados na ligação de computadores são o **par trançado**, o **cabo coaxial**, a **fibra óptica**, as **ondas rádio** e de **satélite** e as **ondas infravermelhas**.

4.1. CABO COAXIAL

Os cabos coaxiais [figura 6] são cabos constituídos de 4 camadas: um condutor interno, o fio de cobre que transmite os dados; uma camada isolante de plástico, chamada de dielétrico que envolve o cabo interno; uma malha de metal que protege as duas camadas internas e, finalmente, uma nova camada de revestimento, chamada de jaqueta.

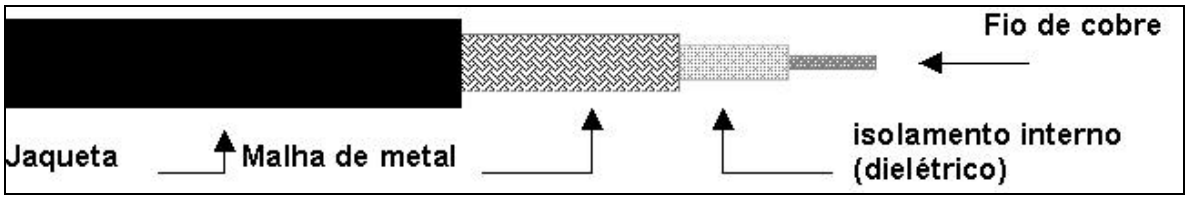


Figura 6 - Cabo Coaxial

Se você envolver um fio condutor com uma segunda camada de material condutor, a camada externa protegerá a primeira da interferência externa. Devido a esta blindagem, os cabos coaxiais (apesar de ligeiramente mais caros que os de par trançado) podem transmitir dados a distâncias maiores, sem que haja degradação do sinal. Existem 4 tipos diferentes de cabos coaxiais, chamados de **10Base5**, **10Base2**, **RG-59/U** e **RG-62/U**.

O cabo **10Base5** é um tipo mais antigo, usado geralmente em redes baseadas em mainframes. Este cabo é muito grosso, tem cerca de 0.4 polegadas, ou quase 1 cm de diâmetro e por isso é muito caro e difícil de instalar devido à baixa flexibilidade. Outro tipo de cabo coaxial pouco usado atualmente é o **RG62/U**, usado em redes *Arcnet*. Temos também o cabo **RG-59/U**, usado na fiação de antenas de TV.

Além da baixa flexibilidade e alto custo, os cabos 10Base5 exigem uma topologia de rede bem mais cara e complicada. Temos o cabo coaxial 10base5 numa posição central, como um backbone, sendo as estações conectadas usando um segundo dispositivo, chamado transceptor, que atua como um meio de ligação entre elas e o cabo principal.

Os transceptores perfuram o cabo 10Base5, alcançando o cabo central que transmite os dados, sendo por isso também chamados de “derivadores vampiros”. Os transceptores são conectados aos encaixes AUI das placas de rede (um tipo de encaixe parecido com a porta de *joystick* da placa de som, encontrado principalmente em placas antigas) através de um cabo mais fino, chamado cabo transceptor. Além de antiquada, esta arquitetura é muito cara, tanto em nível de cabos e equipamentos, quanto em termos de mão de obra.

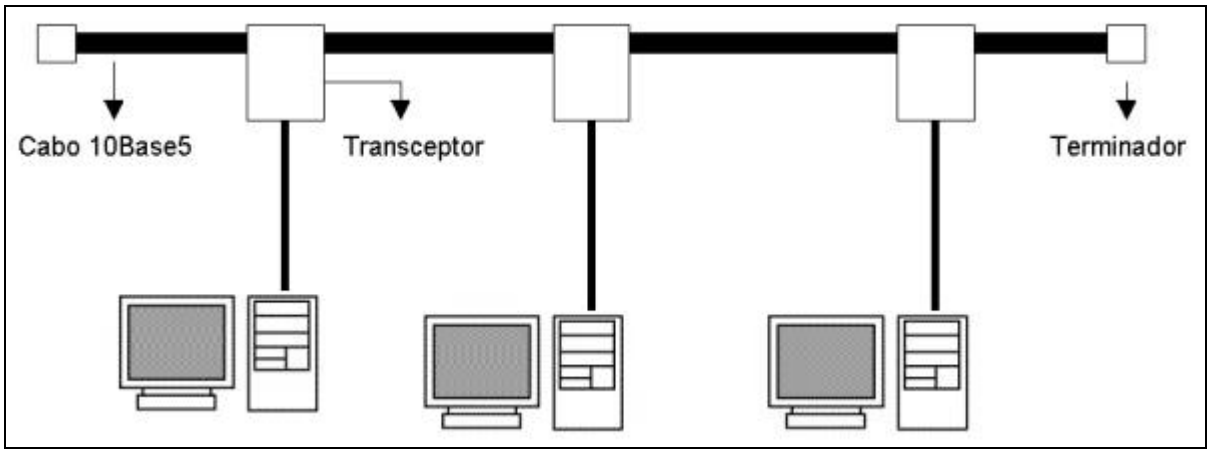


Figura 7 - Exemplo utilização de Transceptor

Os cabos 10Base5 foram praticamente os únicos utilizados em redes de *mainframes* no inicio da década de 80, mas sua popularidade foi diminuindo com o passar do tempo por motivos óbvios.Atualmente você só se deparará com este tipo de cabo em instalações bem antigas ou, quem sabe, em museus.

Finalmente, os cabos **10Base2**, também chamados de cabos coaxiais finos, ou cabos *Thinnet*, são os cabos coaxiais usados atualmente em redes *Ethernet*, e por isso, são os cabos que você receberá quando pedir por “cabos coaxiais de rede”. Seu diâmetro é de apenas 0.18 polegadas, cerca de 4.7 milímetros, o que os torna razoavelmente flexíveis.

Os cabos 10Base2 são bem parecidos com os cabos usados em instalações de antenas de TV. A diferença é que, enquanto os cabos RG-59/U usados nas fiações de antena possuem impedância de 75 ohms, os cabos 10Base2 possuem impedância de apenas 50 ohms. Por isso, apesar dos cabos serem parecidos, nunca tente usar cabos de antena em redes de micros. É fácil diferenciar os dois tipos de cabo, pois os de redes são pretos enquanto os para antenas são brancos.

O valor “10” na sigla 10Base2 significa que os cabos podem transmitir dados a uma velocidade de até 10 megabits por segundo, “Base” significa “banda base” e se refere à distância máxima para que o sinal pode percorrer através do cabo, no caso o valor “2” que teoricamente significaria 200 metros, mas que na prática é apenas um arredondamento, pois nos cabos 10Base2 a distância máxima utilizável é de 185 metros.

Usando cabos 10Base2, o comprimento do cabo que liga um micro ao outro deve ser de no mínimo 50 centímetros, e o comprimento total do cabo (do primeiro ao último micro) não pode superar os 185 metros. É permitido ligar até 30 micros no mesmo cabo, pois acima disso, o grande número de colisões de pacotes irá prejudicar o desempenho da rede, chegando a ponto de praticamente impedir a comunicação entre os micros em casos extremos.

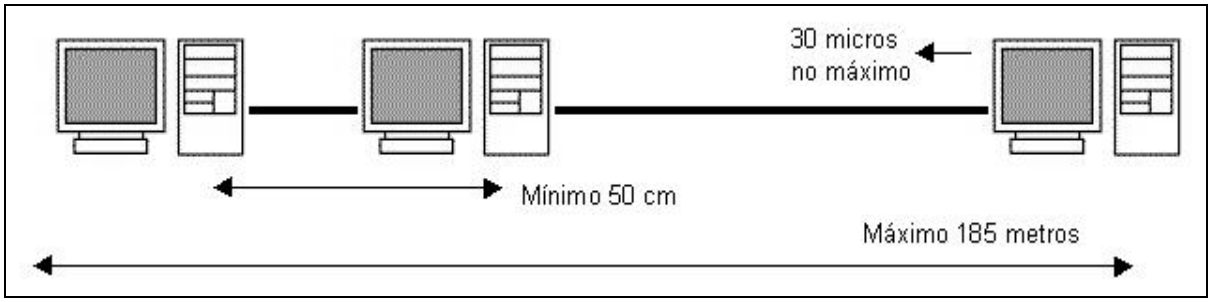


Figura 8 - Exemplo de Utilização do Cabo 10Base2

Conectamos o cabo coaxial fino à placa de rede usando conectores BCN [figura 9], que por sua vez são ligados a conectores T [figura 10] ligados na placa de rede. Usando cabos coaxiais os micros são ligados uns aos outros, com um cabo em cada ponta do conector T.

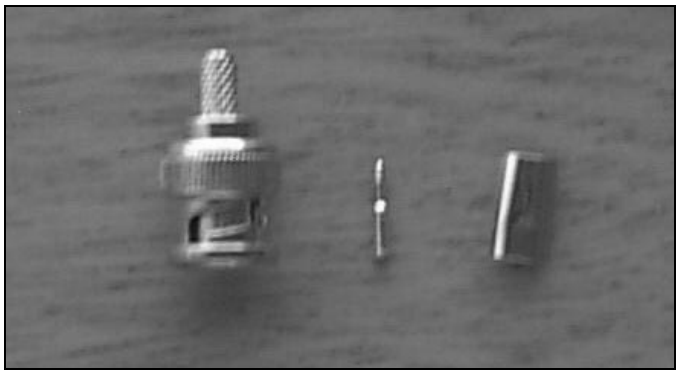


Figura 9 - Conector BCN desmontado

Figura 10 - Conector T na Placa de Rede

São necessários dois terminadores [figura 11] para fechar o circuito. Os terminadores são encaixados diretamente nos conectores T do primeiro e último micro da rede. Pelo menos um dos terminadores, deverá ser aterrado.

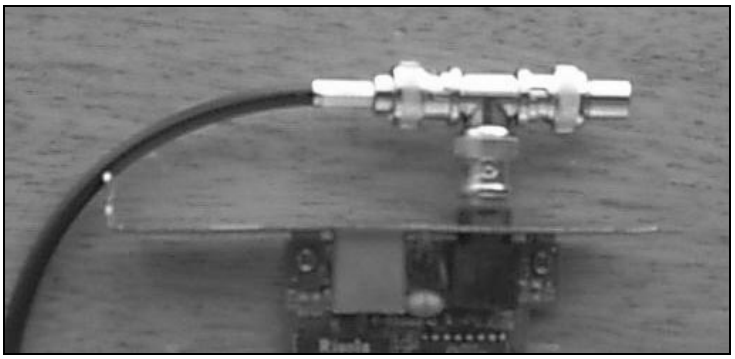


Figura 11 - Exemplo de Terminador

Se você não instalar um terminador em cada ponta da rede, quando os sinais chegarem às pontas do cabo, retornarão, embora um pouco mais fracos, formando os chamados pacotes sombra. Estes pacotes atrapalham o tráfego e corrompem pacotes bons que estejam trafegando, praticamente inutilizando a rede.

Em redes *Ethernet* os terminadores devem ter impedância de 50 ohms (a mesma dos cabos), valor que geralmente vem estampado na ponta do terminador.

4.2. CABO DE PAR TRANÇADO

O cabo de par trançado vem substituindo os cabos coaxiais desde o início da década de 90. Hoje em dia é muito raro alguém ainda utilizar cabos coaxiais em novas instalações de rede, o mais comum é apenas reparar ou expandir redes que já existem. Mais adiante teremos um comparativo entre os dois tipos de cabos.

O nome “par trançado” é muito conveniente, pois estes cabos são constituídos justamente por 4 pares de cabos entrelaçados. Veja que os cabos coaxiais usam uma malha de metal que protege o cabo de dados contra interferências externas; os cabos de par trançado por sua vez usam um tipo de proteção mais sutil: o entrelaçamento dos cabos cria um campo eletromagnético que oferece uma razoável proteção contra interferências externas.

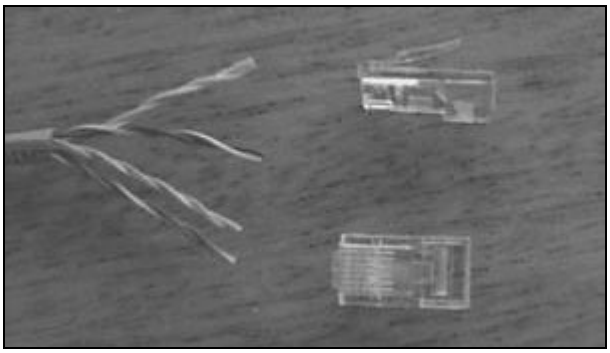


Figura 12 - Cabo de Par trançado

Além dos cabos sem blindagem (como o da foto) conhecidos como **UTP** (*Unshielded Twisted Pair*), existem os cabos blindados conhecidos como **STP** (*Shielded Twisted Pair*). A única diferença entre eles é que os cabos blindados além de contarem com a proteção do entrelaçamento dos fios, possuem uma blindagem externa (assim como os cabos coaxiais), sendo mais adequados a ambientes com fortes fontes de interferências, como grandes motores elétricos e estações de rádio que estejam muito próximas. Outras fontes menores de interferências são as lâmpadas fluorescentes (principalmente lâmpadas cansadas que ficam piscando), cabos elétricos quando colocados lado a lado com os cabos de rede e mesmo telefones celulares muito próximos dos cabos.

Quanto maior for o nível de interferência, menor será o desempenho da rede, menor será à distância que poderá ser usada entre os micros e mais vantajosa será a instalação de cabos blindados. Em ambientes normais, porém os cabos sem blindagem costumam funcionar bem.

Existem no total, 5 categorias de cabos de par trançado. Em todas as categorias a distância máxima permitida é de 100 metros. O que muda é a taxa máxima de transferência de dados e o nível de imunidade a interferências.

Categoria 1: este tipo de cabo foi muito usado em instalações telefônicas antigas, porem não é mais utilizado.

Categoria 2: outro tipo de cabo obsoleto. Permite transmissão de dados a até 4 mbps.

Categoria 3: era o cabo de par trançado sem blindagem usado em redes até alguns anos atrás. Pode se estender por até 100 metros e permite transmissão de dados a até 10 Mbps. A diferença do cabo de categoria 3 para os obsoletos cabos de categoria 1 e 2 é o numero de tranças. Enquanto nos cabos 1 e 2 não existe um padrão definido, os cabos de categoria 3 (assim como os de categoria 4 e 5) possuem atualmente de 24 a 45 tranças por metro, sendo muito mais resistente a ruídos externos. Cada par de cabos tem um número diferente de tranças por metro, o que atenua as interferências entre os cabos. Praticamente não existe a possibilidade de dois pares de cabos terem exatamente a mesma disposição de tranças.

Categoria 4: por serem blindados, estes cabos já permitem transferências de dados a até 16 mbps, e são o requisito mínimo para redes *Token Ring* de 16 mbps, podendo ser usados também em redes *Ethernet* de 10 mbps no lugar dos cabos sem blindagem.

Categoria 5: este é o tipo de cabo de par trançado usado atualmente, que existe tanto em versão blindada quanto em versão sem blindagem, a mais comum. A grande vantagem sobre esta categoria de cabo sobre as anteriores é a taxa de transferência, até 100 mbps.

Os cabos de categoria 5 são praticamente os únicos que ainda podem ser encontrados à venda, mas em caso de dúvida basta checas as inscrições decalcadas no cabo, entre elas está a categoria do cabo, como na foto abaixo:

Figura 13 – Exemplo de Cabo Categoria 5

Independentemente da categoria, todos os cabos de par trançados usam o mesmo conector, chamados RJ-45. Este conector é parecido com os conectores de cabos telefônicos, mas é bem maior por acomodar mais fios. Uma ponta do cabo é ligada na placa de rede e a outra no *hub*.

Para crimpar o cabo, ou seja, para prender o cabo ao conector, usamos um alicate de crimpagem. Após retirar a capa protetora, você precisará tirar as tranças dos cabos e em seguida “arruma-los” na ordem correta para o tipo de cabo que estiver construindo (veremos logo adiante).

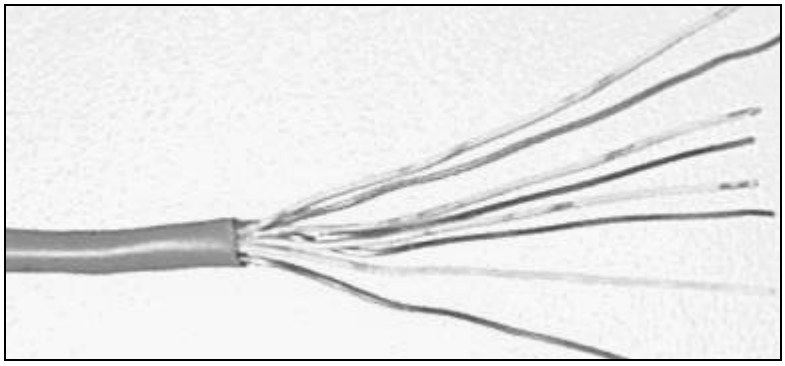


Figura 14 - Exemplo de Cabo Categoria 5 sem Capa Protetora

Veja que o que protege os cabos contra as interferências externas é são justamente as tranças. À parte destrançada que entra no conector é o ponto fraco do cabo, onde ele é mais vulnerável a todo tipo de interferência. Por isso, é recomendável deixar um espaço menor possível sem as tranças, se possível menos de 2,5 centímetros.

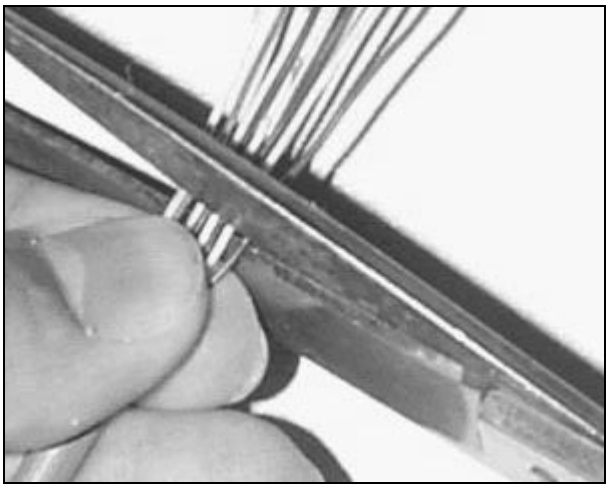


Figura 15 - Demonstração de Corte Cabo Categoria 5

Finalmente, basta colocar os fios dentro do conector e pressiona-lo usando um alicate de crimpagem.

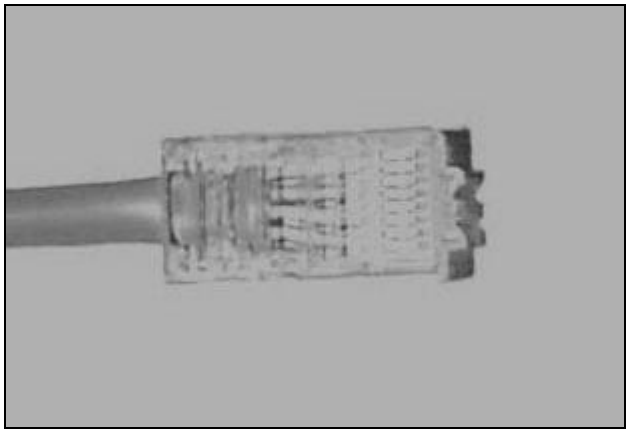
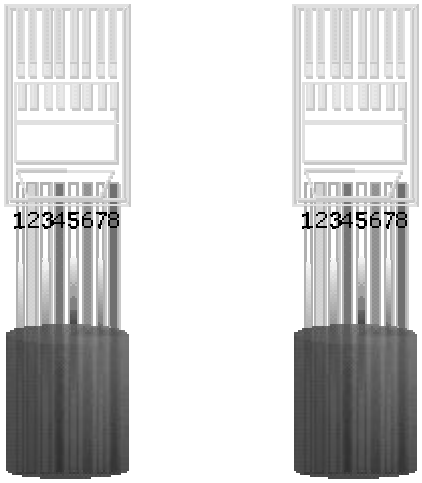


Figura 16 – Cabo de Par Trançado com Conector

Existe uma posição certa para os cabos dentro do conector. Note que cada um dos fios do cabo possui uma cor diferente. Metade tem uma cor sólida enquanto a outra metade tem uma cor mesclada com branco. Para criar um cabo destinado a conectar os micros ao hub, a seqüência tanto no conector do micro quanto no conector do hub será o seguinte:



lado 1 **lado 2**

1- Branco mesclado com Laranja

2- Laranja

3- Branco mesclado com verde

4- Azul

5- Branco mesclado com Azul

6- Verde

7- Branco mesclado com marrom

8- Marrom

É possível também criar um cabo para ligar diretamente dois micros, sem usar um hub, chamado de cabo *cross-over*. Logicamente este cabo só poderá ser usado caso a sua rede tenha apenas dois micros. Neste tipo de cabo a posição dos fios é diferente nos dois conectores, de um dos lados a pinagem é a mesma de um cabo de rede normal,

enquanto no outro a posição dos pares verde e laranja são trocados. Daí vem o nome *cross-over*, que significa, literalmente, cruzado na ponta:

Existe um teste simples para saber se o cabo foi crimpado corretamente: basta conectar o cabo à placa de rede do micro e ao *hub*. Tanto o LED da placa quanto o do hub deverão acender. Naturalmente, tanto o micro quanto o *hub* deverão estar ligados.

6.2.5. Par trançado x Coaxial

Cada uma destas categorias de cabos possui algumas vantagens e desvantagens. Na verdade, o coaxial possui bem mais desvantagens do que vantagens em relação aos cabos de par trançado, o que explica o fato dos cabos coaxiais virem tornando-se cada vez mais raros. Numa comparação direta entre os dois tipos de cabos teremos:

Distância máxima: o cabo coaxial permite uma distância máxima entre os pontos de até 185 metros, enquanto os cabos de par trançado permitem apenas 100 metros.

Resistência a interferências: Os cabos de par trançado sem blindagem são muito mais sensíveis a interferências do que os cabos coaxiais, mas os cabos blindados por sua vez apresentam uma resistência equivalente ou até superior.

Mau contato: Usando cabo coaxial, a tendência a ter problemas na rede é muito maior, pois este tipo de cabo costuma ser mais suscetível a mau contato do que os cabos de par trançado. Outra desvantagem é que usando o coaxial, quando temos problemas de mau contato no conector de uma das estações, a rede toda cai, pois as duas "metades" não contam com terminadores nas duas extremidades. Para complicar, você terá que checar PC por PC até encontrar o conector com problemas imagine fazer isso numa rede com 20 micros...

Usando par trançado, por outro lado, apenas o micro problemático ficaria isolado da rede, pois todos os PCs estão ligados ao hub e não uns aos outros. Este já é um argumento forte o suficiente para explicar a predominância das redes com cabo de par trançado.

Custo: Os cabos coaxiais são mais caros que os cabos de par trançado sem blindagem, mas normalmente são mais baratos que os cabos blindados. Por outro lado, usando cabos coaxiais você não precisará de um hub.

Velocidade máxima: Se você pretende montar uma rede que permita o tráfego de dados a 100 mbps, então a única opção é usar cabos de par trançado categoria 5, pois os cabos coaxiais são limitados apenas 10 mbps. Atualmente é complicado até mesmo encontrar placas de rede com conectores para cabo coaxial, pois apenas as placas

antigas, ISA de 10 megabits possuem os dois tipos de conector. As placas PCI 10/100 possuem apenas o conector para cabo de par trançado.

4.3. FIBRA ÓTICA

Ao contrário dos cabos coaxiais e de par trançado, que nada mais são do que fios de cobre que transportam sinais elétricos, a fibra óptica transmite luz e por isso é totalmente imune a qualquer tipo de interferência eletromagnética. Além disso, como os cabos são feitos de plástico e fibra de vidro (ao invés de metal), são resistentes à corrosão.

À distância permitida pela fibra também é bem maior: os cabos usados em redes permitem segmentos de até 1 KM, enquanto alguns tipos de cabos especiais podem conservar o sinal por até 5 KM (distâncias maiores são obtidas usando repetidores). Mesmo permitindo distâncias tão grandes, os cabos de fibra óptica permitem taxas de transferências de até 155 mbps, sendo especialmente úteis em ambientes que demandam uma grande transferência de dados. Como não soltam faíscas, os cabos de fibra óptica são mais seguros em ambientes onde existe perigo de incêndio ou explosões. E para completar, o sinal transmitido através dos cabos de fibra é mais difícil de interceptar, sendo os cabos mais seguros para transmissões sigilosas.

As desvantagens da fibra residem no alto custo tanto dos cabos quanto das placas de rede e instalação que é mais complicada e exige mais material. Por isso, normalmente usamos cabos de par trançados ou coaxiais para fazer a interligação local dos micros e um cabo de fibra óptica para servir como *backbone*, unindo duas ou mais redes ou mesmo unindo segmentos da mesma rede que estejam distantes.

O cabo de fibra óptica é formado por um núcleo extremamente fino de vidro, ou mesmo de um tipo especial de plástico. Uma nova cobertura de fibra de vidro, bem mais grossa envolve e protege o núcleo. Em seguida temos uma camada de plástico protetor chamado de *cladding*, uma nova camada de isolamento e finalmente uma capa externa chamada bainha.

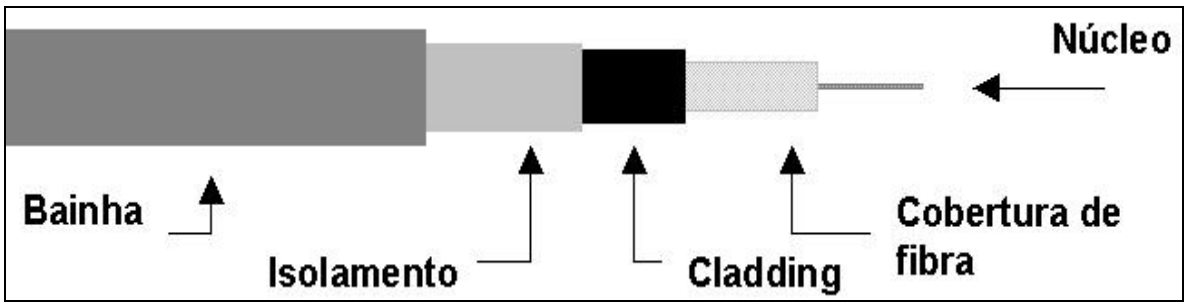


Figura 17 - Cabo de Fibra Óptica

A luz a ser transmitida pelo cabo é gerada por um LED, ou diodo emissor de luz. Chegando ao destino, o sinal luminoso é decodificado em sinais digitais por um segundo circuito chamado de foto-diodo. O conjunto dos dois circuitos é chamado de CODEC, abreviação de codificador/decodificador.

Existem dois tipos de cabos de fibra óptica, chamados de cabos **monomodo** e **multímodo**, ou simplesmente de modo simples e modo múltiplo. Enquanto o cabo de **modo simples** transmite apenas um sinal de luz, os cabos **multímodos** contêm vários sinais que se movem dentro do cabo. Ao contrário do que pode parecer à primeira vista, o cabo monomodo transmite mais rápido do que os cabos multimodo, pois neles a luz viaja em linha reta, fazendo o caminho mais curto. Nos cabos multimodo o sinal viaja batendo continuamente, mas paredes do cabo, tornando-se mais lento e perdendo a intensidade mais rapidamente.

Ao contrário do que se costuma pensar, os cabos de fibra óptica são bastante flexíveis e podem ser passados dentro de conduítes, sem problemas. Onde um cabo coaxial entra, pode ter certeza que um cabo de fibra também vai entrar. Não é necessário em absoluto que os cabos fiquem em linha reta, e devido às camadas de proteção, os cabos de fibra também apresentam uma boa resistência mecânica.

A velocidade de 155 mbps citada assim como a distância máxima dos cabos de fibra refere-se às tecnologias disponíveis para o uso em pequenas redes, cujas placas e demais componentes podem ser facilmente encontrados. Tecnologias mais caras e modernas podem atingir velocidades de transmissão na casa dos Terabits por segundo, atingindo distância de vários quilômetros. Aliás, a velocidade de transmissão nas fibras ópticas vem evoluindo bem mais rápido que os processadores, ou outros componentes, por isso é difícil encontrar material atualizado sobre as tecnologias mais recentes.

4.4. RADIODIFUSÃO

Nas Redes Sem Fio (*Wireless Networks)* os pacotes são transmitidos através do ar, em canais de freqüência de rádio ou infravermelho. É adequado tanto para ligações ponto a ponto quanto para ligações multiponto. É uma alternativa viável onde é difícil, ou mesmo impossível instalar cabos metálicos ou de fibra ótica.

É importante para comunicações entre computadores portáteis em um ambiente de rede local móvel. E também onde a confiabilidade do meio de transmissão é requisito indispensável.

Alguns métodos usados são: Multiplexação por Divisão do Espaço (SDM), Multiplexação por Divisão de Freqüência (FDM), Multiplexação por Divisão de Tempo (TDM).

O SDM pode ser realizado de duas formas: A primeira baseia-se na utilização de antenas direcionais, que emitem sinais de rádio de alta freqüência concentrados em feixes. A segunda é estruturar a rede em células, mas existe uma rápida diminuição da potência do sinal de rádio à medida que se propaga.

Normalmente utilizam freqüências altas em suas transmissões: 915 MHz, 2.4 GHz, 5.8 GHz.

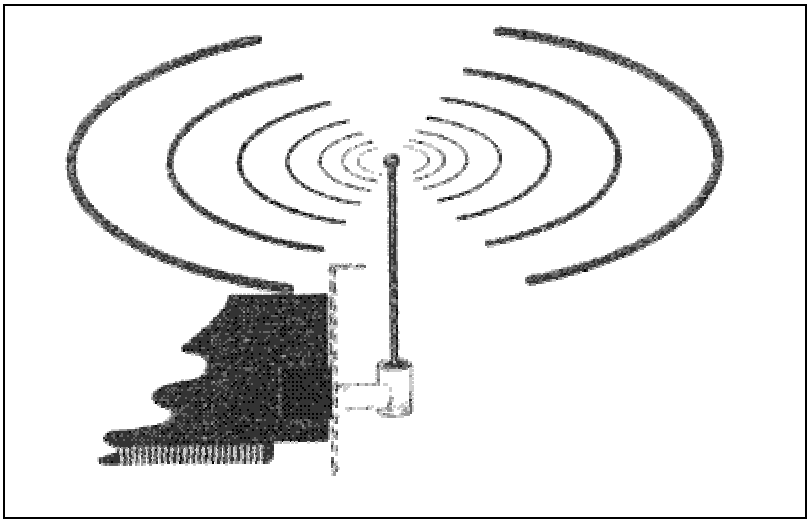


Figura 18 - Transmissão Wireless

Este meio de transmissão particularmente é utilizado nos telefones celulares, nos sistemas de captação de rádio nos automóveis, em redes locais, em redes metropolitanas.

4.5. SATÉLITE

O elemento satélite é o elemento comum de interligação das estações terrenas, atuando como estação repetidora. Devido a sua altitude, permite a transmissão de sinais diretamente entre duas estações, sem que existam necessariamente pontos

intermediários. O primeiro satélite de comunicações foi lançado no início dos anos 60. A comunicação através de satélites é em certas condições a única alternativa possível para a transmissão de dados.

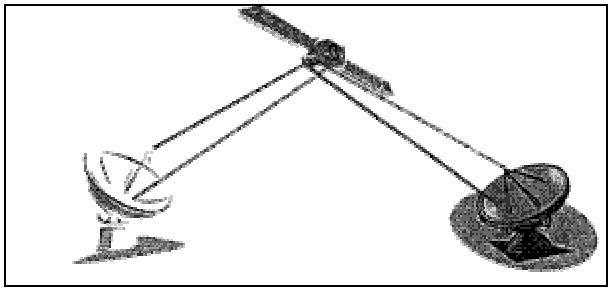


Figura 19 - Transmissão por Satélite

Sem dúvida, o maior fator motivador para a utilização de satélite como meio de transmissão, foi a inexistência de meios físicos entre localidades alvo da comunicação. Como os satélites podem cobrir praticamente quaisquer áreas do globo terrestre, são as melhores opções para atingir pontos de difícil acesso.

O custo dos meios de transmissão analógicos também foi um fator motivador do usa da tecnologia satélite, tendo, todavia, deixado de ser, nos últimos anos.

6.2.6. Características da Comunicação Via Satélite

- Disponibilidade e Qualidade: altas disponibilidade e qualidade são as principais características da transmissão via satélite.
- Flexibilidade na Implantação: outra característica marcante é a flexibilidade no que tange a instalação e mudança de pontos, que podem ser efetuadas sem necessidade da existência de rede telefônica.
- Atraso: uma característica não tão desejável, na transmissão via satélite, é o atraso de propagação.
- Custo: o custo de um canal independe da distância entre os pontos que integram a rede. A multiplexação dos dados permite a recuperação dos mesmos independentemente de sua localização geográfica. O custo da comunicação via satélite é compatível com o custo da comunicação analógica terrestre. Nos últimos anos o custo da transmissão digital caiu constantemente, bem abaixo da via satélite.

6.2.7. Componentes de um Sistema Satélite

Um sistema satélite é composto de um **Segmento Espacial** e um **Segmento Terrestre**. O Segmento Espacial é composto por um ou mais satélites e pelos equipamentos necessários às funções de suporte e operação dos satélites, tais como telemetria, rastreio, comando, controle e monitoração.

O subsistema satélite é uma estação repetidora de microondas, repetindo sinais sobre grandes distâncias. Inicialmente foram utilizados satélites de baixa órbita (LEOs), completando 1 volta no planeta a cada poucas horas. As estações terrenas eram de alto custo, pois tinham de mover-se, e o sistema interrompia a transmissão cada vez que o satélite desaparecia atrás do horizonte, retornado após surgir novamente no lado oposto. Para solucionar esses problemas, os satélites **geoestacionários**, ou **geossíncronos**.

Os satélites de comunicação utilizados para comunicação de dados e propagação de sinais de televisão são do tipo **geossíncrono**. As razões para o emprego desse tipo de satélite são bastante simples: as estações terrenas não precisam ser dotadas de antenas móveis e a área iluminada pelo satélite é constante, sem interrupção de sinal a cada órbita. O satélite de comunicação, em sua essência, é apenas um repetidor de sinal, captando os sinais transmitidos das estações terrenas, amplificando-os e retransmitindo-os para a Terra. A grande vantagem da comunicação através do satélite reside exatamente no fato de que cobre áreas enormes sem encontrar obstáculos geográficos além da própria atmosfera terrestre. Os sinais são transmitidos na forma de radiocomunicação microondas, tipicamente nas freqüências entre 1,5 Ghz (banda L) e 30 Ghz (banda Ka). A ampla área de cobertura permite comunicação entre pontos muito distantes um do outro, sem necessidade de pontos intermediários de retransmissão para compensar a curvatura da crosta terrestre, como no caso dos enlaces microondas terrestres.

6.2.8. Subsistemas de Um Satélite

- Comunicações; Telemetria; comando e rastreio;
- Controle de atitude; Propulsão; Energia;
- Controle térmico.

O subsistema que mais nos interessa é o de comunicações. È um repetidor ativo que recebe, converte a freqüência, amplifica e retransmite para a Terra os sinais recebidos. Os circuitos são denominados ***Transponders***. Cada *Transponder* é

responsável pela recepção e retransmissão de uma determinada banda de freqüência. Um satélite tem, tipicamente, de 20 a 40 *Transponders*.

6.2.9. Faixas de Freqüência

- Banda L – 1,5 a 2,5 GHz
- Banda C – 4,0 a 6,0 GHz
- Banda Ku – 11,0 a 14,0 GHz
- Banda Ka – 20,0 a 30,0 GHz

6.2.10. Os Satélites do SBTS

O SBTS, Sistema Brasileiro de Transmissão Por Satélite, de propriedade da Embratel, é composto por satélites com as seguintes características básicas:

- Giroestabilizados – atitude é mantida pela força centrípeta da metade que gira sobre o próprio eixo;
- Comprimento 7,1 metros;
- Diâmetro 2,16 metros;
- Massa: 1.140 Kg (lançamento) e 671 Kg (órbita);
- 36 transponders, 36 MHz, 36 dBW;
- Redundância TWT ¼;
- Freqüências 6,0 GHz (up) e 4,0 GHz (down);
- Energia: 982 W (inicial) e 799 W (final);
- Potência Irradiada (EIRP/canal): >= 34 dBW;
- Expectativa Vida Útil: 11 anos;
- 36.000 Km de altitude em 65W e 70W.

6.2.11. O Segmento Terrestre

O segmento terrestre é composto pelas estações terrenas de comunicação. Uma estação terrena é composta pelos seguintes componentes:

- Antena;
- Amplificadores de potência de transmissão (HPA);
- Amplificadores de recepção de baixo ruído (LNA e LNB);
- Equipamentos de comunicação (GCE).

6.2.12. Antenas

As antenas utilizadas pelas estações terrenas são do tipo parabólico, podendo variar a disposição do alimentador e refletores. Os diâmetros variam de 1,20 m (micro estação VSAT) até 14 m (estação tipo HUB). Os 3 tipos de antenas mais comuns são:

- *Cassegrain*: 1 sub-refletor hiperbólico e 1 refletor parabólico;
- Ponto Focal: refletor parabólico com alimentador no ponto focal;
- *Cassegrain Offset*: Alimentador s sub-refletor desalinhado do vértice e do foco.

A escolha do tipo das antenas é um dado de projeto. Normalmente as micro estações tipo VSAT utilizam antenas tipo *Offset*. Já estações tipo *hub*, de grandes dimensões, utilizam antenas tipo ponto focal ou *cassegrain*. Cada qual apresenta características diferenciadas de iluminação e absorção de ruído.

5. TÉCNICAS DE COMUTAÇÃO

5.1. REDES DE COMUTAÇÃO

As redes de comutação são constituídas por um conjunto de nós intermédios, com várias ligações entre si. Os nós intermédios funcionam como um conjunto que assegura que os dados chegam ao destino correto, o modo como a rede assegura a transferência dos dados pode obedecer a vários princípios, dada origem a diversos tipos de rede de comutação.

A função de comutação em uma rede de comunicação se refere à alocação dos recursos da rede para possibilitar a transmissão de dados pelos diversos dispositivos conectados.

Em uma rede (LAN, MAN, WAN) sempre existem recursos compartilhados: compartilhamento de enlace (enlaces ponto a ponto: através de técnicas TDM ou FDM e barramento).

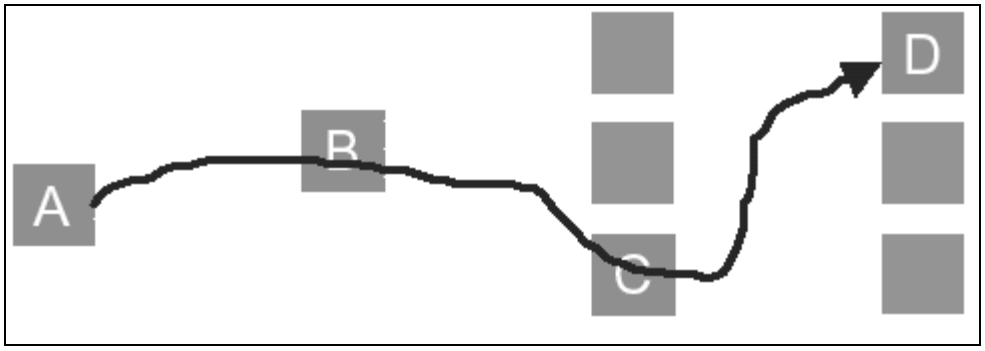


Figura 20 - Exemplo de Compartilhamento de Enlaces

Existem os seguintes tipos de comutação: comutação de circuitos; comutação de mensagem e comutação de pacotes. Os quais serão descritos a seguir.

5.2. COMUTAÇÃO DE CIRCUITOS

Trata-se de uma técnica na qual a rede assegura um circuito físico entre emissor e receptor. Por exemplo, quando um computador faz uma chamada telefônica, o elemento

de comutação[7] do sistema telefônico procura por um caminho físico de "cobre" (incluindo fibra e rádio) no trajeto que vai do telefone do emissor até o telefone do receptor. Esta técnica é chamada de comutação de circuitos. Ou ainda a comutação de circuitos ocorre quando um circuito dedicado (o circuito dedicado pode ser composto por enlaces físicos dedicados, canais de freqüência – FDM[8], canais de tempo – TDM[9]). É alocado para a comunicação entre duas entidades. A comunicação é constituída por três fases características:

- Estabelecimento do circuito físico: nesta fase a rede, mediante o endereço de destino une sucessivos circuitos desde o nó de origem até chegar ao nó de destino.
- Transferência de informações: depois de estabelecido o circuito físico através da rede os dois nós podem comunicar como se existisse uma linha dedicada a unir os dois.
- Liberação do circuito: por ordem de um dos nós o circuito é desativado, liberando os recursos ocupados na rede.

A comutação de circuitos físicos é uma técnica bastante rudimentar, usada, por exemplo, nas redes telefônicas publicas, tendo algumas características que interessa destacar:

- Existe um atraso inicial para o estabelecimento do circuito físico.
- Depois de estabelecido o circuito físico à transferência de dados é feita a uma taxa constante, sem atrasos assinaláveis nos nós intermédios.
- Quando dois nós estão em comunicação encontram-se totalmente inacessíveis para terceiros.
- A gestão dos recursos pela rede é muito deficiente: os recursos necessários à comunicação ficam reservados durante toda a comunicação, independentemente da utilização que tiverem.
- Sob taxas de utilização muita elevada a rede pode simplesmente recusar o estabelecimento do circuito por falta de recursos.

[7] Os comutadores são computadores ou equipamentos destinados a interligação entre duas ou mais linhas de transmissão.
[8] FDM – Multiplexação por Divisão de Freqüência: o espectro de freqüência é dividido entre os canais lógicos com cada usuário tendo posse exclusiva de alguma faixa de freqüência.
[9] TDM – Multiplexação por Divisão de Tempo: os usuários revezam e cada um obtém a largura de banda inteira por um determinado período de tempo.

Num sistema telefônico a comutação do circuito ocorre da seguinte forma: estabelecimento de conexão; transferência de informações; liberação do circuito. Observe que o caminho permanece alocado e dedicado até que uma das entidades desfaça o circuito. Se o tráfego não for constante a capacidade do meio físico será desperdiçada. Por outro lado existe a garantia de que a taxa de transmissão sempre será suportada pela conexão. No caso de uma sobrecarga, em uma rede de comutação por circuitos os pedidos de novas conexões são recusados.

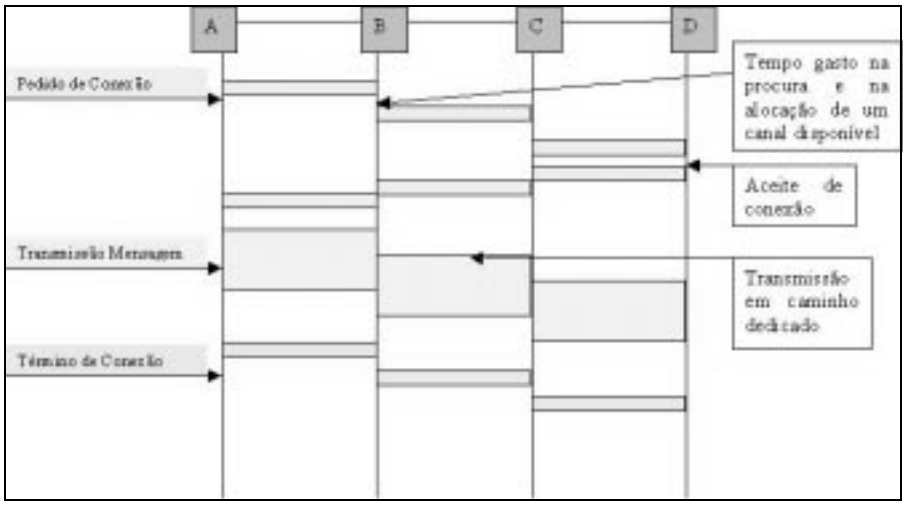


Figura 21 - Comutação de Circuito

A comutação de circuitos é bastante utilizada nos sistemas telefônicos. O PABX é um exemplo típico de sistema de comutação de circuitos. Os primeiros sistemas telefônicos utilizavam chaveamento físico manual, no qual os operadores humanos nas centrais telefônicas recebiam os pedidos de ligação (conexão) e eram encarregados de fechar fisicamente (através de cabos) os circuitos. Mais tarde, a introdução de relés permitiu que a comutação se tornasse automática, sem a necessidade dos operadores humanos. Mais recentemente, com a introdução e proliferação da transmissão digital em sistemas de telefonia, as linhas passaram a ser multiplexadas no tempo (TDM síncrono).

5.3. COMUTAÇÃO DE MENSAGENS

Na comutação de mensagens não é necessário o estabelecimento de um circuito dedicado entre as duas entidades. Trata-se do envio de mensagens através da rede, nó a

nó desde a origem até o destino, não existe qualquer fase anterior ao envio de dados, a mensagem é enviada para a rede juntamente com o endereço de destino e a rede encarrega-se de fazer chegar ao destino.

Sempre que uma entidade desejar transmitir uma mensagem ela adiciona o endereço de destino a esta mensagem que será então transmitida pela rede, nó a nó.

Uma mensagem é uma unidade lógica de informação. Em um determinado ponto da transmissão, a mensagem pode encontrar um caminho ocupado pela transmissão de outra mensagem e ainda com outras mensagens na fila de transmissão. Neste caso ela é colocada no final desta fila.

O conceito de mensagem é aqui extremamente lato, trata-se de blocos de dados de qualquer tipo, mas que deverão ser autônomos. Por exemplo, se pretendemos transferir um arquivo, o arquivo é a mensagem e é enviado integralmente numa única emissão nunca podendo ser dividido em blocos.

As mensagens são integralmente recebidas em cada nó por onde passam, só depois são enviados ao nó seguinte ("*store & forward*"), estes processos introduz atrasos significativos. Sendo **n** o número de nós pelos quais a mensagem passa (também conhecido por número de "*hops*"), o atraso total será **n x Tt**, ignorando atrasos de propagação, processamento e espera em filas nos nós.

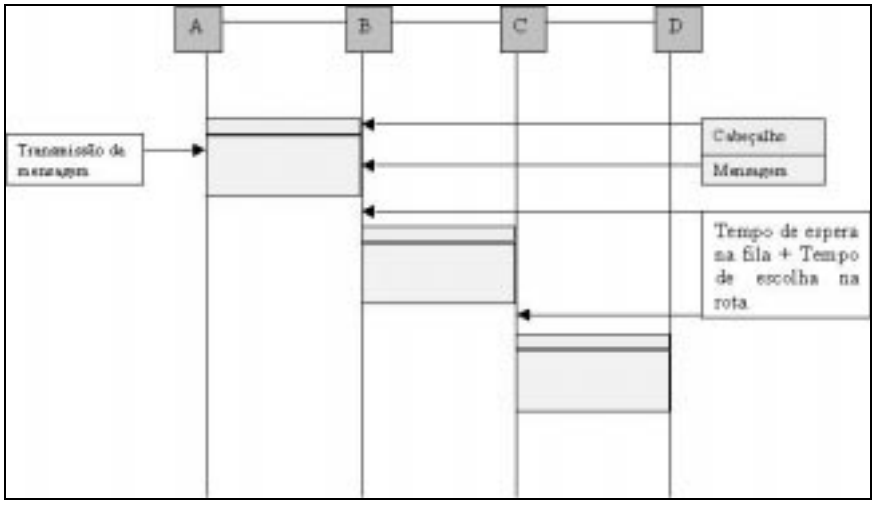


Figura 22 - Comutação de Mensagem

A comutação de mensagens introduz uma seria de possibilidades que não existiam na comutação de circuitos e anula alguns dos seus inconvenientes:

- Melhor aproveitamento das linhas de comunicação, pois as linhas apenas são ocupadas durante o tempo necessário à transferência das mensagens entre os nós.
- No caso de congestionamento, as mensagens são sempre aceitas. O tempo de transferência aumenta nesta situação devido às filas de mensagens. Exemplo: correio Convencional.
- Por mais elevada que seja a utilização existe sempre a possibilidade de as mensagens circularem, embora com atrasos por espera nos nós.
- Não existe necessidade do nó de destino estar ativo, a rede pode armazenar a mensagem e entregar mais tarde.
- Os atrasos nos nós são significativos.
- A mensagem pode ter diversos destinos sendo copiada pela rede de modo a ser entregue a todos eles.
- O conceito de mensagem e os atrasos produzidos tornam este tipo de comutação inadequado para trocas intensas de pequenas quantidades de informação entre nós (tráfego interativo).
- Uma vez que uma mensagem é transmitida sucessivamente entre nós consecutivos o controle de fluxo e erros pode ser realizado pela própria rede.
- A rede pode ser heterogênea, nomeadamente com velocidades de transmissão distintas no seu interior.
- O caminho fica aberto para a definição de graus de prioridade: em cada saída de cada nó existe uma fila de espera. As filas de espera são habitualmente geridas com uma disciplina de serviço FCFS ("*First come First Served*"), mas é simples implementar um sistema de prioridades.

5.4. COMUTAÇÃO DE PACOTES

Os grandes problemas levantados pela comutação de mensagens poderiam ser resolvidos se os dados enviados fossem divididos em blocos menores. Na comutação de pacotes são impostas restrições quanto à quantidade de informação que podem ser enviadas de cada vez. Esses blocos de informação tomam a designação genérica de pacotes, ou especificamente na camada de ligação lógica a designação de "*frames*".

Na comutação de pacotes não é necessário o estabelecimento de um circuito dedicado entre as duas entidades. Opera de forma semelhante à comutação de mensagens. Porém, o tamanho da unidade de dados é limitado. As mensagens a partir de

tamanho acima do limite são quebradas em mensagens menores denominadas pacotes. Geralmente os *pacotes* possuem tamanhos variáveis até um valor máximo imposto. Exemplo da utilização de comutação por pacotes são as redes *Ethernet*.

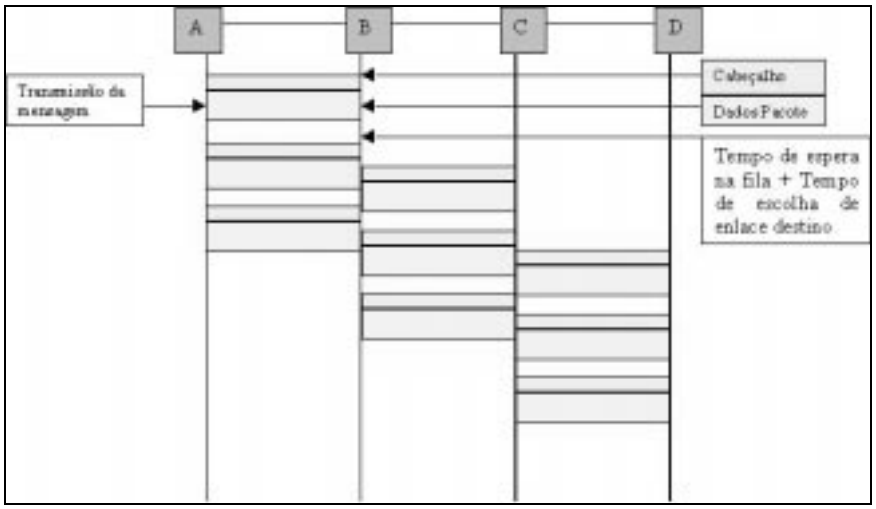


Figura 23 - Comutação de Pacotes

6. TECNOLOGIAS PARA IMPLEMENTAÇÃO DE REDES

Para facilitar o processo de padronização e obter interconectividade entre máquinas de diferentes fabricantes, a Organização Internacional de Normatização (ISO - *International Standards Organization*) aprovou, no início dos anos 80, um modelo dereferência para permitir a comunicação entre máquinas heterogêneas, definindo as diretivas genéricas para construção de redes de computadores que independem da tecnologia de implementação. Esse modelo denominado OSI (*Open Systems Interconnection*) serve de base para qualquer tipo de rede, seja de curta, média ou longa distância.

A construção das redes envolve a seleção e integração de várias tecnologias, cada uma destinada a atender requisitos específicos de custo e desempenho.

Vários organismos normalizadores se empenharam para elaboração de padrões de tecnologia que implementam funções de uma ou mais camadas do modelo OSI.. O processo de elaboração de padrões é bastante evolutivo envolvendo a participação ativa de fabricantes, através do surgimento de novas tecnologias

A ISO *International Organization for Standardization* é a principal organização no que se refere a elaboração de padrões de comunicação de alcance mundial.

6.1. ARQUITETURAS DE REDES

Conceito: Conjunto de tecnologias (camadas e protocolos) que compõem a infra-estrutura completa para construção de uma rede de computadores.

Comunicação entre 2 redes: nenhum dado é transferido diretamente da camada n em uma máquina para outra máquina. Em vez disso, cada camada passa os dados e informações de controle para a camada imediatamente abaixo, até que o nível mais baixo seja alcançado. Abaixo do nível 1 esta o meio físico de comunicação, através do qual a comunicação de fato ocorre.

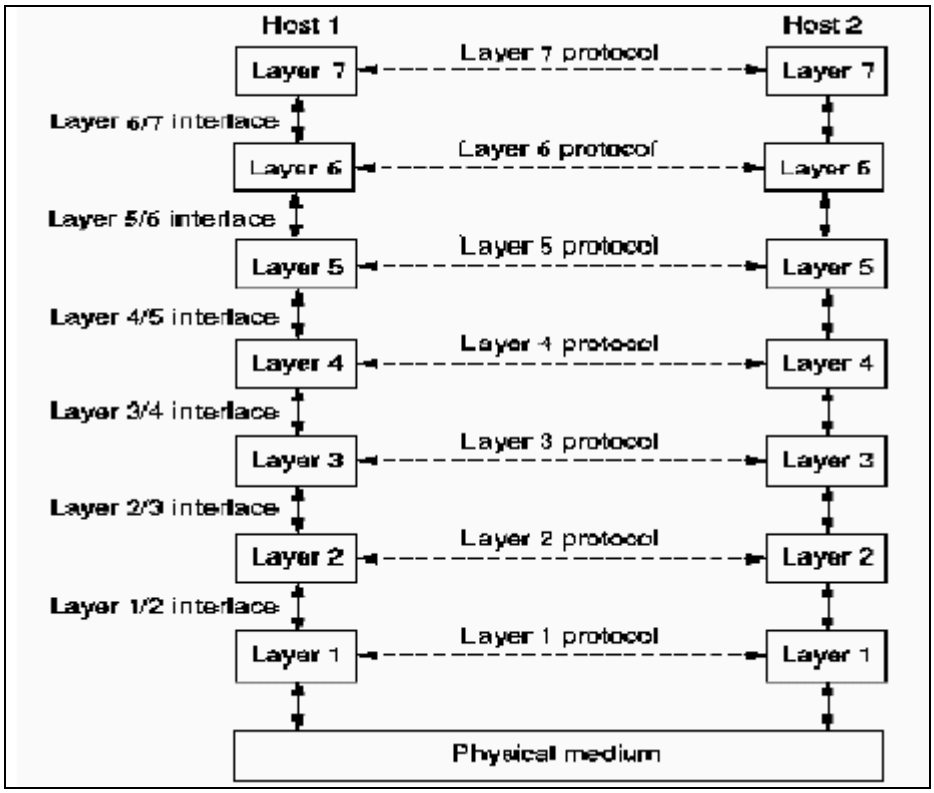


Figura 24 - Comunicação entre duas Redes de Computadores

Fluxo de Informações entre duas redes

Processo de comunicação para o transporte de uma mensagem ‘m’ para uma outra rede. A comunicação virtual se dá através das linhas pontilhas e a comunicação física através das linhas sólidas da figura abaixo.

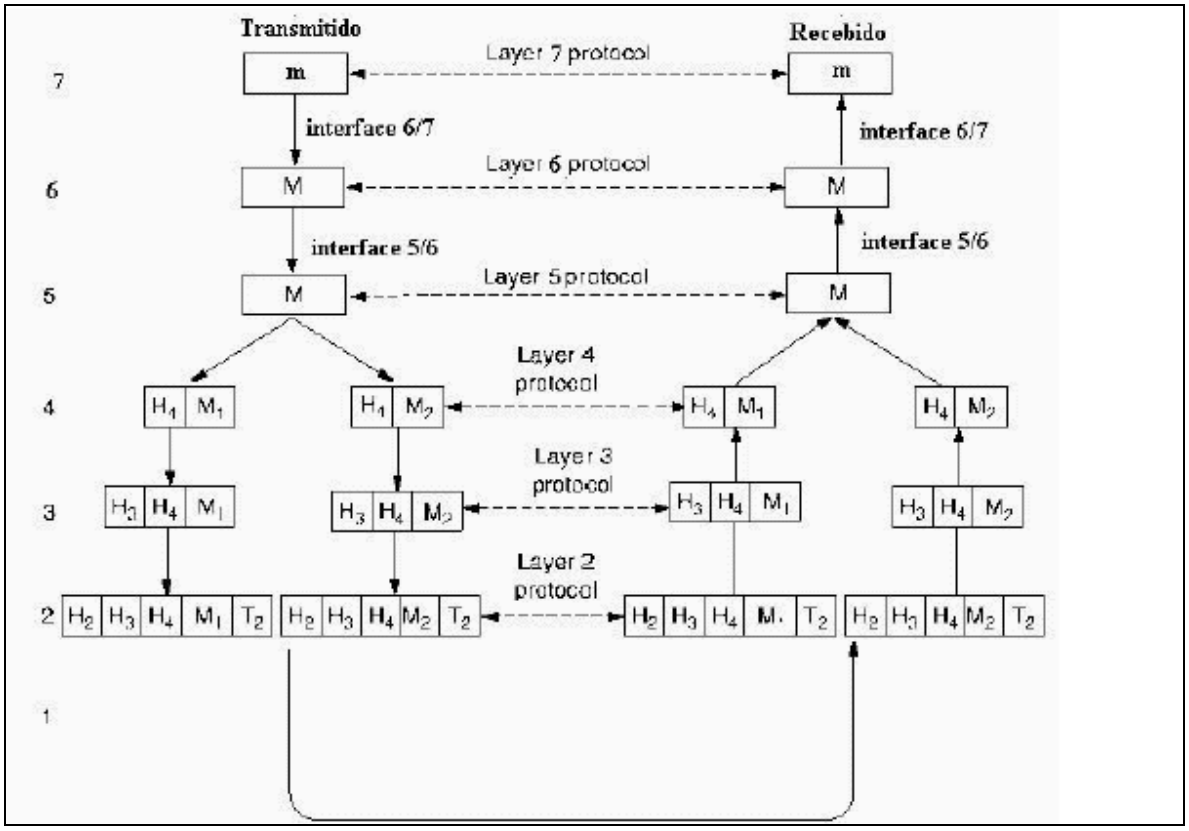


Figura 25 - Fluxo de Informação dando suporte à comunicação Virtual da Camada 7

Maquina 1 e Máquina 2

6.2. ARQUITETURA DO MODELO DE REFERÊNCIA OSI

O modelo OSI define uma arquitetura genérica com 7 camadas. Sua elaboração representou um esforço na tentativa de padronização e direcionamento do desenvolvimento de novas tecnologias para implementação de redes de computadores. Entretanto, nem todas as soluções existentes no mercado seguem o modelo OSI. Arquiteturas alternativas têm sido adotadas para construções de redes no mundo todo. Algumas soluções proprietárias, como a SNA, se impuseram como resultado do sucesso de um grande fabricante. Soluções não proprietárias, como TCP/IP, surgiram como resultado de esforços de pesquisa, incluindo grande participação do mundo acadêmico.

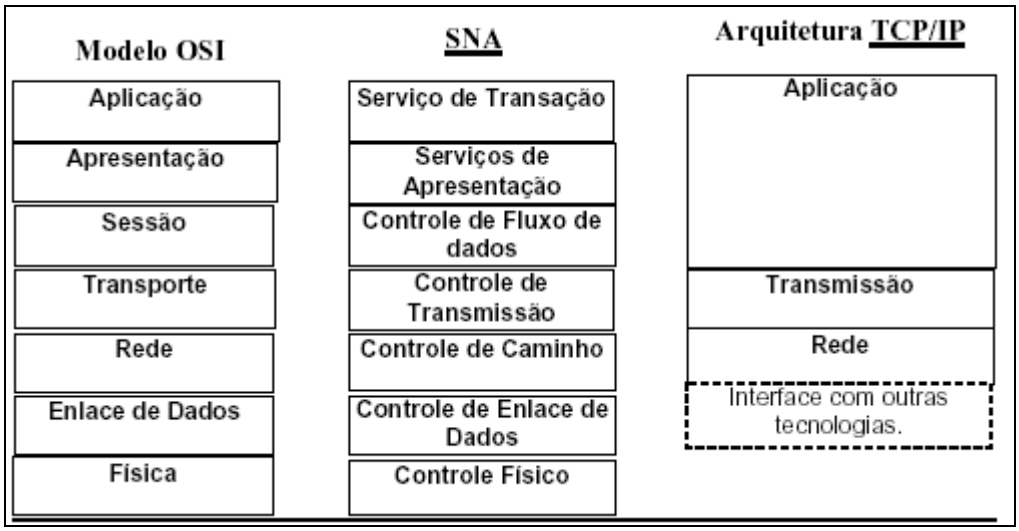


Figura 26 - Exemplos de Arquiteturas de Redes

SNA: *Systems Network Architecture.* Conjunto de produtos de comunicação proprietários da IBM. O SNA inspirou a criação do modelo OSI, guardando muitas similaridades com o padrão proposto pela ISO. A SNA é uma das arquiteturas dominantes no mercado de computadores da atualidade, e é suportada por uma ampla gama de fornecedores.

TCP/IP: Abreviatura de *Transmission Control Protocol/Internet Protocol.* A arquitetura TCP/IP define um modelo com menos camadas que o modelo OSI. As camadas de enlace de dados e física não são especificadas na arquitetura TCP/IP, podendo ser implementadas através de soluções propostas em outras arquiteturas. A arquitetura TCP/IP é muito difundida no mundo acadêmico e comercial, superando em popularidade soluções inteiramente compatíveis com o modelo OSI.

6.2.1 Nível 1: físico

O nível físico tem a função de transmitir uma seqüência de bits através de um canal de comunicação. As funções típicas dos protocolos deste nível são para fazer com que um bit "1" transmitido por uma estação seja entendido pelo receptor como bit "1" e não como bit "0". Assim, este nível trabalha basicamente com as características mecânicas e elétricas do meio físico, como por exemplo:

- Número de volts que devem representar os níveis lógicos "1" e "0";
- Velocidade máxima da transmissão;

- Transmissão simplex, half-duplex ou full-duplex;
- Número de pinos do conector e utilidade de cada um;
- Diâmetro dos condutores.

Os protocolos deste nível são os que realizam a codificação/decodificação de símbolos e caracteres em sinais elétricos lançados no meio físico, que fica logo abaixo dessa camada. Exemplos de protocolos que se enquadram no nível físico do modelo OSI são: RS-232C, X.21 (para redes com transmissão digital), X.21bis (para redes com transmissão analógica), codificação Manchester, codificação Manchester Diferencial, SONET (*Synchronous Optical Network*), e assim por diante.

6.2.2 Nível 2: enlace

O principal objetivo do nível de enlace é receber/transmitir uma seqüência de bits do/para o nível físico e transformá-los em uma linha que esteja livre de erros de transmissão, a fim de que essa informação seja utilizada pelo nível de rede. O nível de enlace está dividido em dois subníveis: o superior é o controle lógico do enlace (LLC - *Logical Link Control*), e o inferior é o controle de acesso ao meio (MAC - *Medium Access Control*), como mostra a figura a seguir.

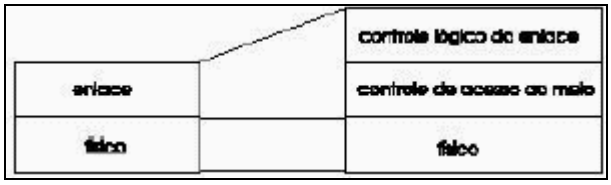


Figura 27 - Nível de Enlace

Subnível LLC

O protocolo LLC pode ser usado sobre todos os protocolos IEEE do subnível MAC, como por exemplo o IEEE 802.3 (Ethernet), IEEE 802.4 (*Token Bus*) e IEEE 802.5 (*Token Ring*). Ele oculta as diferenças entre os protocolos do subnível MAC.

Usa-se o LLC quando é necessário controle de fluxo ou comunicação confiável. Ele oferece três opções de transmissão: serviço de datagrama não-confiável, serviço de datagrama com confirmação e serviço orientado à conexão confiável.

O LLC consegue isso dividindo a mensagem a transmitir em quadros com algumas centenas de bytes de dados e alguns bytes de controle (como CRC, por exemplo).

Enquanto transmite seqüencialmente os quadros de dados, o transmissor deve tratar os quadros de reconhecimento (ACK), que são enviados pelo receptor a fim de indicar se a transmissão ocorreu com ou sem erros. Caso algum quadro não tenha chegado corretamente, o transmissor deve retransmiti-lo, e o receptor deve descartar o quadro errado.

Um ruído mais forte na linha pode destruir completamente um quadro. Nesse caso, os protocolos da camada de enlace devem retransmitir essa informação. Entretanto, múltiplas retransmissões do mesmo quadro podem fazer com que existam quadros duplicados. Um quadro duplicado pode acontecer se, por exemplo, o ACK do receptor foi destruído. É tarefa do LLC tratar e resolver problemas causados por quadros danificados, perdidos e duplicados. Existem várias classes de serviço neste nível, cada uma com seu fator de qualidade.

Outra função do nível de enlace LLC é controle de fluxo, ou seja, o controle de um transmissor rápido para que não inunde de dados um receptor mais lento. Algum mecanismo regulador de tráfego deve ser empregado para deixar o transmissor saber quanto espaço em buffer tem no receptor naquele momento. Freqüentemente, o controle de fluxo e de erro é integrado, simplificando o protocolo.

Para entender quando é necessário controle de fluxo, suponha um transmissor que pode enviar dados a 1Mbps, e um receptor que pode receber dados somente a 100Kbps, como mostra a figura a seguir. Evidentemente, algum controle deve haver para que o receptor não seja obrigado a descartar dados.

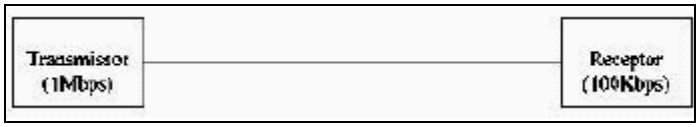


Figura 28- Velocidade de Transmissão 1Mbps x 100Kbps

Outra complicação que deve ser tratada em nível de enlace é quando a linha for utilizada para transmitir tráfego em ambas direções (de A para B e de B para A). Normalmente, uma comunicação envolve a transmissão do pacote de dados e o ACK (*acknowledge*) enviado de volta pela estação receptora, indicando que os dados chegaram sem erros. Entretanto, o problema é que os quadros de ACK competem pelo meio físico da mesma forma que os quadros de dados, prejudicando o desempenho do sistema. Para eliminar esse problema, em alguns protocolos utiliza-se o conceito de *piggybacking*, onde os bits de ACK que devem ser enviados em resposta ao quadro de

dados transmitidos pela estação A vêm junto com o quadro de dados que a estação B quer transmitir para a estação A.

- Resumindo, as principais funções do nível de enlace são as seguintes:
- Entregar ao nível de rede os dados livres de erros de transmissão;
- Retransmissão de quadros errados;
- Controle de fluxo;
- Tratamento de quadros duplicados, perdidos e danificados.

Subnível MAC

O sub-nível MAC possui alguns protocolos importantes, como o IEEE 802.3 (*Ethernet*), IEEE 802.4 (*Token Bus*) e IEEE 802.5 (*Token Ring*). O protocolo de nível superior pode usar ou não o subnível LLC, dependendo da confiabilidade esperada para esse nível. Em intranets se utiliza TCP/IP sobre MAC direto. Esse subnível fica muito próximo ao nível físico, não existindo confirmações de mensagens (ACK) nem controle de fluxo. Caso a mensagem chegue errada no receptor (detectado através do CRC), ele simplesmente descarta o quadro.

As redes baseadas em TCP/IP que utilizam o Ethernet / Token Ring em nível 2 funcionam dessa forma, ou seja, se dá erro num pacote ele é descartado. As confirmações e verificações ficam para o nível mais alto (TCP). Essa é uma boa forma de reduzir overheads na rede, sem repetições e retransmissões a cada nível que a mensagem passa.

6.2.3 Nível 3: rede

O nível de rede tem a função de controlar a operação da rede de um modo geral. O principal aspecto é executar o roteamento dos pacotes entre fonte e destino, principalmente quando existem caminhos diferentes para conectar entre si dois nós da rede. Em redes de longa distância é comum que a mensagem chegue do nó fonte ao nó destino passando por diversos nós intermediários no meio do caminho, e é tarefa do nível de rede escolher o melhor caminho para essa mensagem.

A escolha da melhor rota pode ser baseada em tabelas estáticas, que são configuradas na criação da rede e são raramente modificadas, pode também ser determinada no início de cada conversação, ou ser altamente dinâmica, sendo determinada a cada novo pacote, a fim de refletir exatamente a carga da rede naquele

instante. Na prática, os roteadores atualizam suas tabelas de roteamento de tempos em tempos (30 segundos, no RIP).

Se muitos pacotes estão sendo transmitidos através dos mesmos caminhos, eles vão diminuir o desempenho global da rede, formando gargalos. O controle de tais congestionamentos é tarefa da camada de rede.

Normalmente, a transmissão de mensagens em redes de longa distância é cobrada pela central pública que administra o serviço, e a contabilização é feita pela camada de rede, que deve contar o número de pacotes ou bytes que o usuário utilizou a fim de tarifar o sujeito.

Resumindo, as principais funções do nível de rede são as seguintes:

- Roteamento dos pacotes entre fonte e destino, mesmo que tenha que passar por diversos nós intermediários durante o percurso;
- Controle de congestionamento;
- Contabilização do número de pacotes ou bytes utilizados pelo usuário, para fins de tarifação;

Com relação às redes broadcast (do tipo *Ethernet*), onde a informação é escutada por todas outras estações, o roteamento não é necessário dentro da subrede, fazendo com que a camada de rede seja muito simples. Caso não seja tarefa da subrede, o pacote é enviado ao roteador default.

Exemplos de protocolos desse nível são o IPX, usado pelo *Netware* até a versão 5.0, o IP (*Internet Protocol*), que pertence à família de protocolos TCP/IP, e o PLP (*Packe*t *Layer Protocol*), referenciado no modelo OSI e utilizado nas redes X.25.

A principal diferença entre o protocolo IP e o PLP é que a transmissão de dados no protocolo IP é orientada a datagramas (sem conexão), e no PLP é orientada à conexão (onde um caminho virtual é estabelecido antes de iniciar a comunicação propriamente dita).

Uma transmissão orientada a datagrama é menos confiável, pois as mensagens não seguem um caminho pré-determinado entre fonte e destino, podendo tomar caminhos diferentes dependendo da decisão do roteador, que pode escolher diferentes rotas para enviar cada pedaço da mensagem. Assim, nesse tipo de transmissão, não é garantido que a mensagem chegue ao destino na mesma ordem que foi enviada, sendo uma tarefa das camadas superiores a sua remontagem na seqüência correta. Dessa forma, uma mensagem que foi transmitida e segmentada na seqüência 1, 2 e 3, pode chegar ao destino na ordem 2, 3 e 1. Pode-se associar a transmissão orientada à datagrama com o

envio de uma mensagem por telegrama via correio. No corpo do telegrama constam todos os dados necessários para o carteiro encontrar o endereço destino, e se forem enviados vários telegramas, não se podem garantir qual deles chegará antes.

Na transmissão orientada à conexão, ao contrário, antes de se estabelecer a transmissão de dados propriamente dita, é criada uma rota através da qual todos os pacotes irão trafegar, dessa forma, a correta seqüência dos pacotes é garantida. Pode-se associar a transmissão orientada à conexão com uma ligação telefônica: antes de se estabelecer a comunicação entre origem e destino, é necessário a criação de uma conexão física através de chaves comutadoras da central pública, e, após estabelecida essa conexão, não é mais necessário o reforço do número discado até o término da conversação, onde a conexão é desfeita.

6.2.4 Nível 4: transporte

O nível de transporte inclui funções relacionadas com conexões entre a máquina fonte e máquina destino, segmentando os dados em unidades de tamanho apropriado para utilização pelo nível de rede, seguindo ou não as orientações do nível de sessão. Sob condições normais, o nível de transporte cria uma conexão distinta para cada conexão de transporte requisitada pelo nível superior. Se a conexão de transporte requisitada necessita uma alta taxa de transmissão de dados, este nível pode criar múltiplas conexões de rede, dividindo os dados através da rede para aumentar a velocidade de transmissão, conforme as indicações do nível de sessão. Por outro lado, se é caro manter uma conexão de rede, a camada de transporte pode multiplexar várias conexões de transporte na mesma conexão de rede, a fim de reduzir custos. Em ambos os casos, a camada de transporte deixa essa multiplexação transparente ao nível superior. Existem várias classes de serviço que podem ser oferecidas ao nível superior, e, em última instância, aos usuários da rede. A mais popular é uma comunicação através de um canal ponto a ponto livre de erros, que envia as mensagens seqüencialmente, na mesma ordem que elas foram recebidas. Existem outras classes permitidas, como o envio de mensagens isoladas, sem garantia sobre a ordem da entrega, ou enviar mensagens para múltiplos destinos (*mensagens multicast*). Atualmente, está se popularizando uma classe de serviço que garante um atraso mínimo na transmissão e a variação máxima do atraso entre pacotes, viabilizando assim aplicações de voz e vídeo através da rede.

O nível de transporte é o primeiro que trabalha com conexões lógicas fim a fim, ou seja, um programa na máquina fonte conversa com um programa similar na máquina

destino, diferentemente dos níveis anteriores, que conversavam somente com o nó vizinho. Vale ressaltar que a conexão criada pelo nível de transporte é uma conexão lógica, e os dados são transmitidos somente pelo meio físico, através do nível 1 do modelo. Assim, os dados devem descer nível a nível até atingir o nível 1, para então serem transmitidos à máquina remota.

Resumindo, as principais funções do nível de transporte são as seguintes:

- Criar conexões para cada requisição vinda do nível superior;
- Multiplexar as várias requisições vindas da camada superior em uma única conexão de rede;
- Dividir as mensagens em tamanhos menores, a fim de que possam ser tratadas pelo nível de rede;
- Estabelecer e terminar conexões através da rede.

Como exemplos de protocolos de nível de transporte da família TCP/IP temos o TCP (*Transfer Control Protocol*), orientado à conexão e mais confiável, e o UDP (*User Datagram Protocol*), orientado a datagrama e menos confiável. O protocolo especificado pela ISO nesse nível é o TP4.

6.2.5 Nível 5: sessão

A função do nível 5 do modelo OSI é administrar e sincronizar diálogos entre dois processos de aplicação. Este nível oferece dois tipos principais de diálogo: half-duplex e full-duplex.

O nível de sessão fornece mecanismos que permitem estruturar os circuitos oferecidos para o nível de transporte. Neste nível ocorre a quebra de um pacote com o posicionamento de uma marca lógica ao longo do diálogo. Esta marca tem como finalidade identificar os blocos recebidos para que não ocorra uma recarga, quando ocorrer erros na transmissão.

Uma sessão permite transporte de dados de uma maneira mais refinada que o nível de transporte em determinadas aplicações. Uma sessão pode ser aberta entre duas estações a fim de permitir a um usuário se logar em um sistema remoto ou transferir um arquivo entre essas estações. Os protocolos desse nível tratam de sincronizações (*checkpoints*) na transferência de arquivos.

Um exemplo de protocolo que se enquadra neste nível é o RPC (*Remote Procedure Call*).

6.2.6 Nível 6: apresentação

A função do nível 6 é assegurar que a informação seja transmitida de tal forma que possa ser entendida e usada pelo receptor. Dessa forma, este nível pode modificar a sintaxe da mensagem, mas preservando sua semântica. Por exemplo, uma aplicação pode gerar uma mensagem em ASCII mesmo que a estação interlocutora utilize outra forma de codificação (como EBCDIC). A tradução entre os dois formatos é feita neste nível.

O nível de apresentação também é responsável por outros aspectos da representação dos dados, como criptografia e compressão de dados.

6.2.7 Nível 7: aplicação

O sétimo nível, o de aplicação, fornece ao usuário uma interface que permite acesso a diversos serviços de aplicação, convertendo as diferenças entre diferentes fabricantes para um denominador comum.

Por exemplo, em uma transferência de arquivos entre máquinas de diferentes fabricantes, pode haver convenções de nomes diferentes (DOS tem uma limitação de somente 8 caracteres para o nome de arquivo, UNIX não), formas diferentes de representar as linhas, e assim por diante.

Transferir um arquivo entre os dois sistemas requer uma forma de trabalhar com essas incompatibilidades, e essa é a função do nível de aplicação.

O nível de aplicação sem dúvida nenhuma é o nível que possui o maior número de protocolos existentes, devido ao fato de estar mais perto do usuário, e os usuários possuírem necessidades diferentes. Algumas aplicações deste nível são transferência de arquivos, correio eletrônico e terminais virtuais, entre outras.

Exemplos de protocolos deste nível são o NFS (*Network File System*), o X.400, o SMTP (*Simple Mail Transfer Protocol*), base de dados distribuída, telnet, FTP (*File Transfer Protocol*), SNMP (*Simple Network Management Protocol*), CMIP (*Common Management Information Protocol*), X.500 e assim por diante.

7. ARQUITETURA TCP/IP

A arquitetura TCP/IP é um dos modelos de software de rede mais populares da atualidade. Deve-se observar que o termo consagrado TCP/IP refere-se a apenas 2 protocolos de uma ampla família de protocolos. Um nome mais apropriado para o software de rede baseado nos protocolos TCP/IP seria conjunto de protocolos internet (*Internet Protocol Suite*). Esses protocolos são não-proprietários e constituem a base para construção da rede mundial Internet, o que motivou sua adoção também em redes locais e redes corporativas.

Conceito: A arquitetura TCP/IP apresenta um modelo de software de rede em camadas, similar ao modelo OSI (figura 26). A arquitetura TCP/IP refere-se a uma ampla família de protocolos, que suportam todas as funções necessárias para implementar tanto redes locais (LAN) quanto redes geograficamente distribuídas (WAN). Os protocolos da arquitetura TCP/IP são organizados num modelo com menos camadas que o modelo OSI, o que contribuiu para o seu grande sucesso no mundo comercial e acadêmico.

TCP/IP: Abreviatura de *Transmission Control Protocol/Internet Protocol*.

internet: Conjunto de redes interligadas, formando uma rede geograficamente distribuída.

Rede mundial Internet: rede pública geograficamente distribuída, de alcance mundial, montada segundo a arquitetura TCP/IP.

Gateway internet: Também chamado de roteador internet. Dispositivo que conecta duas ou mais redes dentro de uma internet.

Não-proprietários: termo utilizado para indicar que os direitos de utilização de uma tecnologia não pertencem a nenhum fabricante específico. Os protocolos TCP/IP não são definidos por organismos normalizadores, sendo considerados por isso padrões de facto. (Quando os padrões são definidos por uma instituição legalmente constituída para elaboração de padrões, como a ISO, o padrão é dito de jure).

7.1. CAMADA DE INTERFACE DE REDE

A arquitetura TCP/IP descreve apenas o comportamento das camadas superiores do software de rede, a partir da camada de rede. Não existe nenhuma restrição quanto à tecnologia utilizada aos níveis de enlace de dados e físico.

A arquitetura TCP/IP não impõe nenhuma restrição quanto à implementação dos níveis de enlace de dados e físico das redes que interliga. A função desses níveis pode

ser executada através de qualquer tecnologia para implementação de redes locais, como *Ethernet* ou *Token Ring*.

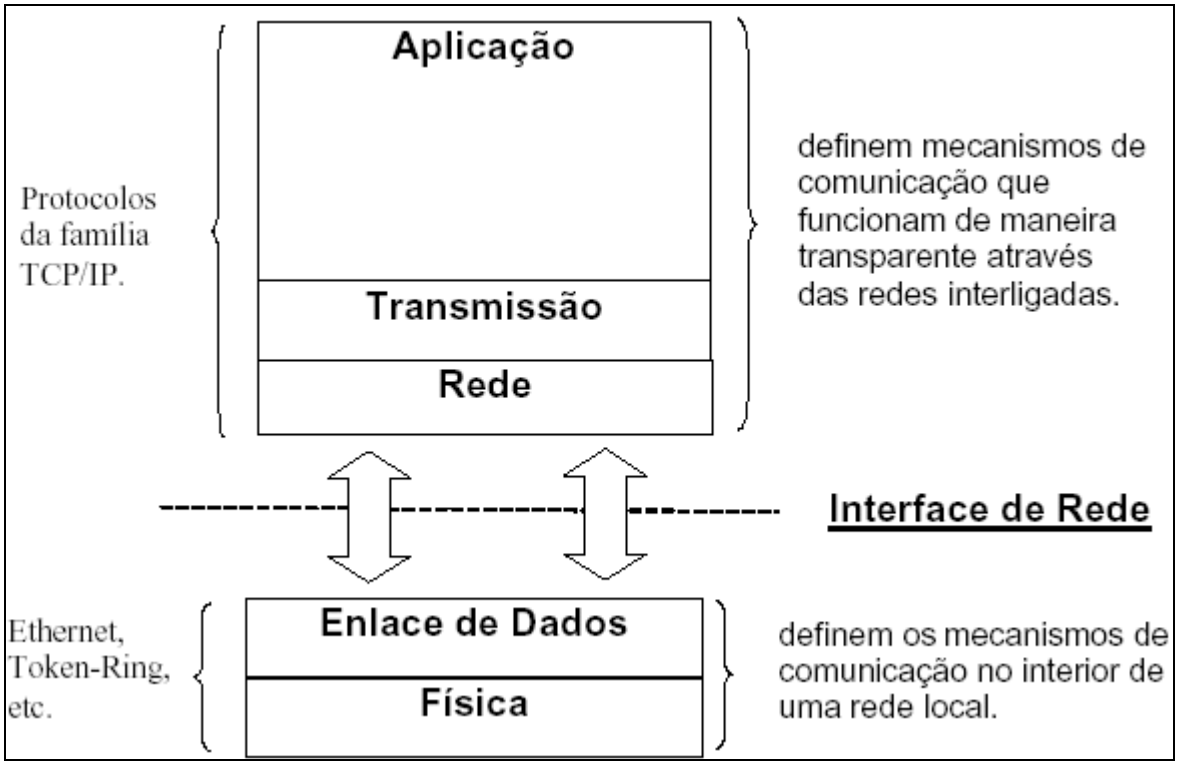


Figura 29 - Arquitetura TCP/IP

Interface de Rede: A integração da arquitetura TCP/IP com as camadas inferiores se faz por meio da interface de rede, responsável por encapsular os datagramas IP nos quadros da camada de enlace de dados.

A camada de interface de rede define os padrões de transmissão de informações através do meio físico. Esta intimamente relacionada ao hardware e a maioria dos protocolos desta camada são implementadas pelo *device drives* da placa de rede.

Os datagramas recebidos da camada de rede são convertidos em sinal elétrico para serem inseridos no meio físico de acordo com o tipo de rede [Quadro 1].

Quadro 1 - Protocolos utilizados na Redes

Tipo de Rede	Protocolo
Redes WAN	ATM, FDDI, Frame Relay e X.25
Redes LAN	Ethernet, Fast Ethernet, Token Ring e FDDI
Acesso Discado	PPP e SLIP

7.2. CAMADA DE REDE

As funções da camada de rede são executadas principalmente pelo protocolo IP (*Internet Protocol*). Sua função é definir a rota dos datagramas e encaminhá-los através dos roteadores internet até seu destino final.

O protocolo IP oferece um serviço de comunicação não orientado a conexão (datagrama). Sua função é definir a rota dos datagramas e encaminhá-los até seu destino final. O protocolo IP associa a cada estação um endereço IP, que permite identificar uma estação de maneira única, mesmo com várias redes interconectadas. As funções do protocolo IP são complementadas pelo protocolo ICMP.

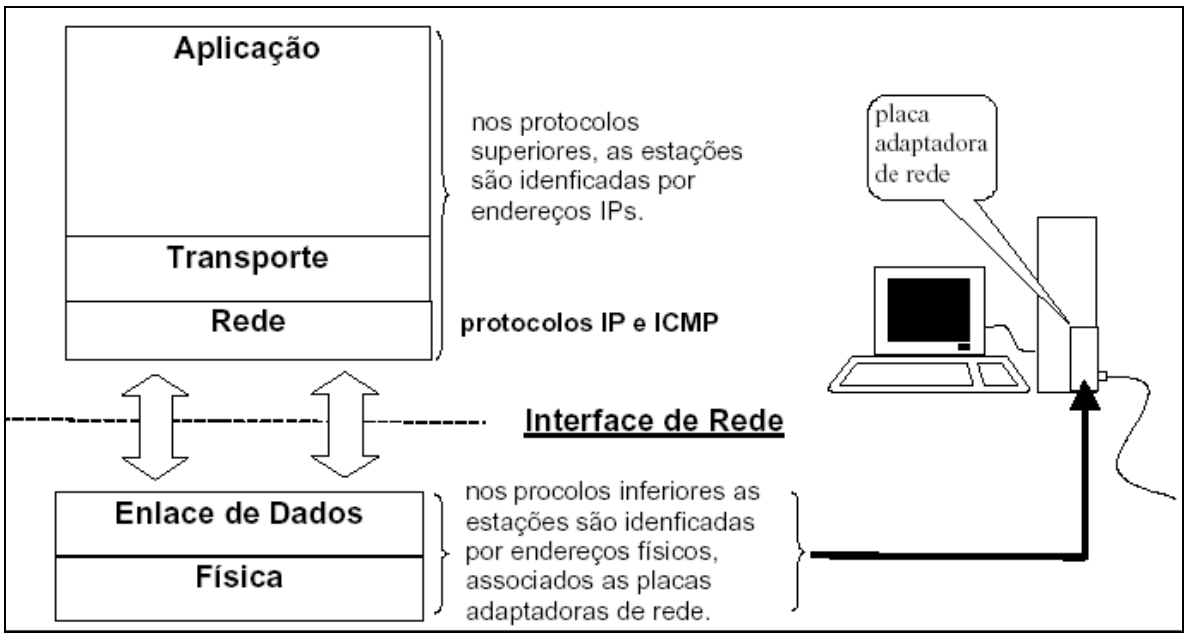


Figura 30 - Protocolo IP e ICMP

TERMOS:

***** Endereço IP: número de 32 bits utilizado para identificar as estações numa arquitetura TCP/IP. Cada endereço IP é único entre todas as estações conectadas na internet.

* Datagrama: Nome da unidade de dados do protocolo de rede não orientado a conexão.

* ICMP: "Internet control message protocol". Protocolo de rede muito simples, complementar ao protocolo IP, usado para trocar mensagens de erro e descobrir

informações sobre a rede. O ICMP é destinado principalmente para uso interno do software TCP/IP, e não para fornecer serviços ao nível de usuário.

* Protocolos são basicamente à parte do sistema operacional da rede encarregada de ditar as normas para a comunicação entre os dispositivos. Vários são os tipos de protocolos, entre os mais utilizados estão:

- TCP/IP - Transfer Control Protocol/Internet Protocol: Ele foi desenvolvido para ser um protocolo roteável, e serve como padrão para redes de longa distância (WAN's) e para acesso a internet (como foi visto anteriormente).
- IPX/SPX - *Internet Packet Exchange/Sequence Packet Exchange*: Ele foi desenvolvido para suportar redes NetWare, e suporta redes de tamanho pequeno e médio e também tem a capacidade básica de roteamento.
- NETBEUI - *Network Basic End User Interface*: Ele suporta pequenas LAN's é rápido e simples. Porém, tem uma estrutura arquitetônica inerente que limita sua eficiência à medida que a rede se expande.

Quando instalar uma rede, você terá a opção de instalar qualquer um ou todos esses transportes, instalar protocolos sem necessidade poderá deixar o equipamento mais lento nas comunicações em rede.

Selecione o IPX/SPX durante a instalação do Windows, ele é simples de definir e oferece um desempenho melhor do que o NetBeui. Ele também deverá ser instalado caso na rede haja a necessidade de comunicação com uma rede NetWare.

O protocolo NetBeui apenas deverá ser instalado caso haja a necessidade de comunicação com redes antigas (LAN manager).

Selecione TCP/IP se você necessita imediatamente estabelecer uma comunicação com a internet ou intranet. Você irá precisar definir parâmetros de provedor, IP etc.O quadro 2 abaixo pode ajudar na escolha do melhor(es) protocolo(s):

Quadro 2 - Aplicabilidade dos Protocolos

Aplicativo	NetBeui	IPX/SPX	TCP/IP
Integrar com NetWare		X	
Conectar a Internet			X
Trabalhar com UNIX			X
Roteamento (WAN)			X
Rede grande			X
Rede pequena	X	X	X

7.2.1 ENDEREÇOS IP

Conceito: Número de 32 bits utilizado para identificar as estações numa arquitetura TCP/IP. Cada endereço IP é único entre todas as estações conectadas numa internet.

Os endereços IPs são números de 32 bits, representados usualmente numa notação decimal pontuada. Cada endereço IP é composto de duas partes, um identificador de rede e um identificador do host.

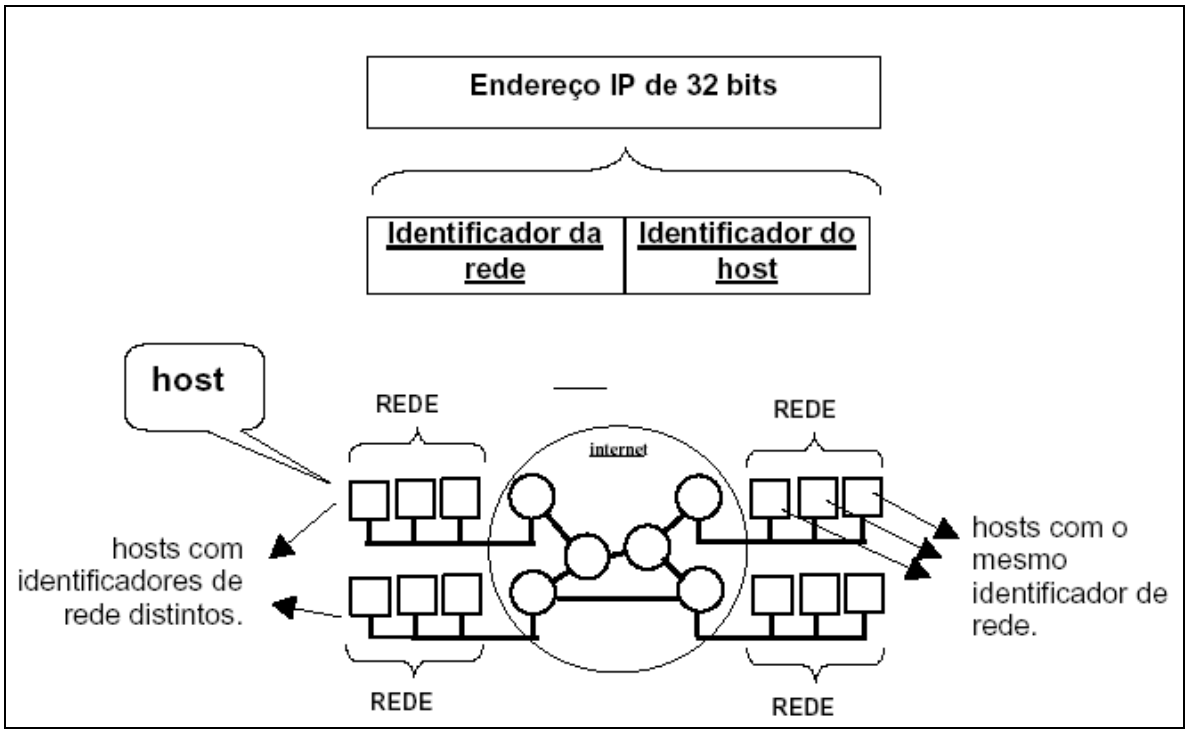


Figura 31 - Hosts e Endereços IP

7.2.1.1. Classes de endereçamento

O número de bits utilizado pelo identificador da rede e pelo identificador de host depende da classe de endereçamento utilizada. São definidas 5 classes de endereçamento:

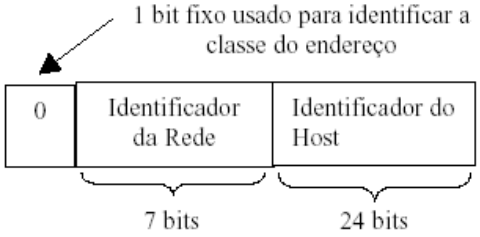
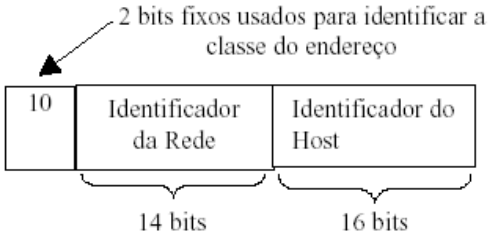
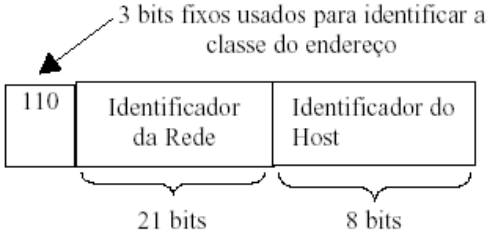
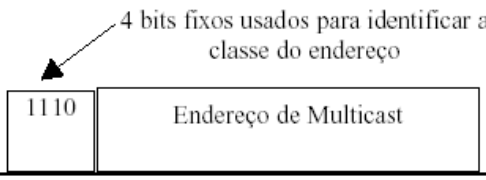
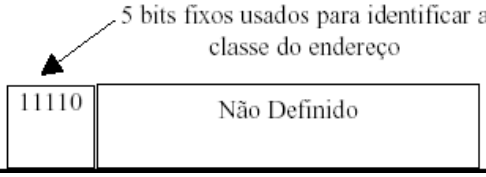
Classe	Formato do Endereço	Organização da Rede	Intervalo dos endereços da classe
A		permite definir 127 redes distintas, cada uma com até 16777216 hosts.	de 1.0.0.0 até 127.255.255.255.
B		permite definir até 16384 redes distintas, cada uma com 65535 hosts.	de 128.0.0.0 até 191.255.2555.255.
C		permite definir até 2097152 redes distintas, cada uma com 255 hosts.	de 192.0.0.0 até 233.255.2555.255.
D		Classe reservada para endereçamento em multicast.	de 224.0.0.0 até 239.255.2555.255.
E		Classe resevada para novas implementações.	de 248.0.0.0 até 247.255.2555.255.

Figura 32 - Classes de Endereços

7.2.1.2 Endereços IP especiais

Alguns endereços IP possuem significados especiais, e não podem ser atribuídos a nenhuma estação. Os endereços especiais estão resumidos na tabela a seguir:

Endereço	Significado
0.0.0.0	Indica o próprio host. Esse endereço só é utilizado no momento da inicialização da estação.
0.x.x.x, onde x.x.x é o endereço do host numa rede classe A 0.0.y.y, onde y.y é o endereço do host numa rede classe B 0.0.0.z, onde z é o endereço o host numa rede classe C	Envia para o host especificado, assumindo a estação transmissora e receptora estão na mesma rede.
255.255.255.255	Envia o datagrama em broadcast na rede local
x.255.255.255, onde x é o identificador de uma rede classe A y.y.255.255, onde y.y é o identificador de uma rede classe B z.z.z.255, onde z.z.z é o identificador de uma rede classe C	Envia o datagrama em broadcast numa rede externa.
127.x.x.x	Reservado para loopback.

Figura 33 - Endereços Especiais

TERMOS

* loopback: Enviar para si mesmo. Os datagramas com endereço IP 127.x.x.x não são enviados para rede. Eles são tratados localmente pela própria estação como datagramas recebidos. Essa função é útil para efetuar testes e para otimizar a comunicação entre processos num mesmo computador.

7.2.1.3 Exemplo de atribuição de endereços IP

Numa rede TCP/IP todas os hosts pertencentes a uma mesma rede devem possuir o mesmo identificador de rede. Para que estações com identificadores de redes distintos possam se conectar é preciso interligá-las através de um roteador.

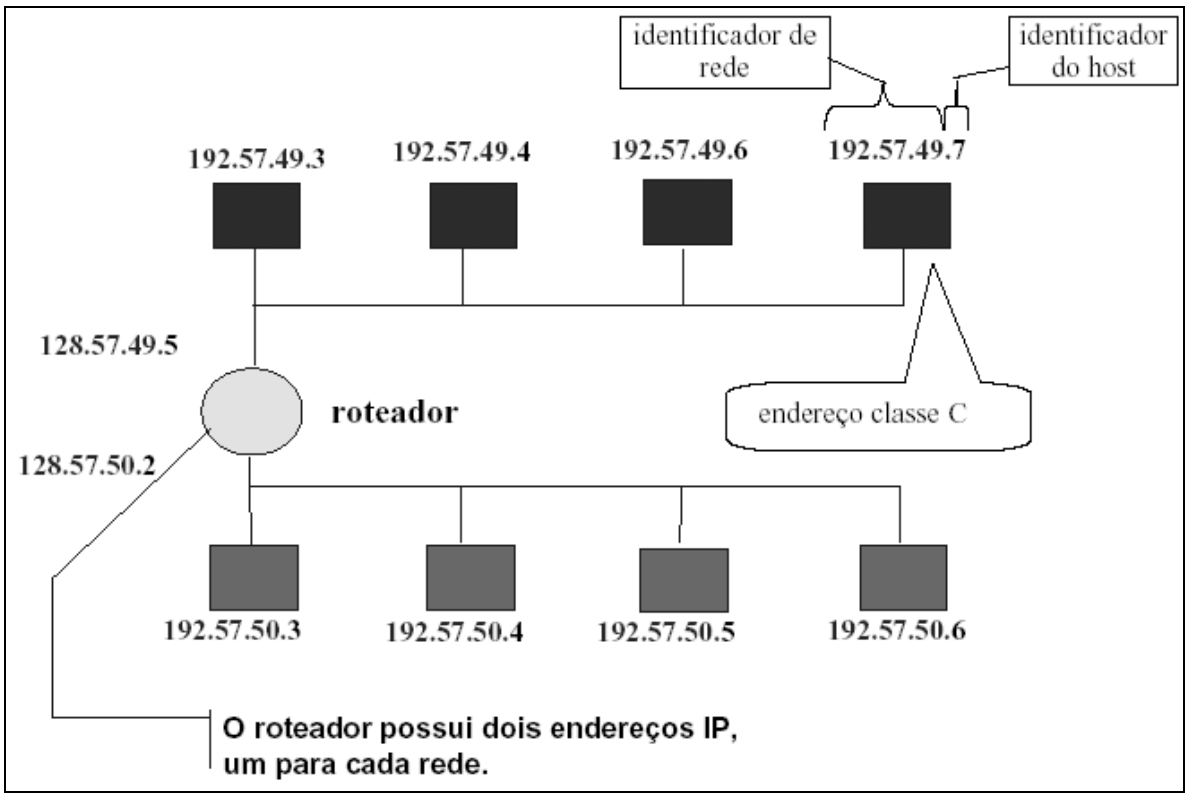


Figura 34 - Exemplo de Atribuição de Endereços IP

TERMOS

* identificador da rede: identifica uma rede conectada à internet. Todos os hosts conectados a uma dada rede possuem o mesmo identificador de rede, o que permite aos roteadores localizar rapidamente a rede a qual pertence uma estação (host).

* identificador do host: identifica uma única estação (host) dentro da rede. Dentro de uma mesma rede não podem haver duas estações com o mesmo identificador de host.

* host: termo utilizado para designar uma estação conectada a uma internet. O host representa genericamente qualquer computador da rede.

* notação decimal pontuada: nesta notação, os 32 bits são agrupados em 4 bytes. Cada byte é convertido para sua representação decimal equivalente, formando um endereço composto por quatro números separados por pontos. Exemplo:

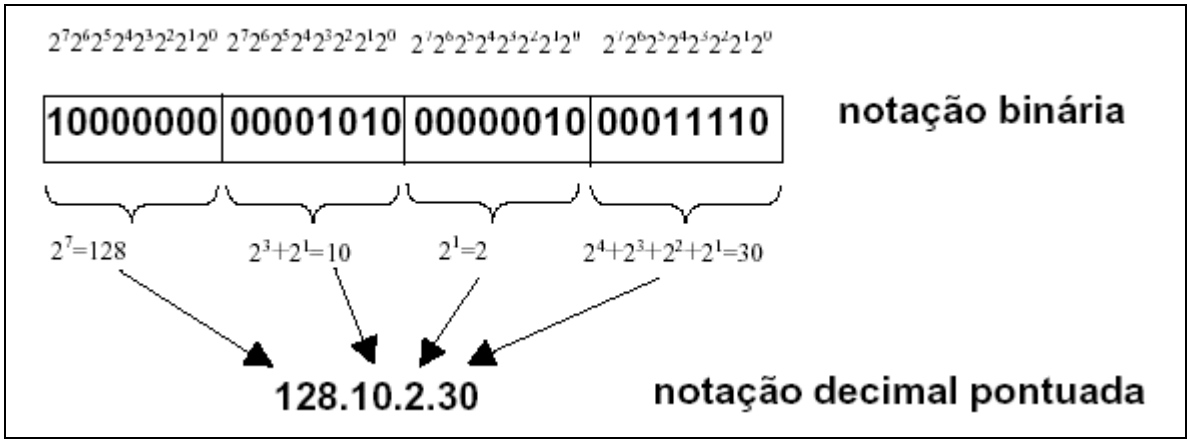


Figura 35 - Notação Decimal Pontuada do Enderço IP

7.2.2 DATAGRAMA IP

Conceito: Denominação dada à unidade de dados do protocolo de rede IP. Na arquitetura TCP/IP o fluxo de dados é transmitido em unidades de dados denominadas datagrama. Um datagrama consiste basicamente em duas partes: um cabeçalho de controle e um campo de dados.

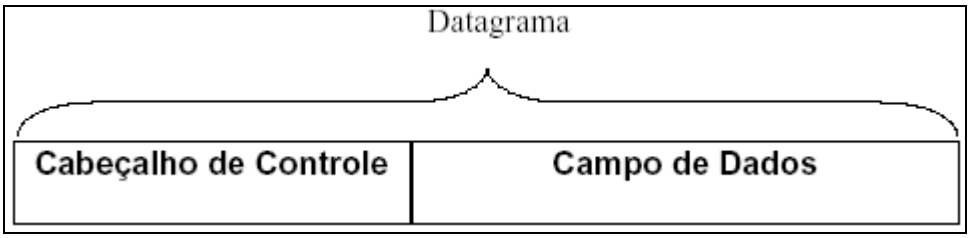


Figura 36 –Datagrama IP

Encapsulamento

Os datagramas são transportados no campo de dados do quadros da camada de enlace de dados, num processo conhecido como encapsulamento.

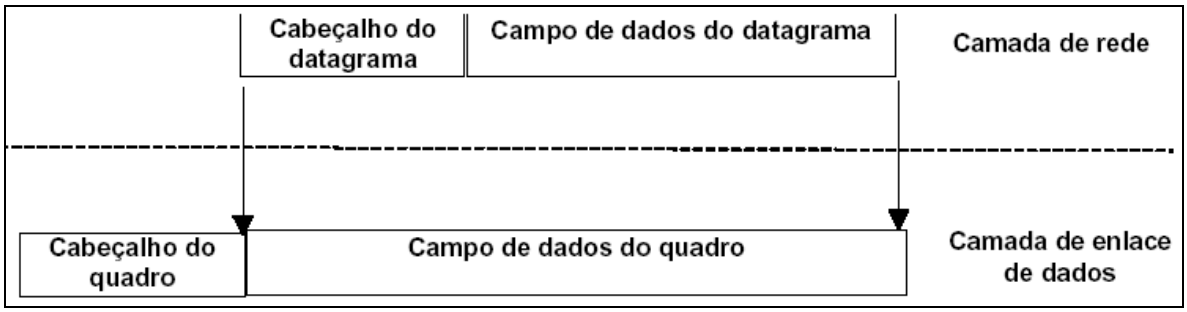


Figura 37 –Datagrama IP

7.2.2.1 Fragmentação e Remontagem de Datagramas

O tamanho máximo permitido para os quadros pode ser inferior ao tamanho máximo de um datagrama. Por exemplo, as redes Ethernet limitam o tamanho dos quadros a apenas 1500 bytes, enquanto os datagramas IP podem chegar até 64 K bytes. Nesse caso, é necessário transmitir um datragrama utilizando vários quadros. Neste processo, o campo de dados é dividido em vários fragmentos, cada um suficientemente pequeno para caber num quadro. Cada fragmento é transportado através da rede TCP/IP como se fosse um datagrama independente. O processo de fragmentação é efetuado pelas estações transmissoras e pelos roteadores que transportam os datagramas. Como os roteadores interligam redes de tecnologias diferentes, sempre que necessário, eles fragmentam ainda mais o datagrama para adaptá-lo a rede de destino. No destino final, a estação receptora reagrupa os fragmentos reconstruindo o datagrama original.

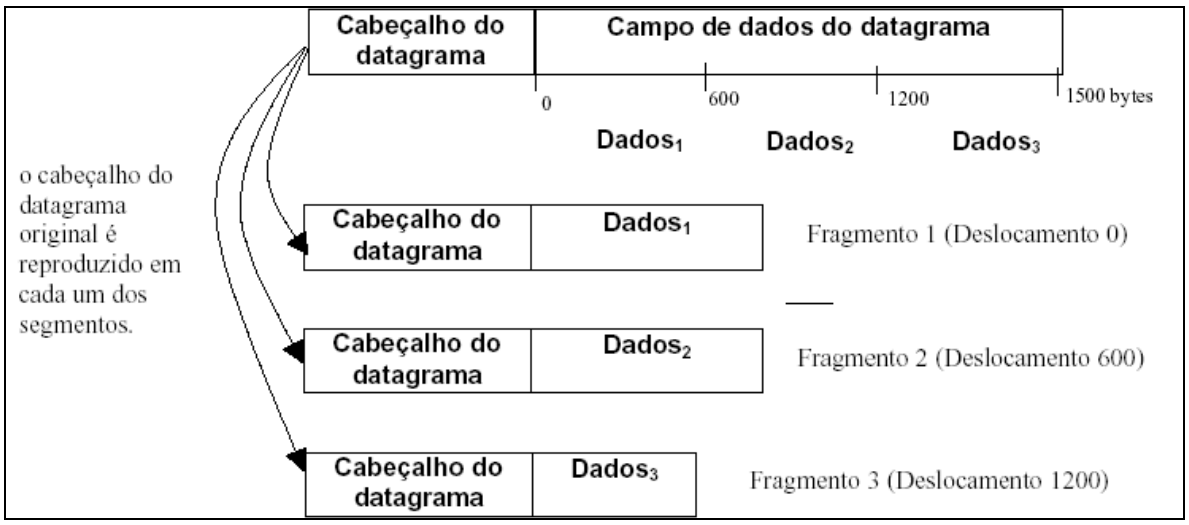


Figura 38 - Fragmentos do Datagrama IP

7.2.2.2 Formato de um Datagrama IP

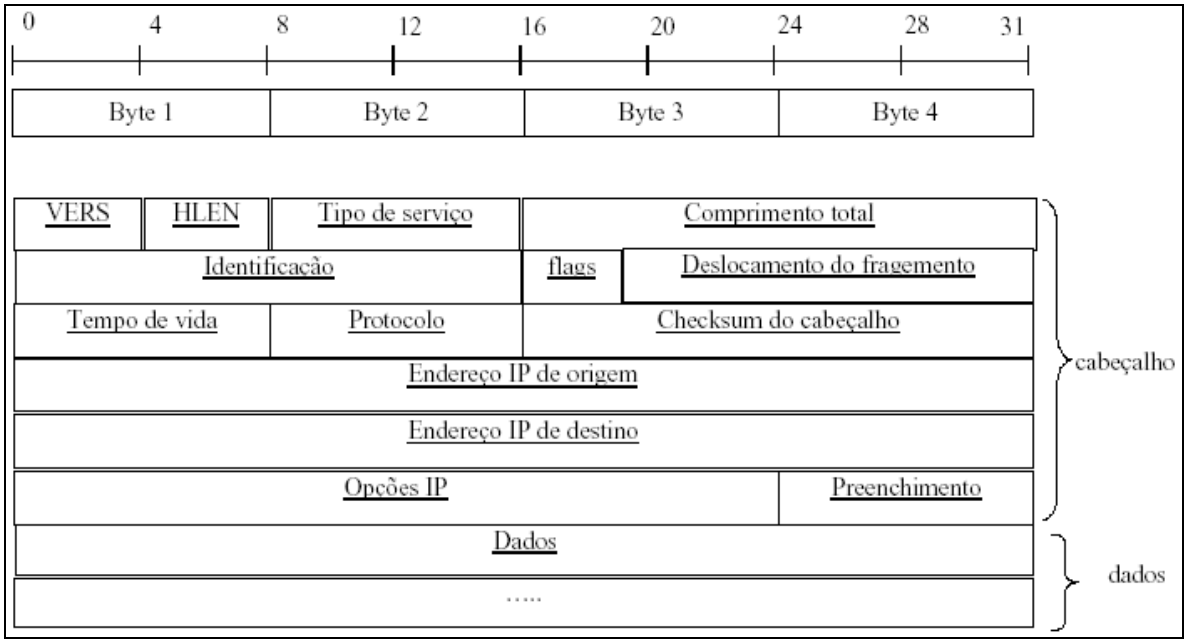


Figura 39 - Formato do Datagrama IP

- VERS: Idenfica a versão do procotocolo IP utilizada para criar o datagrama. A versão atual é 4.
- HLEN: Os 4 bits desse campo determinam o comprimento do cabeçalho do datagrama em múltiplos de palavras de 32 bits. O comprimento do cabeçalho é variável pois os campos "Opções IP" e "Preenchimento" não tem tamanho fixo. O tamanho usual do cabeçalho é de 20 bytes, quando os campos "Opções IP" e "Preenchimento" são nulos. Nesse caso, o campo HLEN apresenta comprimento igual a 5 (5 X 32 bits = 20 bytes).
- Tipo de serviço: contém informações que descrevem a importância do datagrama (através de 8 níveis de prioridade) e a qualidade esperada para o serviço de entrega. A qualidade do serviço é descrita por 3 bits denominados D, T e R. O bit D=1 solicita um baixo atraso, o bit T=1 solicita uma alta taxa de transmissão e o bit R=1 solicita uma transmissão altamente confiável. As informações desse campo são geralmente ignoradas pelos roteadores que transportam o datagrama.
- Comprimento total: informa o comprimento total do datagrama, incluindo o cabeçalho e o campo de dados, em bytes. Como esse campo possui 16 bits, o tamanho máximo de um datagrama é 216 ou 64 Kbytes.
- Identificação: Contém um número inteiro que identifica o datagrama. Esse campo é utilizado no processo de fragmentação e remontagem de datagamas. Todos os

fragmentos de um mesmo datagrama contém o mesmo número de identificação. Dessa forma, o receptor consegue identificar facilmente os fragmentos que precisam ser reagrupados para remontar o datagrama original.

- Flags: Campo composto pelos bits DF (don´t fragment) e MF (more fragments). A estação transmissora assinala DF=1 para indicar que o datagrama não deve ser fragmentado. Nesse caso, se um roteador precisar fragmentar o datagrama para adequá-lo a rede de destino, o datagrama é descartado. O bit MF=1 é utilizado para indicar que o fragmento é o último pedaço do datagrama original. Quando uma estação recebe um fragmento com MF=0, ela sabe que deve esperar a chegada de mais fragmentos para completar a remontagem do datagrama.
- Deslocamento do Fragmento: Esse campo contém a posição relativa do fragmento em relação ao datagrama original, medido em bytes. Os fragmentos de um datagrama não chegam no receptor necessariamente na mesma ordem em que foram transmitidos. Utilizando a informação do campo de Deslocamento, a estação receptora consegue reordenar os fragmentos recebidos, e remontar o datagrama original.
- Tempo de vida: (TTL - Time to Live). Indica o tempo em segundos que o datagrama pode permanecer na rede internet. Quando uma estação transmite um datagrama, ela assinala o valor do TTL. Toda vez que o datagrama é processado por um roteador, o TTL é decrementado. Quando o TTL expira, o datagrama é descartado, mesmo que o destino final não tenha sido atingido.
- Protocolo: O campo protocolo contém um código que especifica o tipo de protocolo de transporte encapsulado no campo de dados do datagrama (geralmente TCP ou UDP).
- Checksum do cabeçalho: Este campo contém o checksum de todos os bytes que compõe o cabeçalho de controle, excluindo apenas o próprio campo de checksum. Este campo é utilizado pela estação receptora para verificar a integridade do cabeçalho de controle do datagrama recebido.
- Endereço IP de origem: contém o endereço IP que identifica a estação transmissora.
- Endereço IP de destino: contém o endereço IP que identifica a estação de destino. Esse campo reflete sempre o destino final, não importando se o datagrama passará ou não por roteadores intermediários.

- Opções IP: Campo com tamanho variável de 0 até vários bytes. Esse campo pode conter uma série de códigos em seqüência, cada um deles definido uma opção relativa ao processamento dos datagramas. As opções são geralmente relacionadas a aspectos como segurança, roteamento, relatórios de erro, depuração, etc.
- Preenchimento: Esse campo completa a seqüência do campo "Opções" com bits de preenchimento de valor "0", garantindo que o tamanho total dos campos "Opções + Preenchimento" seja múltiplo de 32 bits.
- Dados: contém os dados transportados pelo datagrama. Os dados transportados correspondem geralmente a unidade de dados do procotolo de transporte TCP ou UDP.

7.2.3 MAPEAMENTO DE ENDEREÇOS

Conceito: Denominação dada ao processo de associar um endereço IP ao endereço físico de uma interface de rede.

Para poder transmitir um datagrama, a estação transmissora precisa conhecer todos as informações de endereçamento relacionadas ao destinatário, tanto ao nível da camada de rede (endereço IP) quanto ao nível da camada de enlace de dados (endereço físico). Na arquitetura TCP/IP, todas as referências aos endereços das estações são feitas através de endereços IP. O endereço físico do destinatário é descoberto dinamicamente pelo transmissor antes de efetuar a comunicação, utilizando um protocolo auxiliar denominado ARP.

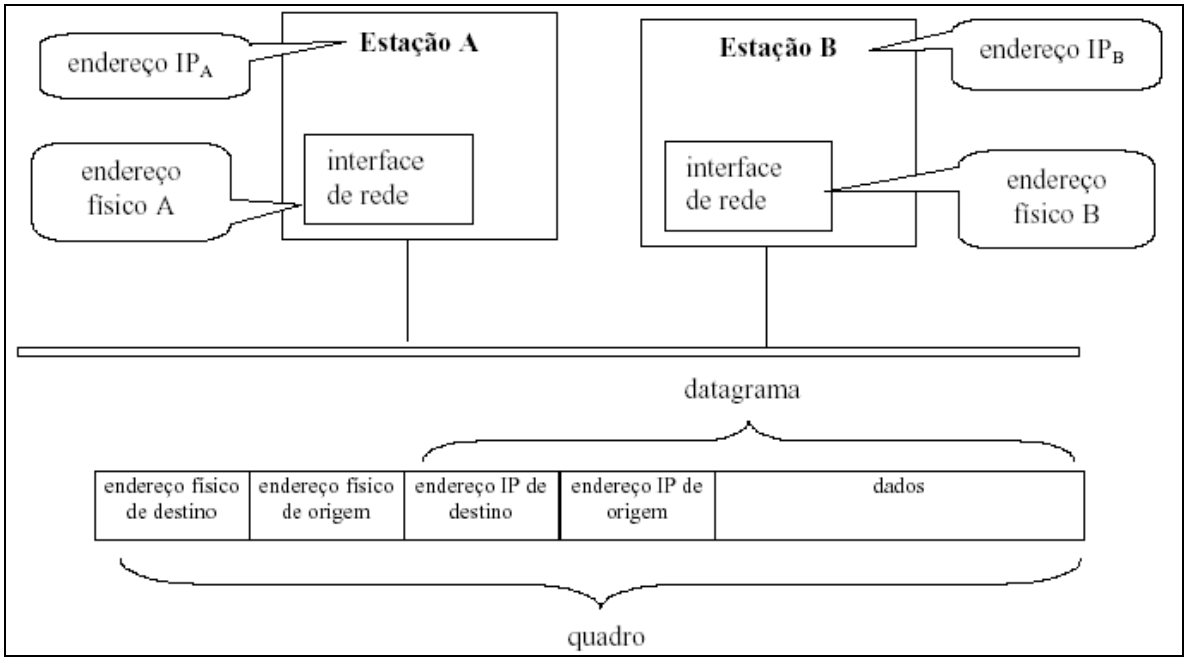


Figura 40 – Representação de Mapeamento de Endereços

As figuras abaixo [a,b e c] ilustram uma Transmissão de um datagrama de A para B.

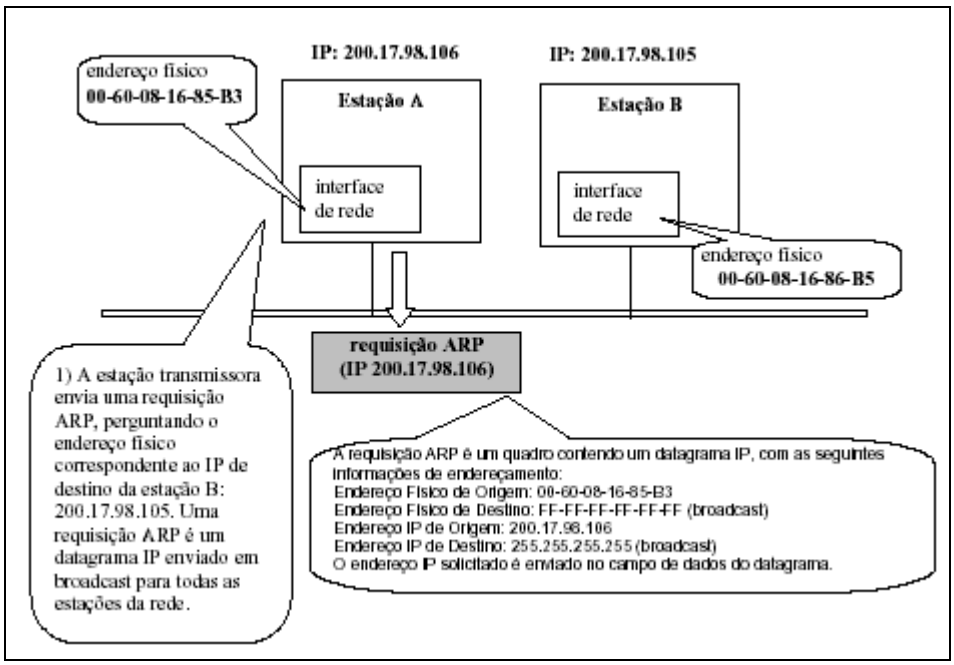


Figura 41 - Transmissão de um datagrama - parte A

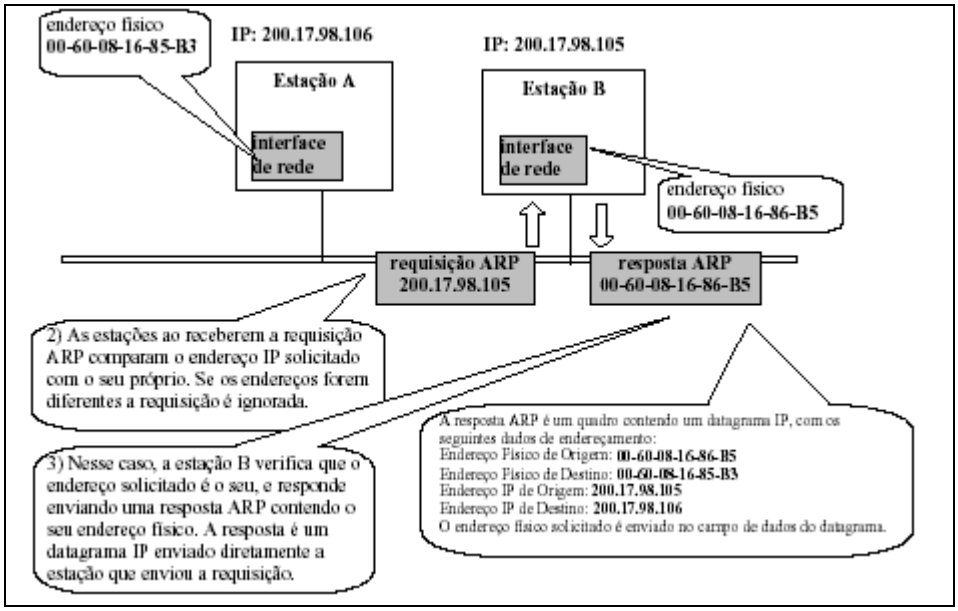


Figura 42 - Transmissão de um datagrama - parte B

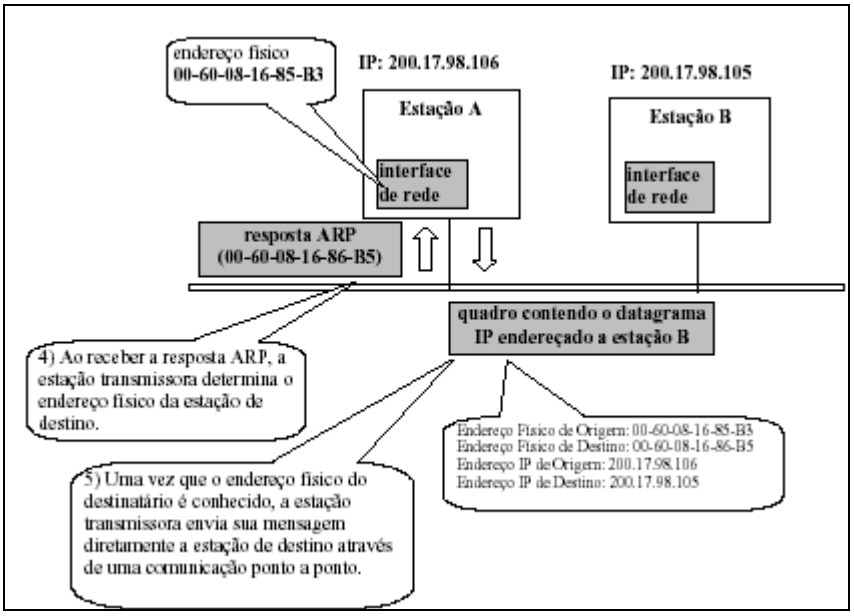


Figura 43 - Transmissão de um datagrama - parte C

TERMOS

* endereço físico: corresponde geralmente ao endereço associado a interface de rede da estação ou roteador. Segundo a terminologia IEEE, o endereço físico é comumente referido como endereço MAC.

* ARP: (Address Resolution Protocol). Protocolo utilizado para que a estação transmissora descubra o endereço físico do destinatário.

7.2.4 Roteamento

Conceito: Operação que consiste em enviar os datagramas até seu destino final, passando se necessário por um ou mais roteadores intermediários.

A arquitetura TCP/IP define os mecanismos para que os datagramas sejam entregues no seu destino final, independente dele estar situado na mesma rede do transmissor (comunicação intra-rede), ou numa rede externa interligada através de roteadores (comunicação inter-redes).

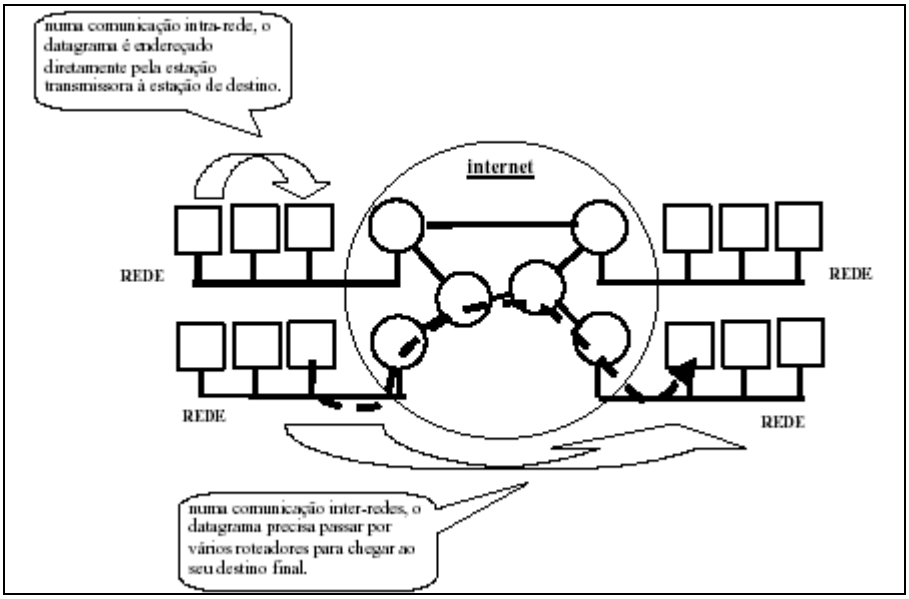


Figura 44 - Ilustração de Roteamento

Comunicação intra-rede

Numa comunicação entre duas estações situadas na mesma rede, o transmissor envia o quadro diretamente ao destino final, preenchendo os campos do destinatário com o endereço físico e o endereço IP da estação receptora.

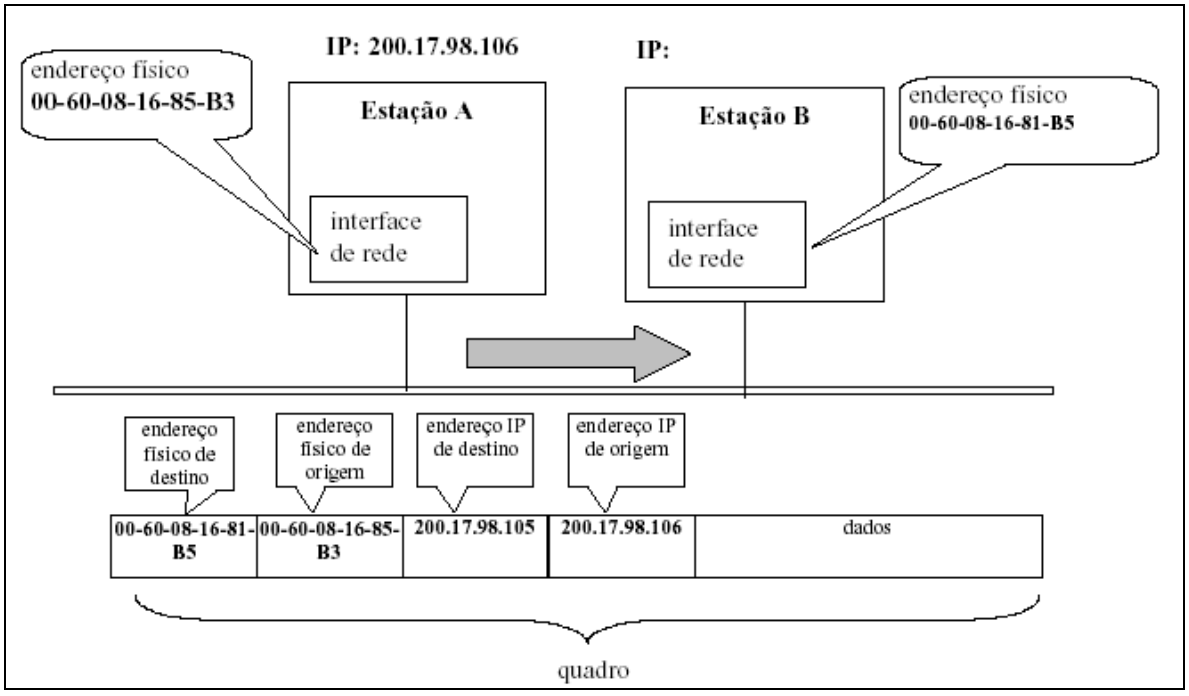


Figura 45 - Transmissão de um Datagrama de A para B

Comunicação inter-redes

Numa comunicação entre estações conectadas a redes diferentes, a comunicação é dividida em vários saltos. Cada salto representa uma comunicação entre um par estação roteador ou roteador-roteador ligados fisicamente. Os endereços IP de origem e de destino se mantêm os mesmos durante todos os saltos do datagrama. O endereço físico, entretanto, é modificado para endereçar os elementos participantes de cada salto.

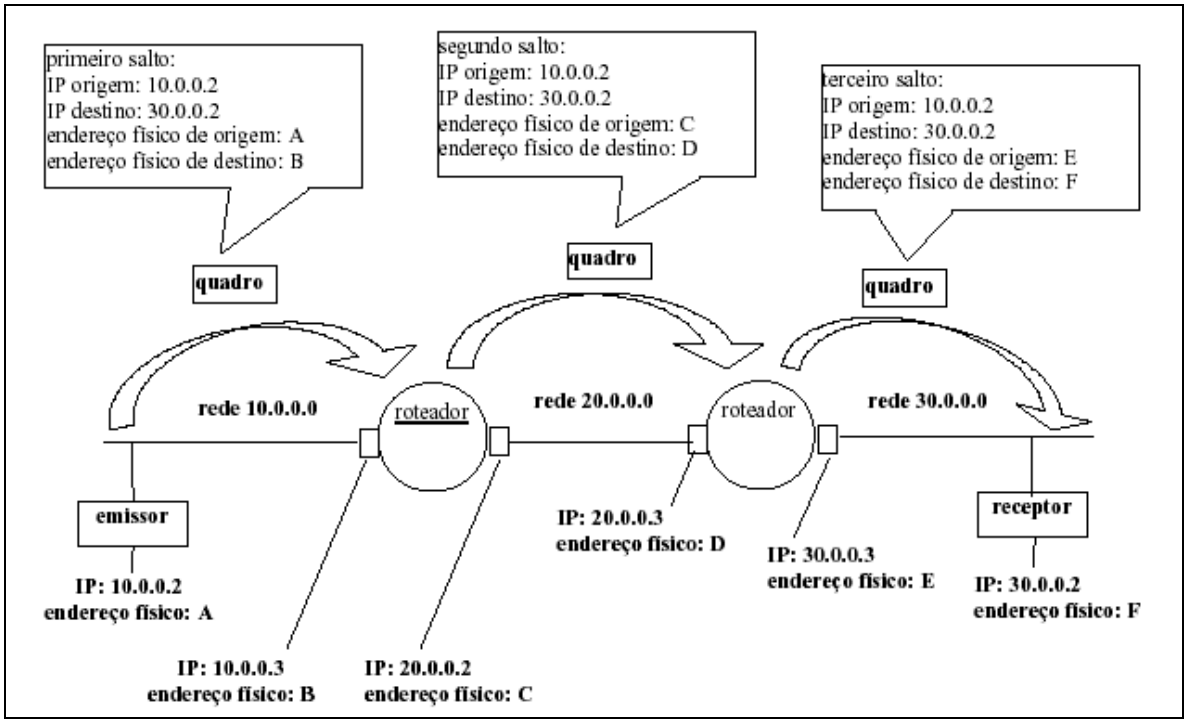


Figura 46 - Exemplo de Comunicação com 3 saltos

* roteador: cada porta do roteador possui um endereço IP distinto, pertencente a mesma rede que interconecta.

7.2.4.1 Tabelas de Roteamento

O processo de roteamento envolve uma série de decisões tomadas tanto pelas estações quanto pelos roteadores. Por exemplo, uma estação precisa determinar se o datagrama a ser transmitido deve ser endereçado diretamente ao destinatário ou a um roteador intermediário. Ao receber um datagrama, os roteadores também precisam determinar se devem retransmití-lo a outro roteador ou diretamente à estação de destino. O processo de decisão quanto ao roteamento é baseado em tabelas armazenadas localmente pelas estações e pelos roteados denominadas "tabelas de roteamento IP".

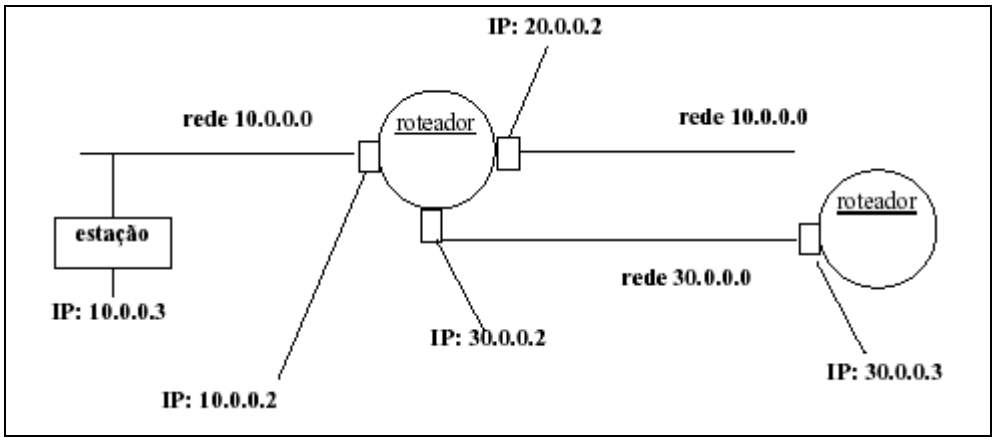


Figura 47 - Roteamento em Redes

Quadro 3 - Tabela de Roteamento da Estação

Endereço de IP	Endereço de Gateway	Interface	Custo
pertence a rede 10.x.x.x	entregar diretamente	10.0.0.3	1
pertence a outra rede	10.0.0.2 (gateway default)	10.0.0.3	1

Quadro 4 - Tabela de Roteamento do Roteador

Endereço de Rede	Endereço de Gateway	Interface	Custo
pertence a rede 10.x.x.x	entregar diretamente	10.0.0.2	1
pertence a rede 20.x.x.x	entregar diretamente	20.0.0.2	1
pertence a rede 30.x.x.x	entregar diretamente	30.0.0.2	1
pertence a outra rede	30.0.0.3 (gateway default)	30.0.0.2	1

* Endereço de rede: parte do endereço IP do destinatário correspondente ao identificador da rede. Cada entrada da tabela de roteamento indica qual ação deve ser tomada em função da rede que pertence o destinatário. Se a rede do destinatário não for encontrada em nenhuma entrada da tabela de roteamento, o datagrama é enviado para o gateway default (geralmente, o roteador que interliga a rede a internet).

* Endereço de gateway: O endereço de gateway não é usado diretamente na formatação do datagrama. Ele é utilizado pelo transmissor para descobrir o endereço físico do destinatário, através do protocolo ARP. Se o destinatário pertencer a uma rede distinta do transmissor, então o endereço de gateway corresponde a uma porta do roteador que irá

encaminhar o datagrama. Se o transmissor e o receptor estiverem na mesma rede, então o endereço de gateway é o próprio endereço do destinatário.

* Custo: medida relativa do custo de utilização da rota. A informação de custo é utilizada pelo roteador quando existir mais de uma rota para o mesmo destino.

7.3. CAMADA DE TRANSPORTE

Conceito: Os protocolos de transporte são capazes de manipular múltiplos endereços numa mesma estação, permitindo que várias aplicações executadas no mesmo computador possam enviar e receber datagramas independentemente.

Dependendo do tipo de serviço de comunicação utilizado, as funções da camada de transmissão podem ser executadas pelos protocolos TCP ou UDP. O protocolo TCP (*Transmission Control Protocol*) oferece serviços de comunicação confiáveis e orientados a conexão. O protocolo UDP (*User Datagram Protocol*) oferece serviços do tipo datagrama, isto é, não orientados a conexão.

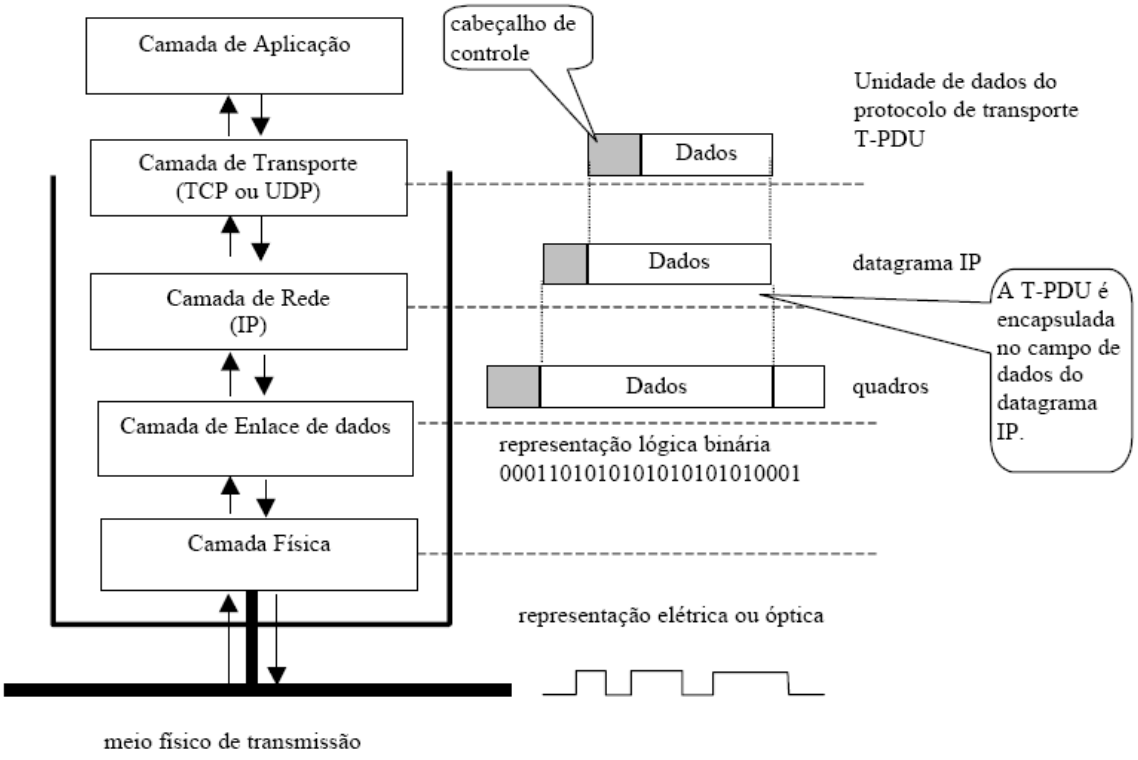


Figura 48 – Protocolo TCP

7.3.1 Protocolo TCP

Conceito: Protocolo da camada de transporte que oferece um serviço de comunicação confiável e orientado a conexão sobre a camada de rede IP.

O Protocolo TCP (*Transmission Control Protocol*) é um protocolo orientado a conexão destinado a construir comunicações ponto a ponto confiáveis. Trata de questões relacionadas com: endereçamento por portas; comunicação confiável; controle de seqüenciação; segmentos TCP.

7.3.1.1. Endereçamento por portas:

O protocolo TCP utiliza um nível de endereçamento complementar aos endereços IP, que permite distinguir vários endereços de transporte numa mesma estação. Os endereços de transporte são números inteiros de 16 bits denominados portas.

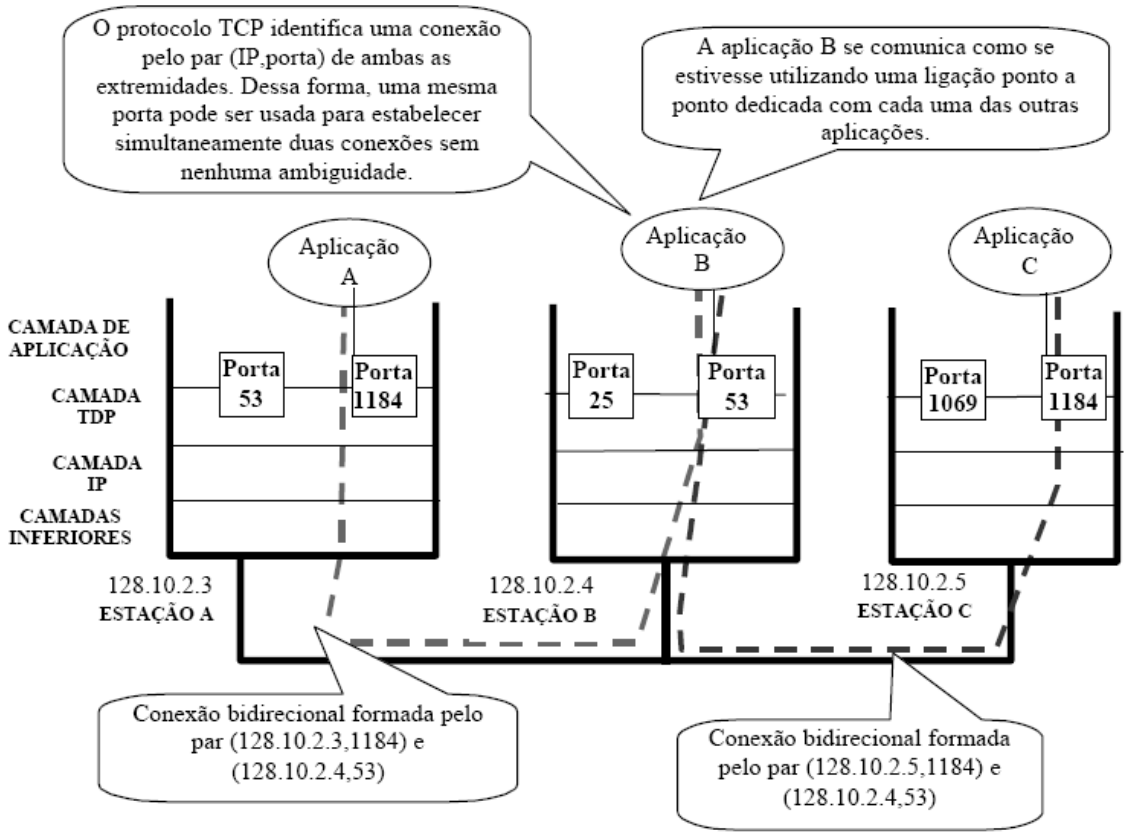


Figura 49 – Endereçamento por Portas

7.3.1.2. Comunicação confiável:

O protocolo TCP oferece um serviço de comunicação confiável utilizando uma técnica conhecida como “confirmação positiva com retransmissão”. Nesse método, o

receptor precisa confirmar o recebimento dos dados através de uma mensagem de confirmação (ACK). O transmissor espera a confirmação de cada mensagem transmitida antes de enviar uma nova mensagem. Se a confirmação demorar mais do que um tempo pré-estabelecido, o transmissor retransmite a mensagem.

7.3.1.3. Controle de Seqüenciação:

O protocolo TCP oferece um serviço de comunicação orientado a conexão, que garante que as mensagens serão recebidas na mesma seqüência em que foram transmitidas. Esta característica permite fragmentar as mensagens muito grandes em porções menores de maneira a compatibilizá-las com o tamanho máximo imposto aos datagramas IP. A mensagem original é reconstruída de maneira transparente pela camada de transporte do receptor.

7.3.1.4. Segmentos TCP

A unidade de dados do protocolo TCP é denominada segmento. Usualmente, cada segmento TCP é encapsulado no campo de dados de um único datagrama. Um segmento TCP é composto de duas partes: um cabeçalho de controle e um campo de dados. O formato do segmento é detalhado abaixo.

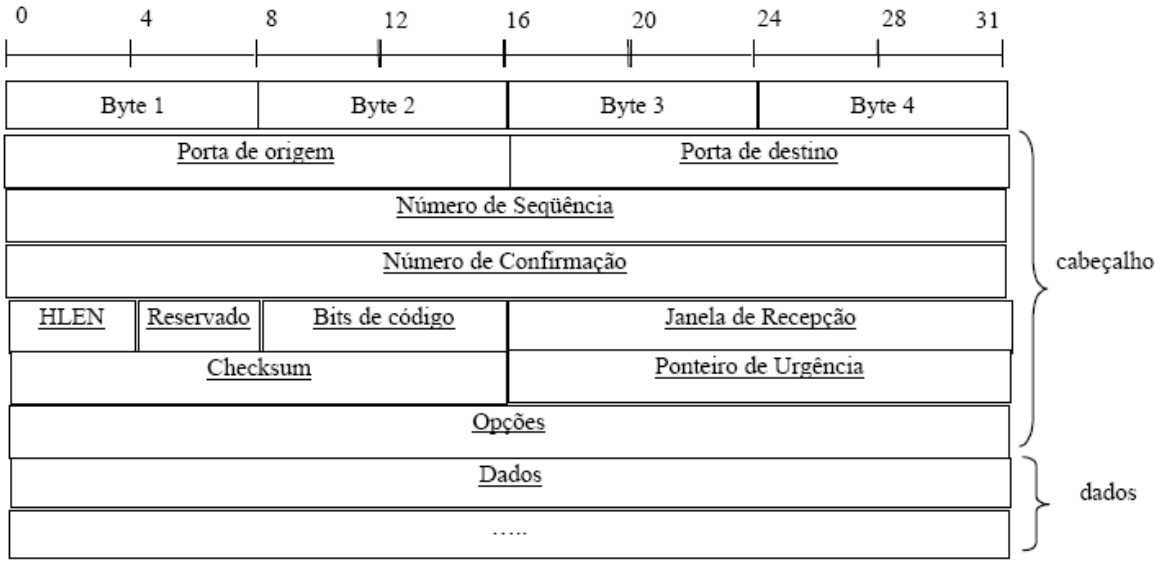


Figura 50 – Segmento TCP

- *Porta de Origem*: identificador de 16 bits que identifica a porta que transmitiu o segmento.
- *Porta de Destino*: identificador de 16 bits que identifica a porta para onde o segmento será transmitido.
- *Número de Seqüência*: O protocolo TCP fragmenta mensagens muito longas e as transmite numa seqüência de segmentos. Este campo indica que porção da mensagem original está sendo transmitida no segmento corrente. Essa informação é utilizada pelo receptor para reordenar os segmentos que cheguem fora de ordem.

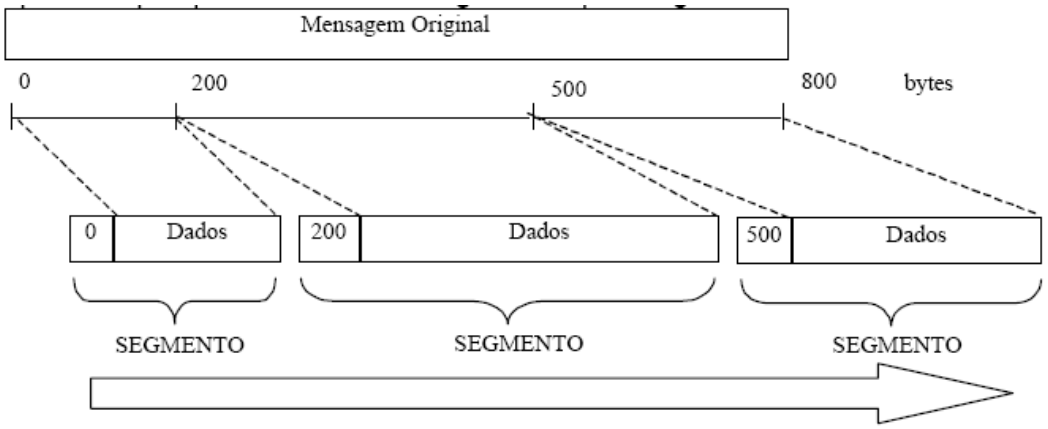


Figura 51 – Seqüência dos Segmentos

- *Número de confirmação*: Identifica o número do próximo byte que o receptor espera receber. Esta informação é enviada pelo receptor ao transmissor através das mensagens de confirmação de recebimento (ACK).
- *HLEN*: contém um número inteiro que determina o comprimento do cabeçalho do datagrama em múltiplos de palavras de 32 bits. O comprimento do cabeçalho é variável pois os campos "Opções " e "Preenchimento" não tem tamanho fixo.
- *Reservado*: campo reservado para uso futuro.
- *Bits de código*: Este campo identifica o tipo de mensagem transportada pelo segmento. Os segmentos podem transportar mensagens de vários tipos: confirmação (ACK), estabelecimento ou liberação de conexões, dados, etc.
- *Janela de Recepção*: TCP provê meios para que o receptor cadencie o fluxo de dados enviados pelo transmissor. Toda vez que o receptor confirma o recebimento de uma mensagem (enviando uma mensagem ACK para o transmissor), ele preenche o campo "Janela de Recepção" informando o número de bytes que ele é capaz de

receber na próxima transmissão. O transmissor leva em consideração essa informação para determinar o tamanho do próximo segmento a ser enviado.

- *Ponteiro de Urgência*: Indica a posição (em bytes) em relação a seqüência de dados recebidos onde dados urgentes poderão ser encontrados. Este mecanismo é utilizado par que o transmissor possa enviar mensagens de alta prioridade ao receptor.
- *Checksum*: Este campo contém o checksum de todos os bytes que compõe o segmento TCP (cabeçalho de controle e dados). Este campo é utilizado pela estação receptora para verificar a integridade do segmento recebido.
- *Opções*: Campo opcional de tamanho variável, múltiplo de 32 bits. Este campo foi criado para que o protocolo TCP possa disponibilizar facilidades adicionais que não foram cobertas pelos campos padronizados do cabeçalho de controle.
- *Dados*: Contém os dados transportados pelo segmento TCP.

7.3.2 PROTOCOLO UDP

Conceito: Protocolo da camada de transporte que oferece um serviço de comunicação não orientado a conexão, construído sobre a camada de rede IP.

O Protocolo UDP (*User Datagram Protocol*) é um protocolo não orientado a conexão que oferece serviços de comunicação bastante elementares. O protocolo é não confiável, isto é, não há garantia de entrega dos datagramas transportados. O protocolo também não garante que os datagramas cheguem na mesma ordem em que foram transmitidos. Sua principal função é permitir a distinção de múltiplos destinos numa mesma estação. Sendo não orientado a conexão, o protocolo UDP pode ser utilizado tanto em comunicações do tipo difusão (*broadcast*) quanto ponto a ponto.

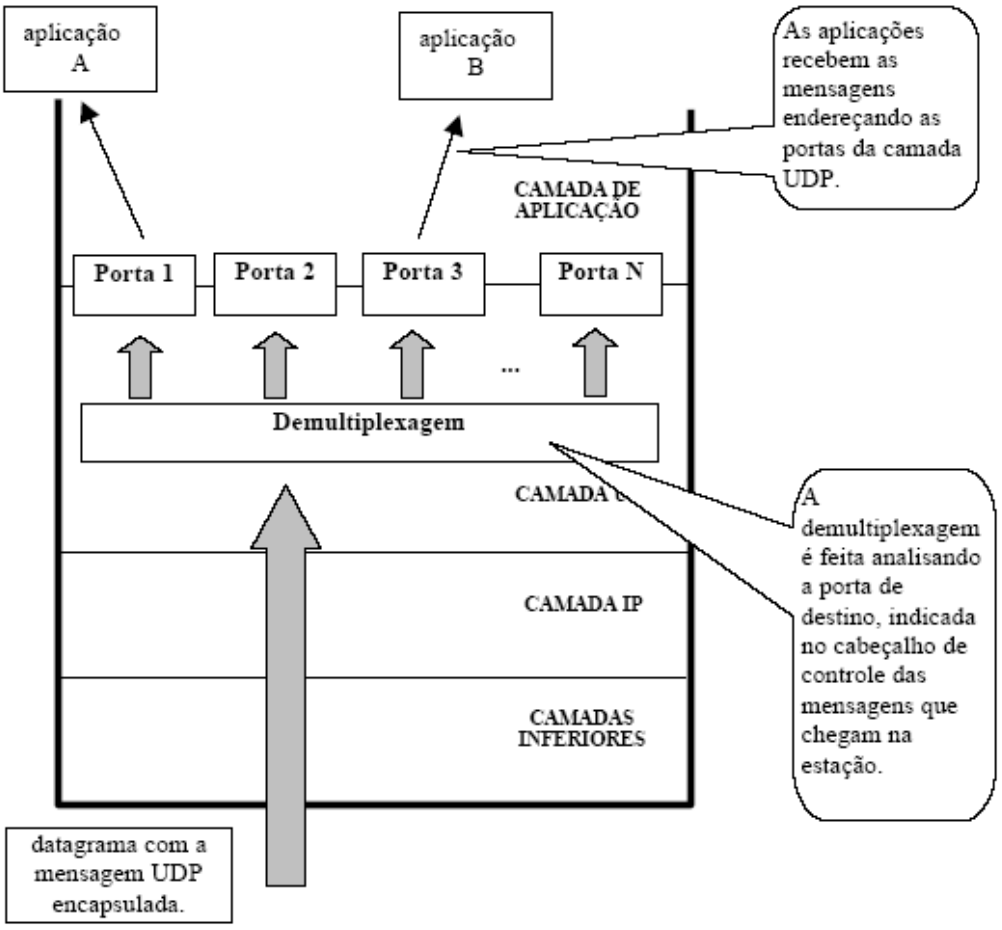


Figura 52- Protocolo UDP

7.3.2.1 Mensagem UDP

A unidade de dados do protocolo UDP é denominada *user datagram*, ou simplesmente mensagem UDP. Uma mensagem UDP é composta de duas partes: um cabeçalho de controle e um campo de dados. O formato da mensagem é detalhado abaixo.

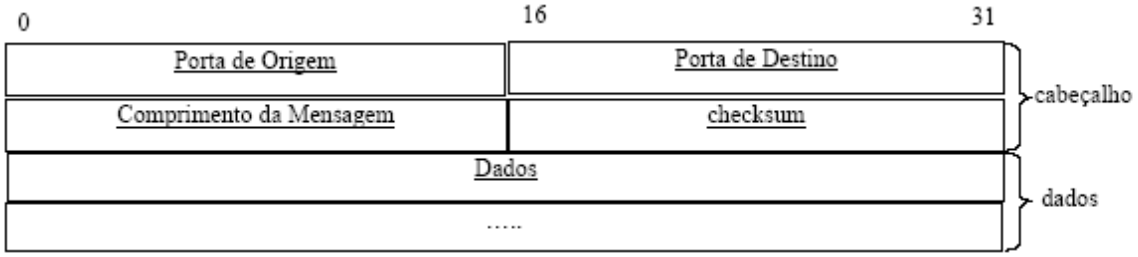


Figura 53 – Mensagem UDP

- *Porta de Origem*: identificador de 16 bits que identifica o endereço, ao nível da camada de transporte, para o qual deve ser enviado uma eventual resposta à mensagem transmitida.
- *Porta de Destino*: identificador de 16 bits que identifica o endereço do destinatário da mensagem ao nível da camada de transporte.
- *Comprimento da mensagem*: corresponde ao comprimento total da mensagem UDP, em bytes, incluindo o cabeçalho e o campo de dados.
- *Checksum*: O preenchimento do campo *checksum* é opcional. A informação deste campo é usada pelo receptor para verificar a integridade dos dados recebidos. No caso de haver erro, o receptor descarta a mensagem.
- *Dados*: O campo de dados contém as informações a serem transmitidas. O comprimento máximo da mensagem UDP, incluindo o campo de dados e o cabeçalho é de 64 Kbytes.

7.4. CAMADA DE APLICAÇÃO

Conceito: Protocolos que disponibilizam serviços padronizados de comunicação, destinados a dar suporte ao desenvolvimento de aplicações para os usuários. As funções da camada de aplicação da arquitetura TCP/IP são executadas por um conjunto amplo de protocolos, que oferecem serviços de comunicação padronizados. Cada um desses protocolos agrupa funções das camadas sessão, apresentação e aplicação do modelo OSI.

Os protocolos de aplicação disponibilizam serviços de comunicação de alto nível para que programadores implementem aplicativos que utilizam recursos da rede. Os protocolos de aplicação estão num processo de evolução contínua, sendo que novos protocolos estão sendo continuamente propostos aumentando a gama de serviços disponibilizados.

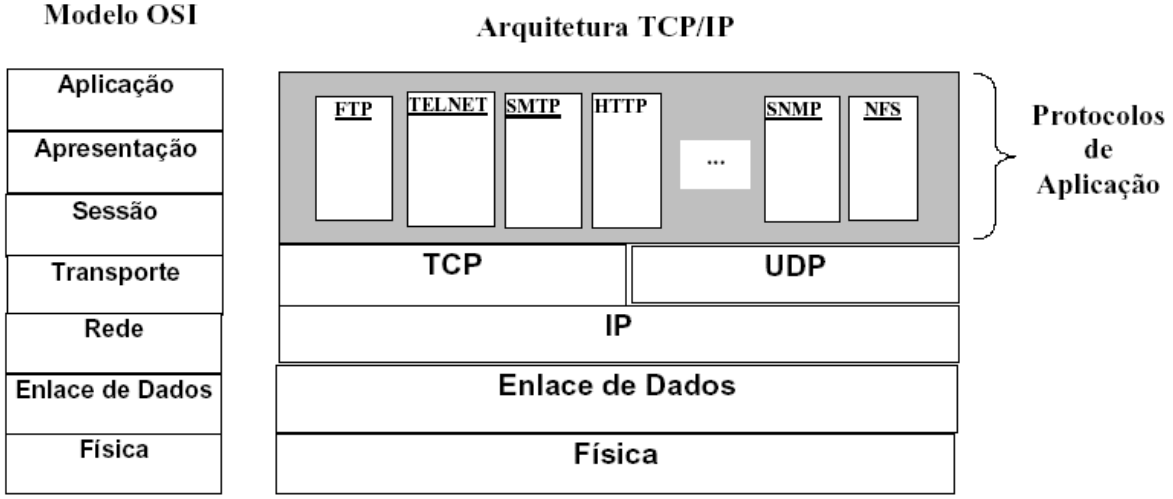


Figura 54- Protocolos da Camada de Aplicação

7.4.1 Protocolos do Nível de Aplicação

FTP: *File Transfer Protocol*. Protocolo que implementa serviços de transferência de arquivos de uma estação para outra (ponto a ponto) através de rede.

TELNET: *Serviço de Terminal Remoto*. Protocolo utilizado para permitir aos usuários controlarem estações remotas através da rede.

SMTP: *Simple Mail Transfer Protocol*. Protocolo utilizado para transferência de mensagens de correio eletrônico de uma estação para outra. Esse protocolo especifica como 2 sistemas de correio eletrônico interagem.

HTTP: *Hypertext Tranfer Protocol*. Protocolo utilizado para transferência de informações multimídia: texto, imagens, som, vídeo, etc.

SNMP: *Simple Network Monitoring Protocol*. Protocolo utilizado para monitorar o estado das estações, roteadores e outros dispositivos que compõe a rede.

NFS: *Network File System*. Protocolo desenvolvido pela "SUN *Microsystems*, *Incorporated*", que permite que as estações compartilhem recursos de armazenamento de arquivos através da rede.

7.4.2 Endereçamento

A rede Internet utiliza um modelo de endereçamento universal, baseado em endereços IP. Um endereço IP permite identificar qualquer computador (host) conectado a rede de maneira única e inconfundível. Essa informação é utilizada em todas as comunicações entre os computadores que se conectam a Internet. Uma vez que os endereços IP contém informações relativas a rede e ao host, sua atribuição está relacionada com a topologia física da Internet. A comunicação entre hosts com endereços IP com identificadores de rede diferentes precisa ser intermediada por um roteador. Hosts pertencentes a mesma rede se comunicam diretamente sem necessidade de roteamento.

Para permitir a integração de redes pelo mundo todo, a atribuição de endereços IPs para os computadores ligados a Internet deve seguir uma política global, pois os endereços não podem ser duplicados ou desperdiçados.

7.4.3 Endereços na Internet

Conceito: a atribuição de endereços IP para os computadores que se conectam a Internet é coordenada por autoridades de abrangência mundial, de maneira a evitar a duplicação e a má distribuição de endereços.

A distribuição de endereços IP para computadores que se conectam a Internet mundial é feita de acordo com políticas definidas na RFC 2050. A implementação dessa política é de responsabilidade da IANA. A IANA implementa a política de distribuição de endereços IP com o auxílio de diversas entidades denominadas "autoridades de registro na Internet". A IANA distribui blocos do espaço total de endereços IP para autoridades

regionais. Cada autoridade regional possui uma abrangência continental. Para facilitar a administração dos endereços IP, as autoridades regionais delegam a tarefa de alocação dos endereços IP para autoridades locais, que possuem geralmente abrangência nacional.

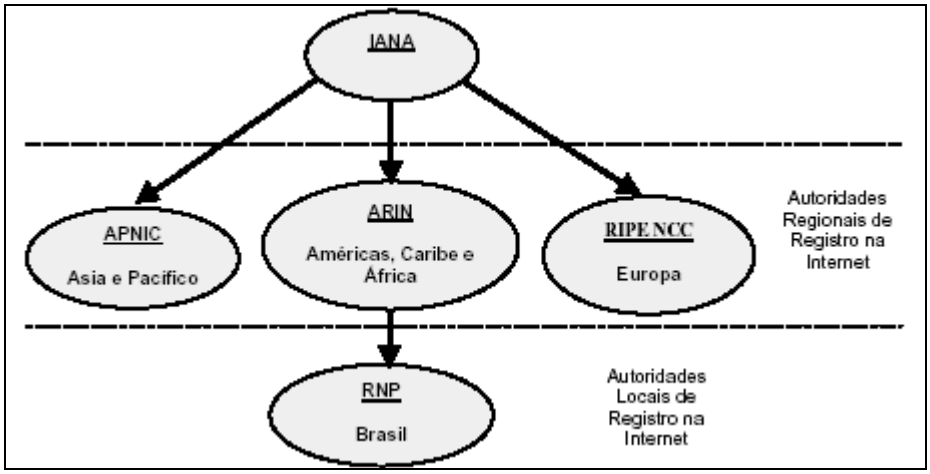


Figura 55 – Hierarquia de Registros de Endereçamento na Internet

Termos:

* RNP: No Brasil, a autoridade de registro na Internet é a RNP (Rede Nacional de Pesquisa). A RNP delega a responsabilidade de alocação de endereços IP a FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo). Deve-se observar que a RNP é apenas um dos provedores de "*backbone*" que possibilitam o acesso a Internet no Brasil. De fato, todos os grandes provedores de "*backbone*" possuem blocos de números reservados a seus clientes. Por isso, não se faz necessário uma solicitação especifica à FAPESP.

* RFC 2050: *Request for Comment number* 2050. Documento elaborado por um grupo de trabalho IETF (*The Internet Engineering Task Force*) e aprovada pelo IESG (*Internet Engineering Steering Group*). Esse documento contém as diretivas para alocação de endereços IP para Internet.

* IANA (*The Internet Assigned Numbers Authority*). Organização que possui a responsabilidade de coordenar a distribuição de endereços IP pelo mundo.

* APNIC (*Asia-Pacific Network Information Center*). Autoridade responsável por alocar endereços IPs para as redes da Ásia e Pacífico.

* ARIN (*American Registry for Internet Numbers*) Autoridade responsável por alocar endereços IPs para a América do Norte, América do Sul, Caribe e regiões da África SubSaariana.

* RIPE NCC (*Reseau IP Europeens*) Autoridade responsável por alocar endereços IPs para as redes da Europa.

7.4.4 Conexão de Intranets com a Internet

Conceito: as Intranets podem ser conectadas a rede pública Internet, permitindo que os usuários de uma rede privada troquem informações com o mundo exterior.

É muito comum que numa mesma rede corporativa convivam aplicações que envolvam apenas comunicações internas juntamente com aplicações que envolvam a comunicação com o mundo exterior. Como conseqüência, certos *hosts* (clientes ou servidores) da rede são acessíveis apenas internamente e outros são acessíveis tanto internamente quanto externamente. A distinção do grau de conectividade com o mundo externo é importante, pois a alocação dos endereços IP dos hosts com conexão externa deve obedecer as regras impostas pelas autoridades que coordenam a Internet. As regras para atribuições de endereços IPs com diferentes graus de conectividade com o mundo externo são definidas pela RFC 1918. Esse documento classifica os hosts em três categorias, de acordo com o grau de conectividade com o mundo externo:

Termos:

* RFC 1918: *Request for Comment number* 1918. Documento elaborado por um grupo de trabalho IETF (*The Internet Engineering Task Force*) e aprovada pelo IESG (*Internet Engineering Steering Group*). Esse documento contém as diretivas para alocação de endereços IP em Intranets.

7.4.4.1 Hosts Categoria 1

Conceito: *Hosts* que se comunicam apenas internamente. Os hosts que se comunicam apenas no interior da rede comporativa e não tem acesso a redes externas ou a Internet são classificados como "Categoria 1". Cada hosts dessa categoria precisa de um endereço IP que seja único na empresa, mas que pode ser duplicado entre empresas diferentes. Numa rede Intranet sem conexão com a Internet, todos os hosts pertencem a categoria 1.

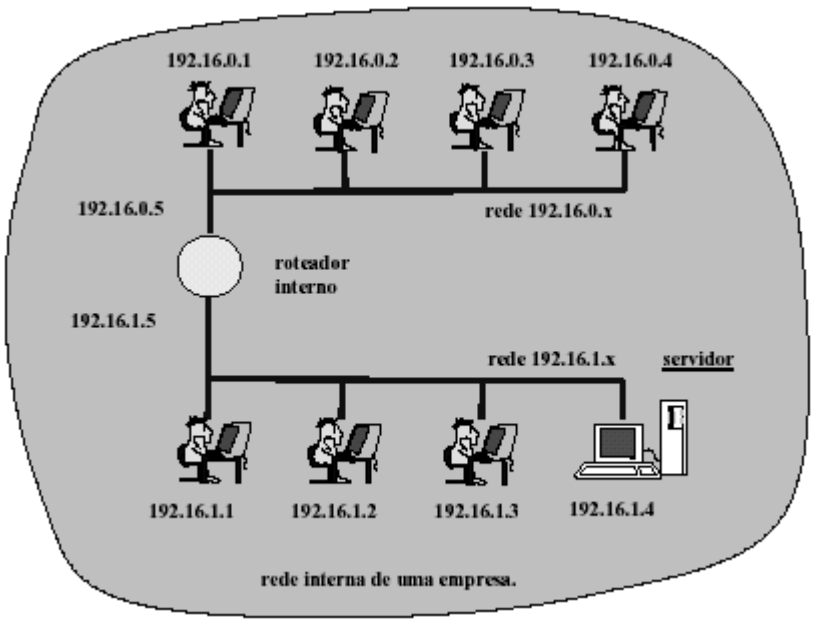


Figura 56 - Exemplo de uma rede Intranet constituída de duas redes físicas conectadas por um roteador

Termos:

* servidor: Computador responsável por armazenar informações e disponibilizar serviços de comunicação para os clientes. Os serviços disponibilizados pelo servidor correspondem àqueles definidos pelos protocolos de aplicação da arquitetura TCP/IP, como por exemplo, FTP (transferência de arquivos), SMTP (correio eletrônico), etc. Para ser funcional, uma rede Intranet precisa de pelo menos um servidor, podendo, se necessário, haver mais de um servidor na mesma rede. A rede Internet é constituída por uma infinidade de servidores.

7.4.4.2 Hosts Categoria 2

Conceito: Hosts que se comunicam indiretamente com o mundo externo. Muitas redes corporativas necessitam disponibilizar o acesso a Internet para seus funcionários,

mas sem comprometer a segurança da sua rede corporativa interna. Para permitir que clientes acessem o mundo externo sem conectá-los diretamente a Internet, utiliza-se usualmente um dispositivo denominado servidor proxy. Os hosts que se comunicam com o mundo externo através de dispositivos intermediários como os servidores proxies são classificados na categoria 2. As regras para atribuição de endereços IP aos hosts da categoria 2 são idênticas as regras da categoria 1. Apenas o servidor proxy necessita de um endereço IP registrado pelas autoridades que coordenam a Internet.

Na figura 57, tem-se um exemplo de uma rede Intranet interligada a Internet através de um servidor proxy. Nessa rede, os hosts estão na categoria 2

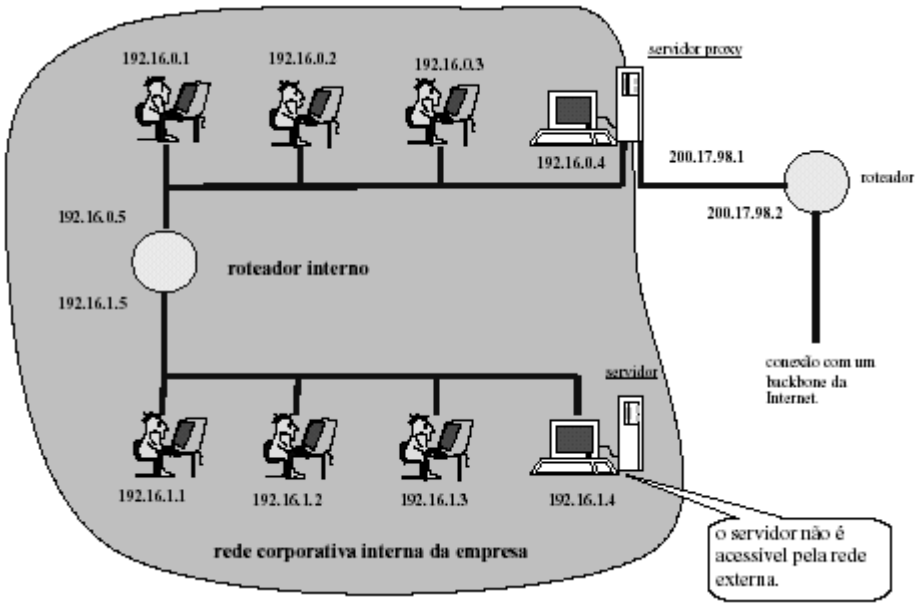


Figura 57 - Exemplo de uma rede Intranet interligada a Internet através de um servidor proxy

Termos:

* servidor proxy: Dispositivo responsável por intermediar a conexão entre os hosts internos e o mundo externo. O servidor proxy (procurador) é geralmente implementado através de um computador com duas interfaces de rede, uma conectada a rede interna e a outra a rede externa. Quando um cliente necessita acessar informações de um servidor externo, ele efetua o pedido ao servidor proxy. O servidor proxy, por sua vez, contata o servidor externo e retorna o resultado ao cliente. Nesse procedimento, o único computador da rede exposto ao mundo externo é o servidor proxy.

* acesso a Internet: O termo "acesso a Internet" implica que um host tem acesso a pelo menos um tipo de serviço de comunicação padronizado, por exemplo trocar mensagens de correio eletrônico, com o mundo exterior.

7.4.4.3 Hosts Categoria 3:

Conceito: Hosts que se comunicam diretamente com o mundo externo. Os hosts são classificados na categoria 3 quando eles estão diretamente integrados a rede Internet. Os endereços IP de cada hosts pertencentes a essa categoria devem ser únicos em toda a rede Internet. Para que cada host que uma empresa precisa conectar na categoria 3, ela precisa conseguir um endereços IP junto as autoridades que coordenam a distribuição de endereços IP na Internet.

A Figura 57 tem-se um exemplo onde os hosts da rede são integrados diretamente ao backbone da Internet. Nesse caso a rede corporativa corresponde a uma extensão da rede Internet.

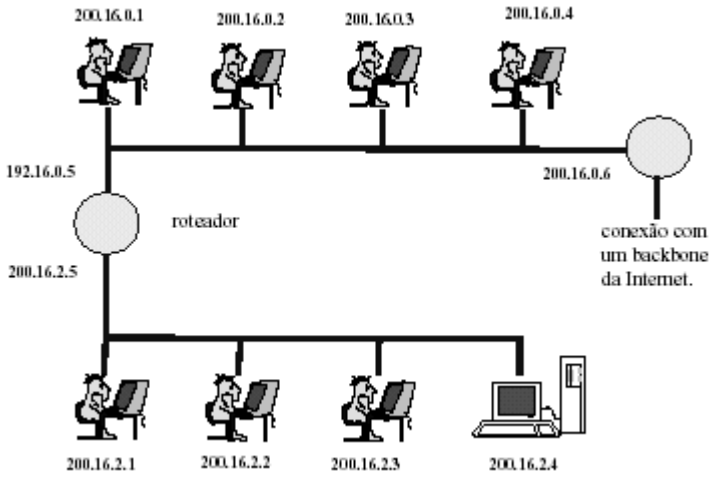


Figura 58 – Integração direta dos Hosts da Rede ao Backbone da Internet

7.4.5 Configuração Dinâmica de Endereços IP

Conceito: Mecanismo que permite atribuir automaticamente um endereço IP para uma host, assim que essa é inicializada ou conectada a rede Internet.

A atribuição de endereços IP numa rede TCP/IP de grande porte pode ser uma tarefa bastante complexa. O administrador da rede deve certificar-se que cada host receba um endereço IP único entre todas as máquinas da rede. A configuração manual de

endereços IP, além de ser trabalhosa, pode levar a duplicação indesejável de endereços. Em redes de grande porte, determinar a localização física de duas máquinas apresentando conflito de endereços IP pode ser uma tarefa bastante difícil. Para auxiliar a resolver este problema, grupos de trabalho IETF (*Internet Engineering Task Force*) padronizaram um serviço que auxilia a configuração automática de endereços IP, denominado DHCP (*Dynamic Host Configuration Protocol*). O DHCP foi padronizado pelas RFCs 1533, 1534, 1541 e 1542.

7.4.5.1 Funcionamento do DHCP

O serviço de DHCP funciona segundo a arquitetura cliente-servidor. Nessa arquitetura, uma máquina denominada "servidor de DHCP" é responsável por atribuir endereços IPs para as demais máquinas, denominadas "clientes DHCP". A atribuição do endereço IP é feita no momento que o computador cliente é ligado, ou mais especificamente, quando seu serviço de rede é iniciado. Deve-se observar que o servidor DHCP apenas "empresta" o endereço IP ao cliente. Cada cliente é responsável por renovar o seu empréstimo de tempos em tempos. Se o empréstimo não for renovado, o endereço IP é considerado livre e pode ser atribuído a outra máquina da rede. Esta característica permite reutilizar endereços IP quando um computador é desativado.

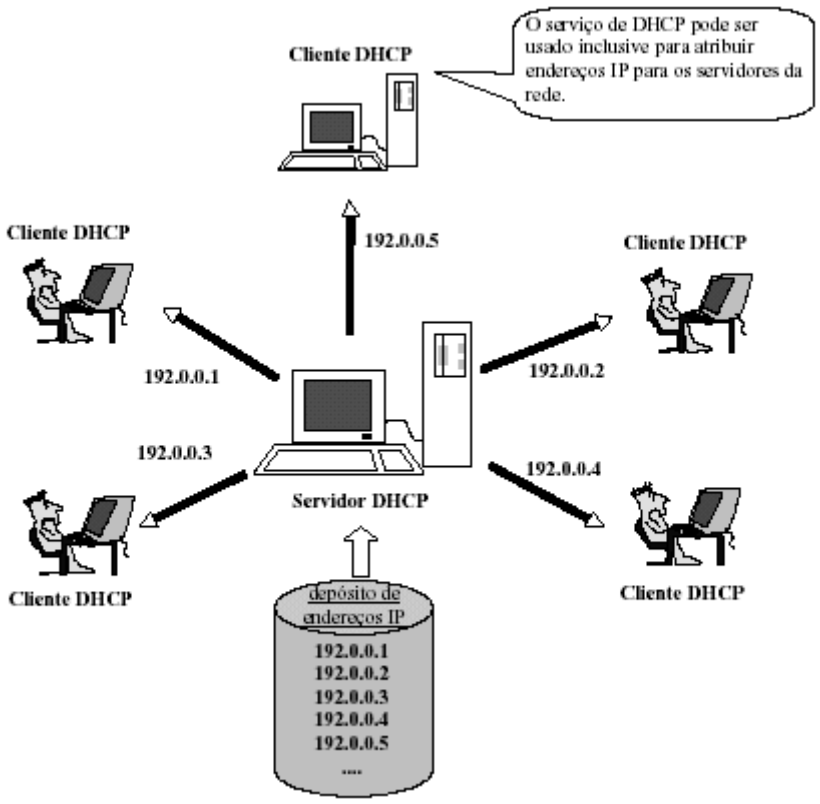


Figura 59 –Exemplo do Funcionamento do DHCP

Termos:

* atribuir endereço IP: De fato, o serviço de DHCP não atribui apenas endereços IP. Outros parâmetros de configuração necessários a comunicação na arquitetura TCP/IP podem ser distribuídos aos clientes juntamente com o endereço IP. Geralmente, esses parâmetros correspondem a máscara de subrede, e o endereço IP do "gateway default", isto é, o roteador para onde são enviadas as mensagens que não possuem uma rota conhecida.

* servidor DHCP: corresponde a um computador qualquer da rede, escolhido para centralizar a distribuição de endereços IP. O servidor de DHCP é um computador comum, sobre o qual é instalado o software que executa o serviço de DHCP. O administrador da rede interage diretamente com o servidor de DHCP para configurar como os endereços IP deverão ser distribuídos.

* clientes DHCP: corresponde aos computadores que recebem os endereços IPs através do serviço de DHCP. Deve-se observar que o termo "cliente" refere-se unicamente ao serviço de DHCP. Um computador que funciona normalmente como servidor na rede TCP/IP (servidor de correio eletrônico, por exemplo) pode ser um cliente DHCP. Um

cliente DHCP negocia o uso de um endereço IP através da troca de mensagens com o servidor. Após haver recebido um endereço IP pela primeira vez, o cliente sempre tenta manter o mesmo IP, solicitando periodicamente ao servidor a renovação do direito de usar o IP.

* depósito de endereços IP: corresponde a um conjunto pré determinado de endereços IP, que o servidor DHCP distribui para os clientes. Quando um cliente que solicita um endereço IP pela primeira vez, o servidor DHCP atribui o primeiro endereço IP do depósito que ainda não foi utilizado. O depósito de endereços IP é configurado diretamente no servidor de DHCP, pelo administrador da rede.

7.4.5.2 Uso do DHCP numa Intranet

O serviço de DHCP pode ser utilizado para simplificar significativamente o processo de configuração de endereços IP em Intranets corporativas. Dependendo da topologia física da rede, pode ser necessária a utilização de mais de um servidor de DHCP. Os clientes localizam o servidor de DHCP através de uma mensagem definida pelo protocolo DHCP, enviada em broadcast pela rede. Como as mensagens em broadcast não se propagam através dos roteadores, os clientes tendem a utilizar o servidor de DHCP que esteja localizado na mesma rede física.

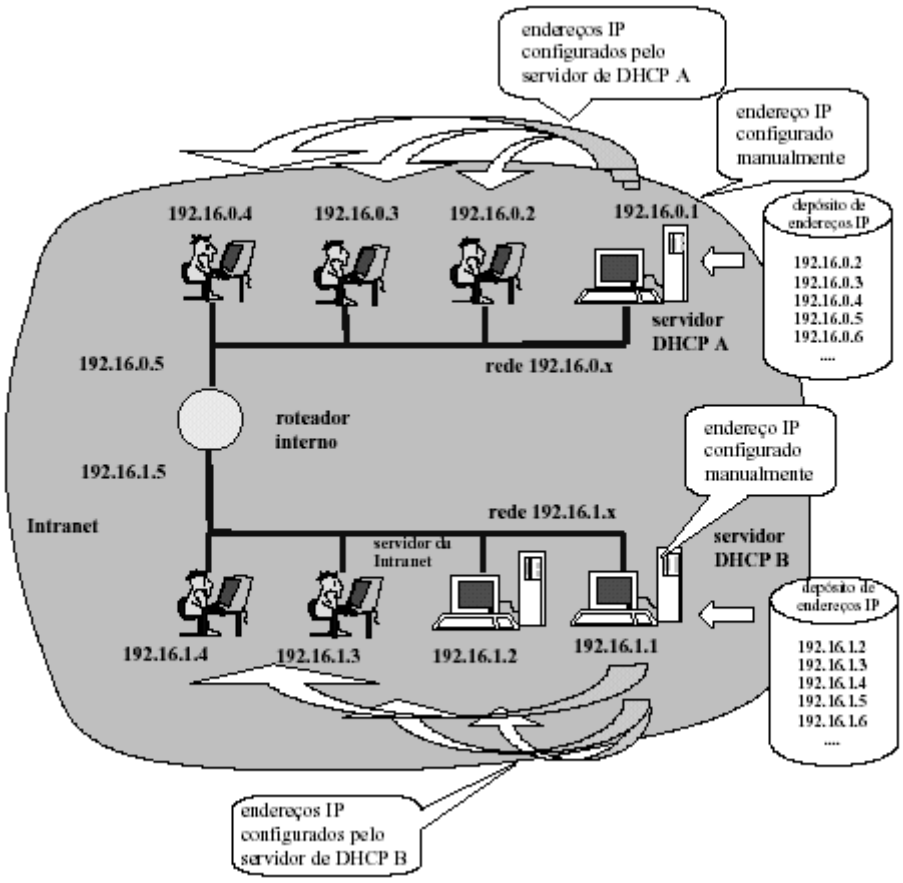


Figura 60 – Uso do DCHP numa Intranet

7.4.5.3 Uso do DHCP por Provedores de Acesso a Internet

O serviço de DHCP é particularmente importante para os grandes provedores de acesso que permitem aos usuários acessarem a Internet através da rede pública de telefonia. Os provedores de acesso possuem um número limitado de endereços registrados junto às autoridades que controlam o acesso a Internet. Esses endereços são atribuídos pelo serviço de DHCP aos clientes assim que a conexão discada com o provedor é estabelecida. A alocação do endereço IP ao cliente é temporária. No momento em que o cliente interrompe sua conexão, o endereço IP passa a estar disponível para outro cliente.

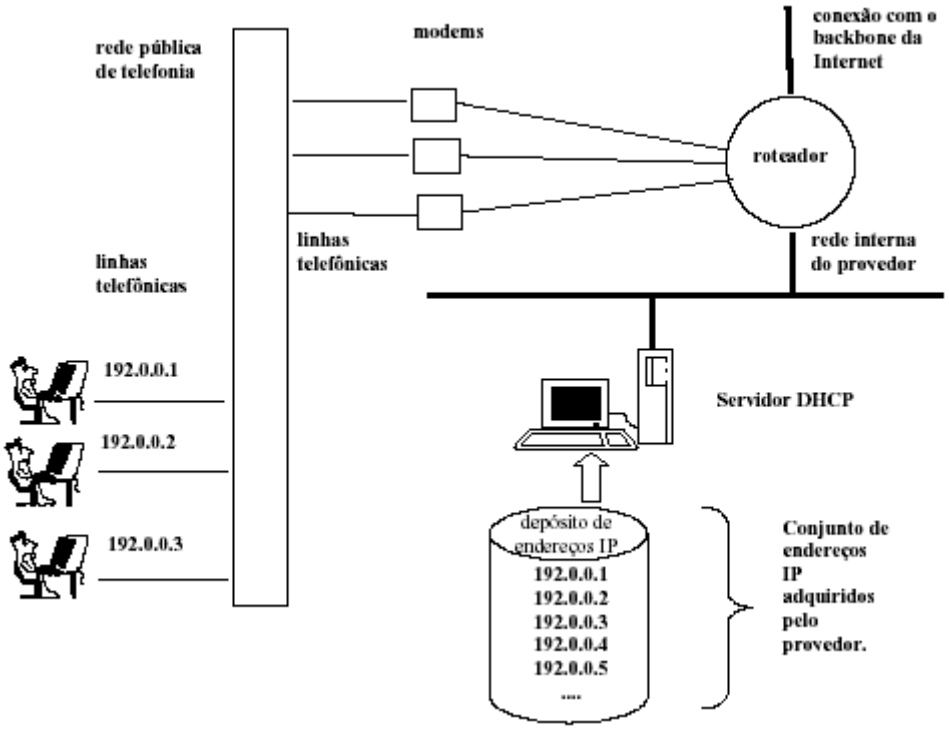


Figura 61 – Uso do DHCP por Provedor de Acesso a Internet

REFERÊNCIAS BIBLIOGRÁFICAS

TANENBAUM, Andrew. Redes de Computadores. Rio de Janeiro: Campus, 1997.

COMER, Douglas E. Redes de Computadores e Internet. Porto Alegre: Bookman, 2001.

SOUSA, L. B. Redes de Computadores: dados, voz e imagem. São Paulo: Érica, 1999.

STARLIN, G; CARVALHO, Alan. Tecnologias de Redes. Rio de Janeiro: Book, 1998.

BENEDETTI, Marco A. Apostila de Redes de Computadores.

Página da World Wide Web. Disponível em: http://www.uem.mz/chess/r_meio1.htm. Acesso em: 08 de agosto de 2003.

Página da World Wide Web. Disponível em: http://www.pop-rs.rnp.br/~berthold/etcom/teleproc-2000/satelite/satelite.htm. Acesso em: 08 de agosto de 2003.