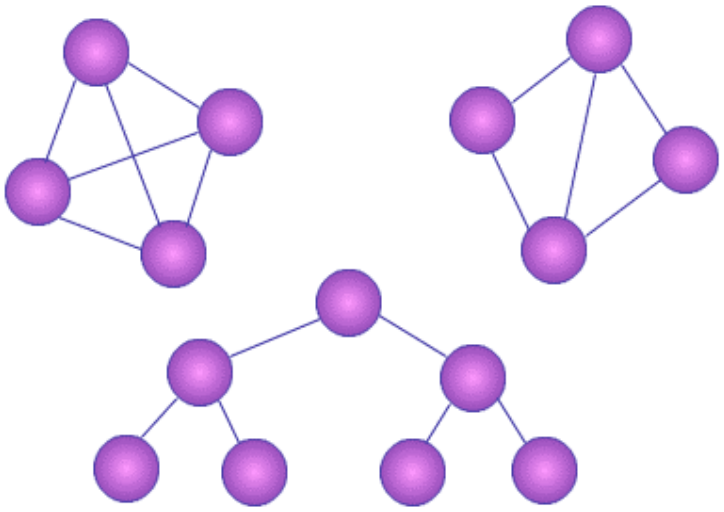
INTRODUÇÃO A REDES DE COMPUTADORES.



Ronei Ximenes Martins

Varginha – Minas Gerais

2002

Prof. Ronei Ximenes Martins, Msc. UFSC (Brasil, 2000)

Graduado em Matemática, Especialista em Informática Gerencial e Mestre em Engenharia de Produção, é Professor do Curso de Ciência da Computação do Centro Universitário do Sul de Minas - UNIS.

Atuando profissionalmente em Informática desde 1982, possui formação específica (cursos certificados) em Redes Novell Netware, Microsoft Windows NT e Linux, dentre outros, tendo projetado e implementado inúmeras redes em diferentes tecnologias.

Atua há 10 anos como docente, dos quais 5 anos como professor universitário, tendo participado da elaboração do Projeto Pedagógico e da implantação do Curso de Bacharelado em Ciência da Computação do UNIS, quando assumiu Chefia do Departamento de Informática e posteriormente a Coordenação do Curso. Atualmente atua como Diretor do Instituto de Tecnologia, Engenharia e Ciências Exatas do Centro Universitário do Sul de Minas, além de ministrar aulas da Disciplina Redes e Teleprocessamento e atuar em projetos de pesquisa.

Alguns projetos de Redes desenvolvidos e implantados:

- Rede da Reitoria da UEMG - Novell Netware e Microsoft Windows em TCPIP.
- Rede Administrativa da FESP - Novell Netware.
- Rede Acadêmica FESP - Novell Netware e WindowsNT TCPIP.
- Rede Acadêmica da FELA - Novell Netware e Windows em TCPIP.
- Rede Acadêmica e Administrativa do UNIS-MG - Novell, WindowsNT, Linux e Microsoft TCPIP
- Provedor de Acesso Minasnet (Passos).
- Rede do Provedor de Acesso Minasnet (São S. Paraiso, Cássia, Itaú de Minas, Carmo do Rio Claro).
- Provedor de Acesso da FELA (lavras).
- Provedor de Acesso da FESP (Passos).
- Provedor de Acesso da FEPESMIG (Varginha).
- Ponto de Presença da Rede Internet Minas na reitoria da UEMG.(Belo Horizonte)
- Rede Acadêmica do Colégio Batista - Varginha - Novell Netware e Windows em TCPIP.
- Rede Acadêmica da FACECA – Microsoft Windows NT e Windows 98 em TCPIP.(Varginha)
- Rede Acadêmica da Faculdade de Direito de Varginha – Microsoft Windows NT e Windows 98 em TCPIP.
- Sala de Videoconferência do UNIS-MG (Varginha).

Endereço para contato:
Prof. Ronei Ximenes Martins
R. Cel. José Alves 256, Vila Pinto.
37010-540 – Varginha – MG.
Tel.: (0xx35) 3219-5275
Fax: (0xx35) 3219-5251
E-mail: ronei@unis.varginha.br

ÍNDICE ANALÍTICO.

ÍNDICE DE FIGURAS

Esta publicação propõe-se a ajudar você a entender as redes de computadores, como funcionam e os conceitos básicos necessários para sua implantação e manutenção. Utilizada em conjunto com atividades práticas, ela o ajudará a desvendar o que acontece dentro dos cabos, equipamentos e programas. Considere que se você entender a estrutura básica e o funcionamento de uma rede, poderá ser um profissional mais eficiente.

Além da formação básica proposta, esta publicação pretende prepará-lo para estudos avançados do tema, em disciplinas de cursos de graduação ou em cursos específicos e de pós-graduação. Os conhecimentos relacionados às redes de computadores são vastíssimos e novas tecnologias surgem a cada dia. Considere esta publicação como sendo a porta de entrada para este mundo.

Além de prover informações, ela é parte integrante de uma proposta metodológica para o ensino de Redes de Computadores. Utilizada em conjunto com estudos de casos e atividades práticas, poderá levar você a exercitar, pesquisar e produzir seu próprio conhecimento. O caderno de atividades práticas e exercícios é disponibilizado durante o curso.

Na organização deste trabalho foram utilizados textos publicados na Internet de diversos autores. Como estamos na era da informação e do compartilhamento, não faria sentido reescrever conteúdos que já estão consolidados e bem organizados, somente para descaracterizar a autoria de terceiros e tornar a "obra inédita". A intenção não é "reinventar a roda". Então, considere este trabalho como sendo a organização de conteúdos em um formato interessante para aqueles que estão iniciando o estudo das redes de computadores, principalmente em cursos de graduação ligados à Informática. Em vários capítulos existem trechos transcritos das publicações obtidas. **Para evitar citações repetitivas, nas referências bibliográficas estão indicadas as contribuições.**

Da mesma forma que vários dos capítulos desta publicação receberam a contribuição voluntária de professores que publicaram trabalhos na Internet de forma gratuita, esta obra está disponível gratuitamente no formato digital. Porém, acredito que todo trabalho deve ser recompensado. Assim, gostaria de manter um **registro de todos os que utilizarem esta publicação**, produzida em muitas horas de trabalho. Com este registro será possível contabilizar quantas pessoas estão utilizando-a e obter contribuições para seu aperfeiçoamento.

Para registrar-se, solicito que faça uma contribuição de qualquer valor para a Instituição Filantrópica de sua preferência, solicite um documento que comprove a contribuição e envie para o endereço indicado abaixo com os seguintes dados:

Nome Completo;
Endereço Completo (incluindo CEP);
Data de Nascimento;
Sexo;
Profissão (se trabalha);
Curso que freqüenta (se está estudando);
Criticas e/ou sugestões sobre a obra.

Endereço para envio: Prof. Ronei Ximenes Martins
R. Cel. José Alves 256, Vila Pinto.
37010-540 – Varginha – MG.

As informações de todos os registros estarão disponíveis no site www.ronei.varginha.br/registros.

Se preferir, você pode fazer uma cópia digital do comprovante e enviar juntamente com os dados solicitados para o e-mail ronei@unis.varginha.br escrevendo no assunto: "Registro de Introdução à Redes de Computadores".

Faça este gesto de boa vontade, contribua com alguém que necessita e registre-se como usuário desta publicação. **Obrigado.**

As informações desta publicação não estão relacionadas a um tipo específico de rede, a um produto ou modelo de equipamento, elas estão relacionadas com os fundamentos que sustentam o funcionamento de todas as redes.

Para complementar os estudos, existe uma série de atividades cujo objetivo principal é criar motivação, incentivar a manipulação do conteúdo, refletir sobre questões teóricas, demonstrar a aplicação dos fundamentos teóricos e fomentar a pesquisa por temas e conceitos não apresentados. Algumas destas atividades vão requerer o uso de um computador e, em alguns casos, de computadores ligados em rede. Assim, para tirar o maior proveito possível, é importante participar das atividades propostas no caderno distribuído no curso. È importante também que você tenha acesso a uma rede local com protocolo tcp/ip.

Você poderá utilizar o presente trabalho de maneiras distintas:

1 – Se você obteve esta publicação, porém não freqüenta o curso de redes que ministro, realize uma leitura seqüencial dos capítulos na ordem em que estão organizados, grifando o que considerar mais importante e os conceitos fundamentais de cada trecho. Após a leitura, procure ter acesso a um ambiente de rede e busque realizar experimentos que comprovem os conceitos teóricos envolvidos. Busque identificar componentes, suportes de transmissão, protocolos, componentes de conexão. Depois tente implantar uma pequena rede em TCP/IP, criando números IP para cada máquina. Busque aplicativos que fazem análise de protocolos (O Ethereal é um bom aplicativo e é gratuito). Tente identificar com o analisador, os protocolos que estão sendo utilizados na rede e os datagramas que estão trafegando. Se tiver chance, instale duas placas de rede em um computador com Linux ou Windows NT. Isto permitirá que você configure rotas e teste o comportamento das pontes e roteadores.

2 – Se teve acesso ao caderno de atividades do curso de redes que ministro, realize uma leitura seqüencial dos capítulos na ordem em que estão organizados, grifando o que considerar mais importante e os conceitos fundamentais de cada trecho. Após toda a leitura, pode realizar o conjunto de atividades, buscando nos capítulos as informações relacionadas a cada uma delas.

3 – Se é aluno do curso de redes que ministro, iniciará o estudo pelas atividades propostas, buscando no texto as informações necessárias para realizar cada tarefa. Todas as atividades indicam o capítulo ou capítulos relacionados a ela. Esta técnica permitirá um acesso mais dinâmico e não seqüencial aos conteúdos. Após concluir cada atividade, deverá realizar uma leitura dos capítulos envolvidos, procurando recordar onde cada conceito ou tecnologia se encaixou nas atividades propostas. As aulas teóricas são um espaço importante para sanar dúvidas e propor novos estudos de casos.

É importante salientar que as atividades propostas no caderno de atividades se relacionam com mais de um capítulo e que este relacionamento não é seqüencial. Em alguns casos, parte das informações deverá ser pesquisada em outras mídias. Isto é proposital. Na aplicação prática dos conhecimentos adquiridos, você não vai encontrar problemas hierarquicamente organizados, cuja solução estará descrita em uma seqüência lógica com elaboração do mais simples para o mais complexo. Terá que entender sua complexidade caótica e dessecá-los, utilizando tudo o que sabe e buscando através da pesquisa o que não sabe.

Desejo que você tenha uma utilização produtiva deste material.

Um bom trabalho!

Ronei Ximenes Martins.

1 – INTRODUÇÃO.

Hoje a maioria dos computadores utilizados no trabalho, nas escolas e nos lares estão conectados em rede e certamente você já utiliza ou utilizará computadores interconectados.

As redes de computadores não surgiram como uma tecnologia única e independente. Os sistemas em rede dependem de muitos conceitos com os quais você já está familiarizado. De fato, as redes modernas têm raízes nos primeiros sistemas de telefones e telégrafos. Assim os laços históricos relacionados às redes de comunicação são utilizados aqui para ilustrar a tecnologia envolvida nas redes. Antes de conhecer e aplicar os conceitos e tecnologias relacionadas às redes de computadores, vamos conhecer um pouco da história e da evolução das redes de comunicação e dos sistemas de computação.

Depois de navegar pela história, vamos nos aprofundar nos aspectos relacionados ao hardware das redes. As tecnologias e suportes de transmissão serão detalhados e comparados. As diversas topologias e a categorização das redes serão estudadas. Os diversos componentes de conexão serão apresentados e sua aplicação estudada.

Conhecendo o hardware das redes, as questões relacionadas ao software de rede serão apresentadas. A hierarquia e a descentralização proposta pelos modelos em camadas, os modelo de referência OSI, a construção de protocolos, as interfaces e os serviços serão analisados e detalhados.

Para complementar o estudo da base conceitual e com os princípios teóricos que sustentam as tecnologias integradas nas redes de computadores, as Arquiteturas de Redes RM-OSI e TCP/IP serão detalhadas e analisadas mais profundamente, principalmente as camadas Física, de Enlace e de Rede, que constituem a base do projeto e implantação de uma rede de computadores. Questões práticas relacionadas ao uso do TCP/IP tais como Endereçamento IP, Sub-Redes IP, Roteamento e os protocolos UDP e TCP serão abordadas.

Encerrando, analisaremos a constituição dos Sistemas Operacionais de Rede, os conceitos relacionados aos modelos Cliente/Servidor e Peer-to-Peer e os servidores dedicados. Neste ponto, já estaremos nos preparando para a complementação do curso de redes, que seguirá na segunda publicação abordando questões relativas a administração e gerência, segurança, aspectos práticos relacionados à instalação, configuração e manutenção de diversos servidores em sistemas operacionais diferentes. Mas até lá, temos muito trabalho. Mãos a obra.

2.1 – EVOLUÇÃO DAS REDES DE COMUNICAÇÃO.

A comunicação é um processo dialogal. Em um processo de comunicação, se produz intercâmbio – troca - de informações. Existe um emissor, um receptor e um meio de transmissão pelo qual a informação (ou mensagem) é levada do emissor ao receptor. Qualquer interferência que dificulte ou impeça a troca de mensagens através do meio de comunicação é considerada ruído. A figura 2.1 ilustra o esquema de um processo de comunicação.

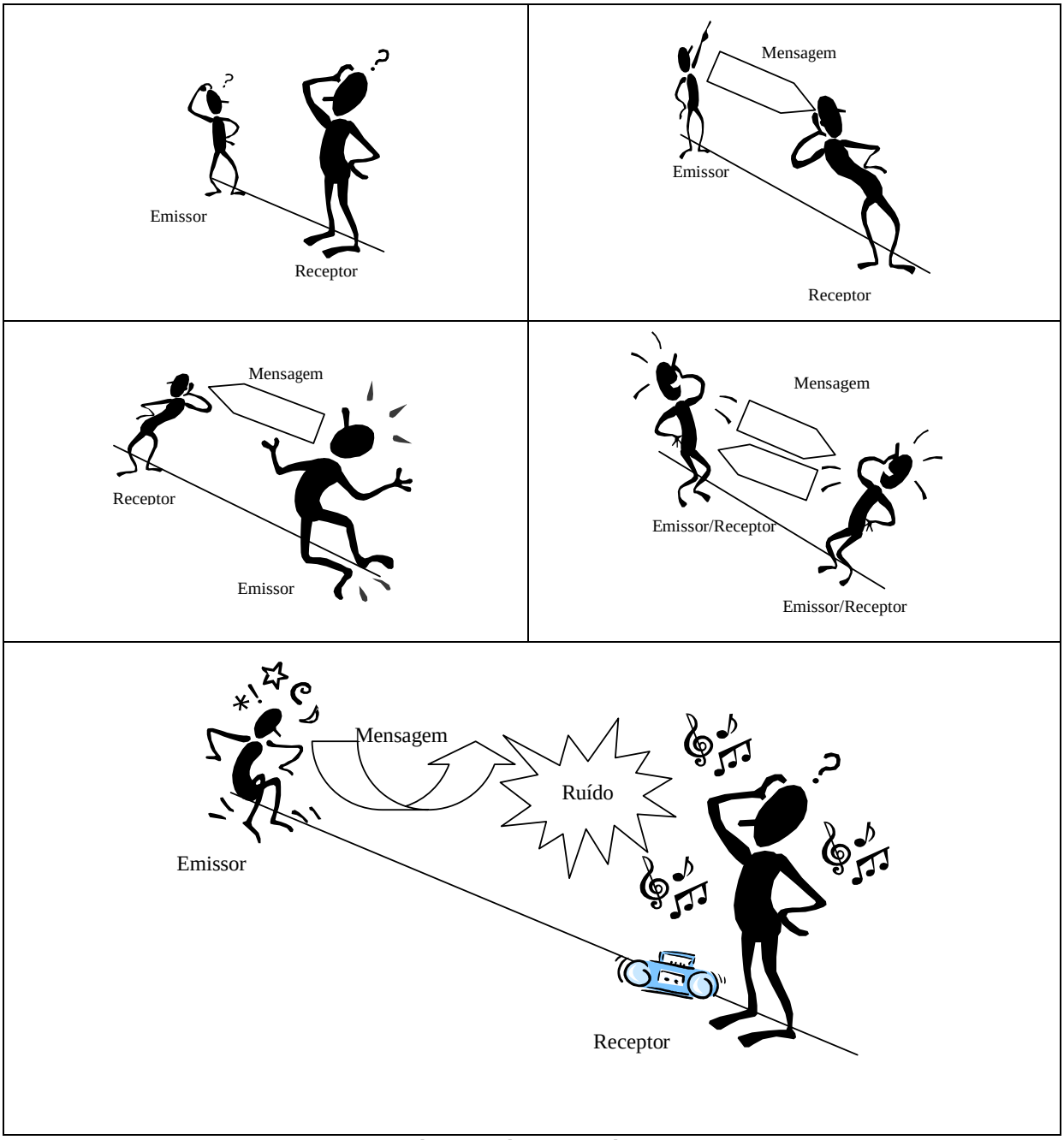


Figura 2.1 – Ilustração do processo de comunicação.

A comunicação é inerente à sociedade humana. Conforme as sociedades foram ocupando espaços geograficamente dispersos, a necessidade de comunicação através de longas distâncias foi tornando-se mais intensa.

Ao inventar o telégrafo em 1838, Samuel Morse instituiu um marco para os sistemas de comunicação que evoluíram para as redes de telefonia, de rádio, de televisão e de computadores.

A rede telegráfica da Western Union, nos Estados Unidos da América, foi a primeira a cobrir todo o continente Norte Americano. Seguindo as estradas de ferro de leste a oeste, a Western Union fechava negócios que consistiam na troca do acesso às linhas das estradas de ferro pelo fornecimento de uma estação de telégrafo e um operador para cada estação de trem. O operador organizava para a estrada de ferro as informações de horários e cargas sem cobrar nada.

O serviço da Western Union era ponto-a-ponto. Para enviar um telegrama para alguém, a pessoa ia a um escritório da Western Union e ditava a mensagem para o operador do telégrafo. O operador iria então enviar a mensagem em código Morse através da linha de telégrafo para a estação apropriada.

Também nos Estados Unidos da América, quando a Bell Telephone começou suas operações no fim da década de 1890, ela não possuía linhas telefônicas. Quando um assinante fazia uma assinatura do serviço, a Bell levava novas linhas até a casa do assinante. Inicialmente, o serviço telefônico também era ponto-a-ponto, o que significava que cada telefone poderia conectar-se com apenas um outro telefone. Muitos dos primeiros assinantes eram médicos; eles conectavam um telefone no consultório a outro em casa. Á medida que o serviço telefônico crescia, os assinantes queriam ter a possibilidade de falar uns com os outros - assim nasceu a rede telefônica.

Desde então, a comunicação através de sinais elétricos passou por uma grande evolução, dando origem aos grandes sistemas que temos hoje e que utilizam satélites, fibra ótica, redes de cabos metálicos e diversos dispositivos capazes de suprir meios de comunicação para todo o planeta.

Embora os padrões e protocolos para comunicações entre computadores façam referências ao trabalho de Morse e Bell, no começo deste século, os padrões e protocolos para interoperação entre computadores não surgiram antes do início da década de 1980. Três correntes distintas alimentaram o fluxo das redes de computadores: a IBM, o US Departament of Defense (DOD) e o Palo Alto Research Center da Xerox Corporation. Posteriormente, outras indústrias e organizações de profissionais, em particular o Institute of Electrical and Electronic Engineers (IEEE) teve uma importante participação no desenvolvimento de padrões, mas a história começa com um sistema de computadores chamado SAGE.

O Semi-Automatic Ground Enviroment, SAGE, foi desenvolvido pela IBM para o DOD no fim da década de 1960. O SAGE, um sistema de defesa aérea que operou até a metade dos anos 80, utilizava computadores a válvulas com bancos de memórias tão grandes que duas pessoas poderiam ficar de pé dentro deles. Os computadores foram instalados aos pares em construções do tamanho de um quarteirão e os filamentos das válvulas em uma par de computadores SAGE forneciam aquecimento para todo o inverno em prédios de três andares. O programa SAGE envolveu os esforços dos melhores cientistas de computadores e comunicações dos Estados Unidos na década de 1960 e resultou em uma rede de computadores interoperantes que se estendeu sobre todos os Estados Unidos. O programa era equivalente ao Golden Spike, que uniu as ferrovias em 1869.

Nos anos 70, o DoD - diante de um inventário de diferentes computadores que não podiam interagir - foi o pioneiro no desenvolvimento de protocolos de software para redes, que poderiam funcionar em mais de uma marca e modelo de computador. O principal conjunto estabelecido pelo DoD é o Transmission Control Protocol/Internet Protocol (TCP/IP). Como o próprio nome implica, estes protocolos são acordos sobre como devem ocorrer as transmissões nas redes.

Mais ou menos na mesma época, na década de 1970, a IBM começou a tornar públicos os padrões e protocolos que utilizava em seus sistemas de computadores proprietários. Os padrões incluíam especificações detalhadas do cabeamento e os protocolos eram desenvolvidos para assegurar comunicações precisas sob alta demanda. Isto levou outros fabricantes a emularem as técnicas da IBM e elevou a qualidade do desenvolvimento para redes em toda a indústria. Culminou também em uma revolta por parte das outras companhias de computadores que questionavam o controle total dos padrões e protocolos mais utilizados feito pela IBM. Esta revolta levou à flexibilidade e interoperabilidade que temos hoje.

Em poucas décadas, a indústria de redes de computadores fez mais progressos em frentes gerais do que a própria indústria de computadores pessoais. A evolução das redes levou consigo a tecnologia telefônica, projetos de hardware de computadores, o desenvolvimento de software e até mesmo a sociologia dos grupos de trabalho.

Hoje, computadores e edificações já incorporam os componentes de redes em seus projetos. As redes modernas integram palavras manuscritas e digitadas, vozes e sons, gráficos e conferências de vídeo no mesmo meio de comunicação. As redes tornam possível às organizações o abandono da estrutura de gerenciamento top-down onde muitas informações ficavam retidas no topo e a mudança para uma estrutura mais ágil e horizontal, onde as informações

estão compartilhadas e publicamente disponíveis.

2.2 – EVOLUÇÂO DOS SISTEMAS DE COMPUTAÇÂO.

Os primeiros sistemas de computadores eram muito grandes e caros. Um computador de grande porte (*mainframe*) típico custava milhões de dólares e necessitava de uma área de centenas de metros quadrados especialmente preparada e com ar condicionado. Além do hardware, os primeiros computadores precisavam de assessoria de técnicos em tempo integral para mantê-los funcionando. Os usuários organizavam as tarefas a serem processadas em *jobs* e o computador as **processava em lote (*batch*)**. Não havia nenhuma forma de interação direta entre usuário final e computador sendo que a rotina consistia em perfurar cartões, entrega-los a um operador qualificado e aguardar o recebimento de relatórios impressos com os resultados. O computador realizava tarefas, uma a uma, organizadas em uma fila de entrada.

Na década de 1960, o desenvolvimento de **terminais remotos** permitiu aos usuários acesso ao computador central através de linhas de comunicação. Assim, o usuário final passou a ter um mecanismo de interação direta com o computador.

Nesta mesma época, pela necessidade de otimização do uso dos *mainframes*, nasceu o conceito de **tempo compartilhado (*time-sharing*)**. Um sistema de tempo compartilhado permite que mais de um usuário - freqüentemente muitas centenas - utilizem o mesmo computador ao mesmo tempo. O usuário final podia executar seus próprios programas e cada usuário final interagia com o computador através de seu terminal. Os primeiros terminais de *mainframes* eram unidades mecânicas semelhantes a uma máquina de escrever (teletipos). Por volta da metade da década de 1970, o terminal de vídeo (VDT) tinha substituído os terminais de impressão em muitas aplicações. . A figura 2.2 ilustra um ambiente de CPD com mainframes e terminais;

Figura 2.2 – Sala de C.P.D. com mainframes e terminais

Apesar dos custos envolvidos, milhares de empresas e universidades instalaram sistemas de grande porte nas décadas de 1960 e 1970, sendo que muitos destes sistemas estão em uso até hoje.

A IBM, na época, era líder no mercado e desenvolvia seu próprio sistema para conectar terminais ao computador central. Entretanto, outros fabricantes (entre eles a *Digital Equipment Corporation*, *Data General* e *Honeywell*) utilizam a conexão RS-232C (uma forma de conexão serial) entre o computador central e os terminais através de cabos. Os usuários que estivessem fora da área de alcance dos cabos poderiam utilizar terminais equipados com modems para acessar o computador central.

Estas conexões permitiram que os terminais saíssem da sala do computador central e fossem instalados sobre as mesas dos usuários finais. Esta realocação aparentemente simples teve um grande efeito sobre a forma de como as pessoas usavam os computadores. A permissão a centenas de usuários para que compartilhassem o mesmo computador fez com que o custo por usuário caísse vertiginosamente. De repente, tornava-se economicamente sensato utilizar o computador para tarefas rotineiras como fazer a contabilidade, organizar o horário de aulas e até mesmo processar textos. Antes do compartilhamento de tempo, o computador era de domínio de grandes corporações, instituições de pesquisa e universidades. Reduzindo o custo por usuário, os computadores de grande porte tornaram-se acessíveis a muitas empresas de médio e pequeno porte, organizações governamentais e não governamentais e diversos tipos de instituições.

Os computadores pessoais surgiram no final da década de 1970. Em muitos casos, estes computadores pessoais eram comprados por médias e grandes empresas, a maioria das quais já dispunha de um grande sistema de computação. No princípio, estes computadores eram utilizados como sistemas isolados para executarem aplicações tais como Lotus 1-2-3, Visicalc, ou WordPerfect. Não era incomum se ver um escritório com um computador pessoal na ponta de uma mesa e um terminal de mainframe em outra. Em pouco tempo, estas mesmas companhias aprenderam que,

acrescentando um programa de comunicação ao computador pessoal, elas poderiam utilizar o computador como um terminal e economizar, além um precioso espaço na mesa, o custo de aquisição e manutenção do terminal. A figura 2.3 apresenta um terminal de acesso remoto a mainframes (a) e um computador pessoal (b).

Assim, os computadores pessoais passaram a ser utilizados como ponto de acesso para o *mainframe* e como minicomputador. Em vez de colocar um computador pessoal e um terminal em cada mesa, muitas companhias retiraram seus terminais e os substituíram por computadores. Com o software de comunicação adequado, um computador pessoal pode realizar todas as funções de um terminal. Na maioria dos casos, um computador pessoal com software de comunicação oferece mais do que o terminal.

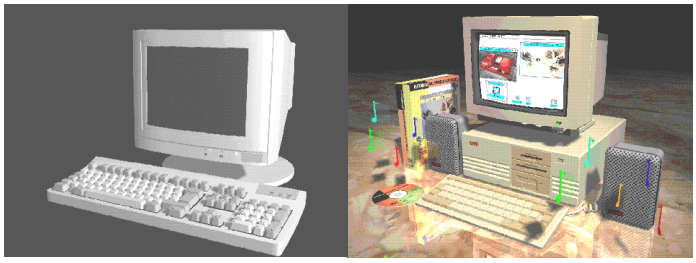


Figura 2.3 – (a) Terminal e (b) Microcomputador

Os softwares de comunicação utilizados para acessar computadores remotos são denominados "Emuladores de Terminais". Além de possuir as características originais do terminal eles oferecem transferência de arquivos e muitos outros recursos. Embora sejam designados para operar com modems, muitos programas proporcionam conexão direta ao *mainframe*, sistemas de minicomputadores ou outros computadores pessoais.

Embora o custo do hardware estivesse caindo, o preço dos equipamentos eletromecânicos ainda era alto. Pela razão do custo, se justificava o uso compartilhado de periféricos tais como impressoras e unidades de armazenamento de dados. Assim, além do tempo compartilhado, surge o conceito de compartilhamento de recursos.

A capacidade de troca de informações também passou a ser explorada nos grandes sistemas que incluíam computador central e terminais. As bases de dados passaram a ser compartilhadas e vários usuários passaram a interagir dentro de um mesmo sistema aplicativo, trabalhando de forma cooperativa. Novos recursos surgiram então, utilizando a interconexão dos equipamentos como meio de compartilhamento da informação. Sistemas de correio eletrônico, área de armazenamento compartilhada para grupos de trabalho e quadro de aviso eletrônico passaram a fazer parte da rotina dos usuários.

Com o aumento do número de usuários e com a saturação do meio de comunicação entre terminais e computador central devido ao volume de informação circulando, a busca por soluções para os problemas de performance impulsionou os pesquisadores a criar novas arquiteturas que propunham distribuição e paralelismo como fora de melhorar o desempenho dos sistemas.

Fruto das propostas para novas arquiteturas, os "**Sistemas de Multiprocessadores Fortemente Acoplados**" foram idealizados para superar a limitação do modelo de *Von Neumann*[1] de computação seqüencial. Estes sistemas introduzem a idéia de sequências múltiplas e independentes de instruções em um sistema composto por vários elementos processadores compartilhando espaço comum de memória.

Finalmente, o conceito de "**Sistemas de Processamento Distribuídos**" é elaborado. A idéia aqui é interconectar lógica e fisicamente uma série de elementos de processamento para executar aplicações (programas) de forma cooperativa sendo que o controle geral dos recursos envolvidos é descentralizado. Nos "Sistemas Distribuídos" o estado do sistema é fragmentado em partes que residem em diferentes processadores e memórias, com a comunicação entre as partes sujeita às variações do meio de comunicação que as une.

[1] Jon Von Neumann: Matemático Húngaro, idealizador da programação interna utilizada ainda hoje nos computadores, participou da construção de primeiro computador eletrônico (projeto ENIAC - Electronic Numeric Integrator And Calculator) e posteriormente do EDVAC (Electronic Discrete Variable Computer) onde foi aplicada a idéia de programação interna que cria a possibilidade de armazenamento de programas, codificados de acordo com certos critérios na memória do computador.

A fusão de computadores e das comunicações alterou profundamente a forma com que os sistemas computacionais passaram a ser organizados. Está totalmente ultrapassado o conceito de “Centro de Processamento de Dados" (CPD) como um local para onde os usuários enviam dados e aguardam as informações processadas em relatórios. Este conceito foi substituído pelo trabalho realizado por uma série de computadores e periféricos geograficamente distribuídos, interconectados, onde cada unidade processadora à disposição de um usuário pode contribuir para o sistema como um todo.

Existe uma classificação para os sistemas com múltiplos processadores, organizados de acordo com tamanho físico. No topo estão as máquinas de fluxo de dados, computadores altamente paralelos com várias unidades funcionais, todas trabalhando no mesmo programa. Estes são os "Sistemas de Multiprocessadores Fortemente Acoplados". Em seguida, vêm os sistemas multiprocessadores, que se comunicam através de memória compartilhada. Estas são as "Máquinas de Arquitetura Distribuida". As redes de computadores estão após os multiprocessadores, sendo computadores que se comunicam através da troca de mensagens.

Como dito anteriormente, um "**Sistema Distribuído**" (SD) é formado por um conjunto de módulos processadores interligados por um sistema de comunicação. Mas um SD não deve ser confundido com uma rede de computadores. Segundo alguns autores, SD são construídos para obtenção de maior desempenho e confiabilidade enquanto as redes de computadores são construídas para o compartilhamento de recursos. Outros autores incorporam as redes de computadores no conceito de SD, porém subdividindo-os em duas categorias: (1) Máquinas de Arquitetura Distribuída e (2) Redes de Computadores.

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

O sistema de comunicação vai se constituir de um arranjo topológico interligando os vários módulos processadores através de enlaces físicos (meios de transmissão) e de um conjunto de regras com o fim de organizar a comunicação (protocolos).

As redes foram feitas para o **compartilhamento**. Compartilhamento de arquivos de processadores de textos e planilhas, impressoras, conexões com redes de computadores distantes além de sistemas de correio eletrônico são algumas das funções de uma rede.

3.1 OBJETIVOS DE UMA REDE DE COMPUTADORES.

3.1.1 - COMPARTILHAMENTO DE RECURSOS.

O compartilhamento de recursos permite que programas, dados e periféricos e área de armazenamento, entre outros, estejam disponíveis para qualquer um na rede, independentemente da localização física do recurso e do usuário.

3.1.2 – AUMENTO DA CONFIABILIDADE.

Considerando-se que passa a existir redundância de recursos disponíveis, dependendo da forma como a rede é projetada e implementada a tolerância a falhas é ampliada consideravelmente, o que amplia a confiança no sistema..

3.1.3 – REDUÇÃO DE CUSTOS.

Computadores de pequeno porte têm uma razão preço/desempenho muito melhor do que os de grande porte. Um *mainframe* pode ser várias vezes mais rápido que o mais rápido microprocessador de um microcomputador, mas custa milhares de vezes mais. Esse desequilíbrio fez com que muitos projetistas de sistemas construíssem sistemas constituídos de computadores pessoais potentes, um por usuário, com os dados guardados em uma ou mais máquinas servidoras de arquivos.

3.1.4 –ESCALABILIDADE.

A possibilidade de aumentar o desempenho do sistema gradualmente, à medida que cresce o volume de trabalho, adicionando-se módulos processadores permite um crescimento gradual e a distribuição dos custos ao longo do tempo.

3.1.5 – COOPERAÇÃO.

Uma rede de computadores pode prover um meio de comunicação muito poderoso entre pessoas dispersas geograficamente. Utilizando-se de uma rede de computadores, duas ou mais pessoas que moram em lugares distantes podem produzir de forma cooperativa.

3.2 – PARÂMETRO DE COMPARAÇÃO PARA A IMPLANTAÇÃO DE REDES DE COMPUTADORES.

A escolha de um tipo de rede de computadores é tarefa complexa. Cada arquitetura possui determinadas

características que a tornam mais ou menos adequada, dependendo de um conjunto de fatores que afetam sua destinação e seu uso. Nenhuma solução pode ser considerada ótima para todos os casos. Muitos atributos entram em jogo: custo, confiabilidade, desempenho, modularidade, compatibilidade, entre outros.

3.2.1 – CUSTO.

O custo de uma rede é dividido entre o custo das estações de processamento (microcomputadores, minicomputadores etc.), o custo das interfaces com o meio de comunicação e o custo do próprio meio de comunicação. O custo das conexões dependerá muito do desempenho que se espera da rede. Redes de baixo a médio desempenho usualmente empregam poucas estações com uma demanda de taxas de dados e volume pequeno, com isso as interfaces serão de baixo custo devido as sua limitações e aplicações. Redes de alto desempenho já requerem interfaces de custos mais elevados, devido em grande parte ao protocolo de comunicação utilizado e ao meio de comunicação.

3.2.2 – CONFIABILIDADE.

A confiabilidade de um sistema em rede pode ser avaliada em termos de tempo médio entre falhas (Medium Time Between Failures- MTBF), tolerância a falhas, degradação amena (Gracefull Degradation), tempo de reconfiguração após falhas e tempo médio de reparo (MTTR - Medium Time to Repair).

O tempo médio entre falhas é geralmente medido em horas, estando relacionado com a confiabilidade de componentes e nível de redundância.

A degradação amena é dependente da aplicação. Ela mede a capacidade da rede continuar operando em presença de falhas, embora com um desempenho menor.

A reconfiguração após falhas requer que caminhos redundantes sejam acionados tão logo ocorra uma falha ou esta seja detectada.

A rede deve ser tolerante a falhas causadas por hardware e/ou software, de forma que tais falhas causem apenas uma confusão momentânea que será resolvida em algum nível de reinicialização do sistema. Falhas em componentes eletrônicos ou destruição de programas necessitam de redundância, mas essas não são as únicas falhas possíveis, devendo o sistema estar preparado para operar em condições de falhas não terminais.

O tempo médio de reparo caracteriza-se pela média dos tempos em que a rede esteve em reparo. Ele pode ser diminuído com o auxílio de redundância, mecanismos de autoteste e diagnóstico e manutenção eficiente.

3.2.3 – DESEMPENHO.

Várias são as medidas que caracterizam o desempenho de uma rede. Para entende-los, faz-se necessário definir o que é retardo de transferência, retardo de acesso e retardo de transmissão.

Retardo de Acesso é o intervalo de tempo decorrido desde que uma mensagem a transmitir é gerada pela estação até o momento em que a estação consiga obter somente para ela o direito de transmitir, sem que haja colisão de mensagens no meio.

Retardo de Transmissão é o intervalo de tempo decorrido desde o início da transmissão de uma mensagem por uma estação de origem até o momento em que a mensagem chega à estação de destino.

Retardo de Transferência é a soma dos retardos de acesso e transmissão, incluindo o todo o tempo de entrega de uma mensagem, desde o momento em que deseja transmiti-la, até o momento em que ela chega para ser recebida pelo destinatário.

O retardo de transferência é, na grande maioria dos casos, uma variável aleatória. No entanto, em algumas redes o maior valor que o retardo de transferência pode assumir é limitado, ou seja, determinístico.

A rede dever ser moldada ao tipo particular de aplicação de modo a assegurar um retardo de transferência baixo. O sistema de comunicação entre os módulos deve ser de alta velocidade e de baixa taxa de erro, de forma a não provocar saturação no trafego de mensagens. Em algumas aplicações (em particular as de controle em tempo real) a necessidade de retardo de transferência máximo limitado é de vital importância.

O desempenho caracteriza-se pela capacidade efetiva de transmissão da rede. Isto envolve diretamente o sistema de comunicação. Sabe-se que a utilização efetiva do sistema de comunicação é apenas uma porcentagem da capacidade total que ela oferece. Uma rede deve, então, proporcionar capacidade suficiente para viabilizar suas tarefas críticas. Certos critérios devem ser elevados em conta para isto: a escolha adequada do sistema de comunicação, a

estrutura de conexão, o protocolo de comunicação e o meio de transmissão.

3.2.4 – MODULARIDADE.

A Modularidade pode ser caracterizada como o grau de alteração de desempenho e funcionalidade que um sistema (rede) pode sofrer ao se modificar seu projeto original. Os três maiores benefícios de uma arquitetura modular são:

1 - a facilidade para modificação que é a simplicidade com que funções lógicas ou elementos de hardware podem ser substituídos, a despeito da relação íntima com outros elementos;

2 - a facilidade para crescimento que diz respeito à configuração de baixo custo (melhora de desempenho);

3 - baixo custo de expansão.

Uma rede bem projetada deve adaptar-se modularmente às várias aplicações, como também deve prever futuras ampliações.

3.2.5 – COMPATIBILIDADE.

A compatibilidade é de fundamental importância e define-se como a capacidade que o sistema (rede) possui para de utilizar a dispositivos de vários fabricantes, quer seja hardware ou software. Essa característica é extremamente importante na economia de custo de equipamentos já existentes.

Uma rede deve ter a capacidade de suportar todas as aplicações para qual foi dedicada e mais aquelas que o futuro possa requer. Quando possível, não deve ser vulnerável à tecnologia, prevendo a utilização de futuros desenvolvimentos, quer seja de novas estações, de novos padrões de transmissão ou novas tecnologias de transmissão.

Agora a que já discutimos alguns aspectos básicos importantes ao projeto de redes de computadores, vamos estudar a forma de estruturação de uma rede.

Em relação à estruturação, podem ser abordadas: a física e a lógica. Para isso serão discutidas as várias topologias de uma rede. O conceito de topologia, até há pouco relacionado apenas com a estruturação física da rede, agora abrange, também, a forma como a mesma é definida logicamente.

A **topologia** de uma rede de comunicação irá caracterizar seu tipo, eficiência e velocidade. A topologia refere-se à forma com que os enlaces físicos e os nós de comunicação estão organizados, determinando os caminhos físicos existentes e utilizáveis entre quaisquer pares de estações conectadas a essa rede.

Como foi definida anteriormente, uma Rede de Computadores é formada por um conjunto de módulos processadores interligados por um sistema de comunicação. Este sistema de comunicação se constituirá de um arranjo topológico interligando os vários módulos processadores através de enlaces físicos (meios de transmissão) e de um conjunto de regras com o fim de organizar a comunicação (protocolos).

Ao organizarmos os enlaces físicos, podemos utilizar diversas formas possíveis de linhas de transmissão.

Existem várias classificações para as diferentes redes de computadores. Dentre elas, duas dimensões se destacam mais:
1 - a tecnologia de transmissão que diz respeito às ligações físicas entre os módulos processadores;
2 - a escala que diz respeito à distribuição espacial dos módulos processadores ou à abrangência da rede.

4.1 – TECNOLOGIA DE TRANSMISSÃO.

Basicamente há dois **tipos de tecnologia de transmissão**: as redes em difusão (ou multiponto) e as redes ponto-a-ponto.

Nas **redes em difusão** há apenas um canal de transmissão compartilhado por todas as máquinas. Uma mensagem enviada por uma estação é "ouvida" por todas as outras estações. Nas **redes ponto-a-ponto** existem várias conexões entre pares individuais de estações. Estes dois tipos de ligação podem ser vistos na figura 4.1 abaixo.

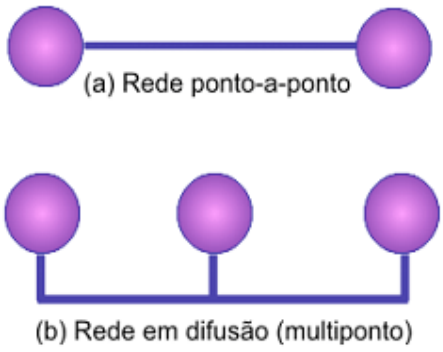


Figura 4.1 – Tipos de tecnologia de transmissão

O meio de transmissão consiste geralmente de um conjunto de recursos e regras que permitem a transmissão de informação de um ponto a outro numa rede de comunicação. A transmissão de bits é uma das formas mais simples de transferência de informação. Este processo é ilustrado pela figura 4.2(a), onde podemos observar os seguintes elementos:

1. a fonte de informação, que pode ser um computador ou um terminal, por exemplo, que gera as informações que deverão ser transmitidas, estas sendo representadas, usualmente, por um conjunto de dígitos binários, ou bits;
2. o transmissor, que é responsável da adaptação ou conversão do conjunto de informações, de bits, para sinal elétrico ou eletromagnético, adaptando-o ao meio de transmissão;
3. o suporte de transmissão, encarregado do transporte dos sinais representando a informação e que pode ser caracterizado por uma das técnicas apresentadas na seção precedente; é o suporte de transmissão quem realiza

a “ligação física” entre os elementos envolvidos na comunicação; o receptor, responsável pela reconstituição da informação a partir dos sinais recebidos via suporte de transmissão, e que, inclusive pode ter sofrido distorções provocadas por ruídos existentes no meio;

4. o destinatário da informação, que pode ser um computador, um terminal ou outro equipamento e que vai consumir a informação gerada pelo elemento fonte.

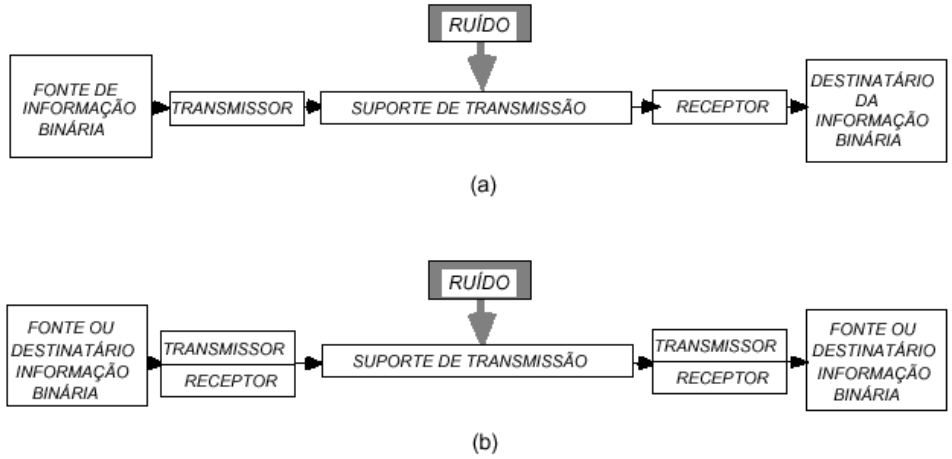


Figura 4.2 - (a) Sistema de transmissão ponto-a-ponto unidirecional; (b) modelo bidirecional.

Geralmente, a transmissão de bits pode ser realizada de forma bidirecional, esta podendo ainda ser realizada de forma alternada ou simultânea. Assim, a cada nó deverá estar associado um equipamento transmissor e um receptor compondo o conjunto transceptor como mostrado na figura 4.2(b).

A transmissão de dados, quando realizada nos dois sentidos é denominada **duplex**. No caso em que ela se realiza alternadamente, ou seja, ora num sentido, ora no outro, ela se denomina **half-duplex**. No caso em que ela se realiza simultaneamente nos dois sentidos, esta será denominada **full-duplex**.

Os modos de transmissão caracterizam as diferentes formas como os bits de informação transmitidos são delimitados e encaminhados ao longo da linha de comunicação. No que diz respeito à forma como os bits são encaminhados ao longo de uma linha de comunicação, pode-se distinguir o modo de transmissão **paralelo** e o modo **serial**.

Na **transmissão paralela**, os bits são transportados simultaneamente por um suporte composto de várias linhas em paralelo. É um modo de transmissão mais adequado à comunicação entre equipamentos localizados a curtas distâncias. A ligação interna na arquitetura de computadores ou entre computadores e periféricos próximos são exemplos da aplicação da transmissão paralela.

Na **transmissão serial**, mais adequada a comunicação entre equipamentos separados por grandes distâncias, os bits são encaminhados serialmente através de uma única linha de comunicação. Pode-se considerar outros parâmetros para a classificação dos modos de transmissão, como, por exemplo, o fator tempo. No caso particular das transmissões seriais, a forma de delimitar os bits pode levar em conta duas diferentes filosofias — a transmissão serial síncrona e a transmissão serial assíncrona.

Na **transmissão síncrona**, os bits de dados são transmitidos segundo uma cadência pré-definida, obedecendo a um sinal de temporização (clock). O receptor, por sua vez, conhecendo os intervalos de tempo permitindo delimitar um bit, poderá identificar a seqüência dos bits fazendo uma amostragem do sinal recebido.

Na **transmissão assíncrona**, não existe a fixação prévia de um período de tempo de emissão entre o transmissor e o receptor. A separação entre os bits é feita através de um sinal especial com duração variável. Um caso típico de transmissão assíncrona é a transmissão de caracteres; neste caso, a cada grupo de bits constituindo um caractere são adicionados bits especiais para representar o início (start bit) e final deste (stop bit). Neste tipo de comunicação, apesar de assíncrona ao nível de caracteres, ocorre uma sincronização ao nível de bit.

Um outro aspecto a ser destacado aqui é aquele da forma como os sinais são transmitidos num suporte de comunicação, particularmente no que consiste à maneira como a banda passante do canal de comunicação é explorada.

No primeiro modo, a transmissão em **banda de base** (baseband), a banda passante do suporte de transmissão é atribuída totalmente a um único canal de transmissão. Neste modo, os sinais são transmitidos através do meio de

comunicação multiplexados no tempo.

No segundo modo, a transmissão em **barda larga** (broadband), a banda passante do suporte de transmissão é dividida num determinado número de canais de faixa de freqüência estreita, permitindo que estes possam então ser transmitidos utilizando uma técnica de multiplexação em freqüência. A banda passante dos canais é normalmente definida em função da taxa de transmissão desejada e do modo de modulação empregado. Neste modo de transmissão, cada canal pode atingir uma taxa de transmissão de até 3 Mbits/s, inferior, portanto, à transmissão em banda de base.

4.1.1 – ARRANJOS TOPOLÓGICOS.

Como já descrito, a **topologia** refere-se à forma com que os enlaces físicos e os nós de comunicação estão organizados A maneira como as diferentes estações serão interligadas denomina-se topologia da rede. Estas topologias estão relacionadas a forma como o canal de comunicação será alocado, ou seja, através de canais ponto-a-ponto ou canais de difusão.

Nas topologias que utilizam canais ponto-a-ponto, a rede é composta de diversas linhas de comunicação, cada linha sendo associada à conexão de um par de estações. Neste caso, se duas estações precisam comunicar-se e não há entre elas um cabo comum, a comunicação será feita de modo indireto, através de uma (ou mais) estações.

Assim, quando uma mensagem é enviada de uma estação a outra de forma indireta, ela será recebida integralmente por cada estação e, uma vez que a linha de saída da estação considerada está livre, retransmitida à estação seguinte. Esta política de transmissão é também conhecida por store and forward. A maior parte das redes de longa distância é do tipo ponto-a-ponto. As redes ponto-a-ponto podem ser concebidas segundo diferentes topologias. As redes locais ponto-a-ponto são caracterizadas normalmente por uma topologia simétrica; as redes de longa distância apresentam geralmente topologias assimétricas. A figura 4.3 apresenta as diferentes topologias possíveis nas redes ponto-a-ponto.

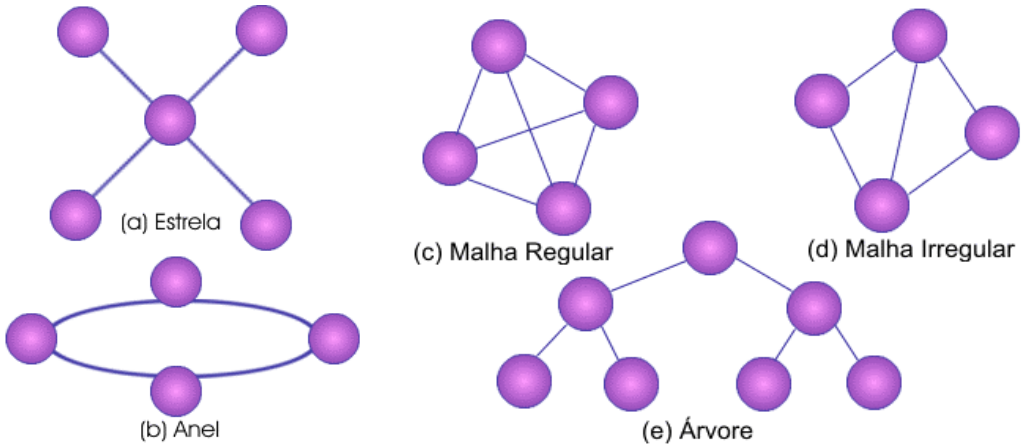


Figura 4.3 - Topologias ponto-a-ponto: (a) estrela, (b) anel, (c) malha regular, (d) malha irregular e (e) árvore.

As redes de difusão (multiponto) são caracterizadas pelo compartilhamento, por todas as estações, de um único canal de comunicação. Neste caso, as mensagens enviadas por uma estação são recebidas por todas as demais conectadas ao suporte de transmissão, sendo que um campo de endereço contido na mensagem permite identificar o destinatário. Na recepção, a máquina verifica se o conteúdo do campo de endereço corresponde ao seu e, em caso negativo, a mensagem é ignorada.

As redes locais pertencem geralmente a esta classe de redes. Nas redes de difusão existe a possibilidade de uma estação enviar uma mesma mensagem às demais estações da rede, utilizando um código de endereço especial. Neste caso, todas as estações vão tratar as mensagens recebidas endereçadas para este endereço comum. Este modo de operação é denominado broadcasting.

Alguns sistemas de difusão também suportam transmissão para um subconjunto de estações, conhecido como multicasting. A figura 4.4 apresenta algumas topologias possíveis no caso das redes em difusão. Numa rede em **barramento**, uma única máquina pode estar transmitindo a cada instante. As demais estações devem esperar para transmissão caso o barramento esteja ocupado. Para isto, um mecanismo de arbitragem deve ser implementado para resolver possíveis problemas de conflito (quando duas ou mais estações querem enviar uma mensagem), este

mecanismo pode ser centralizado ou distribuído.

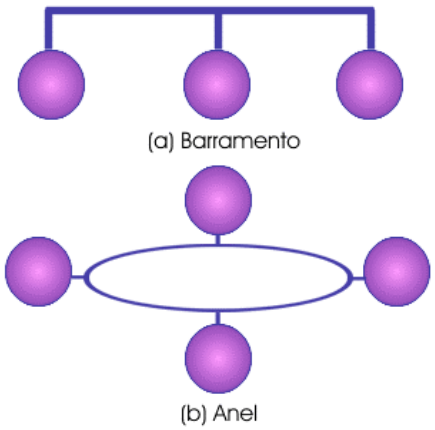


Figura 4.4 - Topologias das redes de difusão: (a) barramento e (b) anel

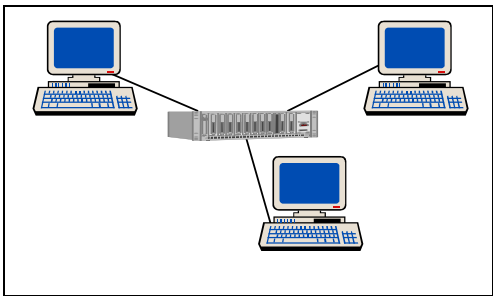
No caso do **anel**, cada bit transmitido é propagado de maneira independente em relação à mensagem ao qual ele pertence. Em geral, cada bit realiza uma volta completa no anel durante o tempo necessário para a emissão de um certo número de bits, antes mesmo da emissão completa da mensagem. Também nesta topologia, é necessária a implementação de um mecanismo de acesso ao suporte de comunicação.

Outra topologia de rede em difusão é a das redes de satélite (ou rádio), cada estação é dotada de uma antena através da qual pode enviar e receber mensagens. Cada estação pode "escutar" o satélite e, em alguns casos, receber diretamente as mensagens enviadas pelas demais estações.

As redes de difusão podem ainda considerar duas classes de mecanismos de acesso ao suporte de comunicação: estáticas ou dinâmicas. Um exemplo do primeiro caso é a definição de intervalos de tempo durante os quais cada estação tem a posse do canal de comunicação, permitindo então que esta emita a mensagem de maneira cíclica. No entanto, esta política é bastante ineficiente do ponto de vista do envio das mensagens, uma vez que muitas estações não vão enviar mensagens nos intervalos a elas destinadas.

Já na outra classe de mecanismos, os dinâmicos, o acesso é dado às estações segundo a demanda de envio de mensagens. Nos mecanismos de acesso dinâmicos, pode-se ainda considerar dois casos:
1 - os mecanismos centralizados, nos quais uma estação central (ou árbitro) é a responsável pela definição do direito de acesso ao suporte de comunicação;
2 - os mecanismos distribuídos, nos quais cada estação define quando ela vai emitir a mensagem.

4.1.1.1 - TOPOLOGIA EM ESTRELA.



Na **estrela**, cada nó é interligado a um nó central (mestre), através do qual todas as mensagens devem passar. O nó central age como centro de controle da rede, interligando os demais nós (escravos) que podem se comunicar apenas em pares de cada vez. Isto não impede que haja comunicações simultâneas, desde que as estações envolvidas sejam diferentes.

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 – um computador, por exemplo. Em outras redes o nó central tem como única função o gerenciamente das comunicações. Quando o nó central tem a função exclusiva de chaveamento (comutação) entre as estações, é denominado *switch* ou comutador.

Esta topologia não necessita de roteamento, uma vez que concentram todas as mensagens no nó central. O gerenciamento das comunicações por este nó pode ser por chaveamento de pacotes ou chaveamento de circuitos. No

primeiro caso, pacotes são enviados do nó fonte para o nó central que o retransmite então ao nó de destino em momento apropriado. Já no caso de chaveamento de circuitos, o nó central, baseado em informações recebidas, estabelece uma conexão elétrica ou realizada por software, entre o nó fonte e nó de destino, conexão esta que existirá durante toda a conversação. Neste último caso, se já existir uma conexão ligando duas estações, nenhuma outra conexão pode ser estabelecida para estes nós. Redes de chaveamentos computadorizadas - CBX("Computerized Branch Exchange") - são exemplos deste último tipo de rede, onde a função de chaveamento é realizada por um PABX("Privat Automatic Branch Exchange").
OBS: As CBX's são apropriadas tanto para o tráfego de voz quanto para o de dados entre terminais e terminais e computadores.

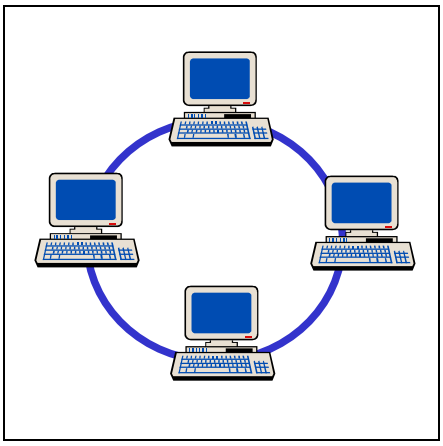
Como mencionado, o nó central pode realizar funções além das de chaveamento e processamento normal. Por exemplo, o nó central pode realizar a compatibilidade da velocidade de comunicação entre o transmissor e o receptor. Os dispositivos fonte e destino podem até operar com protocolos e/ou conjunto de caracteres diferentes. O nó central atuaria neste caso como um conversor de protocolos permitindo a um sistema de um fabricante trabalhar satisfatoriamente com um outro sistema de um outro fabricante. Poderia ser também função do nó central fornecer algum grau de proteção de forma a impedir pessoas não autorizadas de utilizar a rede ou ter acesso a determinados sistemas de computação. Outras, como operações de diagnósticos de rede por exemplo, poderiam também fazer parte dos serviços realizados pelo nó mestre.

A confiabilidade pode ser 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 podem ocasionar a parada total do sistema. Redundâncias podem ser acrescentadas, porém as dificuldades de custo em tornar o nó central confiável podem inviabilizar o projeto, dependendo de que se deseja.

Outro problema da rede em estrela é relativo a modularidade. A configuração pode ser expandida até um certo limite imposto pelo nó central: em termos de capacidade de chaveamento, números de circuitos concorrentes que podem ser gerenciados e número total de nós que podem ser servidos. Embora não seja freqüentemente encontrado é possível a utilização de diferentes meios de transmissão para ligação de nós escravos ao nó central.

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 substituir do nó central.

4.1.1.2 - TOPOLOGIA EM ANEL.



Uma rede em **anel** constitui-se de estações conectadas através de um caminho fechado, evitando os problemas de confiabilidade de uma rede em estrela. O anel não interliga as estações diretamente, mas consiste de uma série de repetidores ligados por um meio físico, sendo cada estação ligada a estes repetidores.

Redes em anel são capazes de transmitir e receber dados em qualquer direção. As configurações mais usuais, no entanto, são unidirecionais para simplificar o projeto dos repetidores mais simples e tornar menos sofisticados os protocolos de comunicação que asseguram a entrega da mensagem corretamente. Os repetidores são em geral projetados de forma a transmitir e receber dados simultaneamente, diminuindo assim o retardo de transmissão.

Quando uma mensagem é enviada por um nó, ela entra no anel e circula até ser retirada pelo de nó de destino, ou então até voltar ao nó fonte, dependendo do protocolo empregado.

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.

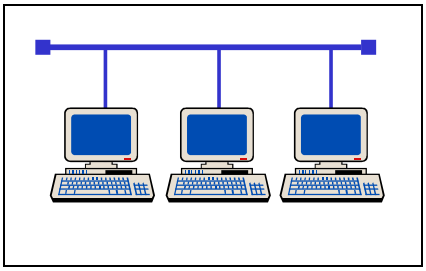
Os maiores problemas com topologia em anel são sua vulnerabilidade a erros e pouca tolerância a falhas.

Qualquer que seja o controle de acesso empregado, ele pode ser perdido por falhas e pode ser difícil determinar com certeza se este controle foi perdido e qual nó deve recriá-lo. Erros de transmissão e processamento podem fazer com que uma mensagem continue eternamente a circular no anel.

A modularidade de uma rede em anel é bastante elevada devido ao fato de os repetidores ativos regenerarem as mensagens. Redes em anel podem atingir grandes distâncias (teoricamente o infinito). Existe, no entanto, uma limitação prática do número de estações em um anel. Este limite é devido aos problemas de manutenção e confiabilidade citados anteriormente e ao retardo cumulativo do grande número de repetidores.

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.

4.1.1.3 - TOPOLOGIA EM BARRA.



A topologia em **barra** (ou barramento) se caracteriza pela ligação de estações (nós) ao mesmo meio de transmissão. A barra é geralmente compartilha tempo ou freqüência, permitindo a transmissão de informação. Ao contrário das outras topologias que são geralmente 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).

Nas redes em barra comum cada nó conectado à barra pode ouvir todas as informações transmitidas.

Existe uma variedade de mecanismos para o controle de acesso ao barramento, que pode ser centralizado ou descentralizado. A técnica adotada para cada acesso à rede (ou a banda de freqüência de rede no caso de redes em banda larga) é a multiplexação no tempo. Em um controle centralizado, o direito de acesso é determinado por uma estação especial da rede. Em um ambiente de controle descentralizado, a responsabilidade é distribuída entre todos os nós.

Diferente da topologia em anel, topologias em barra podem empregar interfaces passivas, nas quais falhas não causam a parada total do sistema. A confiabilidade deste tipo de topologia vai depender em muito da estratégia de controle. O controle centralizado oferece os mesmos problemas de confiabilidade de uma rede em estrela, com atenuante de que, aqui, a redundância de um nó pode ser outro nó comum da rede. Mecanismos de controle descentralizados semelhantes aos empregados na topologia em anel podem também ser empregados neste tipo de topologia, acarretando os mesmos problemas quanto à detecção da perda do controle e sua recriação.

A ligação ao meio de transmissão é um ponto crítico no projeto de uma rede local em barramento. A ligação deve ser feita de forma a alterar o mínimo possível as características elétricas do meio. O meio por sua vez deve terminar em seus dois extremos por uma carga igual a sua impedância característica, de forma a evitar interferência no sinal transmitido. O poder de crescimento, tanto no que diz respeito à distância máxima entre dois nós da rede quanto ao número de nós que a rede pode suportar dependerá: (a) do meio de transmissão utilizado; (b) da taxa de transmissão e (c) da quantidade de ligações ao meio. Caso seja necessário atingir distâncias maiores que a máxima permitida em um segmento de cabo, repetidores serão necessários para assegurar a qualidade do sinal. Tais repetidores, por serem ativos, apresentam um ponto de possível diminuição da confiabilidade da rede.

O desempenho de um barramento é determinado pelo meio de transmissão, pelo número de nós conectados, pelo controle de acesso, pelo tipo de tráfego, além de outros fatores. Por empregar interfaces passivas, a inexistência de armazenamento local de mensagens e a inexistência de retardos no repetidor não vão degradar o tempo de resposta que, contudo, pode ser altamente dependente do protocolo de acesso utilizado.

4.1.1.4 - OUTRAS TOPOLOGIAS.

Dentre ouras topologias ainda podemos citar as topologias em **árvore** e a estrutura de grafos (**malha regular ou irregular**).

A topologia em árvore é, na verdade, uma série de barramentos interconectados. Geralmente existe um barramento central onde outros ramos menores se conectam. Esta ligação é realizada através de derivadores e as conexões das estações realizadas do mesmo modo que no sistema de barramento padrão.

Cuidados adicionais devem ser tomados nas redes em árvores, pois cada ramificação significa que o sinal deverá se propagar por dois caminhos diferente. A menos que estes caminhos estejam perfeitamente casados, os sinais terão velocidades de propagação diferentes e refletirão os sinais de diferentes maneiras. Em geral, redes em árvore, trabalham com taxas de transmissão menores do que as redes em barra comuns, por estes motivos.

A topologia genérica é a estrutura de grafos. Desta derivam as redes completamente ligadas (malha regular), as redes parcialmente ligadas (malha irregular), em estrela e as redes em anel.

Redes interligadas ponto a ponto crescem em complexidade com o aumento do número de estações conectadas. Nestes sistemas não é necessário que cada estação esteja ligada a todas as outras (sistemas completamente ligados). Devido ao custo das ligações é mais comum o uso de sistemas parcialmente ligados baseados em chaveamento de circuitos de mensagens ou de pacotes. O arranjo das ligações é normalmente baseado no tráfego da rede. A generalidade introduzida neste tipo de topologia visa a otimização do custo do meio de transmissão. Devido a isto tal topologia é normalmente empregada em redes de longa distância (geograficamente distribuídas).

Em redes locais os meios de transmissão de alta velocidade podem ser utilizados, pois têm um custo baixo, definido pelas limitações de distâncias. Tal topologia não tem tanta aplicação neste caso, por introduzir mecanismos complexos de decisões de roteamento em cada nó da rede, causado por sua generalidade. Tais mecanismos iriam introduzir um custo adicional nas interfaces de rede que tornariam seu uso proibitivo quando comparado com o custo das estações.

Estruturas parcialmente ligadas têm o mesmo problema de confiabilidade das estruturas em anel. O problema, no entanto, é atenuado pela existência de caminhos alternativos em caso de falha de um repetidor. A modularidade desta topologia é boa, desde que os dois ou mais nós com os quais um novo nó a ser incluído se ligará possam suportar o aumento de carga.

4.1.1.5 - TOPOLOGIA FÍSICA X TOPOLOGIA LÓGICA.

A topologia de uma rede irá determinar, em parte, o método de acesso à rede utilizado. Métodos de acesso são necessários para regular a utilização dos meios físicos compartilhados. A forte tendência de utilização de HUBs nas instalações físicas das redes corresponde, fisicamente, a implantação de uma topologia em estrela. Esta tendência é explicada pela crescente necessidade de melhorar o gerenciamento e a manutenção nessas instalações. A topologia em estrela apresenta uma baixa confiabilidade, porém, os avanços da eletrônica já permitem que se construam equipamentos de alta confiabilidade, viabilizando este tipo de topologia.

A utilização de HUBs não exige, necessariamente, que as interfaces das estações com a rede o percebam como uma topologia em estrela. O funcionamento continua a ser como no acesso a um barramento ou a um anel, com os seus respectivos métodos de acesso. Sendo assim, podemos diferenciar dois tipos de topologias: uma topologia lógica, que é aquela observada sob o ponto de vista das interfaces das estações com a rede (que inclui o método de acesso), e uma topologia física, que diz respeito à configuração física utilizada na instalação da rede.

A construção dos HUBs teve uma evolução contínua no sentido de que os mesmos não implementem somente a utilização do meio compartilhado, mas também possibilitem a troca de mensagens entre várias estações simultaneamente. Desta forma as estações podem obter para si taxas efetivas de transmissão bem maiores. Esse tipo de elemento, também central, é denominado Switch. As redes ATM, por exemplo, baseiam-se na presença de switches de grande capacidade de comutação que permitem taxas de transmissão que podem chegar à ordem de Gbps (gigabits por segundo).

4.2 – ESCALA: CATEGORIAS DE REDES.

As redes também podem ser classificadas por escala. A figura 4.5 mostra uma classificação das várias redes de computadores em relação a sua abrangência. Basicamente elas podem ser classificadas em três grupos**: LAN** – Local Area Network ou Rede Local, **MAN** – Metropolitan Area Network ou Rede Metropolitana e **WAN** – Wide Area Network ou Rede Geograficamente Distribuída (ou de Longa Distância).

Distância entre nós	Abrangência
até 10 m	Sala
até 100 m	Edifício
até 1 km	Campus
até 10 km	Cidade
até 100 km	Pais
até 1.000 km	Continente
até 10.000 km	Planeta

Figura 4.5- Classificação de redes quanto a distância física entre os nós.

Esta classificação não é, de maneira alguma, fechada. Por exemplo, uma rede local pode alcançar dimensões metropolitanas e ainda assim ser considerada local.

4.2.1 – REDES LOCAIS (LANs - Local Area Networks).

As **Redes Locais** são redes privadas contidas em um prédio ou campus universitário, que tem alguns quilômetros de extensão. As redes locais foram definidas e utilizadas inicialmente nos ambientes de institutos de pesquisa e universidades. Elas surgiram para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos preservando a independência das várias estações de processamento e permitindo a integração em ambientes de trabalho cooperativo.

As redes locais distinguem-se pelas aplicações pretendidas e serviços oferecidos, pela topologia da rede, do meio de transmissão e por sua arquitetura de protocolo. Elas foram desenvolvidas para dar suporte a vários tipos de aplicações, incluindo entre elas: aplicações para transmissão de dados e/ou voz e/ou vídeo, comunicações entre terminais e computadores, comunicações entre computadores, controle de processos e automação de escritório, entre outras.

Qualquer que seja a aplicação, vários fatores devem ser levados em consideração, dentre eles: dispersão geográfica, ambiente de operação, número máximo de nós, separação máxima e mínima entre os nós, tempo de resposta, tipo de informação transmitida, tipo de interação entre dispositivos, taxa máxima de informação transmitida, confiabilidade exigida, tipo de tráfego e outros.

As Redes Locais têm em geral três domínios de aplicações quanto à cobertura geográfica: uma única sala (por exemplo, para compartilhamento de dispositivos especiais entre vários computadores), dentro de um edifício (por exemplo, na integração de um serviço de escritório), ou mesmo uma área coberta por vários edifícios (por exemplo, um campus universitário ou uma fábrica). A dispersão geográfica é fundamental na escolha da topologia e meio de transmissão.

O ambiente de operação influencia também na escolha do meio de transmissão e topologia. Problemas no ambiente físico, elétrico ou de segurança determinam requisitos mais fortes quanto à escolha. A ocorrência de erros devido a ruídos gerados por problemas no ambiente exigirá também dos protocolos mecanismos de detecção e recuperação, em alguns casos.

Nas LANs tradicionais os computadores são interconectados por cabos ou através de equipamentos tipo HUB. Neste tipo de rede as velocidades geralmente variam de 10 a 100 Mbps, há um baixo retardo e pouquíssimos erros de transmissão são encontrados. As LANs mais modernas podem operar em velocidades ainda mais altas, alcançando Gbps.

Este tipo de rede apresenta como topologias lógicas mais usadas o barramento e o anel e como topologias físicas: a árvore e a estrela. É fato que em qualquer tipo de rede duas ou mais estações podem necessitar enviar informações pelo meio de transmissão no mesmo instante. Analisando estes arranjos topológicos verificamos que há a

necessidade de um mecanismo de arbitragem para determinação de qual estação poderá transmitir de forma a não existência de conflitos e garantia de tempo para todas as estações que têm dados a transmitir.

4.2.2 – REDES METROPOLITANAS (MAN - Metropolitan Area Network).

Uma **Rede Metropolitana** é, na verdade, uma versão ampliada de uma LAN, pois basicamente os dois tipos de rede utilizam tecnologias semelhantes. Uma MAN pode abranger um grupo de escritórios vizinhos ou uma cidade inteira e pode ser privada ou pública. Este tipo de rede pode transportar voz e dados, podendo inclusive ser associado à rede de televisão a cabo local.

A principal razão para se tratar as redes metropolitanas como uma categoria especial é que elas têm um padrão especial, o DQDB (Distributed Queue Dual Bus) ou IEEE 802.6. Atualmente as redes ATM (Asynchronous Transfer Mode) têm sido a tecnologia com maior aceitação para uso em redes metropolitanas.

4.2.3 – REDES GEOGRATICAMENTE DISTRIBUIDAS (WANs - Wide Area Networks).

As WANs, ou **Redes de Longa Distância** abrangem uma ampla área geográfica, com freqüência um país ou continente. Ela também contém um conjunto de máquinas cuja finalidade é executar programas de usuários, as chamadas aplicações. Estas máquinas são denominadas na literatura como hosts ou end systems. Estes hosts são conectados por uma sub-rede de comunicação, ou somente sub-rede. A tarefa das sub-rede é transportar mensagens de um host para outro, exatamente como o sistema telefônico transporta palavras da pessoa que fala para aquela que ouve. Esta estrutura é simplificada, pois separa os aspectos de comunicação pertencentes à rede (a sub-rede) dos aspectos de comunicação.

Na maioria das redes geograficamente distribuídas, a sub-rede consiste em dois componentes distintos: linhas de transmissão e elementos de comutação. As linhas de transmissão, também chamadas circuitos, canais ou troncos, transportam os bits entre as máquinas. Os elementos de comutação são equipamentos especializados usados para conectar duas ou mais linhas de transmissão. Quando os dados chegam por uma linha de entrada, o elemento de comutação deve escolher uma linha de saída para encaminhá-la. Não existe uma terminologia padrão para identificar estes equipamentos. Dependendo das circunstâncias eles são chamados nós de comutação de pacotes, sistemas intermediários, **centrais de comutação de dados** ou ainda **IMP (Interface Message Processor)**. Mas o termo mais comum para identificar estes elementos de comutação é **roteador**. No modelo mostrado na figura 4.6, os hosts são ligados a algum tipo de rede local onde há também um elemento de comutação, embora em alguns casos um host possa estar ligado diretamente a um elemento de comutação. O conjunto de linhas de comunicação e elementos de comutação forma a sub-rede.

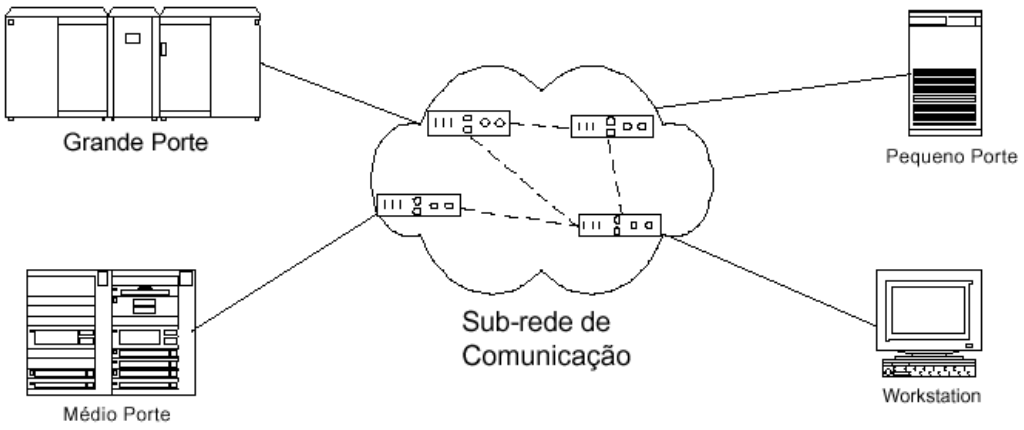


Figura 4.6 - Ligações entre hosts e a sub-rede de comunicação

Em função dos custos de comunicação serem bastante altos, estas redes são, muitas vezes, públicas, isto é, o sistema de comunicação, chamado sub-rede de comunicação, é mantido, gerenciado e de propriedade pública. Também em função dos custos, as velocidades empregadas são relativamente baixas, de alguns kilobits/segundo, podendo chegar a megabits/segundo.

Existem muitas redes no mundo, freqüentemente com hardwares e softwares específicos. Normalmente as pessoas conectadas a diferentes redes precisam comunicar-se e para que isto seja possível são necessárias conexões entre redes que muitas vezes são incompatíveis. Para que esta comunicação possa realizar-se são utilizados os chamados **gateways**, que estabelecem conexões e permitem a comunicação entre usuários de redes diferentes. Um conjunto de redes interconectadas é chamado de ligação inter-rede, ou apenas inter-rede.

A palavra inter-rede deve ser usada de modo genérico, já a Internet é uma inter-rede mundial específica, muito utilizada para interconectar universidades, órgãos do governo, empresas e pessoas físicas.

As sub-redes, redes e inter-redes são freqüentemente confundidas. Uma sub-rede faz mais sentido no contexto de uma rede geograficamente distribuída, onde fazem referência ao conjunto de roteadores e linhas de transmissão do operador da rede. Por outro lado, a combinação de uma sub-rede e seus hosts forma uma rede. Uma inter-rede é formada quando diferentes redes são conectadas.

4.2.4 – REDES SEM FIO (Wireless Networks).

Embora não constituam uma categoria específica quanto à distribuição geográfica, as **Redes Sem Fio** representam um segmento de mercado que vem crescendo muito. Elas são necessárias quando é impossível haver uma conexão por fios, como por exemplo, a partir de carros ou aviões. Outro problema que elas solucionam é quando uma pessoa viaja e quer usar seu computador portátil para enviar e receber mensagens de correio eletrônico, fax, ler arquivos remotos, estabelecer login com computadores remotos, estejam eles em terra, no mar ou no ar.

As redes sem fio são muito utilizadas por empresas transportadoras, por táxis e por funcionários de assistência técnica ou de vendas, pois estes estão sempre necessitando de informações atualizadas de bases de dados de suas empresas. Elas também têm sido muito utilizadas para operações de resgate em caso de catástrofes onde o sistema telefônico foi destruído e em operações militares.

Embora as redes sem fio e a computação móvel tenham uma estreita relação, elas não são iguais. Às vezes os computadores portáteis podem ser conectados por fios. Por exemplo, se uma pessoa conecta um computador portátil na tomada do telefone de um hotel temos mobilidade sem o uso de uma rede sem fio. Por outro lado alguns computadores com comunicação sem fio não são portáteis. Esse é o caso das empresas sediadas em prédios muito antigos nos quais não há possibilidade de passagem de cabeamento de rede. por vezes a instalação de uma rede sem fio pode ser mais barata do que instalar fiação necessária no prédio.

As redes sem fios são fáceis de instalar, mas elas possuem algumas desvantagens: baixa velocidade e altas taxas de erro. Elas também possuem inúmeros formatos. Elas podem variar desde LANs sem fio que cobrem um campus universitário, para que os alunos possam usar seus computadores portáteis e trabalhar sob a sombra de uma árvore, até o uso de telefones celulares para acesso remoto a redes.

4.3 - SUPORTES DE TRANSMISSÃO.

Os **suportes de transmissão** constituem-se pela conexão física entre as estações da rede. Geralmente eles se diferenciam quanto à banda passante, tipo de tecnologia de transmissão (ponto-a-ponto ou multiponto), limitação geográfica (distância entre pontos), imunidade a ruído, custo, disponibilidade de componentes e confiabilidade. A escolha do suporte de transmissão adequado é extremamente importante porque ele influencia diretamente no custo das interfaces com a rede.

Qualquer meio físico capaz de transportar informações eletromagnéticas é possível de ser usado em redes locais. Os mais comumente utilizados são o par trançado, o cabo coaxial e a fibra ótica. Também são utilizados: radiodifusão, infravermelho e microondas.

4.3.1 - PAR DE FIOS TRANÇADOS (PAR TRANÇADO - UTP).

Em diversas aplicações, é necessário se manter uma conexão direta e permanente entre dois computadores. O suporte de transmissão mais clássico utilizado até o momento é o **par de fios trançados (UTP)**, que é composto de dois fios elétricos em cobre, isolados, e arranjados longitudinalmente de forma helicoidal (enrolados em espiral). Esta técnica de enrolar os fios permite diminuir os efeitos das induções eletromagnéticas parasitas provenientes do ambiente no qual o cabo estiver instalado. A figura 4.7 apresenta o cabo UTP.

Figura 4.7– Cabo Par trançado.

A utilização mais comum deste suporte de transmissão é a rede telefônica, onde, graças às suas características elétricas, os sinais podem percorrer várias dezenas de quilômetros, sem a necessidade de amplificação ou regeneração de sinal.

Estes podem, ainda, ser utilizados para a transmissão de sinais analógicos quanto de sinais digitais, a banda passante atingida sendo função da sua composição (particularmente, diâmetro e pureza dos condutores, natureza dos isolantes e do comprimento do cabo). A taxa de transmissão obtida pela utilização deste suporte de transmissão situa-se na faixa de algumas dezenas de Kbits/s, podendo atingir, em condições particulares, na faixa dos Mbits/s em pequenas distâncias.

O fato de representar um baixo custo e uma grande faixa de utilização tornam o UTP um dos suportes mais utilizados atualmente e, provavelmente, nos próximos anos.

A maioria dos cabos UTP produzidos hoje possui quatro pares internos. Eles utilizam condutores rígidos 24AWG (American Wire Gauge) de cobre. O que define a máxima banda de passagem em freqüência é a qualidade do fio de cobre. Quanto mais maciço e com menos variação no diâmetro melhor será o condutor. Pode haver falhas no interior do cabo, como bolhas e até longos dutos que prejudicam sua qualidade. Os cabos UTP são padronizados pela EIA/TIA (Eletronic Industry Association / Telecomunications Industry Associations) sob o código 568. No momento existem cinco padrões de cabos, sendo que em sua maioria eles seguem apenas o padrão 3 ou 5.

O padrão 3 regulamenta que os condutores sejam 24AWG. O condutor de sinal deve estar trançado com a terra do sinal. A impedância deve ser de 100 Ohms e a banda de passagem deve ser no mínimo de 16Mhz dentro de certos padrões de atenuação máxima.

O padrão 4 requer condutores 22AWG ou 24AWG (diâmetro menor). A impedância deve ser de 100 Ohms e a banda de freqüência de 20MHz.

O padrão 5 deve utilizar condutores também 22 ou 24AWG. Cada par sinal-terra também deve estar trançado e a impedância também deve ser de 100 Ohms com banda de 100MHz. Por permitir essa é o mais caro, mas é o único que atende às especificações para que a rede tenha condições de operar em 100Mbps.

Os conectores utilizados para ligar os cabos aos adaptadores e equipamentos de interconexão (como HUBs) são do tipo RJ-45. É bastante simples a montagem do conector RJ-45 no cabo UTP. Só é necessário realizar uma única decapagem fácil e rápida, normalmente com a própria ferramenta de montagem. A figura 4.8 apresenta o conector RJ-45.

Conector RJ-45

Ferramenta de Montagem
Do conector RJ-45 no cabo UTP

Conector RJ-45
Prensado no cabo UTP

Figura 4.8– Conector RJ-45 e ferramenta de prensagem.

O comprimento de um cabo não deve exceder 100m. Além disso, duas máquinas não devem estar separadas por mais de 205m de cabo. Caso isso não seja possível, será necessário utilizar um dispositivo repetidor (um HUB é um repetidor) para reforçar o sinal. Existe um número máximo de interligação de repetidores após o qual o suporte à

transmissão não é mais eficiente. Este número varia de acordo com as características dos equipamentos de interconexão e padrões utilizados.

4.3.2 - CABO COAXIAL.

Os **cabos coaxiais** são também altamente empregados como suporte de transmissão. Dois tipos de cabos são normalmente utilizados: o primeiro tipo apresenta uma impedância característica de 50 ohms, utilizado em transmissões digitais denominadas transmissão em banda de base; o segundo tipo, com uma impedância característica de 75 ohms, é mais adequado para a transmissão de sinais analógicos. Eles são constituídos de dois condutores arranjados de forma concêntrica: um condutor central, a alma, envolto por um material isolante de forma cilíndrica. Esta capa isolante é, por sua vez, envolta por uma trança metálica condutora em cobre. Finalmente, o conjunto é envolto numa capa de proteção em plástico isolante.

Em relação aos pares de fios trançados, os cabos coaxiais apresentam melhores características elétricas, oferecendo uma boa relação entre a banda passante e a proteção contra interferências eletromagnéticas.

A largura de banda vai depender igualmente da qualidade da composição do cabo e do seu comprimento. Para distâncias em torno de 1 km, é possível obter uma taxa de transmissão em torno de 10 Mbits/segundo, podendo-se obter taxas superiores para distâncias mais curtas. Os cabos coaxiais são altamente utilizados como suporte de transmissão nas Redes Locais Industriais.

A informação transmitida pelos cabos coaxiais é geralmente codificada sob a forma de um sinal binário, onde os dígitos 0 e 1 são representados por dois diferentes níveis. (por exemplo, 1 volt para o bit 1 e 0 volt para o bit 0). Esta forma de codificação, embora seja uma convenção bastante adequada, não permite ao receptor do sinal detectar o início e o fim da transmissão de um dígito binário.

Existe uma grande variedade de cabos coaxiais, cada um com características específicas. Alguns são melhores para transmissão em alta freqüência, outros têm atenuação mais baixa, outros são mais imunes a ruídos e interferências, etc. Os cabos de mais alta qualidade não são maleáveis e são difíceis de instalar, mas cabos de baixa qualidade podem ser inadequados para altas velocidades e longas distâncias.

O cabo coaxial, ao contrário do par trançado, mantém uma capacitância constante e baixa independente (teoricamente) do comprimento do cabo, evitando assim vários problemas técnicos. Devido a isto oferecerá velocidades da ordem de megabits por segundo, sem ser necessário regeneração de sinal e sem distorções ou ecos, propriedade que revela a alta tecnologia já dominada.

Os cabos coaxiais podem ser usados em ligações ponto a ponto ou multiponto. Ligações no cabo coaxial causam reflexão devido à impedância não infinita do conector ("transceiver"). A colocação destes conectores em ligações multiponto deve ser controlada de forma a garantir que as reflexões não se somem em fase a um valor significativo. A figura 4.9 apresenta o cabo coaxial de 50 ohms, conector e terminador.

(a) Cabo Coaxial

(b) Conector com Terminador

(c) Terminador

Figura 4.9 – Detalhe de (a) Cabo Coaxial de 50 ohms, (b) Conector BNC para ligação com interfaces e (c) terminador de extremidades dos cabos

4.3.3 - FIBRA ÓTICA.

As **fibras óticas** são o meio de transmissão pelo qual os sinais binários são conduzidos sob a forma de impulsos luminosos. Um impulso luminoso representa um bit a 1, enquanto a ausência deste impulso representa um bit a 0. A luz visível é uma onda luminosa cuja freqüência está na ordem de 10 8 Hz, o que dá ao sistema uma banda passante potencial bastante grande. As taxas de transmissão num suporte a fibra ótica ficam na faixa dos Gbit/s (10 9bit/s).

Um sistema de transmissão a base de fibra ótica é composto de três principais elementos: o suporte de transmissão (a fibra ótica), o dispositivo de emissão e o dispositivo de recepção da onda luminosa.

A fibra ótica é constituída de um fio de vidro bastante fino, à base de silício e outros componentes. A figura 4.10 apresenta cabos de fibra ótica. Ela consiste de um núcleo no qual se propaga a luz e uma capa externa de proteção que mantém a luz no interior do núcleo. O dispositivo de emissão consiste, ou de um diodo emissor de luz (LED) ou de um diodo laser. O dispositivo de recepção é constituído geralmente de um fotodiodo ou de um fototransistor.

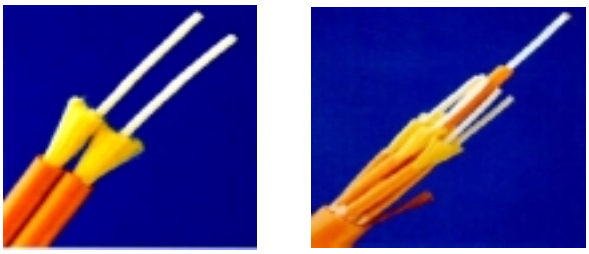


Figura 4.10 – Detalhes de Cabos de Fibra Ótica.

O princípio da transmissão das fibras óticas é o da reflexão da luz na interface entre dois meios. Quando um raio luminoso deixa um meio homogêneo para se propagar num outro meio, o seu percurso sofre um desvio na interface entre os dois meios. Entretanto, existe um ângulo de incidência limite, a partir do qual o raio luminoso, ao invés de ser refratado ele será refletido na interface, sendo mantido no meio no qual ele havia sido introduzido. Desta forma, a luz poderá ser propagada ao longo do meio, em distâncias de alguns quilômetros.

Atualmente, os suportes de comunicação à base de fibra ótica são utilizados em redes de comunicação em longa distância, substituindo sistemas mais antigos à base de cabos coaxiais. Isto deverá continuar a ocorrer nos próximos anos, contribuindo para que se tenha, num futuro próximo, em distâncias relativamente grandes, sistemas de comunicação oferecendo altas taxas de transmissão garantindo assim o salvamento de grandes volumes de informação.

4.3.4 - REDES SEM FIO (RADIODIFUSÃO).

Nas redes sem fio (**wireless networks**) as informações são transmitidas através do ar, em canais de freqüência de rádio (na faixa de KHz até GHz) ou infravermelho (freqüências da ordem de THz).

Por sua natureza, a radiodifusão é adequada tanto para ligações ponto-a-ponto quanto para ligações multiponto. As redes sem fio são uma alternativa viável onde é difícil, ou mesmo impossível instalar cabos metálicos ou de fibra ótica.

As bandas de freqüência ISM (Industrial, Scientific and Medical), que podem ser utilizadas sem que seja necessária uma licença, são alocadas para as aplicações de radiodifusão dentro de edifícios. Os valores destas bandas variam de acordo com o país.

Como várias estações compartilham o mesmo meio de transmissão, é necessário utilizar um método para disciplinar este compartilhamento. Alguns métodos usados são: multiplexação por divisão de freqüência (FDM), multiplexação por divisão de tempo (TDM) e multiplexação por divisão de espaço (SDM).

O método SDM pode ser realizado de duas formas. A primeira delas baseia-se na utilização de antenas direcionais que emitem sinais de rádio de alta freqüência concentrados em feixes. Esse método é usualmente empregado em enlaces de microondas e permite que uma mesma freqüência possa ser reutilizada desde que os feixes de ondas sejam transmitidos em regiões distintas do espaço. A outra forma de realização do SDM é estruturar a rede em células, isto é, dividir a área total da rede em várias áreas menores (células), que normalmente possuem a forma de hexágonos.

O funcionamento dos sistemas celulares baseia-se na rápida diminuição da potência do sinal de rádio à medida que se propaga. No espaço livre, a potência do sinal decai aproximadamente com o quadrado da distância do transmissor, e quando as antenas estão próximas ao solo, a potência diminui com aproximadamente a quarta potência da distância. Essa característica torna possível a reutilização da mesma freqüência, quando os transmissores estão suficientemente distantes uns dos outros.

As redes sem fio normalmente utilizam freqüências altas em suas transmissões: 915 MHz, 2.4 GHz, 5.8 GHz, etc. Parte das ondas de rádio, nessas freqüências , são refletidas quando entram em contato com objetos sólidos, o que implica na formação de diferentes caminhos entre transmissor e receptor, principalmente em um ambiente fechado. Como conseqüência acontece um espalhamento de no tempo do sinal que chega ao receptor, isto é, várias cópias do sinal chegam ao receptor deslocadas no tempo, pois elas percorrem distâncias diferentes. O resultado disso é que, no mesmo ambiente, em alguns locais o sinal pode ser muito fraco e em outros, a poucos metros de distância, pode ser perfeitamente nítido.

Outras considerações importantes dizem respeito à segurança quando este sistema é utilizado. Teoricamente não existem fronteiras para um sinal de rádio, logo, é possível que ele seja captado por receptores não autorizados.

Outro cuidado que deve ser tomado ao se utilizar radiodifusão como meio de transmissão é a possível interferência provocada por fontes que geram sinais na mesma banda de freqüência da rede. Alguns outros problemas estão relacionados a interferências por razões meteorológicas, por exemplo, quando da utilização de infravermelho.

4.3.5 - QUADRO COMPARATIVO DOS MEIOS DE TRANSMISSÃO.

CARACTERÍSTICAS / MEIO	PAR TRANÇADO	CABO COAXIAL "BASE BAND"	CABO COAXIAL "BROADBAND"	FIBRA ÓTICA
TIPO DE SINALIZAÇÃO	DIGITAL	DIGITAL	ANALÓGICA	TRANSMISSÃO DE LUZ
DISPONIBILIDADE DE COMPONENTES	ALTA DISPONIBILIDADE	LIMITADA	ALTA DISPONIBILIDADE	BASTANTE LIMITADA
CUSTO DE COMPONENTE	MAIS BAIXO DE TODOS	BAIXO	MÉDIO	ALTO
COMPLEXIDADE DE INTERCONEXÃO	MAIS BAIXO DE TODOS	BAIXA	MÉDIA	ALTA
FACILIDADES PARA LIGAÇÃO MULTIPONTO	BAIXA	MÉDIA (100 S NÓS)	ALTA (1000 S NÓS)	MUITO BAIXA
TOPOLOGIAS ADEQUADAS	TODAS	TODAS	BARRA	ESTRELA E ANEL
NÚMEROS DE NÓS (TÍPICO EM LIGAÇÃO MULTIPONTO)	10 S	10 S A 100 S	100 S / CANAL	2 (PONTO A PONTO)
RELAÇÃO SINAL/RUÍDO	BAIXA	MÉDIA	MÉDIA	ALTA
DISTÂNCIA MÁXIMA DE TRANSMISSÃO/VELOCIDADE TÍPICA	POUCAS CENTENAS DE METROS 1MBPS	1,0 KM 10 MBPS	10 S DE KM 20 MBPS	10 S DE KM 10 MBPS

4.3.6 – QUADRO COMPARATIVO ENTRE OS PADRÕES ETHERNET / FAST ETHERNET / GIGABIT ETHERNET

	Ethernet 10 BaseT	Fast Ethernet 100 BaseT	Gigabit Ethernet* 1000 Base x
Data Rate	10 Mbps	100 Mbps	1000 Base Mbps (gigabit por seg.)
Cat 5 UTP	100 m (min)	100 m	100 m
STP/Coax	500 m	100 m	25 m
Multimode Fiber	2 km	412 m (hd)** 2 km (fd)*	550 m
Single-mode Fiber	25 km	20 km	5 km

* IEEE espec. full duplex - ** IEEE espec. half duplex

4.4 – COMPONENTES DE CONEXÃO.

No suporte de transmissão, os sinais são transportados por distâncias limitadas antes de perderem energia. De um mode geral, em uma rede Ethernet, um sinal pode ser transportado em uma distância de até 300 metros; em um sistema Token Ring, em até 180 metros. As redes utilizam **repetidores, pontes roteadores e gateways** para gerar e retransmitir sinais transportados em longas distâncias e para estabelecer comunicações com outras redes locais e remotas.

Apesar de alguns conceitos citados estarem relacionados ao software de redes e às arquiteturas de redes que serão estudados posteriormente, veremos agora as características dos principais componentes de conexão.

4.4.1 – REPETIDORES.

Os **repetidores** fazem o que o próprio nome sugere: repetem sinais elétricos entre seções de cabos da rede. Os repetidores retransmitem sinais em ambas as direções indiscriminadamente. Dispositivos mais modernos, como pontes e roteadores, analisam as mensagens transportadas pelos sinais para determinar se é realmente necessário transmitir cada mensagem para o próximo segmento. O repetidor apenas regenera os níveis do sinal elétrico que transporta os bits no suporte de transmissão. A figura 4.11 apresenta a atuação dos repetidores nas camadas OSI.

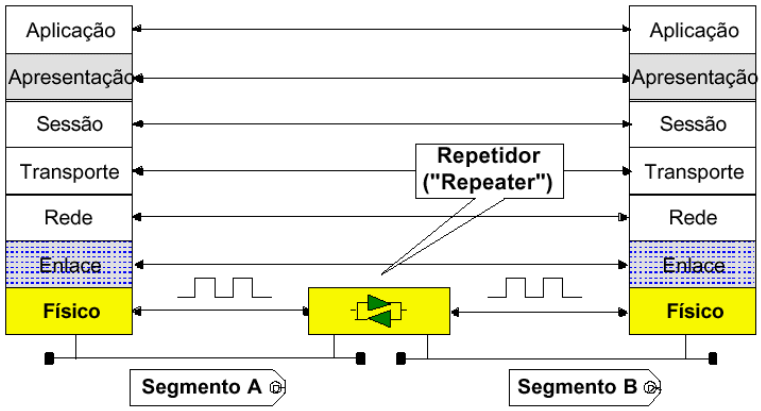


Figura 4.11 - Atuação dos repetidores na arquitetura OSI

O **HUB Ethernet** pode ser considerado um conjunto de repetidores em paralelo. Ele implementa um "curto-circuito" lógico, difundindo os sinais provenientes de uma estação para todas as outras estações na rede, regenerando o sinal elétrico.. No modelo ETHERNET 10BASET, a banda passante do barramento é de 10 Megabits/s.

O **HUB não gerenciável** é um equipamento com portas (normalmente 8 ou mais) com conectores RJ-45 (para cabo par trançado) e porta(s) com conector BNC (para cabo coaxial) ou AUI.

O **HUB gerenciável** é um equipamento com as mesmas características do primeiro, mas dotado de um hardware adicional, que permite a sua gerência à partir de softwares de gerenciamento de redes, instalados em estações de rede que se comunicam com os HUBs através do protocolo TCP/IP. Este HUB, normalmente, possui uma porta serial RS-232C, permitindo a sua configuração, principalmente, o endereço IP, as variáveis a serem monitoradas e as mensagens de alerta.

O **HUB empilhável** é aquele que possui a capacidade de ser colocado junto com outras unidades, ligadas através de um cabo especial, formando assim uma pilha, que introduz na rede apenas um nível de repetição. Uma pilha de HUBs é recomendada quando se têm uma grande concentração de estações dispostas num raio de 100 metros (limite de alcance do cabo de par trançado).

O **HUB Cascateável** é aquele que possui a capacidade de ser interligado a outros HUBs em links de até 100 metros de cabo, devendo portanto incluir as portas que permitem tal cascateamento, seja por par trançado, seja por cabo coaxial. O cascateamento de HUBs é recomendado quando se deve atender estações que estão além de 100 metros de distância. Cada HUB cascateado através de par trançado é considerado um repetidor na rede e, portanto, só podem existir no máximo 4 níveis de cascatemento. HUBs cascateados através de cabo coaxial possuem no máximo 2 níveis de cascateamento e portanto oferecem uma solução com atraso menor, mas estão restritos ao alcance da versão 10 Base 2,

qual seja, de 185 metros para o comprimento máximo do cabo coaxial.

4.4.2 – PONTES.

As **pontes** permitem combinar duas redes locais, além de admitir que estações de uma rede local acessem recursos de outra rede local. As pontes utilizam protocolos de controle de acesso ao meio físico (MAC) na física da rede. Através desse recurso, é possível ligar meios físicos diferentes entre si, como os cabos de fibra ótica e os cabos coaxiais 802.3, desde que as duas partes utilizem o mesmo protocolo de camada MAC (como Ethernet). A figura 4,12 apresenta a atuação da ponte nas camadas OSI.

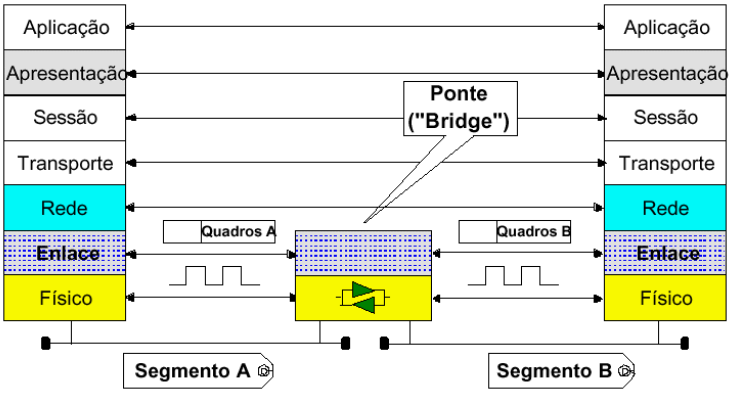


Figura 4.12 - Atuação das pontes na arquitetura OSI

4.4.3 – ROTEADORES.

Os **roteadores** operam na camada de rede do modelo OSI. Sua função é examinar o endereço de cada mensagem e decidir de que lado da ponte está o destinatário. Se a mensagem não precisar ser transportada pela ponte e, por algum motivo, venha a criar tráfego na rede estendida, o roteador não irá enviá-la. Os roteadores podem traduzir sinais enviados por vários cabos e esquemas de sinalização. Por exemplo, um roteador pode receber suas mensagens através da Ethernet e colocá-las em uma rede com comutação de pacotes operando através de modems conectados a linhas telefônicas privativas de alta velocidade. A figura 4.13 apresenta a atuação do roteador nas camadas OSI.

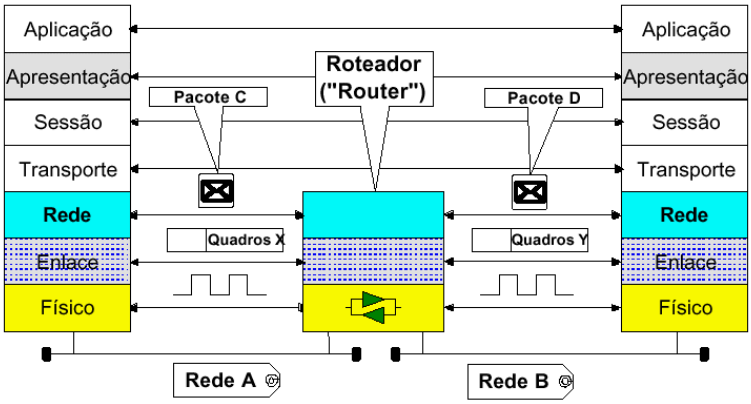


Figura 4.13 - Atuação dos roteadores na arquitetura OSI

O **Switch Ethernet**, a grosso modo, pode ser considerado um misto de ponte e roteador, dependendo da camada OSI em que atua. Os Switches Ethernet usualmente suportam as implementações Ethernet (IEEE 802.3) de 10 Mbps, sem alterar a subcamada MAC. È comum encontrar switches operando com portas em velocidades diferentes, com especificação do meio físico 100BaseT (cabo par trançado em 100 Mbps) ou 100BaseFX (fibra ótica em 100 Mbps). A figura 4.14 ilustra a utilização do switch com portas de velocidades diferentes.

Os Switches são mais rápidos que roteadores (examinam apenas o endereço fonte e o destino e não o pacote

inteiro, com manutenção de tabelas e execução de algoritmos de roteamento), são mais fáceis de gerenciar, pois são do tipo "plug-and-play" e são mais baratos que roteadores.

São características dos Switches Ethernet:

1. Suportam protocolos existentes e garantem migração, sem impactos, para os emergentes (Fast Ethernet e ATM);
2. Realizam uma comutação dinâmica (não estática, como nos HUBs comuns)
3. Implementam canais virtuais dedicados (acesso não compartilhado, como nas Ethernet comuns).
4. Ocorrem transmissões paralelas ponto-a-ponto com canais criados entre uma estação fonte e uma estação destino.
5. Quadros não são transmitidos para todas as estações da rede (“broadcast”);
6. Domínios de Colisão separados. Há pouca ou nenhuma colisão entre quadros;

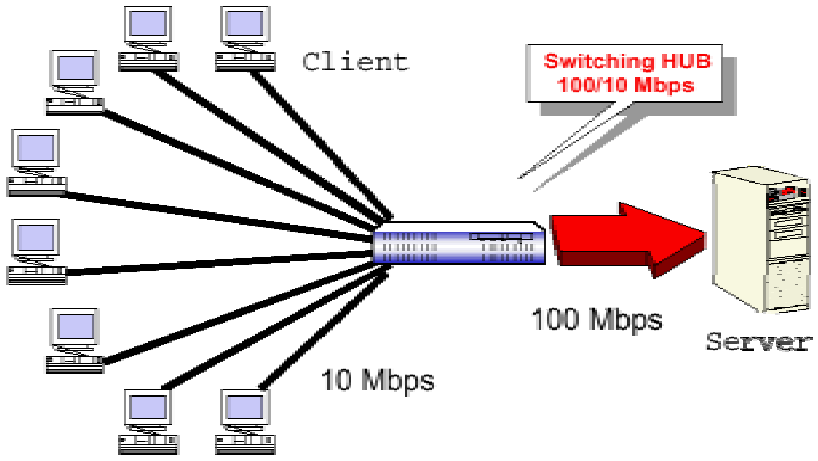


Figura 4.14 - utilização de switch com portas de velocidades diferentes.

4.4.4 – GATEWAYS.

Os **gateways**, que são executados na camada de sessão do modelo OSI, permitem a comunicação entre redes que executam protocolos completamente incompatíveis entre si. A figura 4.15 apresenta a atuação do gateway nas camadas OSI.

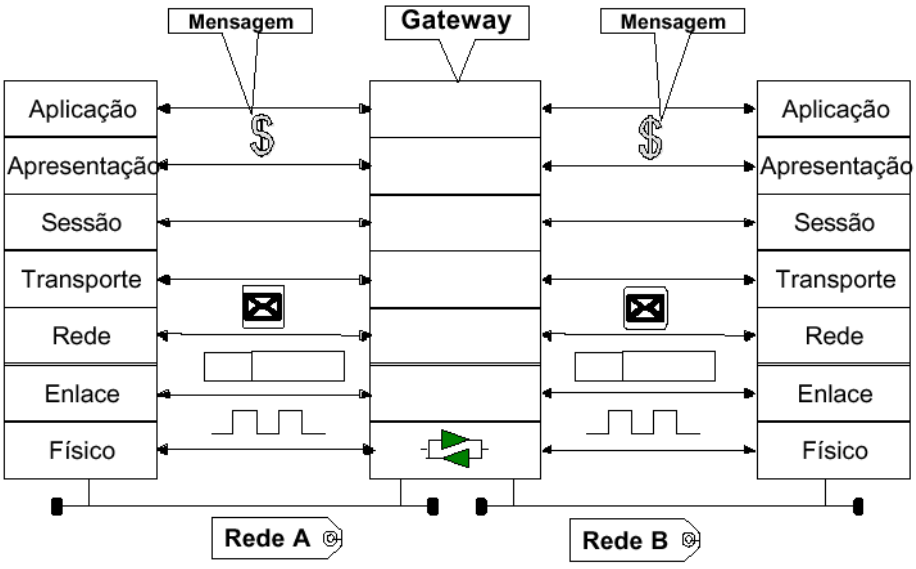


Figura 4.13 - Atuação dos gateways na arquitetura OSI

Nas primeiras redes de computadores os aspectos relacionados ao hardware foram colocados como prioridade e os aspectos de software em segundo plano. No entanto logo foi percebida a fundamental importância dos mecanismos de software de uma rede, e, em função disto, os softwares de rede são altamente estruturados. Os conceitos relacionados a esta estruturação são de vital importância para a compreensão de todos os aspectos relacionados à arquitetura de redes como um todo.

No projeto de uma rede muitos problemas precisam ser resolvidos e podem existir várias soluções para o mesmo problema. Como já vimos, as redes de computadores podem se caracterizar por diferentes configurações e topologias. Apesar da diversidade no que diz respeito a este aspecto, todas as possíveis configurações têm um objetivo comum — a transferência de dados. O maior problema, então, está relacionado com a especificação dos procedimentos e mecanismos a serem implementados para viabilizar o funcionamento da rede. A resolução deste problema é baseada principalmente no conhecimento prévio das funções que devem ser suportadas pela rede, assim como do ambiente no qual ela vai ser inserida.

Uma vez listadas as diferentes necessidades relacionadas a uma rede de comunicação, a questão que se coloca é a da viabilidade de um projeto de rede, dada a quantidade de funções a implementar e o ordenamento destas funções. O controle de fluxo deve ser realizado antes ou depois da correção de erros? Uma vez resolvida esta questão, que elementos da rede serão responsáveis da implementação destas funções? As soluções adotadas são dependentes do suporte de transmissão utilizado? Elas continuam válidas no caso de expansão da rede? Estas questões representam, de certo modo, a necessidade de levar em conta um certo ordenamento no que diz respeito à adoção das soluções para cada problema.

Um exemplo típico do problema é a comunicação entre duas empresas. Vamos supor que o Diretor de uma Empresa A quer comunicar-se com o Diretor de uma Empresa B. Ele convoca a sua Secretária Administrativa e solicita, informalmente, que esta construa um texto relativo ao assunto a ser tratado. A Secretária Administrativa elabora o documento e o entrega ao Office Boy que vai envelopá-lo e encaminhá-lo ao Chefe do Setor de Malote. Este último encaminha o documento ao Serviço Postal para condução à Empresa B.

Considerando que a Empresa B apresenta uma estrutura similar à Empresa A, como é ilustrado na figura 5.1, os mesmos elementos atuam, cada um em suas funções, para fazer com que a correspondência chegue às mãos do Diretor da Empresa.

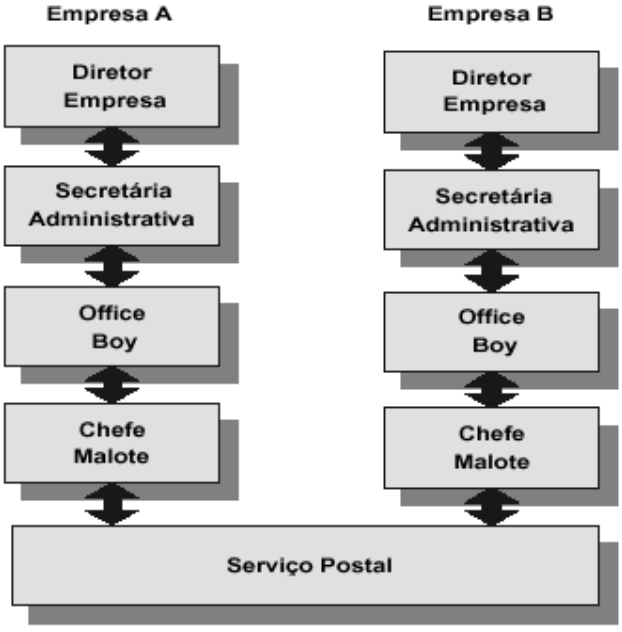


Figura 5.1 - Filosofia das redes, ilustrada por um processo de relações entre empresas.

Este processo caracteriza, na verdade, a filosofia de concepção das redes de comunicação, que é baseada em dois conceitos fundamentais: o da **hierarquia** e o da **descentralização**, cuja conjunção vai permitir responder à questão de ordenação na adoção das soluções. Segundo esta filosofia, uma tarefa global é vista como sendo decomposta à

medida que se vai descendo na hierarquia e que a única interação física se faz no seu nível mais baixo.

Podemos considerar que a comunicação entre dois nós de uma rede é uma tarefa global que afeta um sistema complexo e, consequentemente, sujeita à aplicação dos princípios de hierarquização e de descentralização.

As vantagens da adoção destes princípios são, fundamentalmente:

1. facilidade de estudo e de implementação da rede a partir de elementos de base existentes, o que permite a redução dos custos de instalação;
2. simplificação de sua operação em função da definição de regras formais;
3. garantia de confiabilidade de um sistema que seja aceitável, particularmente graças ao encapsulamento das funções o que permite limitar a propagação de erros e facilitar a manutenção;
4. garantia, pela modularidade, de um grau satisfatório de evolutividade e de extensibilidade da rede;
5. otimização de desempenho.

Todos estes aspectos nos conduzem a conceber uma **arquitetura de comunicação** como sendo uma organização de software e hardware estruturada em níveis ou camadas.

Os conceitos de hierarquia e descentralização podem ser empregados de diferentes formas, cada um podendo implicar num tipo de rede particular. Em função desta provável multiplicidade, surgiu então a necessidade de uma normalização permitindo a conexão de diferentes classes de hardware.

Para possibilitar a normalização, foi necessário estabelecer um modelo teórico capaz de representar as relações entre as diferentes tarefas implementadas nos diferentes níveis hierárquicos. A possibilidade de interconexão de um número qualquer de sistemas, ou seja, de conjuntos autônomos podendo efetuar tarefas de tratamento ou de transmissão de informação, era uma característica essencial para o modelo a ser estabelecido.

A figura 5.2 ilustra uma arquitetura hierarquizada em 4 camadas que permitirá introduzir o conjunto de conceitos relacionados ao modelo estabelecido. O objetivo de cada camada é o oferecimento de um tipo de serviço a sua camada superior de forma a evitar que esta necessite conhecer certos aspectos de como este serviço é realizado. A camada n assume que a comunicação com a camada n de uma outra máquina existe, embora não seja direta. Para que esta comunicação exista, ela se serve de um conjunto de convenções e regras que vão permitir gerenciar esta comunicação. A este conjunto de regras e convenções, dá-se o nome de protocolo. Como se pode ver na figura, não existe meio de comunicação direto entre as diferentes camadas (apenas o meio de transmissão na camada 1), o que significa que não existe transferência direta de dados entre a camada n de uma máquina à camada n de outra máquina.

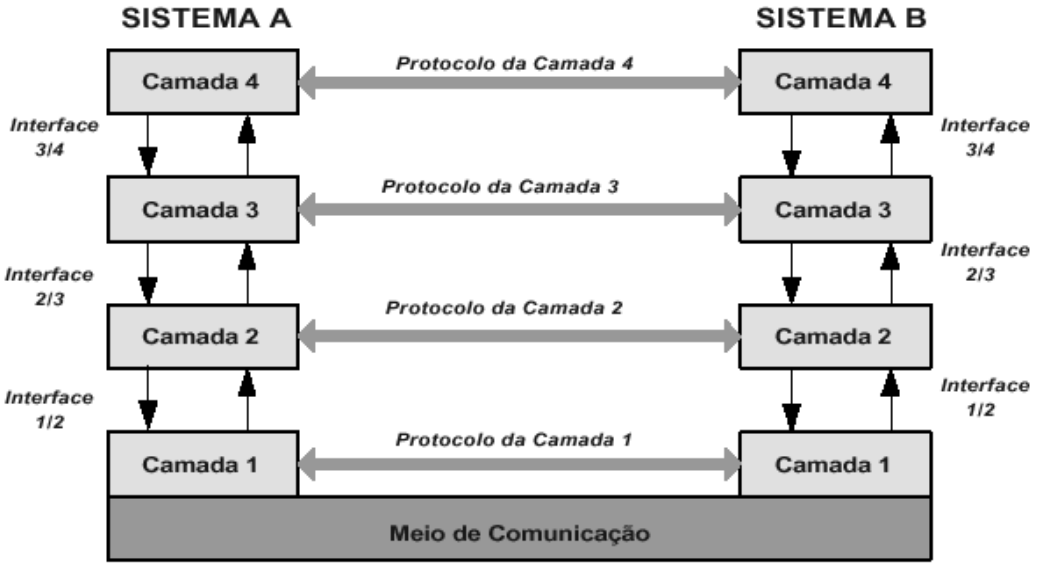


Figura 5.2 - Arquitetura hierarquizada em 4 camadas.

Na realidade, cada camada transfere os dados à camada imediatamente inferior até a camada mais baixa; o dado é então transmitido à outra máquina através do meio de transmissão. A comunicação entre as camadas é vista então como uma comunicação virtual e é representada, na figura 5.2, pelas linhas ligando cada par de camadas.

Cada camada comunica-se com as camadas adjacentes (acima ou abaixo) através de uma interface que define

as informações que podem ser trocadas e os serviços que a camada inferior oferece à camada superior.

Ao conjunto das camadas compondo uma rede dá-se o nome de **arquitetura da rede**, e as especificações da arquitetura devem conter informações suficientes para permitir o correto desenvolvimento da rede, tanto do ponto de vista do software quanto do hardware.

5.1 - HIERARQUIA DE PROTOCOLOS.

Para reduzir a complexidade do projeto, a maioria das redes foi organizada como uma série de níveis ou camadas, que são colocadas uma sobre a outra. O número, o nome, o conteúdo e a função de cada camada difere de uma rede para outra. Em todas as redes, no entanto, o objetivo de cada camada é oferecer determinados serviços para as camadas superiores, ocultando detalhes da implementação desses recursos.

Conforme já vimos, a figura 5.2 (acima) ilustra a arquitetura hierarquizada em 4 camadas que permitirá introduzir o conjunto de conceitos relacionados a uma arquitetura multicamadas. O objetivo de cada camada é o oferecimento de um determinado serviço às camadas superiores utilizando-se, também, dos serviços oferecidos pelas camadas inferiores, de forma a evitar que estas necessitem conhecer certos aspectos da implementação destes serviços.

A camada **n** assume a comunicação com a camada **n** de uma outra máquina. Para faze-lo, ela se serve de um conjunto de convenções e regras que permitem gerir esta comunicação. A este conjunto de regras e convenções, dá-se o nome de **protocolo da camada n**, ou, simplesmente, **protocolo n**. Basicamente, um protocolo é um conjunto de regras sobre o modo como se dará a comunicação entre as partes envolvidas. As entidades representando camadas correspondentes em diferentes sistemas são denominadas processos pares, ou entidades pares. Os processos pares comunicam-se através dos protocolos. Como se pode ver na figura 5.2 (acima), não existe meio de comunicação físico entre as diferentes camadas o que significa que não existe transferência direta de dados entre a camada n de uma máquina à camada n de outra máquina.

Cada camada transfere os dados à camada imediatamente inferior até a camada mais baixa; o dado é então transmitido à outra máquina através do meio de transmissão. A comunicação entre as camadas é vista como uma comunicação virtual e é representada, na figura 5.2, pelas linhas horizontais entre as camadas. Cada camada comunica-se com as camadas adjacentes (acima e abaixo) através de uma interface, que define as operações elementares e os serviços que a camada inferior oferece à camada considerada.

No momento da definição do número de camadas que vai compor uma rede e do papel que cada uma delas deve cumprir, uma tarefa importante será a definição completa das interfaces entre as camadas e isto vai implicar que na definição do serviço oferecido por cada camada. Uma vantagem da correta definição das interfaces é a facilidade da introdução de modificações nas implementações das diferentes camadas; os mecanismos podem ser implementados de forma diferente, desde que as interfaces anteriormente definidas sejam respeitadas.

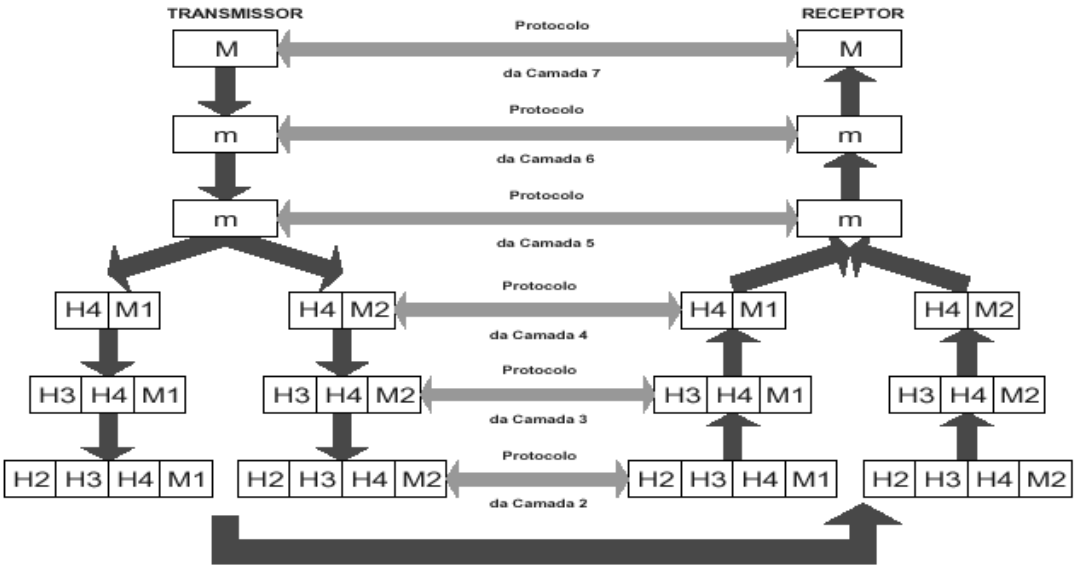


Figura 5.3 Comunicação virtual em uma arquitetura de rede.

Ao conjunto das camadas compondo uma rede dá-se o nome de **arquitetura da rede**, e as especificações da arquitetura devem conter informações suficientes para permitir o correto desenvolvimento da rede, tanto do ponto de vista do *software* quanto do *hardwar*e. Por outro lado, os detalhes de implementação dos mecanismos em cada camada, assim como as especificações detalhadas das interfaces não fazem parte da definição da arquitetura da rede.

A figura 5.3 permite ilustrar o processo da comunicação no contexto de uma arquitetura multicamadas. O processo da camada 7 gera uma mensagem **M**, que será transmitida desta à camada inferior segundo o que estiver definido pela **interface** das camadas 6/7.

Considera-se que esta transmissão introduz algumas modificações na mensagem (por exemplo, uma compressão de dados), o que justifica uma nova representação desta por **m**. Esta mensagem é, por sua vez, transmitida à camada 5, através da interface das camadas 5/6. No exemplo considerado na figura, a mensagem não sofre modificações, mas esta camada efetua o controle de fluxo. A camada 4 é responsável pela decomposição da mensagem a fim de respeitar as restrições de tamanho que podem ser impostas pelas camadas inferiores. Assim, **m** é decomposta em **M1** e **M2**.

Para isto, é inserido também na mensagem (ou nas partes da mensagem) um cabeçalho **H4** contendo uma informação de controle, como, por exemplo, um número de ordem que vai permitir, posteriormente na camada 4 do sistema destinatário, a reconstrução da mensagem a partir das partes recebidas. Outras informações podem ainda estar contidas neste cabeçalho, como, por exemplo, o tamanho da mensagem ou o instante de envio.

Na camada 3, é feita a escolha das linhas de saída e um novo cabeçalho, **H3**, é introduzido às mensagens. Na camada 2, além de um cabeçalho, **H2**, é introduzido também um sufixo, **T2**, contendo informações específicos a esta camada, por exemplo, controle de erro. A mensagem é finalmente entregue
à camada 1 para emissão via meio físico.

No sistema destinatário, o processo inverso acontece, sendo que as mensagens vão subindo, de camada em camada, e os cabeçalhos retirados nas camadas respectivas, de modo a evitar que estes sejam transferidos às camadas que não lhes dizem respeito.

Um aspecto importante mostrado na figura 2.2 é o da comunicação **virtual** ocorrendo entre as diferentes **camadas pares**. As camadas em cada nível possuem uma visão da comunicação **horizontal**, mesmo se as mensagens são na realidade transmitidas às camadas inferiores pertencentes ao mesmo sistema.

5.2 - DIFERENÇAS ENTRE SERVIÇO E PROTOCOLO.

Embora sejam freqüentemente confundidos, **serviço** e **protocolo** são dois conceitos distintos. O importante nesta distinção é de poder estabelecer a relação entre os dois conceitos.

O **SERVIÇO** corresponde a um conjunto de operações que uma camada é capaz de oferecer à camada imediatamente superior. Ele define **o que** uma camada é capaz de executar sem se preocupar com a maneira pela qual as operações serão executadas. O serviço está intimamente relacionado com as interfaces entre duas camadas, sendo a inferior a **fornecedora** do serviço e a superior a **usuária** deste.

O **PROTOCOLO** define um conjunto de regras que permitem especificar aspectos da realização do serviço, particularmente, o significado dos quadros, pacotes ou mensagens trocadas entre as entidades pares de uma dada camada. Em uma determinada camada, o protocolo pode ser mudado sem problema, desde que as interfaces com a camada superior e inferior não sejam alteradas, ou seja, que elas continuem a ter a mesma visibilidade no que diz respeito aos serviços realizados pela camada que foi alterada; isto corresponde, na verdade, a um certo desacoplamento entre os conceitos de serviço e protocolo.

5.3 QUESTÕES DE PROJETO RELACIONADAS ÀS CAMADAS.

Algumas questões de projeto fundamentais das redes de computadores estão presentes em diversas camadas. A seguir serão discutidas as mais importantes.

Todas as camadas precisam de um mecanismo para identificar os transmissores e receptores. Como em geral uma rede tem muitos computadores, e alguns deles têm vários processos, é necessário um meio para que um processo de uma máquina especifique com quem ele deseja se comunicar. Como pode haver vários destinos, há a necessidade de se criar uma forma de **endereçamento** para definir o destino específico.

Outra preocupação recai sobre as **direções do tráfego**. Em alguns sistemas, os dados são transferidos em apenas uma direção. Em outros, eles podem ser transferidos em ambas as direções, mas não simultaneamente. Também é possível transmitir em ambas as direções simultaneamente. O protocolo também deve determinar o número de canais lógicos correspondentes à conexão e quais são as suas prioridades. Muitas redes oferecem pelo menos dois canais lógicos por conexão, um para dados normais e outro para dados urgentes.

O **controle de erro** é uma questão importante, pois os circuitos de comunicação física podem não ser perfeitos. Muitos códigos de detecção e correção de erros são conhecidos e as partes envolvidas em uma conexão devem chegar a um consenso quanto ao que deve ser usado. Além disso, o receptor deve ter alguma forma de informar ao emissor as mensagens que foram recebidas corretamente e as que não foram.

Nem todos os canais de comunicação preservam a **ordem das mensagens** enviadas por eles. Para lidar com uma possível perda de seqüência, o protocolo deve fazer uma provisão explícita para que o receptor possa remontar adequadamente os fragmentos recebidos. Uma solução óbvia é numerar os fragmentos, mas isso ainda deixa aberta a questão do que deve ser feito com os fragmentos que chegam fora de ordem ou, pior ainda, o que fazer quando alguns se perdem.

Um problema que deve ser resolvido em diversas camadas é a falta de habilidade de todos os processos para aceitarem arbitrariamente mensagens longas. Esta propriedade nos leva ao uso de mecanismos para **desmontar, transmitir e remontar** mensagens. Uma questão é o que fazer quando estas unidades se tornam tão pequenas que o envio de cada uma em separado se torna ineficiente. Nesse caso a solução é reunir as pequenas mensagens com um destino comum em uma grande mensagem e desmembrá-la na outra extremidade.

Uma outra questão que afeta todas as camadas diz respeito à **velocidade dos dados**, particularmente quando o emissor é mais rápido que o receptor. Várias soluções foram adotadas e serão discutidas posteriormente. Algumas delas trabalham com a possibilidade do receptor determinar dinamicamente sua situação atual. Outras limitam o emissor a uma taxa de transmissão predeterminada.

Quando for inconveniente, ou algumas vezes caro, configurar uma conexão para cada par de processos de comunicação, a camada inferior pode usar a mesma conexão para diversas conversações não relacionadas. Desde que seja feita de modo transparente, a **multiplexação** e a **demultiplexação de conexões** podem ser executadas por qualquer camada.

Quando houver vários **caminhos** entre a origem e o destino, um deles deve ser escolhido. Algumas vezes essa decisão deve ser dividida em duas ou mais camadas. Para enviar dados de Londres para Roma, por exemplo, devem ser tomadas duas decisões: uma de alto nível, decidindo sobre o trajeto a ser escolhido (via França ou Alemanha, com base nas respectivas leis de privacidade) e uma de baixo nível, escolhendo sobre quais dos circuitos físicos disponíveis os dados serão transmitidos (com base na carga de tráfego atual).

5.4 - INTERFACES E SERVIÇOS.

A função de cada camada é oferecer serviços para a camada acima dela. Os elementos ativos de uma camada, ou seja, os processos que a implementam são chamados **entidades**. Estas podem ser entidades de *software* ou de *hardwar*e. Às entidades localizadas em diferentes sistemas, mas associadas a um mesmo nível (ou camada), dá-se o nome de **entidades pares**. As entidades recebem também uma denominação complementar em função da camada à qual elas estão relacionadas — por exemplo, entidade de aplicação, entidade de transporte, entidade de enlace, entre outras.

As entidades de uma camada **N** (ou entidades N) implementam um serviço que é utilizado pela camada **N+**1. Assim, a camada **N** é um **fornecedor de serviço** e a camada **N+1** é **usuária de serviço**. Por outro lado, a camada **N** poderá utilizar os serviços da camada imediatamente inferior, a camada **N-**1, para oferecer os serviços à camada superior. Ela pode ainda oferecer diferentes categorias (ou classes) de serviços: serviços mais eficientes e mais "caros" ou serviços lentos e "econômicos".

Os serviços oferecidos por uma camada são acessíveis em **pontos de acesso aos serviços**, ou **SAP** (*Service Access Point*). Os SAPs da camada **N** são os lugares onde a camada **N+1** poderá ter acesso aos serviços oferecidos, cada SAP sendo identificado por um endereço único. Por exemplo, os SAP de uma rede telefônica são as tomadas às quais podem ser conectados os aparelhos telefônicos e seus endereços são os números de telefone associados às tomadas.

Para que duas camadas possam trocar informações, existe uma série de regras a serem respeitadas, definidas pela **interface**. Através de uma interface, a camada **N+1** envia uma **unidade de dados de interface**, ou **IDU** *(Interface Data Unit*) à entidade da camada **N** pelo **SA**P. A IDU é composta de uma parte denominada **unidade de dados de**

serviço, ou **SDU** *(Service Data Unit*) e de outras informações de controle. A SDU é a informação transmitida via rede à entidade par e, em seguida, à camada **N**+1. A informação de controle é utilizada para auxiliar a gestão da camada inferior em seu trabalho (por exemplo, o número de *bytes* compondo a SDU correspondente).

Para transmitir uma SDU, a entidade da camada **N** pode fragmentá-la em diversas partes, e cada parte vai receber um cabeçalho, sendo enviada como uma **unidade de dados de protocolo**, ou **PDU** *(Protocol Data Unit*). Os cabeçalhos de PDU são utilizados pelas entidades pares para o transporte do protocolo. Elas identificam a PDU contendo os dados e aquelas contendo informações de controle (números de seqüência, contagens, etc). A figura 5.4 ilustra o processo descrito. As PDUs recebem normalmente uma denominação segundo a camada à qual estão associadas. Por exemplo, as PDUs de aplicação são ditas APDU, assim como as de apresentação são as PPDU, as de sessão SPDU, e assim por diante.

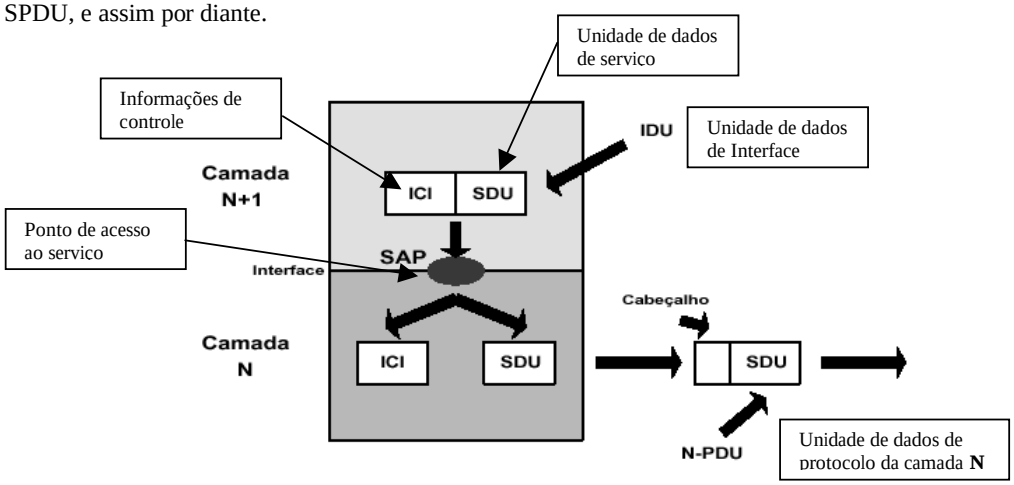


Figura 5.4 - Diferentes conceitos associados à interface entre camadas.

5.5 - SERVIÇOS ORIENTADOS À CONEXÃO E SEM CONEXÃO.

As camadas de uma arquitetura de rede podem oferecer diferentes classes de serviços às camadas superiores. Estes serviços podem ser **orientados a conexão** ou **não orientados a conexão** (também chamada **sem conexã**o).

Quanto aos **serviços orientados à conexão**, podemos citar como exemplo típico o sistema telefônico. Para que seja possível falar com alguém no telefone é necessário, inicialmente, tirar o fone do gancho, digitar (ou discar) um número, esperar que o interlocutor atenda, falar com a pessoa que precisamos e, finalmente, desligar. Este é o princípio básico de um serviço orientado à conexão:

1. estabelecimento da conexão,
2. utilização do serviço (ou enviar mensagem) e
3. término da conexão.

O aspecto principal da conexão é o fato de que ela funciona como uma espécie de canal virtual através do qual irão transitar as mensagens envolvidas na realização do serviço.

Já os **serviços sem conexão** são estruturados como o sistema postal, onde cada mensagem (ou carta, se consideramos o exemplo citado) contém o endereço do destinatário e é encaminhada no sistema, independente de outras. O princípio básico é então apenas: enviar mensagem.

Normalmente, se duas mensagens são enviadas a um mesmo destinatário, a primeira a ser enviada deve ser a primeira a ser recebida. Por outro lado, neste modo de serviço pode ocorrer que uma mensagem seja atrasada fazendo com que a segunda mensagem seja recebida primeiro. Já nos serviços orientados à conexão, isto jamais poderá acontecer.

Cada serviço é caracterizado por uma **qualidade de serviço**. Tendo em vista o parâmetro qualidade, os serviços podem ser divididos em confiável e não-confiável. Um serviço **confiável** é aquele em que os dados não podem ser jamais perdidos, ou melhor, jamais podem deixar de realizar o serviço adequadamente e, por vezes, algum mecanismo de recuperação em caso de falha deve ser utilizado. Serviços **não confiáveis** são aqueles onde, eventualmente, dados podem ser perdidos e não recuperados pela camada em questão.

Normalmente, a implementação de serviços confiáveis é feita através da definição de mensagens de reconhecimento enviadas pelo receptor, para cada mensagem recebida do emissor. Este processo, embora extremamente benéfico, introduz uma lentidão na transferência de dados, o que significa que nem sempre ele é desejável num sistema.

Os serviços confiáveis orientados conexão apresentam duas variantes. No primeiro caso, as fronteiras das mensagens são sempre preservadas. Se duas mensagens de 1 *Kbytes* são enviadas, elas chegarão sob a forma de duas mensagens de 1 *Kbytes* e nunca como uma única mensagem de 2 *Kbyte*s. Já na segunda variante, se uma mensagem de 2 *Kbytes* é recebida, não há como identificar se ela foi enviada realmente como uma única mensagem de 2 *Kbyte*s, como duas mensagens de 1 *Kbyte*s, ou ainda como 2048 mensagens de 1 *byte*. Porém em algumas aplicações, é necessário resguardar as fronteiras entre as mensagens enviadas; por exemplo, no caso do envio de um documento a uma impressora é interessante poder preservar as fronteiras entre as páginas.

No que diz respeito aos dois tipos de serviços (orientados à conexão e sem conexão), nem todas as aplicações requerem a utilização de conexão. Um exemplo disto pode ser o de uma aplicação de correio eletrônico. Pode-se imaginar uma aplicação de correio em que o usuário não se interesse no estabelecimento de conexão e tampouco a uma confiabilidade de 100% no que diz respeito à chegada das mensagens. Os serviços sem conexão e não-confiáveis são denominados serviços de **datagrama**.

Existem casos, porém, em que, apesar de não necessitar o estabelecimento de conexão, a confiabilidade é essencial. O serviço utilizado neste caso é o **datagrama com reconhecimento**. O serviço de **pedido-resposta** é outro tipo de serviço no qual o emissor envia um datagrama contendo um serviço e o receptor envia um outro contendo a resposta a este pedido.

O quadro a seguir ilustra os diferentes serviços com e sem conexão, com exemplos de aplicação destes serviços.

SERVIÇO	MODALIDADE	EXEMPLO
Transferência confiável de mensagens	Com conexão	Seqüência de páginas
Transferência confiável de bytes	Com conexão	Login remoto
Transferência não confiável	Com conexão	Voz digitalizada
Datagrama não confiável	Sem conexão	Correio eletrônico
Datagrama confiável	Sem conexão	Correio eletrônico registrado
Pedido-Resposta	Sem conexão	Consulta a base de dados

5.6 - PRIMITIVAS DE SERVIÇO.

Um serviço é definido formalmente por um conjunto de **primitivas** (ou operações) disponíveis a um usuário ou a outras entidades para o acesso àquele serviço. Estas primitivas permitem indicar a ação a ser executada pelo serviço ou ainda um pedido de informação sobre uma ação executada previamente.

As primitivas de serviço são divididas em quatro classes: **pedido** *(reques*t), **indicação** *(indicatio*n), **resposta** *(respons*e) e **confirmação** *(confir*m).

O quadro a seguir mostra o significado de cada uma destas primitivas no que diz respeito à execução de um serviço.

PRIMITIVA	SIGNIFICADO
Request	Pedido enviado por uma entidade (um processo de uma camada) que solicita um serviço
Indication	A entidade par é informada de uma solicitação de serviço
Response	A entidade par responde ao pedido de serviço
Confirm	A entidade solicitante é informada do resultado do serviço

Uma analogia ao funcionamento das primitivas pode ser feita através do sistema telefônico. O quadro a seguir apresenta um telefonema como uma seqüência de primitivas.

	AÇÃO	PRIMITIVA
1	Você disca o número do telefone de outra pessoa	CONNECT.request
2	O telefone da outra pessoa toca	CONNECT.indication
3	Ela atende dizendo “alô”	CONNECT.response

4	Você ouve o “alô” da outra pessoa	CONNECT.confirm
5	Você solicita uma informação	DATA.request
6	A pessoa ouve a solicitação	DATA.indication
7	Ela informa o que você solicitou	DATA.request
8	Você ouve a informação	DATA.indication
9	Você desliga seu telefone	DISCONNECT.request
10	A pessoa ouve o sinal desconexão e faz o mesmo	DISCONNECT.indication

A figura 5.5 mostra essa mesma seqüência de procedimentos como uma série de primitivas de serviço, inclusive a confirmação final de encerramento de conexão. Cada procedimento envolve a interação entre duas camadas de um dos computadores. Cada request ou response provoca logo em seguida um indication ou confirm do outro lado.

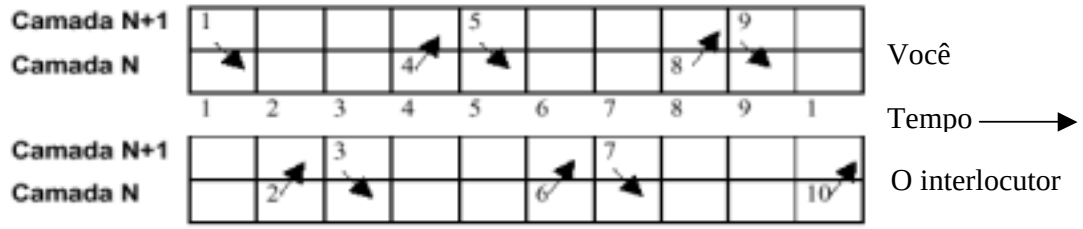


Figura 5.5 – Mapeamento das primitivas da uma conversação através do sistema telefônico. Os números próximos à extremidade das setas fazem referência às primitivas de serviço utilizadas no exemplo anterior.

Consideremos o exemplo de utilização das primitivas de serviço para o seguinte serviço orientado à conexão com oito primitivas de serviço:

CONNECT.*request* – Solicita o estabelecimento de conexão.
CONNECT.*indication* – Sinalização da parte para a qual foi feita a chamada.
CONNECT.*response* – Usada pelo receptor da chamada para aceitá-la (ou rejeitá-la).
CONNECT.*confirm* – Permite que a origem da chamada saiba que ela foi aceita.
DATA.*request* – Solicita o envio de dados.
DATA.*indication* – Sinal de chegada de novos dados.
DISCONNECT.*request* – Solicita o encerramento de uma conexão.
DISCONNECT.*indication* – Sinal do par sobre a solicitação.

Para requisitar o estabelecimento de uma conexão, a entidade que quer iniciar o diálogo envia uma primitiva de serviço de pedido de abertura de conexão, CONNEC*T.request* que vai se refletir, na entidade destinatária, por uma primitiva de indicação, CONNEC*T.indicatio*n.

A entidade que recebeu a indicação vai enviar uma primitiva de resposta, CONNEC*T.response*, para informar se esta aceita ou não a conexão. Finalmente, a entidade emissora vai saber do resultado do seu pedido pela recepção de uma primitiva de serviço de confirmação, CONNEC*T.confir*m.

Parâmetros podem ser associados às primitivas; no caso do serviço de conexão, por exemplo, os parâmetros podem especificar os seguintes aspectos relacionados à conexão desejada: a máquina com a qual se deseja dialogar, o tipo de serviço desejado, o tamanho máximo das mensagens, entre outras. Se a entidade invocada não está de acordo com os parâmetros contidos na primitiva de indicação recebida, esta pode fazer uma contra-proposta, através dos parâmetros da primitiva de resposta, que será transmitida à entidade emissora através dos parâmetros da primitiva de confirmação.

Os serviços podem ser de dois tipos: confirmados ou não-confirmados. No caso dos serviços confirmados, as quatro classes de primitivas são definidas, ou seja, pedido (request), indicação (indication), resposta (response) e confirmação (confirm). Isto significa que a entidade que requisitou o serviço terá sempre uma informação sobre as condições de realização deste e até se este foi realizado com sucesso ou não.

Nos serviços não-confirmados, apenas as duas primeiras classes de primitivas são utilizadas, ou seja, pedido (request) e indicação (indication). Neste tipo de serviços, a entidade emissora do pedido não receberá nenhuma informação sobre as condições de realização do serviço requisitado, nem mesmo se este foi realizado.

As redes de computadores propõem o compartilhamento de recursos físicos e lógicos, com a vantagem de se ter um sistema descentralizado. De maneira geral, o objetivo de uma rede é tornar disponível a qualquer usuário todos os programas, dados e outros recursos, independente de sua localização física. Além disso, a rede deve proporcionar maior disponibilidade e confiabilidade, dada a possibilidade de migração para outro equipamento quando a máquina sofre alguma falha. O uso de uma rede de computadores proporciona um meio de comunicação poderoso por sua velocidade e confiabilidade.

A arquitetura de uma rede é o conjunto das camadas que compõem esta rede e as especificações da arquitetura devem conter informações suficientes para permitir o correto desenvolvimento da rede, tanto do ponto de vista do software quanto do hardware.

Para compreender as diversas posturas, abordagens e atitudes políticas relacionadas com a área de comunicação de dados, como também para acompanhar o se desenvolvimento tecnológico, é necessário conhecer suas origens e sua história.

Em meados da década de 60, o governo dos EUA, por intermédio do Departamento de Defesa, iniciou estudos relacionados à viabilidade do desenvolvimento de redes de computadores. Em 1968 tiveram início as atividades do Projeto ARPA (Advanced Research Project Agency), tendo por base o conhecimento e o potencial de pesquisa das universidades e dos centros de pesquisa norte-americanos. A figura 6.1 apresenta um esboço original do Projeto ARPA.

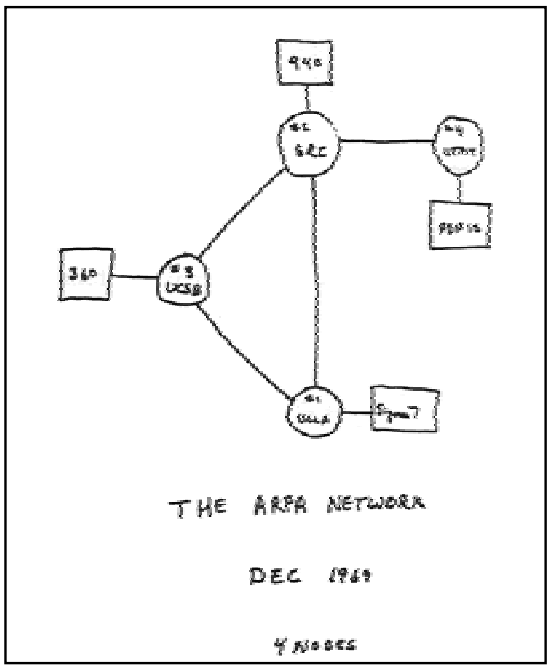


Figura 6.1 Cópia um esboço original do Projeto ARPA

Em 1972 entrou em funcionamento o projeto piloto da rede ARPA. Começava ai a era da tecnologia de redes de computadores, caracterizada pela distribuição das aplicações entre vários comutadores interligados de acordo com uma topologia determinada. Na rede ARPA foi, pela primeira vez, implementada a tecnologia de comutação de pacotes, assim como o método de divisão em várias camadas funcionais das tarefas de comunicação entre aplicações residentes em computadores distintos, conectados por meio da rede, criando-se o conceito de Arquitetura de Rede de Computadores. Também na década de 70, o crescimento da ARPA permitiu a interligação de computadores de universidades americanas e de alguns computadores situados em outros países. A figura 6.2 apresenta um mapa do Projeto ARPA em setembro de 1971.

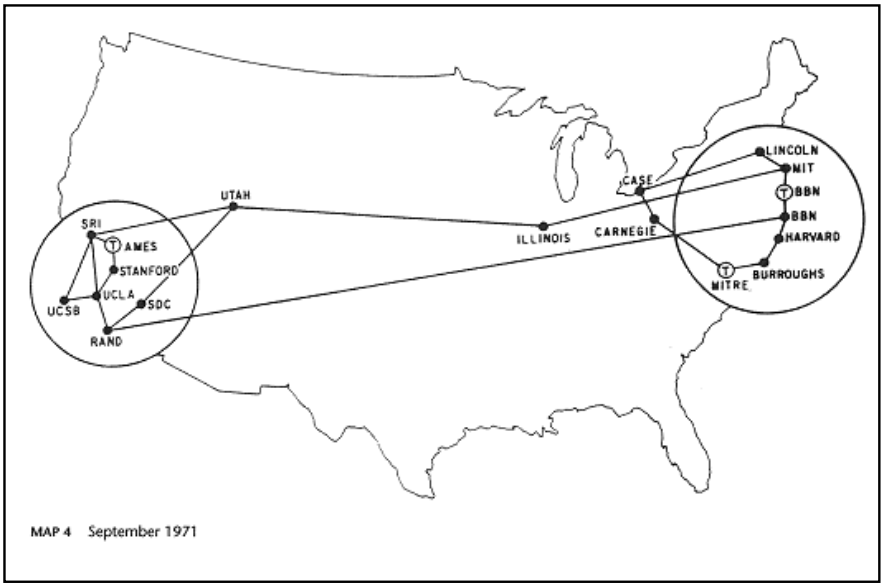


Figura 6.2 - Mapa do Projeto ARPA em setembro de 1971.

Na mesma época, os grandes fabricantes de equipamentos de processamento de dados criaram seus próprios métodos para interligar em rede seus respectivos produtos. Surgiram, assim, as Arquiteturas Proprietárias, primeiro com a IBM, que lanços a arquitetura SNA (Systems Network Architecture), depois com a Digital e a sua arquitetura Decnet, além de várias outras.

Também nos anos 70, a IBM e a Digital Equipment Corporation desenvolveram formas de grandes computadores interagirem sobre redes locais, mas o mais importante trabalho em redes locais para um grande número de computadores foi feito pelo Palo Alto Research Center (PARC), da Xerox Corporation, no final da década de 1970 e começo de 1980. No PARC, um importante conjunto de padrões e protocolos, chamado Ethernet, foi concebido e desenvolvido até o ponto de se tornar um produto comercial. Na mesma época, profissionais trabalhando na Datapoint Corporation, desenvolveram um padrão chamado ARCnet, mas a Datapoint manteve o ARCnet como um conjunto de especificações proprietário e, assim, não alcançou o sucesso comercial do Ethernet. Posteriormente, a IBM desenvolveu a tecnologia Token-Ring.

As primeiras arquiteturas de redes locais, como a Ethernet e ARCnet, combinavam especificações inflexíveis de hardware com estritas descrições de protocolos. Tipos específicos de fios de cobre, conectores especiais para cabos, uma única configuração física e algumas funções em software eram concentradas na definição de cada LAN. Entretanto, governos e indústrias forçaram a flexibilidade, aquele conjunto simples de especificações para cada tipo de rede expandiu-se de forma a incluir diferentes tipos de fios, configurações e protocolos. Hoje, pode-se misturar e combinar hardware e software para criar uma rede padronizada e continuar dentro das especificações de muitos sistemas de redes suportados por produtos de diversas empresas.

Durante a metade da década de 1980, um grupo de fabricantes deu início a um movimento em direção ao que veio a ser denominado protocolos abertos ou protocolos que não favorecem um único fabricante. Muitos fabricantes trabalharam no desenvolvimento de programas escritos para os padrões de protocolos abertos, mas, no início dos anos 90, o movimento perdeu o ímpeto. A ênfase passou do desenvolvimento de um único conjunto de novos protocolos abertos, para o uso prático dos protocolos já experimentados e em funcionamento, de fabricantes diferentes. À medida que os programadores e desenvolvedores aprendiam mais sobre protocolos e desenvolviam mais programas e ferramentas, eles encontraram formas de fazer com que computadores e redes diferentes interagissem sem o uso de um padrão único, porém aberto. Hoje, é fácil combinar computadores pessoais Macintosh e IBM na mesma rede e operar computadores conectados a diferentes tipos de redes.

Para as entidades especializadas em venda de serviços de telecomunicações abriu-se um novo mercado: a oferta de serviços de comunicação de dados por meio do fornecimento de uma estrutura de comunicação, a sub-rede, baseada funcionalmente no princípio de comutação de pacotes. O CCITT (atual ITU-T) elaborou documentos que permitiram que estes serviços fossem padronizados, a partir dos quais publicou, em 1976, a primeira versão da Recomendação X.25, propondo a padronização de redes públicas de comutação de pacotes.

Ao mesmo tempo, novas famílias de programas tornaram mais fácil compartilhar arquivos e recursos, como impressoras e modems. Nos anos 80, programadores criaram os processadores de textos, planilhas eletrônicas e bancos de dados que as pessoas usam para criar arquivos de dados. Nos anos 90, os desenvolvedores introduziram novas categorias de programas, conhecidos como programas para produtividade em grupos de trabalho e programas de controle de fluxo de trabalho, que tornam fácil pesquisar, organizar e ligar dados de documentos, planilhas e bancos de dados para que possam ser compartilhados. Compartilhar agora significava mais do que esperar em uma fila para utilizar um arquivo ou uma impressora, significa trabalhar em conjunto e de forma integrada.

6.1 - A ARQUITETURA DO RM/OSI.

O quadro que o segmento de redes de computadores apresentava no final da década de 70 caracterizava-se, de um lado, por enormes perspectivas de crescimento, mas, de outro, por uma situação de crise criada pela heterogeneidade dos padrões, protocolos e equipamentos de comunicação de dados existentes no mercado. Cada interessado havia definido, unilateralmente, sua arquitetura. Os fabricantes, as arquiteturas proprietárias; as operadoras de telecomunicações, as arquiteturas das redes públicas; e algumas entidades, como era o caso da ARPA, possuíam arquiteturas específicas para atender às suas redes.

A solução foi encontrada pela ISO (International Organization for Standardization), sob a forma de propostas de elaboração de um modelo que viesse a sintetizar, de modo abstrato, o funcionamento de computadores integrados por redes de comunicação de dados. Baseada nas experiências advindas do funcionamento dos sistemas de teleprocessamento, da rede ARPA e das redes públicas e proprietárias, a ISO, entre 1978 e 1984, elaborou o **RM-OSI** ou Modelo de Referência para Interconexão de Sistemas Abertos (**Reference Model - Open Systems Interconnection**), que é a expressão, assim, de todo o conhecimento tecnológico adquirido pelo mundo a respeito de comunicação de dados.

No modelo OSI foi abordado o conceito de **sistema aberto**, definido como “o sistema capaz de suportar os padrões de comunicação OSI de modo a interfuncionar com outros sistemas abertos de diferentes fornecedores”. Ao modelo OSI se deve, também, a consolidação dos princípios de arquitetura de rede de comunicação de dados.

A receptividade em relação ao Modelo OSI foi muito grande nos anos seguintes à sua divulgação e, em alguns setores, mantém-se até hoje. Especialistas da área baseiam-se me seus princípios, e é comum encontrar na literatura ou em palestras menções do tipo: “as tarefas correspondentes à camada X do Modelo OSI” ou “faltam tais funções correspondentes à camada Y do Modelo OSI”, mesmo quando se faz referência a sistemas que não propõem a aderir a esse modelo.

O esforço de padronização não foi concluído com a elaboração do Modelo OSI. Ao contrário, iniciou-se uma intensa atividade, em nível mundial, no sentido de projetar, especificar, implementar e testar os protocolos das várias camadas definidas pelo modelo, nascendo, assim, a Arquitetura OSI: uma estrutura funcional dos elementos envolvidos na comunicação entre sistemas abertos de comunicação de dados, suportada por um conjunto de protocolos padronizados elaborados de acordo com os princípios do Modelo OSI.

Desde a sua criação, e cada vez que um novo padrão de protocolo é elaborado, a Arquitetura OSI impõe-se como o grande projeto de Engenharia de Protocolos. As soluções apresentadas, os mecanismos de protocolos, a estrutura de camada de aplicação e as aplicações desenvolvidas de acordo com os princípios da metodologia orientada a objetos e da computação distribuída contribuem para essa colocação.

O Modelo OSI é mostrado na figura 6.3. Como já dito, este modelo foi desenvolvido com um primeiro passo na direção da padronização internacional dos protocolos usados nas diversas camadas e denominado de Modelo de Referência para a Interconexão de Sistemas Abertos ou RM-OSI (Reference Model for Open Systems Interconnection), pois trata da interconexão de sistemas abertos, ou seja, sistemas que estão abertos à comunicação com outros sistemas.

O modelo OSI foi criado seguindo a filosofia das arquiteturas multicamadas, como já descrita anteriormente. Como mostra a figura, sua arquitetura define 7 camadas, cujos princípios de definição foram os seguintes:

1. cada camada corresponde a um nível de abstração necessário no modelo;
2. cada camada possui suas funções próprias e bem definidas;
3. as funções de cada camada foram escolhidas segundo a definição dos protocolos normalizados internacionalmente;
4. a escolha das fronteiras entre cada camada deveriam ser definidas de modo a minimizar o fluxo de informação nas interfaces;
5. o número de camadas deve suficientemente grande para que funções distintas não precisem ser colocadas na mesma camada, e ser suficientemente pequeno para que a arquitetura não se torne difícil de controlar.

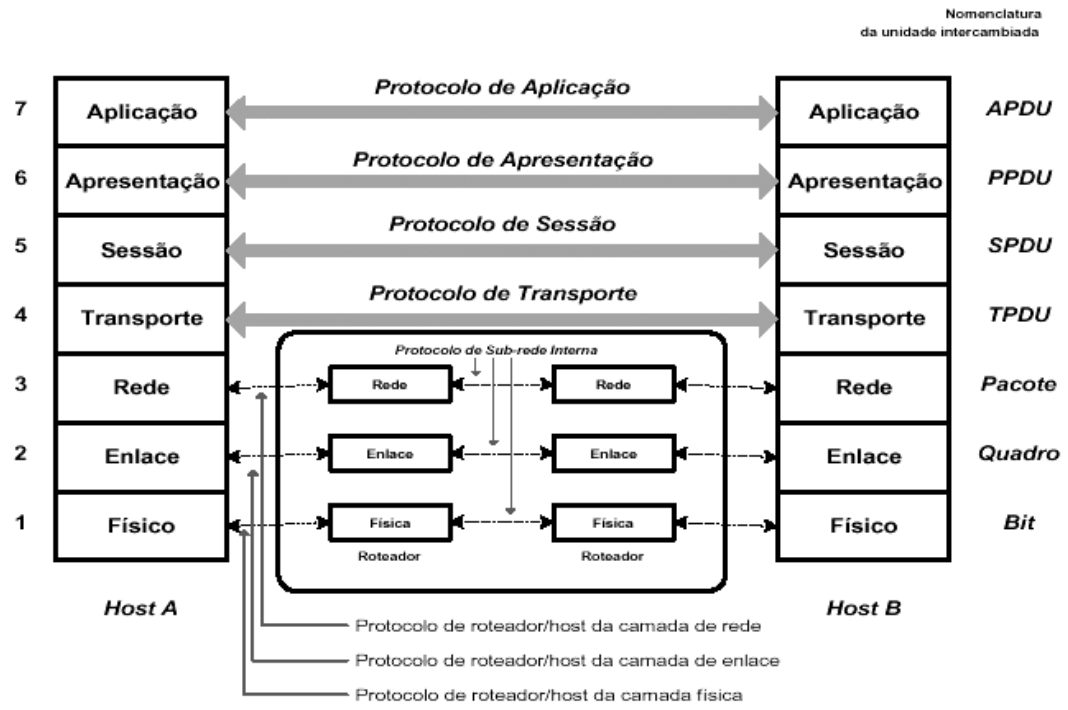


Figura 6.3 - Arquitetura de sete camadas do modelo OSI.

Como pode ser visto na figura 6.3, o modelo prevê a comunicação entre sub-redes através de processadores de interface de mensagem, ou **IMPs** *(Interface Message Processor*s).

A forma como os dados são transmitidos ao longo do modelo OSI é ilustrada na figura 6.4. Como se pode ver, o processo emissor vai enviar uma certa quantidade de dados ao processo receptor. Ele envia, então, os dados à camada de Aplicação que introduz a estes um cabeçalho de aplicação, *A*H, e envia a mensagem resultante à camada de Apresentação. Esta camada, por sua vez, introduz à mensagem recebida um cabeçalho de apresentação, *P*H, enviando a mensagem, em seguida à camada inferior. É importante ressaltar aqui que esta camada não toma conhecimento da existência e significado do cabeçalho de aplicação, considerando este como parte dos dados compondo a mensagem. Este processo de transferência de camada a camada vai se repetindo até o nível físico, quando os dados serão, enfim, transmitidos ao sistema destino.

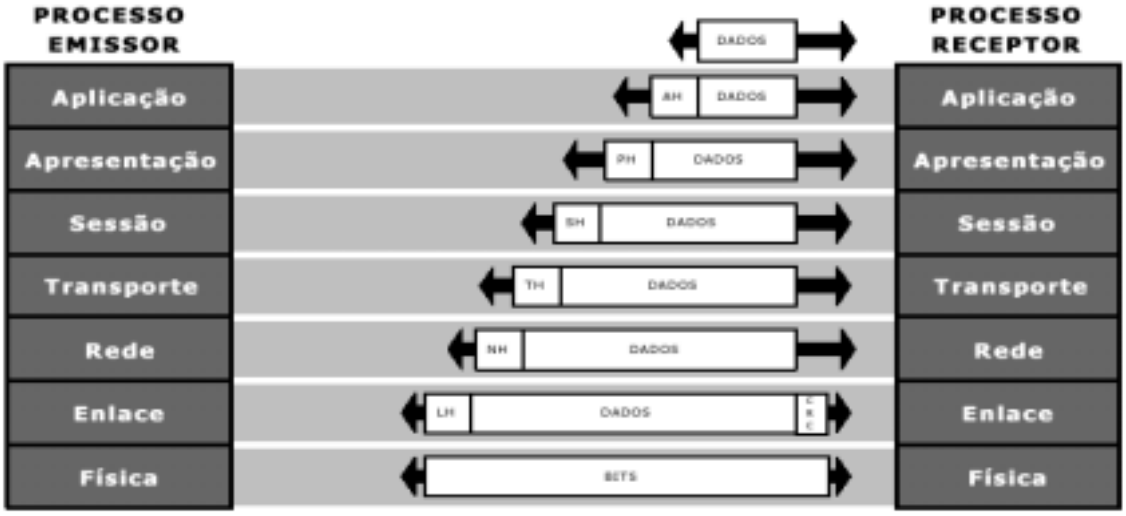


Figura 6.4 - Ilustração da comunicação no modelo OSI.

Neste sistema, os diversos cabeçalhos introduzidos nas camadas de rede do sistema fonte vão sendo interpretados e eliminados nas camadas correspondentes até que os dados cheguem ao processo receptor. O conceito

fundamental da transferência de dados é que cada camada foi projetada como se ela fosse realmente horizontal, quando na verdade a transmissão se dá de modo vertical.

Isto fica claro, por exemplo, quando a camada de Transporte emissora recebe um dado da camada de Sessão; ela insere um cabeçalho de transporte e envia a mensagem à camada de Rede emissora. Este processo, portanto, para a camada de Transporte, não é mais do que um detalhe técnico. Um exemplo análogo é aquele de um diplomata de um país fazendo um discurso, na sua própria língua, nas Nações Unidas. Este considera estar se dirigindo aos seus colegas diplomatas de outros países, embora, na prática, ele esteja dirigindo-se ao seu intérprete.

6.1.1 - AS CAMADAS DO RM-OSI.

Vamos estudar, a seguir, as principais funções realizadas por cada uma das camadas definidas no Modelo OSI.

6.1.1.1 - A CAMADA FÍSICA.

A **Camada Física** é responsável da transferência de bits num circuito de comunicação. De maneira geral, a sua função é garantir que cada bit enviado de um lado será recebido do outro lado sem ter alterado o seu valor, ou seja, se o bit enviado está a 1, ele será recebido a 1 e não a 0.

Para isto, as questões a serem resolvidas neste nível são:

1. os modos de representação dos bits 0 e 1 de maneira a evitar ambigüidades ou confusões (valor da tensão em volts para a representação dos valores 0 e 1 dos bits, duração de cada sinal representando um bit, a codificação dos sinais, etc.);
2. os tipos de conectores a serem utilizados nas ligações (número de pinos utilizado, as funções
3. associadas a cada pino, etc.);
4. a maneira como as conexões são estabelecidas para a iniciação de um diálogo e como é feita a desconexão ao final deste;
5. modo de transmissão adotado (unidirecional, bidirecional);
6. modo de conexão adotado (ponto-a-ponto, multiponto);
7. modo de tratamento dos erros (detecção, tratamento, etc).

A concepção desta camada deve se relacionar à definição das interfaces elétricas e mecânicas, seus modos de funcionamento e o suporte de comunicação adotado. O objetivo da camada Física é assegurar o transporte dos dados, representados por um conjunto de bits, entre dois equipamentos terminais, via um **suporte de transmissão**, já apresentado na seção 4.3.

6.1.1.2 - A CAMADA DE ENLACE DE DADOS.

A **Camada de Enlace de Dados** tem por função principal a transformação do meio de comunicação "bruto" em uma linha livre de erros de transmissão para a camada de Rede. Ela efetua esta função através do fracionamento das mensagens recebidas do emissor em unidades de dados denominadas quadros, que correspondem a algumas centenas de bytes. Estes quadros são transmitidos seqüencialmente e vão gerar quadros de reconhecimento enviados pelo receptor. Nesta camada, as unidades de dados são enriquecidas com um conjunto de bits adicional (no início e fim de cada quadro) de modo a permitir o reconhecimento destes.

Um problema típico deste nível é o da ocorrência de uma perturbação sobre a linha de transmissão que provoque a destruição (perda) do quadro enviado. Neste caso, o quadro deve ser retransmitido para garantir a integridade da informação transferida. Por outro lado, deve-se também evitar múltiplas retransmissões de um mesmo quadro, o que pode provocar a sua duplicação, por exemplo, se o quadro de reconhecimento é perdido.

Uma outra função desta camada é evitar uma alta taxa de envio de dados da parte do emissor no caso do sistema emissor não ter capacidade de absorver a informação à mesma taxa. Este mecanismo deve permitir informar ao emissor a necessidade de armazenamento dos dados a transmitir (controle de fluxo).

Dentre os fatores com os quais a camada de Enlace deve preocupar-se estão:

1. a forma como os bits provenientes da camada Física serão agrupados em **quadros** (*frames*);
2. os mecanismos de detecção e correção de erros a serem implantados, uma vez que as informações trocadas através da camada Física não são isentas de erros de transmissão,pelos fatores que já foram levantados;
3. os mecanismos de controle de fluxo para limitar o volume de informação trocados entre entidades fonte e destino;
4. a gestão das ligações entre as entidades de Rede.

A camada de Enlace de Dados oferece serviços para a camada de Rede classificados em três principais categorias, estas dependendo do sistema no qual elas serão implantadas:

1. serviço sem conexão e sem reconhecimento;
2. serviço sem conexão com reconhecimento;
3. serviço orientado à conexão.

Na primeira classe de serviços, a máquina fonte da informação envia os quadros de dados à máquina destinatária e esta não envia um quadro de reconhecimento da informação recebida; além disso, não existe estabelecimento prévio de conexão e, por conseqüência, não existe liberação desta ao final do diálogo. Se um quadro de dados é perdido no meio de transmissão como conseqüência de um ruído, por exemplo, não existe nenhum mecanismo que permita solucionar o problema. Esta classe de serviços é adequada quando implantados sobre um suporte de comunicação cuja taxa de erros é muito baixa ou que a correção dos erros é prevista nas camadas superiores. Eles podem ser empregados particularmente no caso de aplicações tempo real e em redes locais.

A segunda classe de serviços, embora ainda não defina o estabelecimento prévio de conexão, prevê a existência de quadros de reconhecimento, de modo que a máquina fonte será notificada pela máquina destinatária da recepção do quadro previamente enviado. Um mecanismo que pode ser implantado no caso de perda do quadro — o que corresponde à não recepção do quadro de reconhecimento após um certo tempo (timeout) — é a retransmissão daquele. Num serviço sem conexão, existe a possibilidade da retransmissão de quadros provocando a recepção múltipla do mesmo quadro (duplicação de mensagem).

A terceira classe de serviços é a mais sofisticada, uma vez que ela define a necessidade do estabelecimento prévio de conexão e a liberação destas ao final do diálogo. Neste caso, cada quadro enviado é numerado e a camada de Enlace garante que cada quadro enviado será recebido, uma única vez, e que o conjunto de quadros enviados será recebido ordenado da mesma forma que foi enviado. Esta classe de serviços oferece à camada de Rede um canal de comunicação confiável.

Os serviços orientados conexão são caracterizados por três principais etapas:

1. a etapa de **estabelecimento de conexão**, durante a qual são definidos todos os parâmetros relacionados à conexão, como por exemplo, os contadores de seqüência de quadros;
2. a etapa de **transmissão de dados**, durante a qual são realizadas todas as trocas de informação correspondentes ao diálogo entre duas máquinas;
3. a etapa de **liberação da conexão**, que caracteriza o fim do diálogo e na qual todas as variáveis e outros recursos alocados à conexão serão novamente disponíveis.

Para que o serviço seja oferecido à camada de Rede, a camada de Enlace utiliza-se dos serviços fornecidos pela camada Física que, como já foi descrito na parte precedente, é responsável da transmissão de bits de um ponto a outro na rede de comunicação, sendo que o conjunto de bits transmitido pode sofrer distorções produzindo erros de transmissão. Uma conseqüência típica pode ser que o número de bits recebidos seja inferior ao número de bits enviados ou os valores de alguns bits podem ter sido modificados.

Com o objetivo de permitir um controle de erro eficiente, a camada de Enlace decompõe as mensagens em porções menores denominadas **quadros** (*frames*), aos quais são adicionados códigos especiais de controle de erro. Desta forma, o receptor pode verificar se o código enviado no contexto de um quadro indica ou não a ocorrência de erros de transmissão e ele pode, assim, tomar as providências necessárias para evitar as conseqüências devido àquele erro.

Os erros que por vezes ocorrem nos suportes de transmissão podem ter como causas os mais diversos fenômenos físicos, como por exemplo, o ruído térmico, provocado pela agitação dos elétrons nos cabos de cobre. Outro fenômeno importante está relacionado aos ruídos impulsivos, capazes de provocar, numa linha transmitindo dados a 9600 bit/s, a perda de 96 bits. Os ruídos impulsivos são causados pelos arcos devido ao chaveamento de relês ou outros dispositivos eletromecânicos. O que se tem notado, entretanto, é que, independentemente do fenômeno causador de erro, estes tendem a gerar normalmente verdadeiros pacotes de erros e não erros simples. Isto pode ter um aspecto positivo, uma vez que, num conjunto relativamente grande de bits, um menor número de pacotes vai conter erros. Por outro lado, os erros agrupados em pacotes são mais difíceis de detectar.

O **controle de erros** de transmissão é uma das funções mais importantes asseguradas pela camada de Enlace. Esta função é baseada na possibilidade de informação para entidade emissora da mensagem do que ocorreu na extremidade de recepção.

Os protocolos de controle de erro são caracterizados, em geral, pela definição de um quadro de controle, correspondente a um reconhecimento positivo ou negativo. Caso a entidade emissora receba um reconhecimento positivo de um quadro previamente enviado, ela entende que aquele foi corretamente recebido. Por outro lado, se ela recebe um reconhecimento negativo, ficará consciente que o quadro foi mal transmitido e que, neste caso, ele deverá ser retransmitido.

Ainda, se, por uma intensidade relativamente forte de ruído, o quadro inteiro não é recebido pela entidade destinatária, esta não vai reagir ao quadro emitido e a entidade emissora corre o risco de esperar indefinidamente pelo reconhecimento — isto é evitado pela adição de **temporizadores**, estabelecendo assim um tempo máximo de espera pelo reconhecimento, antes da retransmissão. O tempo de espera deve ser determinado em função dos atrasos relativos à transmissão dos quadros, de modo que os quadros de reconhecimento, se existentes, cheguem antes do esgotamento da temporização (timeout).

Deste modo, se o quadro ou o reconhecimento são perdidos, a temporização será esgotada, podendo provocar a retransmissão do quadro. Neste caso, é possível que o quadro seja aceito mais de uma vez pela camada de Enlace e transmitido à camada de Rede ocorrendo a duplicação de quadros. Para evitar este problema, deve-se introduzir um mecanismo de distinção dos quadros a fim de que o receptor possa separar os quadros duplicados de seus originais.

Existem basicamente duas técnicas para a correção de erro. A primeira consiste na introdução, nos quadros, de informações redundantes que permitam ao receptor reconstituir os dados enviados a partir da informação recebida. A segunda técnica consiste em adicionar unicamente um conjunto de informações redundantes o suficiente para que o receptor possa detectar a ocorrência de um erro (sem corrigi-lo) e requisitar a retransmissão do quadro. Ao primeiro tipo de informação é dado o nome de **código corretor** e ao segundo tipo de informação **código detector**.

Um método de detecção de erros largamente utilizado é a definição de códigos de detecção de erros polinomiais, também denominados **CRC (Cyclic Redundancy Code)**. Nos códigos polinomiais, considera-se que os bits de uma cadeia de caracteres são os coeficientes de um polinômio, coeficientes estes, capazes de assumir apenas dois valores: 0 ou 1. Assim, um bloco de k bits é visto como uma série de coeficientes de um polinômio de *k* termos, indo de X_{k-1}a X_0. A palavra 110001 contém 6 *bits* — ela representa então o seguinte polinômio: $x_5 + x_4 + x_0$.

A utilização de códigos de detecção polinomiais é baseada na escolha de um código especial que caracteriza um **polinômio gerador**, ou *G(x)*. Uma exigência em relação a este polinômio é que os *bits* mais significativo e menos significativo (correspondendo, respectivamente aos coeficientes de mais alta ordem e de mais baixa ordem do polinômio) sejam de valor 1. A técnica consiste em adicionar a um bloco de dados (caracterizando um polinômio *M(x)*) um conjunto de *bits* de controle de modo que o quadro (dados + *bits* de controle) seja divisível por *G(x)*. Na recepção, a entidade de Enlace efetua a divisão dos *bits* compondo o quadro pelo polinômio gerador. Caso o resto seja diferente de zero, é caracterizada então a ocorrência de um erro de transmissão.

Outra função importante da camada de Enlace de Dados é a de contornar o problema decorrente de transmissor que envia quadros mais rapidamente do que um receptor é capaz de aceitá-los. Esta situação pode ocorrer quando o transmissor está sendo executado em um computador muito rápido (ou que não esteja sobrecarregado) e o receptor está utilizando um computador lento (ou sobrecarregado). Mesmo que a transmissão não contenha erros, em um determinado ponto o receptor não mais será capaz de receber os quadros e começará a perder alguns deles. Desta forma há a necessidade de mecanismos que impeçam que esta situação aconteça.

A solução mais comum é incluir algum mecanismo de **controle de fluxo** para que o transmissor não mais envie quadros tão rapidamente a ponto do receptor não ser capaz de recebê-los corretamente. Geralmente estes mecanismos incluem informações que devem ser enviadas do receptor para o transmissor para que este último possa saber se o receptor é ou não capaz de acompanhá-lo.

Existem diversos esquemas de controle de fluxo. No entanto, a maioria deles utiliza o mesmo princípio básico. O protocolo contém regras bem definidas sobre quando o transmissor pode enviar o quadro seguinte. Com freqüência, essas regras impedem que os quadros sejam enviados até que o receptor tenha concedido permissão para transmissão, implícita ou explicitamente. Por exemplo, quando uma conexão for estabelecida, o receptor poderá dizer: “Você está autorizado a me enviar n quadros agora, mas depois que eles tiverem sido enviados, não envie mais nada até eu dizer para continuar”.

6.1.1.3 - A CAMADA DE REDE.

A **Camada de Rede** é responsável da gestão de sub-redes; ela define a forma como os pacotes de dados serão encaminhados do emissor ao receptor. Os caminhos a serem utilizados podem ser definidos em função de tabelas

estáticas ou determinados dinamicamente no momento de cada diálogo em função das condições de tráfego da rede. Esta camada deve ainda efetuar a gestão dos problemas de congestionamento provocados pela presença de uma quantidade excessiva de pacotes de dados na rede.

O objetivo da camada de Rede é assegurar o transporte de unidades de dados denominadas **pacotes** do sistema fonte ao sistema destinatário, definindo uma trajetória apropriada. Esta trajetória pode significar a passagem por diversos nós intermediários da rede, o que significa que a camada de Rede deve ter o conhecimento de todos os aspectos topológicos da rede considerada e, com esta informação, ser capaz de escolher o melhor caminho a ser realizado por estes pacotes. Nesta escolha, é interessante que seja levado em conta o estado corrente de toda a rede, particularmente no que diz respeito ao tráfego de mensagens, evitando assim a sobrecarga de certos trechos das linhas de comunicação. Ainda, se o sistemas fonte e destinatário estão conectados a redes diferentes, estas diferenças devem ser levadas em conta e compensadas pela camada de Rede.

A camada de Rede é a camada mais baixa que trata a transmissão fim-a-fim. As duas funções essenciais da camada de Rede são **roteamento** e **controle de congestionamento**. Além destas, são funções desta camada:

1. multiplexação;
2. endereçamento;
3. mapeamento entre endereços de rede e endereços de enlace;
4. estabelecimento e liberação de conexões do serviço de rede;
5. transmissão de unidades de dados do serviço de rede (pacotes);
6. segmentação e blocagem de SDUs/PDUs;
7. detecção e recuperação de erros;
8. seqüenciação.

A camada de Rede oferece serviços à camada de Transporte na interface entre estas duas camadas. Geralmente esta interface tem importância especial por outra razão: costuma ser a interface entre a concessionária de comunicações e o cliente, ou seja, é a fronteira da sub-rede. Em geral, a concessionária de comunicações tem o controle dos protocolos e interfaces até (e inclusive) a camada de rede. Sua tarefa é entregar pacotes que recebe a seus clientes. Por isso esta interface deve ser especialmente bem definida.

Os serviços da camada de Rede foram projetados com os seguintes objetivos em mente:

1. os serviços devem ser independentes da tecnologia de sub-rede;
2. a camada de Transporte deve ser protegida contra a quantidade, o tipo e a topologia das sub-redes presentes;
3. os endereços de rede que se tornaram disponíveis para a camada de Transporte devem usar um plano de numeração uniforme, mesmo nas LANs e WANs.

6.1.1.3.1 - ENDEREÇAMENTO DE REDE

O **endereçamento dos pontos de acesso ao serviço de rede** (SAPs de rede) deve ser completamente independente dos demais endereçamentos dos outros níveis de protocolo. Basicamente dois tipos de endereçamento são possíveis: o hierárquico e o horizontal.

No **endereçamento hierárquico** o endereço é constituído de acordo com os endereços correspondentes aos vários níveis de hierarquia de que faz parte. Um exemplo comum é um endereço de SAP de rede formado pelo número da rede a que pertence, pelo número da estação dentro dessa rede e pelo número da porta associada. O protocolo IP da ARPAnet é um exemplo de utilização de endereço hierárquico, onde a identificação de um SAP de rede (único por estação) é formada pelo endereço da rede e pelo endereço da estação.

O endereço hierárquico é também o método sugerido pelo ITU-T, através da recomendação X.121, para interconexão de redes públicas de pacotes. Nessa recomendação os endereços são decimais formados por três campos: um código do país (três dígitos), um código para a rede (um dígito – no máximo dez redes) e um campo para o endereçamento dentro da rede (dez dígitos).

No **endereçamento horizontal**, os endereços não têm relação alguma com o lugar onde estão as entidades dentro da rede. Um exemplo comum desse tipo de endereçamento serão os endereços globalmente administrados, constituídos pelo número de assinatura do usuário, como os utilizados pelo padrão IEEE802.

Considerações sobre o roteamento parecem indicar vantagens na utilização de endereços hierárquicos, uma vez que estes contém informações explícitas sobre o local onde se localizam as entidades, informações que podem ser usadas quando necessário. Já o endereço horizontal, por ser independente da localização, facilita os esquemas de reconfiguração por permitir uma mobilidade das entidades sem renumeração das mesmas.

O mapeamento do endereço de um SAP de rede em um endereço de sub-rede (muitas vezes o endereço no nível de enlace se a rede não possui a subcamada de acesso à sub-rede do RM-OSI) para o envio de pacotes é uma tarefa a ser resolvida pelo nível de rede (subcamada dependente da sub-rede). Existem duas técnicas usuais para essa conversão: resolução através de **mapeamento direto** e resolução através de **vinculação dinâmica**.

No **mapeamento direto**, a estação sabe como computar, de modo eficiente, o endereço de sub-rede, através de uma função que mapeia o endereço inter-redes no endereço de sub-rede. Por exemplo, suponha o caso do endereçamento hierárquico onde o campo de endereço de estação corresponde exatamente ao endereço da estação no nível da sub-rede. Neste caso a conversão é trivial. Conversões mais complicadas podem ser realizadas através de tabelas de conversão e técnicas de acesso rápido a estas tabelas.

Para evitar o uso de tabelas de conversão, uma vinculação dinâmica pode ser efetuada entre o endereço da inter-rede e o endereço da sub-rede, através da utilização de algum protocolo de resolução. Por exemplo, suponha o caso extremo onde a cada comunicação é enviada uma mensagem a toda a inter-rede, perguntando o endereço de sub-rede correspondente ao SAP de rede do destino. A estação de destino responderia à requisição enviando seu endereço de sub-rede, possibilitando ao SAP de rede de origem realizar a comunicação.

A questão, neste caso é: uma vez que se está enviando uma mensagem por difusão perguntando o endereço de sub-rede, por que não enviar diretamente os dados por difusão? A razão vem do fato de que a realização de difusão toda vez que se quer enviar um pacote, é muito onerosa, em termos de tráfego gerado na rede e de processamento que cada estação tem que realizar, quer o pacote seja destinado a ela ou não. Para reduzir esses custos, as estações mantêm em memória *cache* os endereços de sub-rede recentemente requeridos e sua vinculação com os endereços dos SAPs de rede, de forma a não ter de realizar o protocolo de resolução a todo pacote transmitido.

6.1.1.3.2 - FUNÇÃO DE ROTEAMENTO.

Como já vimos, a função principal da camada de Rede é efetuar o encaminhamento dos pacotes trocados entre duas entidades oferecendo uma comunicação fim-a-fim. Durante a trajetória os pacotes sofrerão uma série de saltos, sendo que a decisão de que caminho utilizar é feita na camada de Rede, esta decisão podendo levar em conta (ou não) a situação da rede do ponto de vista do tráfego de informação. Pode-se distinguir os diferentes algoritmos de **roteamento** em duas principais classes: os algoritmos **adaptativos** e **não adaptativos** (ou de **rota fixa**). Os algoritmos não adaptativos não levam em conta a situação de tráfego da rede, fazendo o denominado **roteamento estático**, já os adaptativos o fazem, considerando modificações de topologia da rede e do tráfego real, ou **roteamento dinâmico**. A implementação do roteamento exige uma estrutura de dados que informe os possíveis caminhos e seus custos, a fim de que se possa decidir qual o melhor caminho.

No encaminhamento **não adaptativo**, a tabela de roteamento, uma vez criada, não é mais alterada. As rotas são fixas e caminhos alternativos são tomados somente em caso de falhas. Esse método tem a vantagem de ser bastante simples, mas em geral leva à má utilização dos meios de comunicação, a não ser que o tráfego da rede seja bem regular e bastante conhecido.

Um exemplo de roteamento estático é o *flooding* (ou inundação). Neste algoritmo cada pacote de entrada é enviado para todas as linhas de saída, exceto para aquela em que chegou. Este mecanismo obviamente gera muitos pacotes duplicados e alguma técnica deve ser empregada para amortecer este processo. Uma das técnicas consiste em descartar o pacote depois que ele já percorrer um número máximo de roteadores em seu caminho.

Já no encaminhamento **adaptativo**, a rota é escolhida de acordo com a carga na rede. Nas tabelas de rotas são mantidas informações sobre o tráfego (como por exemplo o retardo sofrido em um determinado caminho), que são consultadas para a escolha do caminho mais curto (por exemplo, o de menor atraso). As tabelas devem ser periodicamente atualizadas, podendo tal atualização ser realizada de vários modos:

1. No modo **isolado** a atualização é realizada com base nas filas de mensagens para os diversos caminhos e outras informações locais.
2. No modo **distribuído**, cada nó envia periodicamente aos outros nós, incluindo os roteadores, as informações locais sobre a carga da rede. Essas informações são utilizadas para o cálculo da nova tabela.

3. No modo **centralizado** cada nó envia a um ponto central da rede as informações locais sobre a carga. Essas informações são utilizadas pelo ponto central para o cálculo das novas tabelas, que são então enviadas aos roteadores e demais nós.

Com relação ao **caminho mais curto,** existem várias formas de medir o "comprimento" do caminho. Uma forma é o número de saltos, isto é, o número de nós intermediários pelos quais deve passar o pacote até chegar ao destino. Outra medida é a distância geográfica. Ainda outra medida poderia ser o retardo de transferência do pacote. Nesse caso o caminho mais curto seria, na verdade, o caminho mais rápido.

6.1.1.3.3 - CONTROLE DE CONGESTIONAMENTO.

Durante o funcionamento de uma aplicação distribuída construída sobre uma rede, existem instantes em que o fluxo de mensagens sendo trocadas pode atingir valores bastante grandes, de tal forma que os nós intermediários, responsáveis do tratamento dos pacotes, não sejam mais capazes de tratar os pacotes para retransmissão. Isto, naturalmente, terá como conseqüência uma degradação no funcionamento da rede, podendo trazer prejuízos (lentidão, perdas de pacotes) ao desempenho da aplicação, comprometendo o seu correto funcionamento. As causas desta sobrecarga, conhecida por **congestionamento**, podem ser de várias naturezas. Um exemplo disto pode ser a lentidão dos nós na realização do roteamento ou um mau funcionamento do mecanismo de controle de fluxo.

O congestionamento consiste, normalmente, de um processo a realimentação positiva, o número de mensagens tendendo a crescer se a rede está congestionada. Sendo assim, a camada de Rede deve também fazer este papel, através da implementação de funções de controle de congestionamento.

A primeira forma de controlar o congestionamento da rede é através da **pré-alocação de *buffer*s**, particularmente se o serviço é orientado à conexão. Isto significa que, no momento do estabelecimento do circuito virtual que vai caracterizar a conexão, um determinado número de *buffers* deve ser alocado em cada nó para permitir o armazenamento dos pacotes a serem retransmitidos por aquele circuito virtual.

Evidentemente, o número de *buffers* a ser alocado vai depender do protocolo implementado entre cada par de nós intermediários (IMPs). Um algoritmo do tipo "envia-espera" vai exigir um número de *buffers* evidentemente menor do que um algoritmo que autorize o envio de diversos pacotes antes da retransmissão.

Outro mecanismo que é adotado para o controle de congestionamento é o da **destruição de pacotes**. Neste caso, não existe reserva prévia de *buffer*s, de modo que, se um pacote chega num IMP (processador de interface de mansagem) e este não dispõe de *buffer* para o seu armazenamento, este é simplesmente destruído (ou descartado). Se o serviço oferecido é do tipo "datagrama", não há mais nada a fazer; por outro lado, se este é orientado à conexão, o pacote deverá ser armazenado em algum nó para uma possível retransmissão. Ainda, a destruição de pacotes deve seguir uma certa disciplina, por exemplo, destruir um pacote de reconhecimento pode não ser uma boa solução, uma vez que este pacote poderia permitir ao nó o apagamento de um pacote de informação e, por conseqüência, a liberação de um *buffe*r. Uma solução para isto é a reserva, para cada linha de chegada, de um *buffer* que possibilite a recepção de pacotes de reconhecimento endereçados àquele nó.

O **controle de fluxo** consiste em outra técnica de controle de congestionamento, embora não muito eficiente nesta tarefa. O problema do controle do fluxo é o fato que os limites do tráfego não podem ser estabelecidos em valores muito baixos, pois isto pode provocar problemas de eficiência na aplicação se um pico de tráfego é necessário. Por outro lado, a escolha de um limite alto de tráfego pode resultar num controle medíocre de congestionamento.

Outras técnicas de controle de congestionamento são ainda implementadas, como por exemplo:
- o **controle isarítmico**, baseado na existência em cada nó de um certo número de fichas. O nó que tiver um pacote a transmitir, deve obter uma ficha, se existir alguma disponível. Isto permite manter constante o número de pacotes em circulação na rede;

- os **pacotes de estrangulamento**, enviados por um nó ao usuário do serviço de rede, indicando que determinadas linhas de saída estão no limite da saturação. Isto faz com que o usuário reduza o envio de pacotes para o destino utilizando aquela linha até que a situação retome a normalidade.

6.1.1.4 - A CAMADA DE TRANSPORTE.

A **Camada de Transporte** recebe os dados enviados da camada de sessão, decompô-los, se for o caso, em unidades de dados menores e garantir que todas as partes da mensagem vão ser transmitidas corretamente à outra

extremidade. Esta função deve ser suprida de maneira eficiente, inclusive, sem que a camada de Sessão tome conhecimento de possíveis alterações na tecnologia da parte material da rede.

Esta camada cria, normalmente, uma conexão de rede para cada conexão de transporte requerida pela camada de Sessão, embora, se as necessidades de velocidade transmissão são justificadas, ela possa estabelecer diversas conexões de rede para uma mesma conexão de transporte. Por outro lado, se o custo da manutenção de uma conexão de rede é considerado elevado, esta camada pode efetuar a função inversa, ou seja, a **multiplexação** de várias conexões de transporte sobre uma mesma conexão de rede, esta tarefa sendo feita de modo transparente para a camada de Sessão.

Ela deve determinar, também, o tipo de serviço oferecido à camada de Sessão e, por conseqüência, aos usuários da rede. Uma conexão de transporte típica é aquela de um canal ponto-a-ponto, livre de erros de transmissão, transmitindo as mensagens na mesma ordem em que elas foram enviadas. Por outro lado, outras classes de serviços podem fornecer uma conexão capaz de enviar as mensagens de modo isolado, mas sem a garantia de uma ordem correta na transmissão. O tipo do serviço a ser fornecido é definido no momento do estabelecimento da conexão.

Uma característica desta camada é que ela implementa um verdadeiro diálogo fim-a-fim, ou seja, o programa executando no sistema fonte dialoga com o programa executando na máquina destino através dos cabeçalhos e informações de controle contidas nas mensagens deste nível. Já nas camadas mais baixas, os protocolos operam entre máquinas vizinhas e não entre os sistemas fonte e destino, dado que estes podem estar separados por vários IMPs (centrais de comutação de dados ou *Interface Message Processo*r). Esta diferença fundamental, que se estende igualmente às camadas superiores (até a camada 7) pode ser verificada pela ilustração da figura 6.3.

Dado que esta camada é responsável do estabelecimento e término das conexões de rede, ela deve definir um mecanismo de endereçamento que permita a um sistema indicar com qual sistema ele deseja dialogar. Finalmente, ela deve implementar um mecanismo de controle de fluxo fim-a-fim para evitar que o sistema fonte envie mensagens numa taxa superior àquela com a qual o sistema destino pode consumi-las.

6.1.1.4.1 - SERVIÇOS OFERECIDOS PELA CAMADA DE TRANSPORTE.

Segundo o modelo OSI, os usuários da camada de Transporte são as entidades de Sessão, às quais deve ser oferecido o serviço confiável de transporte dos *bits* de informação fim-a-fim, este serviço sendo fornecido através de uma entidade de software ou de hardware denominada entidade de transporte.

De maneira similar à camada de Rede, a de Transporte pode fornecer dois tipos de serviço: sem conexão e orientados à conexão. Os serviços de Transporte orientados à conexão são caracterizados pelas três etapas já descritas para outros níveis do modelo OSI, isto é, estabelecimento de conexão, transferência de dados e liberação da conexão.

Estes serviços são bastante similares aos serviços oferecidos pela camada de Rede, o que poderia colocar em dúvida a necessidade desta camada. No entanto, a sua existência se justifica pela necessidade de serviços de supervisão da camada de Rede do ponto de vista das entidades efetivamente envolvidas na comunicação. Uma supervisão fim-a-fim entre as aplicações, uma vez que, até o nível Rede, as comunicações se fazem ponto-a-ponto, na sub-rede de comunicação.

Outra contribuição importante da camada de Transporte é que ela permite a utilização de primitivas de serviço padrão pelas diversas aplicações construídas sobre a rede efetuando um perfeito “isolamento” em relação às camadas superiores e tornando transparentes as possíveis alterações tecnológicas que poderiam ocorrer nos níveis inferiores. Por esta razão, costuma-se fazer uma distinção entre os níveis de 1 a 4 e os de 5 a 7. Os primeiros quatro níveis seriam mais orientados ao transporte efetivo das informações e os três níveis superiores, mais orientados às aplicações que serão construídas sobre a rede.

Poderíamos sintetizar o serviço fornecido pela camada de Transporte como de **supervisor da qualidade de serviço** oferecido pela camada de Rede. Isto significa que, se a camada de Rede é confiável, a camada de Transporte não terá muito a fazer.

Por outro lado, se o serviço de Rede é deficiente, a camada de Transporte assume a função de suprir as diferenças entre a qualidade de serviço que a camada de Sessão necessita e aquilo que a camada de Rede pode oferecer. Para isto, o conceito de qualidade de serviço **(QOS** para *Quality Of Servic*e) é um aspecto importante na concepção da camada de Transporte, baseado sobre um certo conjunto de parâmetros, entre os quais destacam-se:

1. retardo no estabelecimento de uma conexão;
2. probabilidade de falha no estabelecimento da conexão;
3. desempenho *(throughput*);

4. retardo de trânsito;
5. taxa de erros residuais;
6. proteção;
7. prioridade;
8. resiliência.

O **retardo no estabelecimento** de uma conexão é o tempo decorrido entre a solicitação de uma conexão de transporte e o recebimento de sua confirmação pelo usuário do serviço de transporte. Nessa característica também está incluído o retardo do processamento na entidade de transporte remota. A exemplo de todos os parâmetros que medem retardo, quanto menor o retardo, melhor o serviço.

A **probabilidade de falha** no estabelecimento da conexão é a possibilidade da conexão não se estabelecer dentro de um período máximo estabelecido devido a, por exemplo, um congestionamento na rede, à falta de espaço de tabela em algum lugar ou a outros problemas internos.

O parâmetro **desempenho *(throughput*)** calcula o número de *bytes* de dados do usuário transmitidos por segundo durante um determinado intervalo de tempo. Ele é medido separadamente para cada direção de fluxo.

O **retardo de trânsito** calcula o tempo transcorrido desde o envio de uma mensagem pelo usuário de transporte da máquina de origem até seu recebimento pelo usuário de transporte da máquina destino. A exemplo do *throughput*, cada direção do transporte é analisada separadamente.

A **taxa de erros residuais** calcula o número de mensagens perdidas ou corrompidas em uma porcentagem do total enviado. Na teoria, a taxa de erros residuais deveria ser zero, pois o trabalho da camada de transporte é esconder os erros da camada de rede. Na prática, essa taxa pode apresentar um valor baixo finito.

O parâmetro **proteção** oferece uma forma de o usuário de transporte especificar seu interesse no fato da camada de transporte fornecer proteção contra a leitura, ou a modificação, de dados por parte de terceiros.

O parâmetro **prioridade** oferece ao usuário de transporte um modo de indicar que algumas conexões são mais importantes do que outras e, em caso de congestionamento, garantir que as conexões de maior prioridade sejam atendidas primeiro.

O parâmetro de **resiliência** oferece à camada de transporte a probabilidade de finalizar uma conexão espontaneamente devido a problemas internos ou congestionamento.

No momento do pedido de um estabelecimento de conexão, o usuário do transporte que está solicitando a conexão encaminha os seus parâmetros desejados de **QoS** nas primitivas de serviço. Se a camada de Transporte julga certos parâmetros longe da realidade, ela pode sinalizar isto ao usuário iniciante, sem mesmo ter tentado estabelecer a conexão, através de uma mensagem de erro que vai, também, indicar a natureza do erro sinalizado.

Outra possibilidade é a camada de Transporte julgar que um certo valor para um parâmetro seja impossível de ser oferecido mas que um valor não muito longe daquele poderia ser oferecido. Neste caso, ela pode modificar os valores dos parâmetros enquadrados e encaminhar o pedido de conexão à máquina remota.

Ainda, se a máquina distante verifica que ela não pode oferecer determinados valores especificados nos parâmetros do pedido, ela pode modificar também aqueles parâmetros. Se ela verifica não poder determinados parâmetros nos valores mínimos permitidos, neste caso ela vai rejeitar a conexão.

Esse procedimento é chamado **negociação de opção** *(option negotiatio*n). Uma vez negociadas as opções serão mantidas durante toda a conexão. Muitas concessionárias de serviços de rede tendem a cobrar mais caro por serviços de melhor qualidade para evitar que os seus clientes fiquem obcecados por esses detalhes.

6.1.1.4.2 - ENDEREÇAMENTO.

Quando um processo de aplicação deseja estabelecer uma conexão com um processo de aplicação remoto, é necessário especificar a aplicação com que se conectar. O transporte sem conexão também tem o mesmo problema. O método normalmente utilizado é definir os endereços de transporte que os processos podem ouvir para receber solicitações de conexão. Na arquitetura Internet, essas extremidades (endereço IP, porta local) formam pares. Em redes ATM, eles são os AAL-SAPs. O termo **TSAP** *(Transport Service Access Poin*t) é um termo mais neutro. Os pontos finais análogos da camada de rede são chamados **NSAPs**. Os endereços IP são exemplos de NSAPs.

A figura 6.5 ilustra a relação entre o NSAP, o TSAP, a conexão de rede e a conexão de transporte para uma sub-rede orientada à conexão. Cabe observar que normalmente uma entidade aceita vários TSAPs. Em algumas redes também existem vários NSAPs; no entanto, em outras, cada máquina tem somente um NSAP (por exemplo, um endereço IP).

A seguir é apresentado um cenário para uma conexão de transporte através de uma camada de rede orientada à conexão.

1. um processo servidor para informar a hora do dia no *host* 2 se associa ao TSAP 122 para aguardar a chegada de uma chamada. O processo de associação do processo a um TSAP é dependente do sistema operacional local;

2. um processo de aplicação no *host* 1 deseja encontrar a hora do dia e, portanto, transmite uma solicitação especificando o TSAP 6 como origem e o TSAP 122 como destino;

3. a entidade de transporte no *host* 1 seleciona um endereço de rede em sua máquina (se houver mais de um) e estabelece uma conexão de rede entre eles; através desta conexão a entidade de transporte do *host* 1 pode se comunicar com a entidade de transporte do *host* 2;

4. a entidade de transporte do *host* 1 diz à sua correspondente no *host* 2 que quer estabelecer uma conexão de transporte entre o seu TSAP 6 e o TSAP 122 dele;

5. a entidade de transporte no *host* 2 então pergunta ao servidor da hora do dia no TSAP 122 se ele está disposto a aceitar uma nova conexão; se ele concordar, a conexão de transporte será estabelecida.

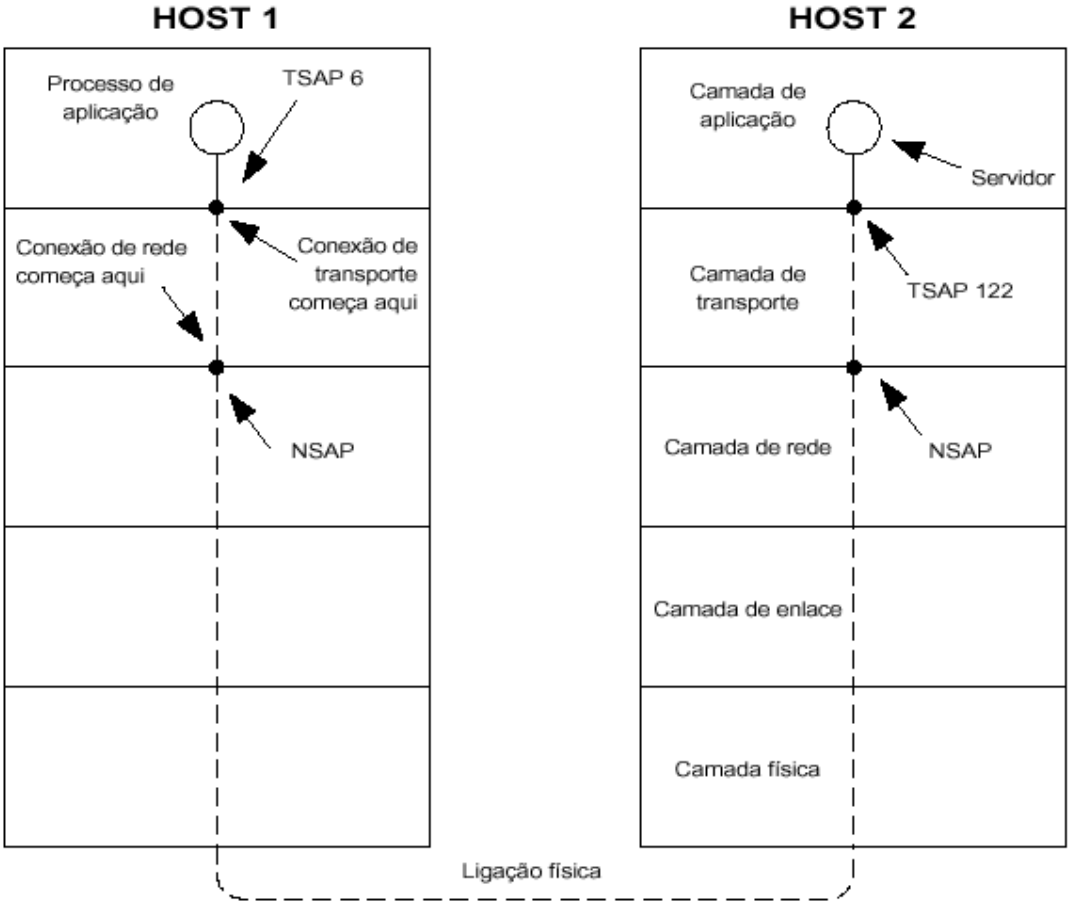


Figura 6.5 – TSAPs, NSAPs e conexões.

Observe que a conexão de transporte acontece de TSAP para TSAP, enquanto a conexão de rede só faz parte do caminho, de um NSAP para outro NSAP. Porém fica uma questão: como o processo de usuário do *host* 1 sabe que o servidor de hora do dia está associado ao TSAP 122? Uma possibilidade é que o servidor de hora esteja associado ao

TSAP 122 há muito tempo e que, aos poucos, todos os usuários da rede tenham se acostumado com isso. Nesse modelo os serviços têm endereços TSAP fixos ou estáveis que podem ser divulgados aos novos usuários quando eles se associam à rede.

Mas nem sempre os processos de aplicação possuem estes endereços estáveis. Um esquema diferente é utilizado em *hosts* UNIX na Internet e é conhecido como **protocolo de conexão inicial**. Neste esquema, ao invés das aplicações estarem conectadas a TSAPs conhecidos, existe um **servidor de processos** que funciona como um *proxy* para os servidores menos usados. Ele atende a uma série de portas ao mesmo tempo, aguardando uma solicitação de conexões TCP. Os usuários potenciais de um serviço devem iniciar por uma solicitação de conexão especificando o endereço TSAP (porta TCP) do serviço de que necessitam. Se nenhum servidor os estiver aguardando, eles estabelecem uma conexão com o servidor de processos, como mostra a figura 6.6 (a).

Depois de receber a solicitação, o servidor de processos encerra a conexão para o servidor solicitado, permitindo que herde a conexão já existente com o usuário. Em seguida o novo servidor executa a tarefa solicitada, enquanto o servidor de processos volta a aguardar novas solicitações , como mostra a figura 6.6 (b).

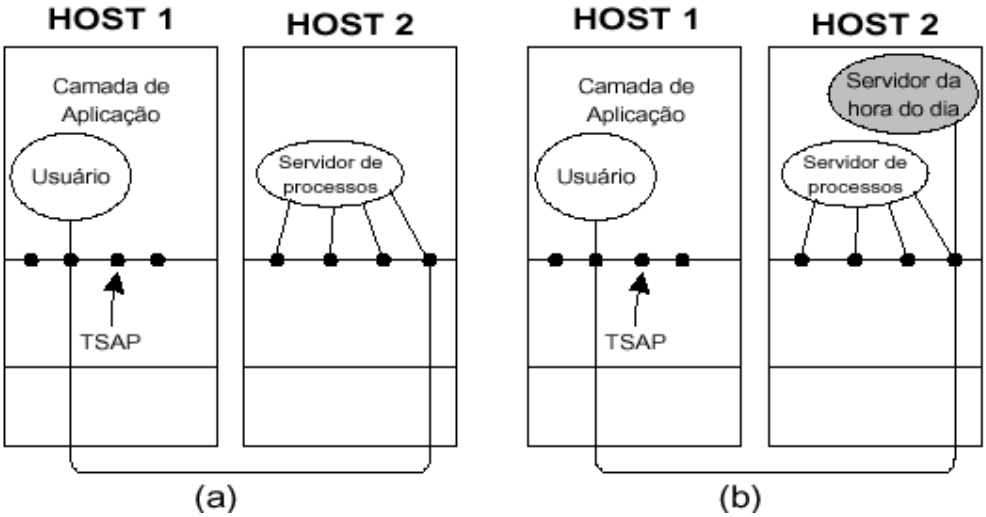


Figura 6.6 – Exemplo de estabelecimento de conexão entre hosts para acesso a um servidor de hora do dia.

Enquanto o protocolo de conexão inicial funciona bem quando os servidores podem ser criados quando necessários, há muitas situações em que os serviços existem de forma independente do servidor de processos. Um servidor de arquivos, por exemplo, deve ser executado em um hardware especial (uma máquina com grande capacidade de disco) e não pode ser criado dinamicamente quando alguém deseja se comunicar com ele.

Com freqüência, é usado um esquema alternativo para administrar essa situação. Nesse modelo existe um processo especial chamado **servidor de nomes** *(name server*), ou, às vezes, **servidor de diretórios** *(directory server*). Para localizar o endereço TSAP correspondente a um determinado nome de serviço, um usuário estabelece uma conexão com o servidor de nomes (que está associado a um TSAP bem conhecido). Em seguida, o usuário envia uma mensagem especificando o nome do serviço, e o servidor de nomes retorna o endereço TSAP. Depois disso o usuário encerra a conexão com o servidor de nomes e estabelece uma nova conexão com o serviço desejado.

Ainda nesse modelo, quando um serviço é criado ele deve se registrar no servidor de nomes, fornecendo seu nome de serviço (normalmente um *string* ASCII) e o endereço de seu TSAP. O servidor de nomes registra essas informações em seu banco de dados interno para que possa fornecer as respostas quando houver consultas.

Vamos supor que o usuário tenha encontrado o endereço do TSAP com que deseja estabelecer a conexão. Outra questão interessante é a seguinte: como a entidade de transporte local sabe em qual máquina esse TSAP está localizado? Mais especificamente, como a entidade de transporte sabe qual endereço da camada de rede será necessário para estabelecer uma conexão de rede com a entidade de transporte remota que administra o TSAP solicitado?

A resposta depende da estrutura dos endereços TSAP. Uma das possibilidades é que os endereços TSAP sejam endereços hierárquicos *(hierarchical address*). Dessa forma, os endereços consistem em uma seqüência de campos usados para particionar o espaço de endereço de modo disjunto. Por exemplo, um endereço realmente universal poderia ter a seguinte estrutura:

endereço = <galáxia> <estrela> <planeta> <país> <rede> <host> <porta>

Com este esquema, fica fácil localizar de forma direta um TSAP em qualquer lugar do universo. Do mesmo modo, se um endereço TSAP é uma concatenação de um endereço NSAP e de uma porta (um identificador local especificando um dos TSAPs locais), quando uma entidade de transporte recebe um endereço TSAP para se conectar, ela usa o endereço NSAP contido no endereço TSAP para chegar à entidade de transporte remota correta.

Uma alternativa ao uso de um espaço de endereçamento hierárquico é um espaço de endereço simples (flat address space). Se os endereços TSAPs não forem hierárquicos, um segundo nível de mapeamento será necessário para localizar a máquina apropriada. Seria necessário um servidor de nomes que utilizasse os endereços de transporte como entrada e retornasse endereços de rede como saída. Outra alternativa para algumas situações (por exemplo, em uma LAN), é fazer uma consulta solicitando à máquina de destino que se identifique enviando um pacote especial para este fim.

6.1.1.4.3 - MULTIPLEXAÇÃO E SPLITTING

A multiplexação é encontrada nos vários níveis do RM-OSI. A multiplexação de um NSAP por vários TSAPS pode surgir por vários motivos e o mais comum é o custo. Várias concessionárias de serviços de rede fazem a sua tarifação baseada no tempo em que uma conexão de rede está aberta. Em uma aplicação com tráfego em rajada essa conexão pode ficar muito tempo ociosa, tendo o usuário de pagar por este tempo. Uma solução é a multiplexação de várias conexões de transporte na conexão de rede. A multiplexação também se justifica por outros motivos além da tarifação. Por exemplo, quando a conexão de rede oferece uma banda passante muito maior que a utilizada pelas conexões de transporte.

Por outro lado, pode acontecer o inverso, a conexão de rede pode oferecer uma banda passante muito mais baixa do que a necessária pela conexão de transporte. Uma solução nesse caso é realizar a divisão *(splittin*g) da conexão de transporte em várias conexões de rede. No caso de uma estação possuir vários canais de saída no nível físico, o *splitting* pode ser usado para aumentar o desempenho.

6.1.1.4.4 - ESTABELECIMENTO E ENCERRAMENTO DE CONEXÕES

O estabelecimento e encerramento de conexões de transporte seria simples, se a rede não perdesse, armazenasse ou duplicasse pacotes. Uma solução para prevenir que erros decorrentes destes problemas aconteçam pode ser conseguida estabelecendo um tempo de vida máximo na rede para um pacote, isto é, passado este tempo ele é destruído. O tempo de vida de um pacote pode ser limitado usando-se um contador de saltos para cada um, incrementado cada vez que passa por um nó intermediário da rede ou um tempo de nascimento *(timestam*p) com a hora da criação. Com essas precauções podemos calcular o tempo T a partir do qual podemos ter certeza de que o pacote e suas confirmações causarão problemas. As técnicas utilizadas para evitar estes problemas são através da utilização de *timers* e números de seqüência e também através de um *handshake* de três vias.

Os problemas no encerramento de uma conexão estão relacionados ao fato de existirem três formas de encerramento, quais sejam: um dos usuários solicita desconexão, os dois solicitam desconexão simultaneamente ou a camada de transporte desiste e transmite pedido de desconexão para ambas as partes. Em todas as situações as liberações são abruptas e pode haver perda de dados.

6.1.1.4.5 - CONTROLE DE FLUXO E BUFFERIZAÇÃO

Existe uma certa semelhança com a camada de enlace, pois também evita que transmissor rápido sobrecarregue receptor lento, só que no caso o emissor e receptor são aplicações da rede. Um diferença é que um IMP tem número pequeno de linhas e os *hosts* podem ter um número indeterminado de conexões. A estratégia de "buferização" deve levar em consideração três questões relacionadas a estratégia a ser adotada pelo transmissor quanto a "buferização" de TPDUs enviadas. Isto deve ser feito quando:

1. o serviço de rede não é confiável (redes tipos B e C);
2. o receptor não pode garantir aceitação de todas as TPDUs recebidas;
3. confirmação da camada de rede só pode garantir recebimento, não confirmação.

Algumas das técnicas usadas para determinação de tamanho do *buffer* são:
1. *buffers* de tamanho fixo encadeados;
2. *buffers* de tamanho variável encadeados;
3. *buffer* circular estendido para cada conexão;
4. alocação dinâmica de *buffer*s.

6.1.1.5 - A CAMADA DE SESSÃO.

A **Camada de Sessão** é responsável dos estabelecimentos de sessões de diálogo para os usuários da rede. Uma sessão objetiva permitir o transporte de dados, da mesma forma que os serviços oferecidos pela camada de Transporte, mas ela oferece serviços mais sofisticados de comunicação que podem ser úteis a determinadas aplicações. Um exemplo disto é a possibilidade de envio, através de uma sessão, de um arquivo de dados (ou programa) de um sistema a outro. Outro serviço da camada de Sessão é efetuar a gestão do diálogo, ou seja, definir, por exemplo, se o diálogo vai ser efetuado em modo uni ou bidirecional.

Um serviço também importante é aquele da sincronização do diálogo. Por exemplo, se um arquivo deve ser transferido através de uma sessão e este deve durar duas horas. Se, por uma razão qualquer, o tempo médio entre duas panes é de uma hora. Após uma primeira interrupção por pane, a transferência deverá reiniciar, podendo ocasionar em erros de transmissão. Uma forma de evitar isto é a inserção de pontos de teste junto aos dados fazendo com que, após uma interrupção de transferência, os dados sejam retomados apenas a partir do último ponto de teste.

Segundo o modelo OSI, os usuários dos serviços de Sessão são as entidades de Apresentação. A principal função desta camada é oferecer aos seus usuários meios para o estabelecimento das conexões, denominadas sessões, de modo que estes possam trocar dados.

Uma sessão pode ser utilizada para permitir a conexão à distância a um computador, por exemplo, através de um terminal, para uma transferência de arquivo, para o carregamento de programas, etc.

No que diz respeito à conexão de Sessão (ou à sessão, como definido acima), pode-se estabelecer as diferentes possíveis relações entre uma conexão de Sessão e uma conexão de Transporte, como mostra a figura 6.7 que mostra, em (a) uma correspondência de 1 a 1 entre uma conexão de Sessão e uma de e em (b), uma mesma conexão de Transporte para suportar diferentes sessões. Ainda, pode-se ter o quadro inverso, onde, pela quebra de uma conexão de Transporte, a abertura de uma nova é providenciada para garantir a continuidade de uma mesma sessão. Este último cenário, ilustrado (c), se caracteriza, por exemplo, quando as entidades de Transporte assumem a tarefa de retomada de diálogo após uma pane.

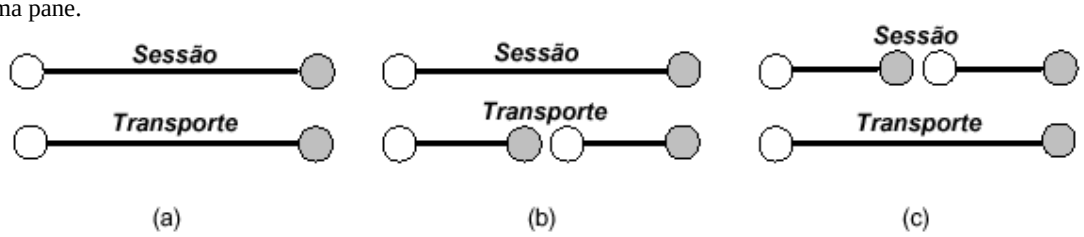


Figura 6.7 - Diferentes relações entre conexão de Sessão e de Transporte: (a) correspondência 1 a 1; (b) uma conexão de Transporte para várias sessões; (c) várias conexões de Transporte para uma única sessão.

A camada de Sessão deve cobrir igualmente os problemas relacionados à **sincronização**. Esta tarefa é útil para a manutenção da coerência do estado entre dois usuários interlocutores em caso de erro ou outro problema.

Apesar da camada de Transporte ter, por princípio, a função de cobrir todos os problemas relacionados à retomada após erros ou panes, esta camada cobre unicamente os problemas relacionados à transmissão de dados propriamente dita, não levando em conta os problemas que podem ocorrer nas camadas superiores. Estes erros podem ocasionar perdas de dados que a camada de Transporte é incapaz de detectar (uma vez que esta não é a sua função!).

A camada de Sessão vem, então, ao socorro do sistema efetuando a tarefa de sincronização, através da inserção a nível dos dados de **pontos de sincronização**, que permitem manter a sessão num estado correspondendo a um antigo ponto de sincronização. Um exemplo disto pode ser ilustrado na transmissão de um documento via rede, no qual este pode ser decomposto em páginas às quais se pode associar os pontos de sincronização. Neste caso, a **resincronização** vai consistir na retransmissão do documento a partir de uma dada página que estava sendo transmitida quando o problema ocorreu.

A sincronização é implementada da seguinte forma: o usuário emissor insere, nas suas mensagens, pontos de sincronização, cada ponto contendo um número de série. Quando um usuário envia uma primitiva *(reques*t) para inserir um ponto de sincronização, o outro usuário vai receber uma primitiva de *indicação* correspondente, isto ocorrendo de igual maneira no caso de uma resincronização.

É importante notar aqui que a camada de Sessão oferece unicamente as ferramentas para a solução dos problemas de erros e incoerência por sincronização/resincronização. Na realidade, quem ativa estas ferramentas quando da ocorrência de um problema são as entidades das camadas superiores.

6.1.1.6 - A CAMADA DE APRESENTAÇÃO.

A **Camada de Apresentação** utiliza algumas funções freqüentemente necessárias de modo a poupar o usuário deste trabalho. Esta camada assume particularmente as funções associadas à sintaxe e à semântica dos dados transmitidos. Um exemplo típico das funções efetuadas por esta camada é a codificação da informação num padrão bem definido (ASCII, EBCDIC, etc.).

Esta camada pode ainda suprir outras funções associadas à compreensão dos dados, se utilizando do conhecimento do significado da informação para reduzir a quantidade de informação enviada, inclusive para implementar funções de confidencialidade e de autenticação.

6.1.1.7 - A CAMADA DE APLICAÇÃO.

A **Camada de Aplicação** implementa um conjunto de protocolos bastante diversificado e orientado a aplicações bem definidas. Um exemplo disto é o protocolo de terminal virtual, que permite gerar a utilização de um determinado programa (por exemplo, um editor de textos) de forma independente do tipo de terminal conectado à rede. Outro serviço importante é o de transferência de arquivos, que permite adaptar o tipo do arquivo transferido à forma implementada pelo sistema de arquivamento do sistema considerado. Na parte dedicada a esta camada veremos, além destas, outras classes de serviços implementados a este nível.

A camada de Aplicação tem por função o gerenciamento dos programas de usuário (programas de aplicação) que executam em máquinas conectadas e utilizam o sistema de comunicação para a troca de informações.

Os programas de aplicação executados via sistema de comunicação baseada no modelo OSI vão utilizar-se dos serviços de comunicação oferecidos pela camada de Apresentação.

Esta camada é a que mantém o contato direto com os usuários da arquitetura de comunicação, abrindo caminho para todos os serviços oferecidos pelas camadas inferiores.

A grande diversidade das aplicações podendo ser construídas sobre uma arquitetura de comunicação e a questão da heterogeneidade dos sistemas, fator importante da concepção do modelo OSI, conduziu, no âmbito da ISO, à definição de uma arquitetura unificada para a camada de Aplicação, ALS *(Application Layer Structur*e), definida pela norma ISO 9545.

Nesta definição, a norma não propõe serviço de Aplicação, mas introduz um conjunto de conceitos relacionados à estrutura da camada, que pode servir como base para a definição de outras normas ou propostas de serviços de Aplicação.

Dado que a camada de Aplicação é a mais alta do modelo OSI, ela não fornece serviço a nenhuma outra camada, a noção de conexão ficando, então, inadequada no nível de Aplicação. Por outro lado, a comunicação entre entidades de Aplicação pares deve ser suportada por alguma forma de relação que permita a troca de informações de controle dos protocolos de Aplicação, esta forma de relação sendo definida como uma **Associação de Aplicação**.

Os elementos compondo a arquitetura da camada de Aplicação vão se utilizar as facilidades oferecidas pela camada de Apresentação para a manipulação e a representação de dados, e os mecanismos de controle de diálogo oferecidos pela camada de Sessão. As interações entre os programas aplicativos permitem modelar a operação cooperativa entre os sistemas abertos reais, necessitando porem o compartilhamento de uma quantidade de informações que viabilize estas interações, a fim de que o tratamento das atividades seja feito de maneira coerente.

Três tipos de informação são, particularmente, relacionados à natureza das interações entre os programas aplicativos:

1. o conjunto de objetos sujeito às atividades de tratamento de informação;
2. os procedimentos de controle e de cooperação do tratamento distribuído para a comunicação entre programas;
3. os estados das interações passadas entre programas de aplicação.

6.2 - O RM-OSI E AS REDES LOCAIS.

As Redes locais possuem características que afetam principalmente os níveis mais baixos de protocolo de uma arquitetura de rede. Esses níveis não devem deixar de levar em consideração o elevado desempenho, o baixo retardo, a baixa taxa de erros, o roteamento simples (em geral único) e as aplicações a que se destinam as redes locais.

O RM-OSI, embora teoricamente, possa ser utilizado tanto em redes geograficamente distribuídas como em redes locais, foi projetado para uso em redes geograficamente distribuídas. Sua aplicabilidade em redes locais não pode deixar de levar em consideração as características intrínsecas destas redes.

As distâncias limitadas a que são destinadas as redes locais permitem que seu protocolo de nível físico possa utilizar um meio de alta velocidade com baixíssimas taxas de erros. Este fato influencia muito os outros níveis de protocolos.

Várias diferenças existem na camada de enlace de dados, a começar pela delimitação dos quadros. Ao contrário das redes de longa distância, nas redes locais o método mais apropriado para delimitação de quadro pode ser a simples presença ou ausência de sinal no meio.

Devido ao alto desempenho do meio de transmissão e sua baixa taxa de erros, não cabe ao nível de enlace utilizar muitos bits de redundância para a recuperação de erros. Mais ainda, se levarmos em consideração que para determinadas aplicações os requisitos de tempo real são bem mais importantes do que sua confiabilidade exagerada da transmissão. Muitas vezes nem a recuperação de erros por retransmissão é desejável neste nível. Ao nível de enlace caberia apenas um esforço máximo para entregar pacotes de nível 3 sem erros, mas não a sua recuperação caso esse serviços ocorram.

Em redes locais as regras que disciplinam o acesso ao meio físico para transmissão de dados são chamadas protocolos de acesso. Como exemplo pode-se citar as regras para controle de acesso ao barramento compartilhado. Nas redes locais a transmissão de dados é feita por difusão ou possuem roteamento único. Neste sentido os protocolos de ligação poderiam estar no nível 2 do RM-OSI, uma vez que tratam do envio do pacote de uma máquina para outra, mas igualmente poderiam ser colocados no nível de rede uma vez que se trata do envio de um pacote da estação de origem até a estação de destino, isto é, fim-a-fim. Existem também propostas que os colocam no nível físico, uma vez que determinam a ligação física ao meio. O comitê de padronização de redes locais, o IEEE 802, os coloca como parte do nível 2.

Como nas redes locais a transmissão de dados é feita por difusão ou possuem roteamento único o nível de rede não tem aqui grande relevância. Em muitas redes o nível de transporte vai ser construído imediatamente acima do nível de enlace. Opcionalmente devemos permitir que o nível de transporte seja construído acima do nível inter-redes.

O nível 3 em redes locais teria então como função o roteamento de pacotes entre estação origem e destino em redes diferentes ou na interconexão de redes locais entre si. Neste nível ainda o mais adequado é a utilização de datagrama não confiável, deixando para os níveis superiores a recuperação, se necessária, dos erros. A arquitetura Internet TCP/IP, que utiliza essa abordagem, é uma alternativa bastante utilizada para interligação de redes locais de computadores.

Em redes locais o nível de transporte, ao tornar transparente para os níveis superiores toda a parte de transmissão, pode ainda tirar vantagem que o meio lhe oferece, como por exemplo, a confirmação de vários circuitos virtuais em uma única mensagem em uma rede do tipo difusão. A implementação dos demais níveis de protocolo depende muito das aplicações da rede. O RM-OSI pode ser seguido na íntegra, podendo suas funções serem realizadas por processos de um sistema operacional distribuído, onde a interface do nível 4 seria vista simplesmente como primitivas de comunicação do núcleo desse mesmo sistema operacional.

6.3 - O PADRÃO IEEE 802.

O projeto IEEE 802 teve origem na Sociedade de Computação do Instituto de Engenheiros Eletricistas e Eletrônicos dos EUA, ou IEEE Computer Society. O comitê 802 publicou um conjunto de padrões que foram adotados como padrões nacionais americanos pelo American National Standards Institute (ANSI). Estes padrões foram posteriormente revisados e republicados como padrões internacionais pela ISO com a designação ISO 8802.

O objetivo foi o estabelecido de uma arquitetura padrão, orientada para o desenvolvimento de redes locais, que apresentasse as seguintes características:

1. correspondência máxima com o RM-OSI;
2. interconexão eficiente de equipamentos a um custo moderado;
3. implantação da arquitetura a custo moderado.

A estratégia adotada na elaboração da arquitetura IEEE 802 é a de definir mais de um padrão de forma a

atender aos requisitos dos sistemas usuários da rede. Na verdade, a arquitetura IEEE 802 pode ser vista como uma adaptação das duas camadas inferiores da arquitetura RM-OSI da ISO. Nesta arquitetura existem 3 camadas, ou seja, uma equivalente à camada física e duas sub-camadas que juntas equivalem a camada de enlace. Elas são assim denominadas:

1. camada física (PHY);
2. sub-camada de controle de acesso ao meio (MAC);
3. sub-camada de controle de enlace lógico (LLC).

Para atender o modelo elaborado devemos observar que as funções de comunicação mínimas e essenciais de uma rede local, equivalentes aos níveis inferiores do RM-OSI, podem ser assim definidas:

1. fornecer um ou mais SAPs (pontos de acesso ao serviço) para os usuários da rede;
2. na transmissão, montar os dados a serem transmitidos em quadros com campos de endereço e detecção de erros;
3. na recepção, desmontar os quadros, efetuando o reconhecimento de endereço e detecção de erros;
4. gerenciar a comunicação no enlace.

Estas quatro funções são fornecidas pelo nível de enlace do RM-OSI. A primeira função, as sub-funções a ela relacionadas, são agrupadas pelo IEEE 802 na camada Logical Link Control (LLC). As três restantes são tratadas em uma camada separada, chamada Medium Access Control (MAC), que podem, então, ser otimizadas para as diferentes topologias de redes locais, mantendo uma interface única, a camada LLC, para os usuários da rede local.

Em um nível físico, mais baixo, estão as funções normalmente associadas ao nível físico: codificação/decodificação de sinais, geração e remoção de preâmbulos para sincronização e transmissão/recepção de bits. Como no RM-OSI, essas funções foram atribuídas ao nível físico no modelo de referência elaborado pelo IEEE 802.

A figura 6.8 apresenta a relação entre alguns dos principais padrões IEEE 802 e o RM-OSI. É importante ressaltar que já existem outros padrões IEEE 802.X, que já foram ou serão aqui citados, tais como IEEE 802.11 (FDDI) e IEEE 802.12 (100VGAnyLAN).

O padrão IEEE 802.1 é um documento que descreve o relacionamento entre os diversos padrões IEEE 802 e o relacionamento deles com o modelo de referência OSI. Este documento contém também padrões para gerenciamento da rede e informações para ligação inter-redes. O padrão ANSI/IEEE 802.2 (ISO 8802/2) descreve a sub-camada superior do nível de enlace, que utiliza o protocolo Logical Link Control Protocol. Os outros padrões que aparecem na figura 6.8 especificam diferentes opções de nível físico e protocolos da sub-camada MAC para diferentes tecnologias de redes locais. São eles:

1. padrão IEEE 802.3 (ISO 8802/3), rede em barra utilizando **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) como método de acesso;
2. padrão IEEE 802.4 (ISO 8802/4), rede em barra utilizando passagem de permissão como método de acesso;
3. padrão IEEE 802.5 (ISO 8802/5), rede em anel utilizando passagem de permissão como método de acesso;
4. padrão IEEE 802.6 (ISO 8802/6), rede em barra utilizando o Distributed Queue Dual Bus (DQDB) como método de acesso.

Os padrões IEEE 802.3 (CSMA/CD) e IEEE 802.5 (Token Ring) são os mais conhecidos em função de terem sido a base para os produtos **Ethernet** (Xerox, Digital, etc.) e Token Ring (IBM). O padrão IEEE 802.4 é denominado Token Bus e o padrão IEEE 802.6 é denominado DQDB. Há ainda a definição de vários padrões dentro deste projeto.

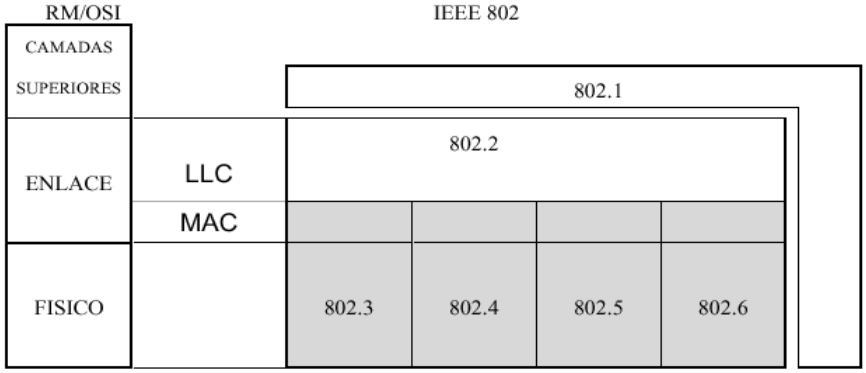


Figura 6.8 - Relação entre os padrões RM-OSI e IEEE 802.

6.4 - INTERCONEXÃO DE REDES LOCAIS.

A interconexão de redes locais é uma necessidade nos dias atuais. Esta é a tarefa mais importante da camada de rede em redes locais. Ela se faz necessária quando máquinas origem e destino estão em redes diferentes. Na execução da função de ligar rede locais entre si pode-se criar topologias parcialmente ligadas fazendo com que existam caminhos diferentes por redes intermediárias, com diferentes protocolos. O principal problema que decorre disto é que existem diversos tipos de redes com características próprias. Assim, a tarefa do nível de rede é compatibilizar as diferentes tecnologias e protocolos empregados nas redes a serem interconectadas.

Nem sempre a interconexão de redes exige alto grau de complexidade. Por vezes é apenas necessário ligar dois segmentos de rede exatamente iguais, ou que possuam apenas o meio físico diferente. Por exemplo, quando desejamos interconectar duas redes Ethernet com cabeamento diferente. Outro problema, um pouco mais complexo, seria interconectar duas redes com protocolos de acesso diferentes, porém com o mesmo protocolo de rede. Por exemplo, se desejarmos interconectar uma rede Ethernet com uma rede Token Ring.

As motivações que podem levar à necessidade de interconectar de redes entre si são:
1. de ordem econômica, por exemplo, para compartilhar uma interface de rede pública;
2. de ordem tecnológica, por exemplo, para interconectar várias redes locais em áreas ou prédios distintos;
3. para melhorar desempenho e confiabilidade, por exemplo, dividir uma rede local com grande número de estações em 2 ou mais redes;
4. de ordem funcional, por exemplo, para atender necessidades do usuário, tais como acesso a recursos como bancos de dados, disponíveis em outras redes.

Algumas questões a serem abordadas para a interconexão:
1. endereçamento e encaminhamento das mensagens;
2. fragmentação das mensagens;
3. detecção e recuperação de erros;
4. serviço com ou sem conexão;
5. nível de interconexão;
6. controle de fluxo;
7. controle de congestionamento;
8. segurança;
9. tarifação de serviços;
10. nomes e endereçamento.

A ligação entre equipamentos heterogêneos deve ter convenções para representação de nomes e endereços de processos que tenham significado em toda a rede. As referências às redes são feitas por nomes ou por endereços, e isto é importante para identificação de recursos na rede. A maneira mais comum é o endereçamento hierárquico, ou seja, o endereço do processo constituído de endereço da rede, endereço do equipamento hospedeiro (host) e endereço dentro do hospedeiro (porta). Há também uma alternativa, o endereçamento plano, ou não-hierárquico, onde há um endereço para cada recurso na rede.

É importante lembrar que a interconexão de duas redes exige a implementação, em cada rede, de um protocolo inter-redes que realize, pelo menos, as funções de tratamento de endereços. Os principais equipamentos para interconexão de redes são: repetidores, pontes e roteadores.

6.5 - A ARQUITETURA TCP/IP – INTERNET.

A arquitetura Internet é largamente utilizada para interconexão e interoperação de sistemas computacionais heterogêneos. Tal arquitetura foi lançada pelo Departamento de Defesa do governo americano e escolhida para ser o padrão obrigatório de comunicação entre os diversos sistemas daquela organização. Ela tornou-se um padrão de fato do mercado. Seus padrões não são definidos por entidades de padronização internacional como a ISO, por exemplo. As definições dos protocolos são encontradas em documentos denominados **RFC** (Request for Comments), os quais são elaborados pelo **IAB** (Internet Activities Board).

A arquitetura Internet também é organizada em camadas. Ela é composta por dois protocolos principais: o **IP (Internet Protocol)** e o **TCP (Transmission Control Protocol**). O IP é responsável pelo encaminhamento de pacotes de dados através das diversas sub-redes, desde a origem até o seu destino. O TCP tem por função o transporte fim-a-fim, confiável, de mensagens de dados entre dois sistemas.

O IP é um protocolo do tipo datagrama, operando, portanto, no modo não orientado à conexão, enquanto o TCP é um protocolo de transporte orientado à conexão.

O conjunto TCP/IP pode, desta forma, oferecer um serviço relativamente confiável. Para uso em redes de alta qualidade, onde o problema de confiabilidade não assume grande importância, foi definido o protocolo UDP (User Datagram Protocol) que opera no modo não orientado à conexão e possui funcionalidades bem mais simplificadas que o TCP.

Dentre os protocolos correspondentes de cada camada, o protocolo IP é que desempenha as atividades mais importantes de toda a arquitetura. O IP tem como função a fragmentação/desfragmentação e o roteamento de unidades de dados através dos equipamentos roteadores existentes no caminho a ser seguido até o destino da comunicação.

O IP atualmente se encontra na versão 4.0 que foi apresentada em 1978 e possui problemas para ser utilizado nos dias atuais, dentre os quais destacam-se a baixa quantidade de endereços de interfaces oferecido, a não hierarquização dos endereços e a falta de recursos de segurança e de controle de qualidade de serviço para a transmissão dos dados. Devido a esses e outros problemas, além da necessidade de inclusão de novos requisitos tecnológicos a este protocolo, está sendo criado uma nova versão do IP, o IPv6 (ou IPng).

A Internet cresceu muito além do que se podia imaginar. A Internet é hoje uma coleção de redes acadêmicas, militares e comerciais espalhadas pelo mundo, interconectadas através do protocolo TCP/IP.

Uma vez que toda a rede conectada à Internet deve falar o protocolo TCP/IP, é natural que o interesse comercial por este protocolo tenha crescido muito, ao ponto de hoje estar disponível em quase todas as plataformas. Além disso, é comum encontrarmos TCP/IP sendo utilizado em redes locais que não estão conectadas à Internet.

O sucesso e a popularidade do protocolo TCP/IP não se deve apenas à imposição das agências militares americanas, mas também ao fato der ter sido o primeiro protocolo a atingir a importante meta da comunicação de dados com abrangência mundial. Isto somente foi possível graças a algumas de suas características:

1. TCP/IP é um protocolo aberto, público e completamente independente de equipamentos e de sistemas operacionais;
2. TCP/IP não define protocolos para o nível físico, possibilitando sua implementação sobre uma grande variedade de protocolos já existentes, tais como: Ethernet, Token Ring e X.25;
3. O esquema de endereçamento do TCP/IP permite designar univocamente qualquer máquina, mesmo em redes globais como a Internet;
4. TCP/IP inclui protocolos do nível de aplicação que atendem muito bem à demanda de serviços imposta pelos usuários.

Uma vez que a padronização foi essencial para a definição do TCP/IP como o protocolo mais utilizado no mundo, é importante que se conheça como ele foi, e continua sendo, padronizado.

Originalmente, os protocolos básicos do TCP/IP foram padronizados através de Military Standards (MILSTD) e de Internet Engineering Notes (IEN). Atualmente, a maior parte da padronização do TCP/IP é feita através de Requests For Comments (RFC), que, além da especificação formal dos protocolos, inclui informações importantes sobre seu funcionamento e uso.

6.5.1 - AS CAMADAS DO TCP/IP.

A descrição da arquitetura do protocolo TCP/IP em camadas como as do modelo de referência OSI é controversa. As camadas OSI foram definidas por pesquisadores ao longo de anos, sempre com o compromisso acadêmico de ser um modelo de referência, enquanto que o protocolo TCP/IP não teve qualquer compromisso que não a funcionalidade. Assim sendo, tentar estabelecer uma relação precisa entre as camadas OSI e TCP/IP é algo praticamente impossível.

O modelo mais aceito para descrever a arquitetura TCP/IP é composto de quatro camadas: acesso à rede (ou camada de interface) , Internet (ou camada de rede), transporte e aplicação. Este modelo é apresentado na figura 6.9, em comparação ao modelo de referência OSI.

Da mesma forma que no modelo de referência OSI, os dados descem a pilha de protocolos para chegar a rede e sobem para chegar às aplicações. Cada camada da pilha de protocolos adiciona um cabeçalho com informações de controle e trata o que recebe da camada superior como sendo dados. Esta adição de informações de controle em cada nível é denominada encapsulamento e é ilustrada pela figura 6.10. O processo reverso acontece quando uma camada passa dados às superiores, ou seja, o cabeçalho é removido e o restante é passado para cima como dados.

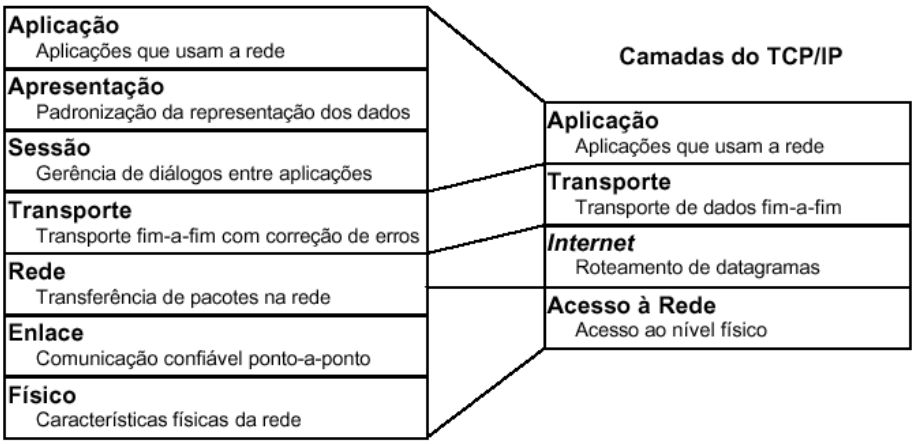


Figura 6.9 – Camadas da arquitetura TCP/IP em comparação com as camadas do RM-OSI

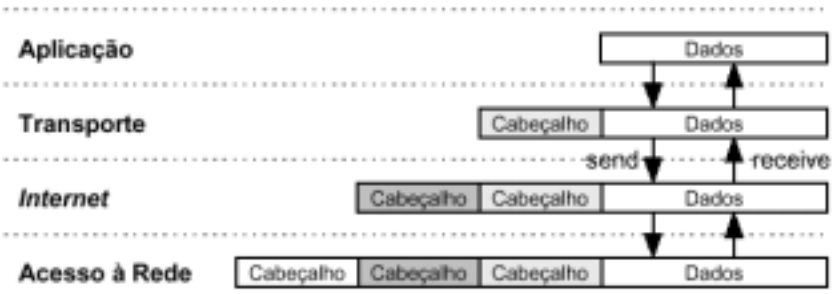


Figura 6.10 - Encapsulamento de dados na pilha TCP/IP.

Cada camada da pilha possui estruturas de dados próprias e independentes. Assim sendo, cada protocolo faz referência aos dados de forma específica. Por exemplo, aplicações que fazem uso do protocolo TCP se referem aos dados como streams, ao passo que aplicações que fazem uso do protocolo User Datagram Protocol (UDP) se referem aos dados como mensagens. O protocolo TCP, por sua vez, se refere aos dados como segmentos, enquanto que o UDP se refere aos dados como pacotes. O protocolo IP sempre se refere aos dados como datagramas, enquanto que os dados passados à camada de acesso à rede são referidos como frames ou quadros.

6.5.1.1 - A CAMADA DE ACESSO À REDE.

A **Camada de Acesso à Rede (ou Camada de Interface)** é a mais baixa na hierarquia de protocolos TCP/IP. Os protocolos nesta camada provêem meios para que os dados sejam transmitidos a outros computadores na mesma rede física. Esta camada pode abranger as três primeiras camadas do modelo de referência OSI: física, de enlace e de rede. Entretanto, a camada de acesso à rede do TCP/IP não define propriamente os protocolos para estes três níveis, mas sim como utilizar os protocolos já existentes para suportar a transmissão de um datagrama IP. À medida que novas tecnologias de rede vão surgindo, novos protocolos são acrescidos à camada de acesso à rede. As principais funções da camada de acesso à rede são: o encapsulamento de datagramas IP em *frames* para transmissão e a tradução de endereços IP em endereços físicos de rede. Estas duas funções apresentam implementações específicas para cada tipo de rede.

6.5.1.2 - A CAMADA INTERNET.

A **Camada Internet (ou Camada de Rede)** fica exatamente sobre a camada de acesso à rede. O *Internet Protocol* (IP), é o coração desta camada. Ele provê um serviço básico de datagrama sobre o qual as redes TCP/IP são implementadas. Todos os protocolos das camadas superiores a esta fazem uso do protocolo IP. As principais funções do protocolo IP são:

1. definir o datagrama IP, que é a unidade básica de transmissão de dados da arquitetura TCP/IP;
2. definir o esquema de endereçamento IP;

3. passar dados da camada de acesso à rede à camada de transporte;
4. rotear datagramas IP;
5. fragmentar e remontar datagramas IP.

O **IP** é um protocolo não orientado a conexão, ou seja, não existe negociação prévia de uma conexão para a transmissão de dados. Isto não impede a existência de protocolos orientados à conexão nas camadas superiores, mas eles deverão negociar o estabelecimento de conexões por si próprios. Além de ser não orientado à conexão, o protocolo IP também é não confiável, uma vez que não suporta mecanismos de detecção e recuperação de erros. Em outras palavras, o protocolo IP não verifica se um datagrama foi recebido corretamente, deixando esta responsabilidade para os protocolos das camadas superiores.

Outros protocolos da Camada Internet são o *Internet Message Control Protocol* (ICMP) e o *Address Resolution Protocol* (ARP).

O **ICMP** é utilizado para enviar alertas aos hosts sobre anormalias na rede. Também é utilizado para a obtenção de informações sobre a rede. O comando "PING", muito utilizado para verificar se um *host* está ativo, é uma aplicação do ICMP.

O **ARP** é um protocolo de resolução de endereços que permite a associação dos endereços físicos das interfaces de rede com a numeração promovida pelo endereçamento do protocolo IP.

6.5.1.3 - A CAMADA DE TRANSPORTE.

A **Camada de Transporte** fim-a-fim está localizada exatamente sobre a camada Internet na hierarquia TCP/IP. Os principais protocolos desta camada são: *Transmission Control Protocol* (TCP), o *User Datagram Protocol* (UDP).

O **TCP** é um protocolo orientado a conexão com detecção e correção de erros fim-a-fim. O **UDP** é um protocolo não orientado a conexão e não confiável, sendo portanto muito leve. Ambos os protocolos passam dados entre as camadas de aplicação e Internet. Cada aplicação é livre para escolher o protocolo que melhor se adapta a sua natureza.

O User Datagram Protocol (UDP) provê meios para que aplicações tenham acesso direto ao serviço de datagrama IP. Aplicações que usam este protocolo inserem pouco overhead na rede. Como o próprio IP, o protocolo UDP é não orientado a conexão e não confiável. Note que a expressão não confiável implica apenas a inexistência de mecanismos de confirmação do correto recebimento do datagrama. O protocolo UDP é utilizado principalmente por aplicações que transmitem dados em pequenas quantidades, de tal forma que o overhead de uma conexão é maior do que o da retransmissão dos dados em caso de erro. Além disto, as aplicações do modelo cliente/servidor freqüentemente fazem uso de protocolos do tipo requisição/resposta que são melhor implementados sobre UDP, uma vez que não existem conexões preestabelecidas entre clientes e servidores.

O Transmission Control Protocol (TCP) é um protocolo orientado a conexão e confiável. A transmissão de dados através de uma conexão, ou stream, se dá através de segmentos. De forma similar ao pacote UDP, cada segmento carrega informações sobre as aplicações origem e destino (ports).

Os protocolos da camada de transporte serão estudados com mais profundidade posteriormente.

6.5.1.4 - A CAMADA DE APLICAÇÃO.

A **Camada de Aplicação** fica no topo da pilha TCP/IP e inclui todos os processos que utilizam serviços das camadas inferiores para transmitir dados através da rede. Alguns protocolos desta camada são :

1. Telnet: serviço de terminal virtual que permite sessões remotas sobre a rede;
2. File Transfer Protocol (FTP): serviço de transferência de arquivos pela rede;
3. Simple Mail Transfer Protocol (SMTP): serviço de correio eletrônico;
4. Domain Name Service (DNS): serviço de tradução de nomes de hosts em endereços IP;
5. Routing Information Protocol (RIP): suporta a troca de informações de roteamento entre gateways;
6. Network File System (NFS): sistema de arquivos remotamente acessíveis.

A figura 6.11 demonstra o processamento de uma solicitação para transferência de arquivo entre 2 computadores através da arquitetura TCP/IP em uma aplicação baseada no FTP – "File Transfer Protocol". C.4, C.3,

C.2 e C.1 são as camadas de aplicação (no caso FTP), de transporte (o TCP), internet (o IP) e de acesso ao meio que varia conforme o enlace físico sendo, no caso,: PPP, Ethernet - ETH e "Asynchronous Transfer Mode" - ATM.

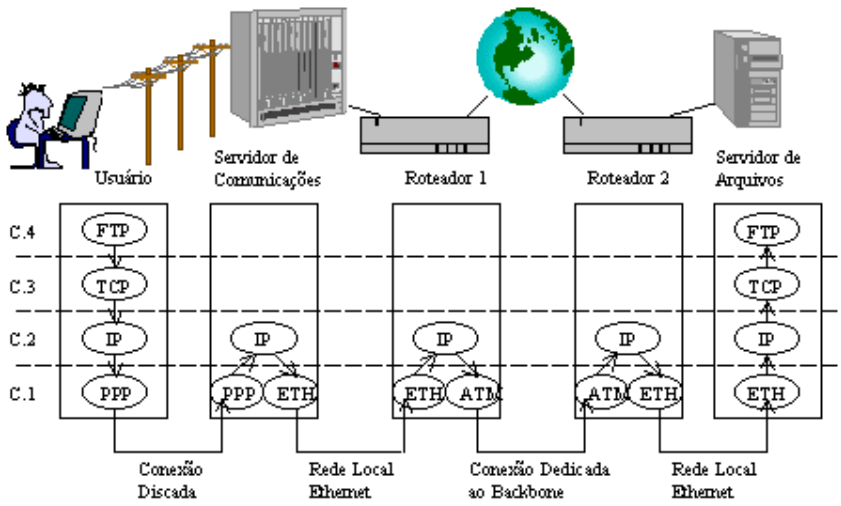


Figura 6.11 - Processamento de uma requisição FTP através da arquitetura TCP/IP

A figura 6.11 também ilustra uma das formas mais comuns de acesso à Internet:

1. O usuário utiliza um computador ligado a uma linha telefônica por um MODEM e conecta-se a um Provedor de Acesso, representado pelo Servidor de Comunicação e pelo Roteador 1.
2. O Provedor de Acesso recebe o usuário pelo servidor de comunicação e atribui ao seu computador um endereço para que as informações enviadas e recebidas possam trafegar pela arquitetura TCP/IP.
3. Uma vez conectado e com o endereço correto, a aplicação requisitada pelo usuário passa a trafegar através de roteadores e "backbones", representados pelo globo terrestre, até encontrar o seu destino.
4. No destino, sua requisição é atendida e enviada de volta, pelo mesmo principio de identificação de endereços de origem e destino.

6.5.2 – ENDEREÇAMENTO IP.

Como já vimos. o protocolo IP é responsável pelo **endereçamento** dos componentes ativos em uma rede de arquitetura TCP/IP. Ele atua na camada internet e sua unidade de informação é o datagrama (ou pacote) que, entre outras informações, possui o número identificador do equipamento origem da informação transportada e o número do equipamento de destino. O endereçamento baseado em um identificador, que independe da tecnologia de interconexão envolvida, é obtido em uma representação binária de 32 bits que deve ser único na rede. No caso da Internet, não existem dois equipamentos com o mesmo identificador em todo o mundo.

O formato de apresentação dos endereços IP é uma representação decimal em grupos de 4 dígitos separados por ponto. Teoricamente, esses endereços variam de 0.0.0.0 até 255.255.255.255 - pois 255_{10} é a representação decimal de 11111111_2 , valor máximo representado com 8 algarismos binários ou 1 byte. A figura 6.12 exemplifica a representação decimal de um endereço IP.

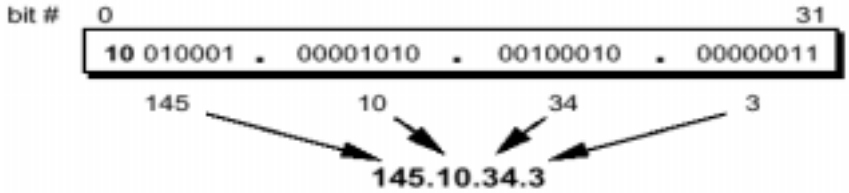


Figura 6.12 - Representação de um endereço IP.

As sequências numéricas que identificam redes e equipamentos a ela associados, são organizadas na forma de classes. Cada byte do endereço pode significar uma rede ou um host, dependendo da classe a qual o endereço pertence.

As classes definidas pelo InterNIC para a Internet são:

CLASSE A - o primeiro byte representa o número da rede e os três restantes são números de hosts.

CLASSE B - os dois primeiros bytes representam o número da rede e os dois restantes são números de hosts.

CLASSE C - o último byte representa números de hosts e os três primeiros identificam a rede.

CLASSE D - Especifica "multicast address" utilizados para transmissão simultânea de informação a um grupo de hosts identificados por um endereço especial de destino.

CLASSE E - Reservada para uso futuro.

A figura 6.13 detalha as faixas de endereçamento das classes A, B e C.

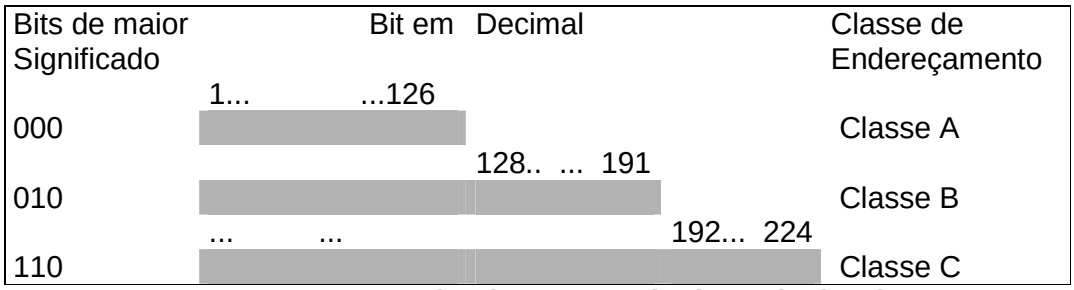


Figura 6.13 - Faixas de endereçamento IP das classes adotadas pelo InterNIC.

Pela convenção apresentada, é possível identificar a classe e, através dela, o endereço de rede e do host na rede IP. Como exemplos:

1 - O endereço 200.195.20.37 pertence à classe C - o primeiro byte é maior que 192. Portanto, o endereço de rede é composto dos 3 primeiros bytes, ou seja, 200.195.20 e o endereço do equipamento ligado a esta rede é .37.

2 - O endereço 128.127.50.112 pertence à classe B - o primeiro byte é maior que 127 e menor que 191. Portanto o endereço de rede é composto dos 2 primeiros bytes: 128.127 e o endereço do equipamento pertencente a esta rede é .50.112.

O InterNIC convencionou os seguintes endereços para redes internas, definidas no documento RFC1597, e que não estão disponíveis em redes ligadas à Internet :

10.0.0.1 até 10.255.255.255	Classe A
172.16.0.0 até 172.31.255.255	Classe B
192.168.0.0 até 192.168.255.255	Classe C

Alguns endereços são reservados para funções especiais:

1. **Endereço de Rede**: Identifica a própria rede e não uma interface de rede específica, representado por todos os bits de hostid com o valor ZERO.
2. **Endereço de Broadcast**: Identifica todas as máquinas na rede específica, representado por todos os bits de hostid com o valor UM.
3. **Endereço de Broadcast Limitado**: Identifica um broadcast na própria rede, sem especificar a que rede pertence. Representado por todos os bits do endereço iguais a UM = 255.255.255.255.
4. **Endereço de Loopback**: O endereço de rede 127.0.0.0 é reservado para o tráfego local da máquina. Normalmente o endereço 127.0.0.1 é definido para uma interface especial denominada interface local (loopback interface) ou local host, que atua como um circuito fechado. Qualquer pacote IP enviado para esta interface a partir dos protocolos TCP ou UDP será retornado ao próprio host que o enviou como se estivesse chegando da rede.

Desta forma, para cada rede A, B ou C, o primeiro endereço e o último são reservados e não podem ser usados por interfaces de rede.

As máquinas com mais de uma interface de rede (caso dos roteadores ou máquinas interligadas à mais de uma rede, mas que não efetuam a função de roteamento) possuem um endereço IP para cada uma, e podem ser identificados por qualquer um dos dois de modo independente. Um endereço IP identifica não uma máquina, mas uma conexão à

rede.

Para interligar uma rede à Internet, é necessário requisitar um bloco de endereços ao orgão responsável pelo controle da numeração IP designado como responsável para a área geográfica onde a rede se encontra. No Brasil, existem empresas, entidades e orgãos governamentais que oferecem backbone Internet. Esses provedores de backbone normalmente se incumbem de fornecer o bloco numérico de IP.

Os endereços de computadores e redes oferecidos pelo protocolo IP não são suficientes para localizar uma aplicação ou serviço na rede. Existe um outro identificador para serviços denominado "port" associado a um protocolo da camada de transporte (TCP ou UCP) para o estabelecimento de comunicação entre a aplicação que gera o serviço e o usuário que irá utilizá-la. O conjunto: IP + PORT + (TCP ou UDP), é denominado "socket". Existem "ports" convencionados na Internet para serviços utilizados em toda a rede. Os mais difundidos são:

Serviço:	"Port":	Protocolo:
FTP	21	TCP
TELNET	23	TCP
SMTP	25	TCP
POP3	110	TCP
DNS	53	UDP
HTTP	80	TCP

6.5.2.1 - REDES IP.

Redes IP estão estruturadas de uma forma similar aos Correios. Toda a Internet consiste em um número de redes próprias, denominadas sistemas autônomos. Cada sistema destes executa qualquer roteamento interno entre seus membros, porém a tarefa de entregar um datagrama resume-se em encontrar-se um caminho para a rede da máquina de destino. Isso significa que assim que o datagrama é enviado para qualquer máquina que esteja em uma rede, processos adicionais são executados exclusivamente pela rede de destino (como no caso dos correios locais).

Ao se escrever uma carta para alguém, deve ser colocado o endereço completo do destinatário no envelope, especificando-se o País, Estado, CEP, etc. Após isso ela é colocada em uma caixa de correio e os Correios a enviarão para o seu destino: a carta vai até o País indicado, onde o serviço de correio local a enviará para o estado indicado, para a cidade de destino, etc. A vantagem deste sistema hierárquico é óbvia: toda vez que uma carta for postada, o correio local saberá o endereço do destinatário, mas não tem que se preocupar em como a carta irá viajar até chegar ao seu destino Final. Assim funcionam as redes IP.

A figura 6.14 abaixo mostra exemplos de endereçamento de máquinas situadas na mesma rede e em redes diferentes. Pode ser observado que como o endereço começa por 200, eles são de classe C. Por isto, os três primeiros bytes do endereço identificam a rede. Como na primeira figura, ambas as estações tem o endereço começando por 200.18.171, elas estão na mesma rede. Na segunda figura, as estações estão em redes distintas e uma possível topologia é mostrada, onde um roteador interliga diretamente as duas redes.

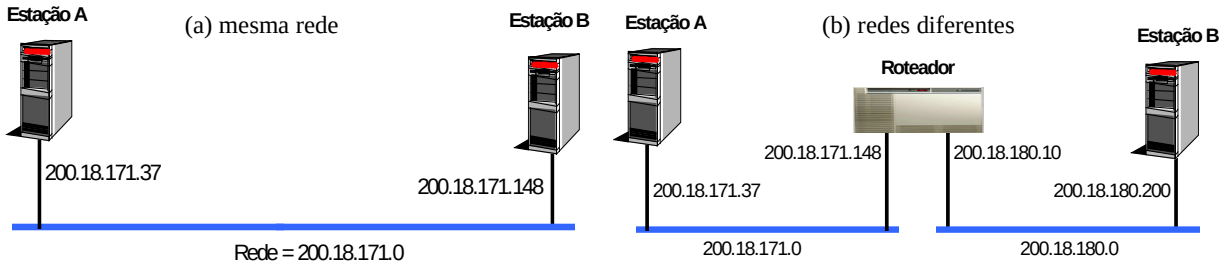


Figura 6.14 - Exemplos de endereçamento de máquinas situadas (a) na mesma rede e (b) em redes diferentes

6.5.2.2 - SUB-REDES IP.

A estrutura de sub-redes IP (*subnet*) é produzida através da divisão de um endereço IP em uma parte destinada à identificação da rede e outra parte destinada à máquina. Por padrão a rede de destino é derivada da parte do endereço

IP definida para redes. Obviamente, hosts com endereços IP de rede idênticos devem estar localizadas na mesma rede.

A RFC 950, de 1985, define o procedimento padrão de suporte à sub-redes e a divisão de redes classes A,B e C em partes menores.

O protocolo IP permite a divisão de uma rede IP em diversas sub-redes. Uma sub-rede assume a responsabilidade pela entrega de datagramas em uma determinada faixa de endereços IP de uma rede IP da qual ela faça parte. Assim como nas classes de rede A, B ou C, ela é identificada pela parte de rede do endereço IP. A parte de rede é porém expandida, incluindo-se alguns bits da parte de endereço de máquina. O número de bits que são interpretados como o número da sub-rede é definido pelo parâmetro denominado máscara de sub-rede, ou sub*net mask*. Esta é composta por um número de 32 bits que especifica a parte de rede do endereço IP. Os bits do endereço IP e da máscara de sub-rede têm correspondência em um para um. Para obter o endereço de rede, é realizada uma operação lógica AND entre os bits do endereço IP e os bits da máscara de sub-rede. Na máscara de sub-rede, o bit 1(um) indica endereço de rede e o bit 0 (zero) endereço de host. O exemplo seguinte demonstra a constituição de uma mascara de sub-rede.

	Notação Decimal	Notação Binária
Endereço IP	130.5.5.1	10000010.00000101.00000101.00000001
Máscara de sub-rede	255.255.0.0	11111111.11111111.00000000.00000000
	Operação AND para obter o endereço de rede	10000010.00000101.00000000.00000000
Endereço de rede IP	130.5.0.0	

A máscara de sub-rede 255.255.0.0 é característica da Classe B. Do mesmo modo, a Classe A é definida pela máscara 255.0.0.0 e a Classe C por 255.255.255.0.

Existe outro modo convencionado para representar máscaras de sub-rede. Elas podem ser representadas por um valor decimal correspondente ao número de bits 1 (um) utilizados para compor a máscara colocado logo após o endereço IP. Para separar o valor que representa a máscara de sub-rede do número IP utiliza-se uma barra (/). Exemplificando, no quadro acima o endereço IP 130.5.5.1 e sua máscara 255.255.0.0 podem ser descritos da seguinte maneira: 130.5.5.1/16, pois 16 é o número de bits 1 (um) utilizado na máscara de sub-rede.

É importante frisar que a definição de sub-rede é somente uma divisão interna da rede. Sub-redes são geradas pelos administradores locais das redes. Freqüentemente, sub-redes são criadas para redefinir limites existentes, sejam físicos (entre duas redes Ethernets), administrativos (entre dois departamentos) ou geográficos, sendo que a autoridade sobre essas sub-redes é delegada a alguma pessoa de contato. De qualquer forma, esta estrutura afeta somente o comportamento interno da rede e é completamente invisível para o mundo externo.

Para ilustrar a criação de sub-redes IP em uma rede IP de classe C, vamos dividir a rede IP 193.1.1.0/24 em oito sub-redes.

```
Base Net:  11000001.00000001.00000001.00000000 = 193.1.1.0/24

Subnet #0: 11000001.00000001.00000001.00000000 = 193.1.1.0/27
Subnet #1: 11000001.00000001.00000001.00100000 = 193.1.1.32/27
Subnet #2: 11000001.00000001.00000001.01000000 = 193.1.1.64/27
Subnet #3: 11000001.00000001.00000001.01100000 = 193.1.1.96/27
Subnet #4: 11000001.00000001.00000001.10000000 = 193.1.1.128/27
Subnet #5: 11000001.00000001.00000001.10100000 = 193.1.1.160/27
Subnet #6: 11000001.00000001.00000001.11000000 = 193.1.1.192/27
Subnet #7: 11000001.00000001.00000001.11100000 = 193.1.1.224/27
```

Podemos observar que a máscara utilizada para obter oito sub-redes é /27, porque a máscara padrão para uma rede IP classe C é 255.255.255.0 (24 bits com valor igual a 1) e além dela foram elevados para 1 (um) mais três bits (24 + 3 = 27). Em binário: 11111111.11111111.11111111.**11100000.** Convertendo-se 11100000_2 para decimal teremos o valor $224_{10.}$ Então esta máscara pode ser escrita também como sendo: 255.255.255.224.

Os endereços das sub-redes formadas pela aplicação da máscara serão os que resultam da aplicação da operação AND, como descrito acima. Assim, serão endereços de rede IP no exemplo acima: 193.1.1.0/27; 193.1.1.32/27; 193.1.1.64/27; 193.1.1.96/27; 193.1.1.128/27; 193.1.1.160/27; 193.1.1.192/27 e 193.1.1.224/27. O último endereço de cada conjunto de IPs formado é utilizado pela rede para *broadcasting*, ou seja, para acesso simultâneo a todos os endereços válidos do conjunto. Então, serão endereços de *broadcasting* no exemplo:

193.1.1.31/27; 193.1.1.63/27; 193.1.1.95/27; 193.1.1.127/27; 193.1.1.159/27; 193.1.1.191/27; 193.1.1.223/27 e 193.1.1.255/27.

Para saber quantos endereços poderão ser utilizados em cada sub-rede com a aplicação de uma determinada máscara basta aplicar a seguinte fórmula:

$$\text{número de endereços válidos} = 2^{(\text{número de bits iguais a zero da máscara de sub-rede})} - 2$$

Para saber quantss sub-redes serão geradas com a aplicação de uma determinada máscara basta aplicar a seguinte fórmula:

$$\text{número de sub-redes} = 2^{(\text{número de bits iguais a um da máscara de sub-rede})}$$

6.5.2.3 - RESOLUÇÃO DE ENDEREÇOS IP EM ENDEREÇOS DE REDE.

Os protocolos de rede compartilhada como Ethernet, Token-Ring e FDDI possuem um endereço próprio para identificar as diversas máquinas situadas na rede. Em Ethernet e Token-Ring o endereçamento utilizado é chamado endereço físico ou endereço MAC - Medium Access Control , formado por 6 bytes, conforme a figura 6.15 abaixo:

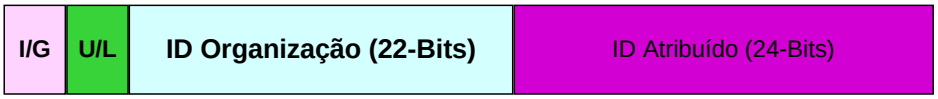


Figura 6.15 – Constituição do endereço MAC.

Este tipo de endereçamento só é útil para identificar diversas máquinas, não possuindo nenhuma informação capaz de distinguir redes distintas. Para que uma máquina com protocolo IP envie um pacote para outra máquina situada na mesma rede, ela deve se basear no protocolo de rede local, já que é necessário saber o endereço físico. Como o protocolo IP só identifica uma máquina pelo endereço IP, deve haver uma associação entre o endereço IP e o endereço de rede MAC. Esta associação, realizada pelo protocolo *Address Resolution Protocol* (ARP) é conhecida como mapeamento.

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

A figura 6.16 mostra uma rede com 3 estações, onde uma máquina A com endereço IP 200.18.171.1 deseja enviar uma mensagem para a máquina B cujo endereço é 200.18.171.3. A mensagem a ser enviada é uma mensagem IP. No caso deste exemplo, antes de efetivamente enviar a mensagem IP, a estação utilizará o protocolo ARP para determinar o endereço MAC da interface cujo endereço IP é o destino da mensagem.

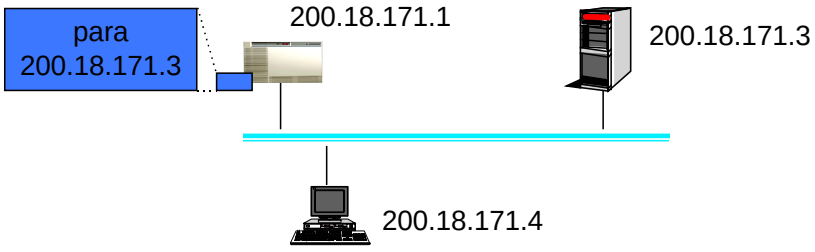


Figura 6.16 (a) – Exemplo do funcionamento do protocolo ARP. Inicio do envio da mensagem.

O funcionamento do protocolo ARP é descrito abaixo:

1. Estação A verifica que a máquina destino está na mesma rede local, determinado através dos endereços origem e

destino e suas respectivas classes.

2. O protocolo IP da estação A verifica que ainda não possui um mapeamento do endereço MAC para o endereço IP da máquina destino.

3. O protocolo IP solicita ao protocolo que o endereço MAC necessário

4. Protocolo ARP envia um pacote ARP (ARP Request) com o endereço MAC destino de broadcast (difusão para todas as máquinas)

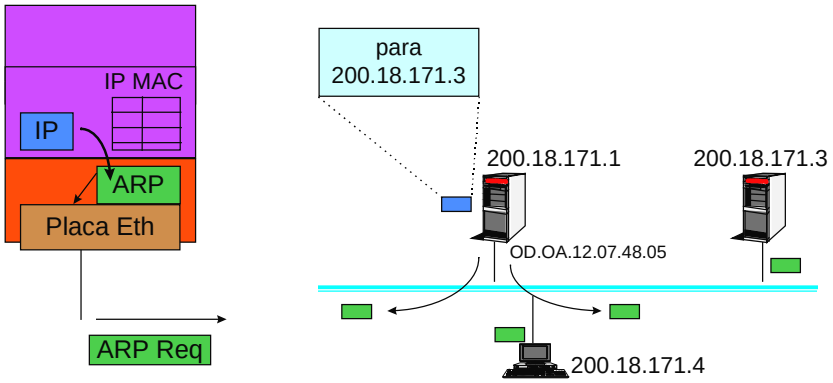
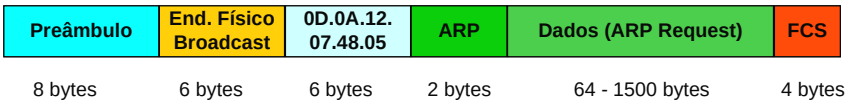


Figura 6.16 (b) – Exemplo do funcionamento do protocolo ARP. Envio de pacote ARP em difusão.

5. A mensagem ARP enviada é encapsulada em um pacote Ethernet conforme diagrama abaixo:



6. Todas as máquinas recebem o pacote ARP, mas somente aquela que possui o endereço IP especificado responde. A máquina B já instala na tabela ARP o mapeamento do endereço 200.18.171.1 para o endereço MAC de A.

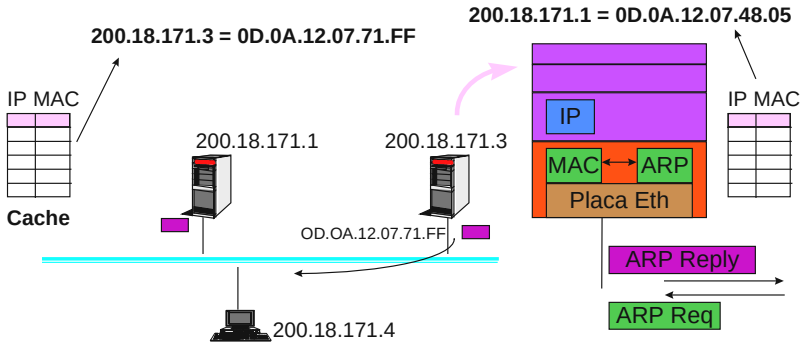
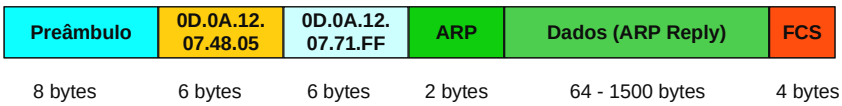


Figura 6.16 (c) – Exemplo do funcionamento do protocolo ARP. Resposta à requisição ARP.

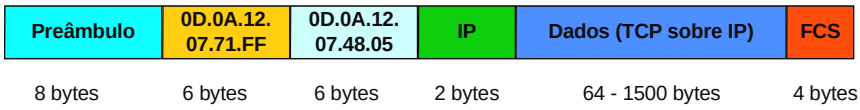
7. A resposta é enviada no pacote Ethernet, encapsulado conforme mostrado abaixo, através de uma mensagem ARP Reply endereçado diretamente para a máquina origem.



8. A máquina A recebe o pacote e coloca um mapeamento do endereço IP de B e seu endereço MAC respectivo. Esta

informação residirá em uma tabela que persistirá durante um certo tempo.

9. Finalmente a máquina A transmite o pacote IP inicial, após saber o endereço MAC da estação destino.



Os protocolos de nível de Rede como Ethernet possuem um identificador para determinar o tipo do protocolo que está sendo carregado no seu campo de dados. Um pacote Ethernet pode, por exemplo, carregar os protocolos ARP, IP, RARP, IPX, Netbios e outros. A figura 6.17 mostra o formato do quadro Ethernet. Note que o campo protocolo, de 2 bytes de tamanho identifica o protocolo sendo carregado no campo de dados. No caso de transporte de um pacote ARP, o valor é 0806h (hexadecimal), enquanto que no caso de IP este campo tem o valor 0800h.

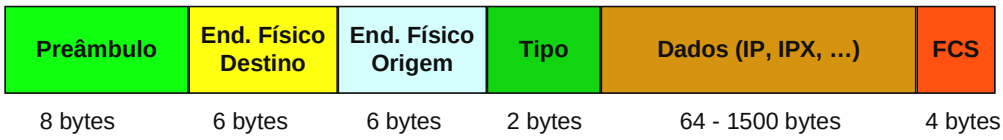


Figura 6.17 – Quadro (frame) Ethernet

6.5.3 – ROTEAMENTO IP.

O destino de um datagrama IP sendo enviado por um host pode ser a próprio host, um host situado na mesma rede ou um host situado numa rede diferente. No primeiro caso, o pacote é enviado ao nível IP que o retorna para os níveis superiores. No segundo caso, é realizado o mapeamento por meio de ARP e a mensagem é enviada por meio do protocolo de rede.

Quando um host deve enviar um pacote para outra rede, o protocolo IP deve enviá-lo para um roteador situado na mesma rede. O roteador por sua vez irá enviar o pacote para outro roteador, e assim sucessivamente até que o pacote chegue ao destino final. Este tipo de roteamento é chamado de *Next-Hop Routing*, já que um pacote é sempre enviado para o próximo roteador no caminho.

Neste tipo de roteamento, não há necessidade de que um roteador conheça a rota completa até o destino. Cada roteador deve conhecer apenas o próximo roteador para o qual deve enviar a mensagem. Esta decisão é chamada de decisão de roteamento. Um host situado em uma rede que tenha mais de um roteador deve também tomar uma decisão de roteamento para decidir para qual roteador deve enviar o pacote IP.

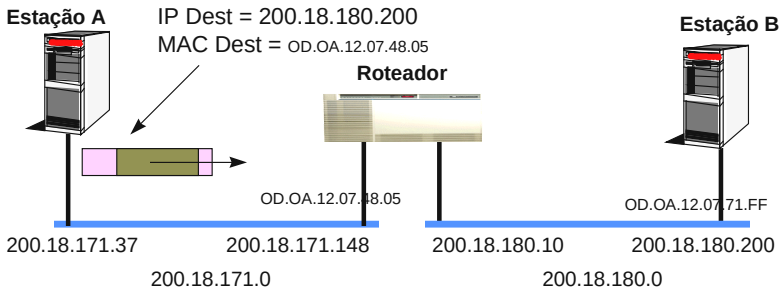
Quando uma estação deve enviar uma mensagem IP para outra rede, ela deve seguir os seguintes passos:

1. Determinar que o hist destino está em outra rede e por isto deve-se enviar a mensagem para um roteador.
2. Determinar, através da tabela de rotas da máquina origem, qual roteador é o correto para se enviar a mensagem.
3. Descobrir, através do protocolo ARP, qual o endereço MAC do roteador.
4. Enviar a mensagem IP com o endereço de nível de rede apontado para o roteador e o endereço IP (na mensagem IP) endereçado para a máquina destino.

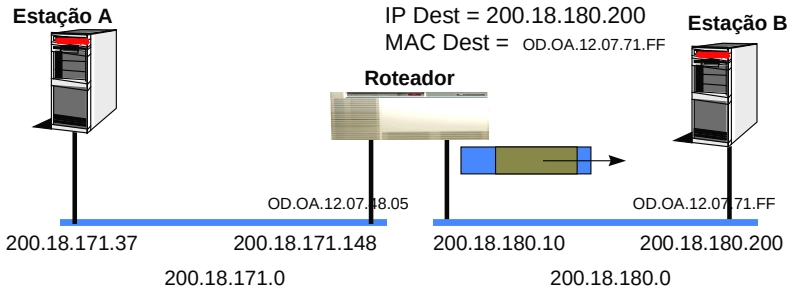
Uma questão importante no pacote roteado consiste no fato de que o pacote a ser roteado é endereçado fisicamente ao roteador (endereço MAC), mas é endereçado logicamente (endereçamento IP) à máquina destino. Quando o roteador recebe um pacote que não é endereçado a ele, tenta roteá-lo.

A decisão de roteamento é baseada em uma tabela, chamada de **tabela de rotas**, que é parte integrante de qualquer protocolo IP. Esta tabela relaciona cada rede destino ao roteador para onde o pacote deve ser enviado para chegar a ela.

A figura 6.18 ilustra o funcionamento do roteamento.



(a) A estação A envia um datagrama com destino a B



(b) O roteador recebe o pacote e transfere para o meio de transmissão que tem acesso à estação B.

Figura 6.18 – Roteamento de um datagrama IP por um roteador.

Na figura 6.18 o roteamento é realizado somente por um roteador. Caso houvesse mais de um roteador a ser atravessado, o primeiro roteador procederia de forma idêntica à Estação A, ou seja, determinaria a rota correta e enviaria a mensagem para o próximo roteador.

Os Algoritmos de transmissão e recepção de um pacote IP são descritos a seguir.

ALGORITMO DE TRANSMISSÃO

1. Datagrama pronto para ser transmitido

2. Caso:

2.1 Endereço Destino == Endereço Transmissor

2.1.1 Entrega datagrama pela interface loopback (127.0.0.1)

2.2.2 Fim

2.2 Endereço de rede do destino == endereço de rede local

2.2.1 Descobre o endereço físico do destino (ARP)

2.2.1 Transmite datagrama pela interface correta

2.2.2 Fim

2.3 Endereço de rede do destino != endereço de rede local

2.3.1 Verifica tabela de rotas

2.3.2 Descobre rota que se encaixa com a rede destino

2.3.3 Descobre o endereço físico do gateway (ARP)

2.3.4 Transmite o datagrama para o gateway

2.3.5 Fim

3. Fim

ALGORITMO DE RECEPÇÃO

1. Datagrama recebido da camada intra-rede, defragmentado e testado

2. Caso:

2.1 Endereço Destino = Endereço do Host, ou E.D. = outras interfaces do Host, ou E.D. = Broadcast

2.1.1 Passa datagrama para níveis superiores -> FIM

2.2 Caso:

2.2.1 Máquina que recebeu não é roteador

2.2.1.1 Descarta datagrama -> FIM

2.2.2 Máquina é roteador (possui mais de uma interface IP)

2.2.2 Caso:

2.2.2.1 Endereço IP destino = Rede IPcom interface direta

2.2.2.1.1 Descobre o endereço físico do destino (ARP)

2.2.2.1.2 Transmite datagrama pela interface respectiva -> FIM

2.2.2.2 Caso Endereço de rede do destino endereço de rede local

2.2.2.2.1 Verifica tabela de rotas

2.2.2.2.2 Descobre o endereço físico do gateway (ARP)

2.2.2.2.3 Transmite o datagrama para o gateway -> FIM

3. Fim

A figura 6.19 ilustra uma estrutura de redes. As tabelas de rotas de cada roteador são diferentes uma das outras. Note nestas tabela a existência de rotas diretas, que são informações redundantes para identificar a capacidade de acessar a própria rede na qual os roteadores estão conectados. Este tipo de rota apesar de parecer redundante é útil para mostrar de forma semelhante as rotas diretas para as redes conectadas diretamente no roteador.

Outra informação relevante é a existência de uma rota default. Esta rota é utilizada durante a decisão de

roteamento no caso de não existir uma rota específica para a rede destino da mensagem IP. A rota default pode ser considerada como um resumo de diversas rotas encaminhadas pelo mesmo próximo roteador. Sem a utilização da rota default, a tabela de rotas deveria possuir uma linha para cada rede que pudesse ser endereçada. Em uma rede como a Internet isto seria completamente impossível.

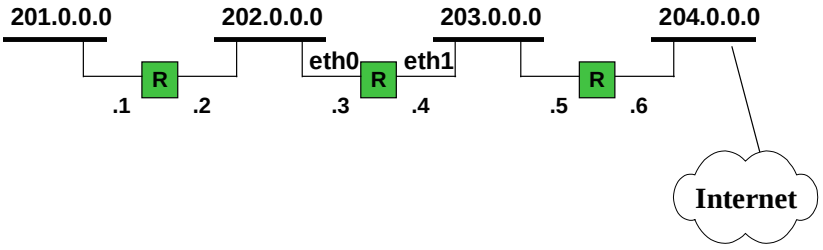


Figura 6.19 – Exemplo de estrutura de rede incluindo três roteadores (R).

A tabela de rotas para o roteador da esquerda na figura 6.19 é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
201.0.0.0	eth0 (rota direta)	0
202.0.0.0	eth1 (rota direta)	0
203.0.0.0	202.0.0.3	1
204.0.0.0	203.0.0.3	2
Default	203.0.0.3	--

A tabela de rotas para o roteador central na figura 6.19 é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
202.0.0.0	eth0 (rota direta)	0
203.0.0.0	eth1 (rota direta)	0
201.0.0.0	202.0.0.2	1
204.0.0.0	203.0.0.5	1
Default	203.0.0.5	--

A tabela de rotas para o roteador da direita na figura 6.19 é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
203.0.0.0	eth0 (rota direta)	0
204.0.0.0	eth1 (rota direta)	0
202.0.0.0	203.0.0.4	1
201.0.0.0	203.0.0.4	1
Default	204.0.0.7**	--

** Não mostrado na figura.

A rota default geralmente é representada nos sistemas operacionais como a rede 0.0.0.0.

6.5.3.1 - ROTEAMENTO ESTÁTICO X ROTEAMENTO DINÂMICO

A alimentação das informações na tabela de rotas pode ser de modo estático ou dinâmico ou ambos. Na alimentação estática, as rotas são preenchidas manualmente, geralmente pela configuração inicial da máquina. Na alimentação dinâmica, protocolos como RIP, RIP2, OSPF ou BGP4 são responsáveis pela aquisição de informações sobre a topologia da rede e a publicação de rotas na tabela de rotas dos roteadores envolvidos.

6.5.4 – FRAGMENTAÇÃO DE PACOTES IP.

Um pacote IP pode ter um tamanho de até 64 Kbytes. Entretanto o nível de rede geralmente tem um tamanho máximo menor que 64K. Por exemplo, uma rede Ethernet pode transmitir uma mensagem de até 1500 bytes. Este valor

é chamado de MTU - Maximum Transmission Unit - para este tipo de rede. A camada IP deve então ser capaz de dividir um pacote IP maior que 1500 bytes em diversos fragmentos de até 1500 bytes cada um.

A fragmentação do pacote IP pode ocorrer na máquina origem ou em algum roteador que possua uma rede com MTU menor que o tamanho do pacote IP sendo roteado. Note que durante o percurso até o destino, um fragmento pode ser novamente fragmentado se o MTU da rede seguinte for ainda menor que o tamanho do fragmento. A remontagem do pacote só é realizada pela máquina destino, baseado nas informações de FRAGMENT OFFSET e bit MF. A perda de um fragmento inutiliza o datagrama inteiro.

O campo FRAGMENT OFFSET identifica a posição em Bytes do fragmento face ao pacote IP completo conforme pode ser visto na figura 6.20.

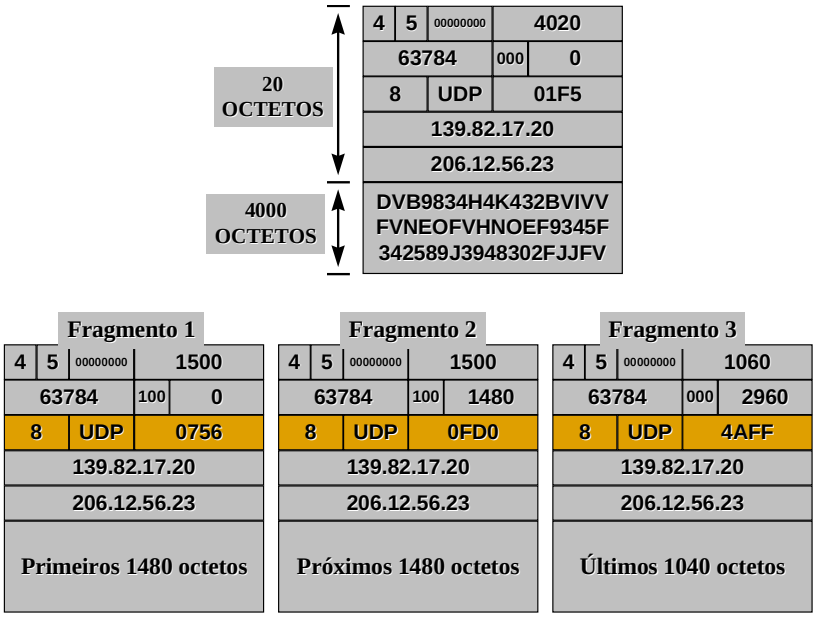


Figura 6.20 – Fragmentação do pacote IP.

A figura 6.21 demonstra a fragmentação de um pacote quando este passa para uma rede com MTU menor que o tamanho do pacote IP.

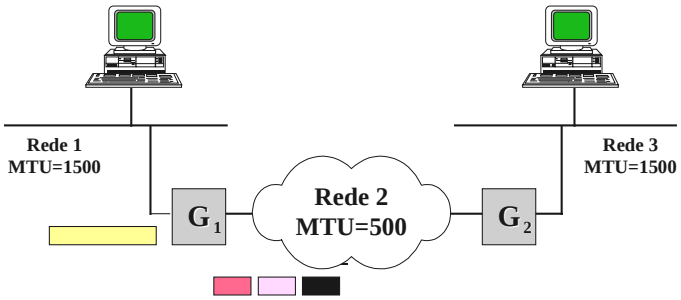


Figura 6.21 – Exemplo de fragmentação do pacote IP.

6.5.5 – PROTOCOLOS DA CAMADA DE TRANSPORTE

A camada de transporte do TCP/IP reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, ou seja, considerando apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários. A camada de transporte possui dois protocolos que são o UDP (User Datagram Protocol) e TCP (Transmission Control Protocol).

O protocolo UDP realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente.

O protocolo TCP realiza além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP o controle de fluxo, o controle de erros, o sequenciamento e a multiplexação de mensagens.

A camada de transporte oferece para o nível de aplicação um conjunto de funções e procedimentos de acesso ao sistema de comunicação que permitem a criação e a utilização de aplicações de forma independente da implementação. Desta forma, as interfaces socket (ambiente Unix) e Winsock (ambiente Windows) fornecem um conjunto de funções-padrão para permitir que as aplicações possam ser desenvolvidas independentes do sistema operacional no qual serão executadas.

6.5.5.1 - PROTOCOLO UDP

O protocolo UDP fornece uma forma simples de acesso ao sistema de comunicação, provendo um serviço sem conexão, sem confiabilidade e sem correção de erros. A principal função do nível de transporte implementada em UDP é a capacidade de multiplexação de acesso ao sistema de comunicação. Esta função permite que vários processos ou programas executando em um computador possam acessar o sistema de comunicação e o tráfego de dados respectivo a cada um deles seja corretamente identificado, separado e utilize buffers individuais.

Um processo é o programa que implementa uma aplicação do sistema operacional, e que pode ser uma aplicação da camada de aplicação TCP/IP.

A forma de identificação de um ponto de acesso de serviço (SAP) do modelo OSI é a **porta** ou “port” de protocolo em TCP/IP. A porta é a unidade que permite identificar o tráfego de dados destinado a diversas aplicações. A identificação única de um processo acessando os serviços TCP/IP é, então, o endereço IP da máquina e a porta (ou portas) usada pela aplicação. Cada processo pode utilizar mais de uma porta simultaneamente, mas uma porta só pode ser utilizada por uma aplicação em um dado momento. Uma aplicação que deseje utilizar os serviços de comunicação deverá requisitar uma ou mais portas para realizar a comunicação. A mesma porta usada por uma aplicação pode ser usada por outra, desde que a primeira tenha terminado de utilizá-la.

A forma de utilização de portas mostra uma distinção entre a parte cliente e a parte servidor de uma aplicação TCP/IP. O programa cliente pode utilizar um número de porta qualquer, já que nenhum programa na rede terá necessidade de enviar uma mensagem para ele. Já uma aplicação do tipo servidor deve utilizar um número de porta convencionado ou “popular” (Well-known ports) de modo que um cliente qualquer que deseje utilizar os serviços do servidor, possa requisita-lo conhecendo apenas o endereço IP do host servidor.

Se não houvesse a utilização de um número de porta convencionado, a arquitetura TCP/IP deveria possuir um mecanismo de diretório para que um cliente pudesse descobrir o número da porta associado ao servidor.

Os números de porta de **1 a 1023 são números convencionados para serviços (aplicações) atribuídos pela IANA (Internet Assigned Numbers Authority)**. Os números de 1024 a 65535 podem ser atribuídos para outros serviços e são geralmente utilizados pelos programas-cliente de um protocolo. Este conjunto de números tem ainda a atribuição de alguns serviços de forma não oficial, já que os primeiros 1024 números não conseguem comportar todos os protocolos TCP/IP existentes.

A figura 6.22 ilustra a multiplexação/demultiplexação realizada pelo protocolo UDP na camada de transporte:

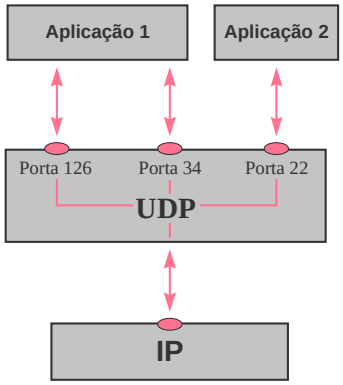


Figura 6.22 - Multiplexação/Demultiplexação realizada na camada de transporte

A mensagem UDP é representada pela figura 6.23. O dado carregado é o pacote de nível de aplicação. UDP acrescenta apenas mais 8 bytes que são a porta de protocolo origem a porta de protocolo destino, o tamanho da mensagem UDP e um checksum para averiguar a correção dos dados do cabeçalho UDP.

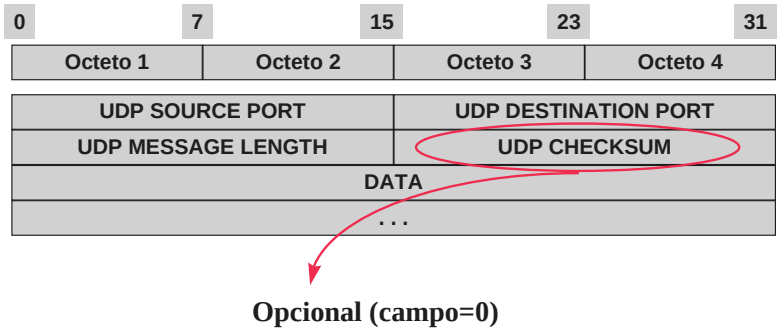


Figura 6.23 - Mensagem UDP

6.5.5.2 - PROTOCOLO TCP

O protocolo TCP trabalha no mesmo nível que o protocolo UDP, mas oferece serviços mais complexos, que incluem controle de erros e de fluxo, serviço com conexão e envio de fluxo de dados. O TCP utiliza o mesmo conceito de porta do UDP. Para o TCP, uma conexão é formada pelo par (Endereço IP de Origem, Porta de Origem) e (Endereço IP de Destino, Porta de Destino).

O protocolo TCP oferece as seguintes características:

1. Controle de Fluxo e Erro fim-a-fim.
2. Serviço confiável de transferência de dados.
3. Comunicação full-duplex fim-a-fim.
4. A aplicação necessita apenas enviar um fluxo de bytes.
5. Desassociação entre quantidade de dados enviados pela aplicação e pela camada TCP.
6. Ordenação de mensagens.
7. Multiplexação de IP, através de várias portas.
8. Opção de envio de dados urgentes.

A conexão TCP é ilustrada na figura 6.24 abaixo.

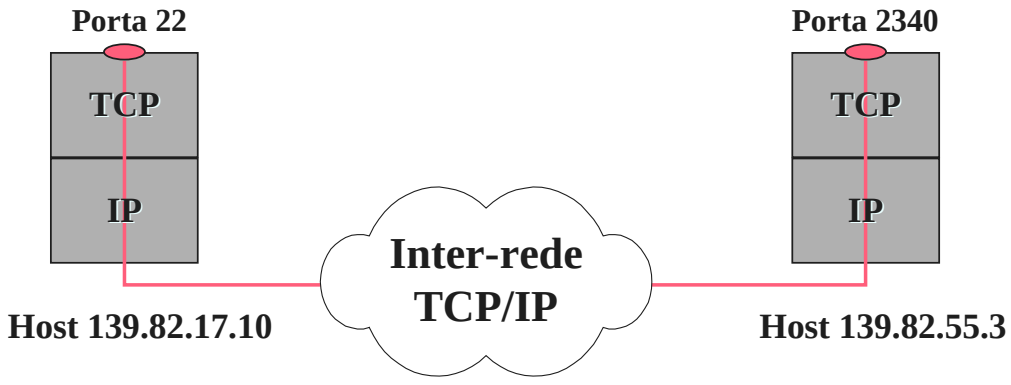


Figura 6.24 – Exemplo de conexão TCP.

Uma conexão TCP é formada por três fases: o estabelecimento de conexão, a troca de dados e a finalização da conexão, conforme ilustrado na figura 6.25.

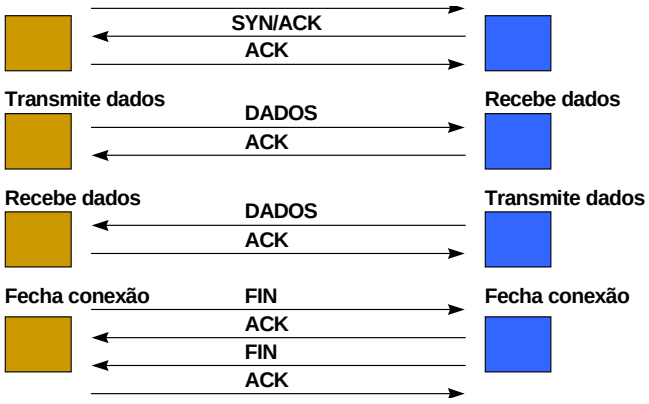


Figura 6.25 – Fases de uma conexão TCP.

O pacote TCP é formado pela mensagem mostrada na figura 6.26. Os campos do pacote são definidos da seguinte forma:

- TCP SOURCE PORT: Porta origem da mensagem

- TCP DESTINATION PORT: Porta destino da mensagem

- SEQUENCE NUMBER: número de sequência dos dados sendo transmitidos face ao conjunto total de dados já transmitidos. Este número indica a posição do primeiro byte de dados sendo transmitido em relação ao total de bytes já transmitidos nesta conexão. O primeiro número de sequência utilizado não é zero ou um, mas começa de um valor aleatório. Logo se um pacote está transmitindo do 1234º byte até o 2000º byte de uma conexão e o SEQUENCE NUMBER inicial utilizado nesta conexão foi 10000, o campo SEQUENCE NUMBER conterá o valor 11234. O sequence number em um sentido da conexão (máquina A para B) é diferente do sequence number do sentido inverso, já que os dados transmitidos por um e outro lado são distintos.

- ACKNOWLEDGE NUMBER: número que significa o reconhecimento dos dados recebidos até então no sentido inverso. O ACK de um sentido é transmitido em *piggy-backing* no outro sentido. O ACK contém o número do próximo byte do fluxo de dados recebido, que a origem deste pacote espera receber da outra máquina. Este valor leva em consideração o número de SEQUENCE NUMBER inicial praticado pela outra máquina. O valor de ACK informa sempre o próximo byte ainda não recebido do conjunto contíguo de bytes recebidos do transmissor.

- CODE BITS: São formados por seis bits, URG, ACK, PSH, RST, SYN e FIN, cuja utilização é mostrada abaixo:

- URG: bit de Urgência: significa que o segmento sendo carregado contém dados urgentes que devem ser lidos com prioridade pela aplicação. A aplicação origem é responsável por acionar este bit e fornecer o valor do URGENT POINTER que indica o fim dos dados urgentes. Um exemplo da utilização desta facilidade é o aborto de uma conexão (por exemplo por Control-C), que faz com que a aplicação destino examine logo o pacote até o fim da área de urgência, descubra que houve um Control-C e termine a conexão.

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

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

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

- SYN: bit de Sincronismo: é o bit que informa os dois primeiros segmentos de estabelecimento da conexão.

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

- WINDOW: Este campo informa o tamanho disponível em bytes na janela de recepção da origem deste pacote. Por meio deste valor, o TCP pode realizar um controle adequando de fluxo para evitar a sobrecarga do receptor. Quando este valor é igual a zero, o transmissor não envia dados, esperando receber um pacote com WINDOW maior que zero. O transmissor sempre vai tentar transmitir a quantidade de dados disponíveis na janela de recepção sem aguardar um ACK. Enquanto não for recebido um reconhecimento dos dados transmitidos e o correspondente valor de WINDOW > 0, o transmissor não enviará dados.

- OPTIONS: O campo de opções só possui uma única opção válida que é a negociação do MSS (Maximum Segment Size) que o TCP pode transmitir. O MSS é calculado através do MTU ou através do protocolo ICMP Path MTU Discovery.

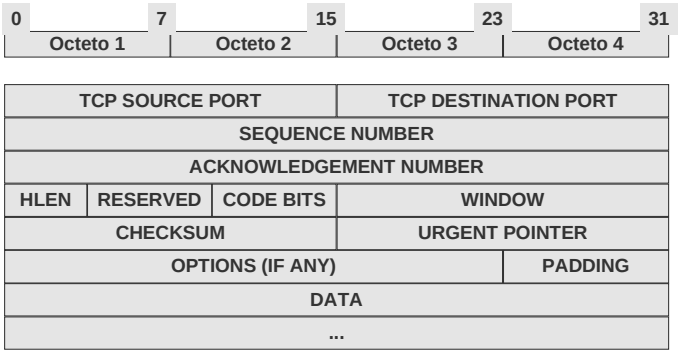


Figura 6.26 – Mensagem TCP.

6.5.6 – PROTOCOLOS DA CAMADA DE APLICAÇÃO.

Os protocolos de aplicação TCP/IP são aqueles que realizam as funções de alto nível e que utilizam os serviços da camada de transporte UDP ou TCP para a comunicação.

Os protocolos de aplicação podem realizar funções diretamente acessíveis pelo usuário como FTP, HTTP, SMTP, POP3, IMAP4, Finger, Telnet, Chat, NFS, TFTP, NNTP e outros. Além disto, podem também realizar funções mais próximas do sistema de comunicação, tais como os protocolos DNS, BOOTP, DHCP, SNMP, BGP4, e outros.

6.5.6.1 – PROTOCOLO DNS

Destacaremos em nosso estudo o protocolo DNS (Domain Name System), que especifica duas partes principais: regras de sintaxe para a definição de domínios e o protocolo utilizado para a consulta de nomes.

O DNS é basicamente uma associação entre endereços IP e nomes. A abordagem inicial para esta associação era a utilização de nomes simples, ou seja, sem hierarquia. Esta abordagem possui limitações intrínsecas quanto a escalabilidade e a manutenção. O sistema de nomes utilizado na Internet tem o objetivo de ser escalável, suportando a definição de nomes únicos para todas as redes e máquinas na Internet e permitindo que a administração seja descentralizada.

A estrutura de nomes na Internet tem o formato de uma árvore invertida onde a raiz não possui nome. Os ramos imediatamante inferiores à raiz são chamados de TLDs (Top-Level Domain Names) e são por exemplo .com, .edu., .org, .gov, .net, .mil, .br, .fr, .us, uk, etc. Os TLDs que não designam países são utilizados nos EUA. Os diversos países utilizam a sua própria designação para as classificações internas. No Brasil, por exemplo, temos os nomes .com .br., .gov.br, .net.br, .org.br e outros.

Cada ramo completo até a raiz como, por exemplo, fepesmig.br, empresa.com.br, nasa.gov, e outros são chamados de domínios. Um domínio é a área administrativa englobando ele próprio e os subdomínios abaixo dele. Por exemplo o domínio .br engloba todos os subdomínios do Brasil. O domínio empresa.com.br tem a responsabilidade por todos os domínios abaixo dele.

A hierarquia de domínios pode ser observada na figura 6.27.

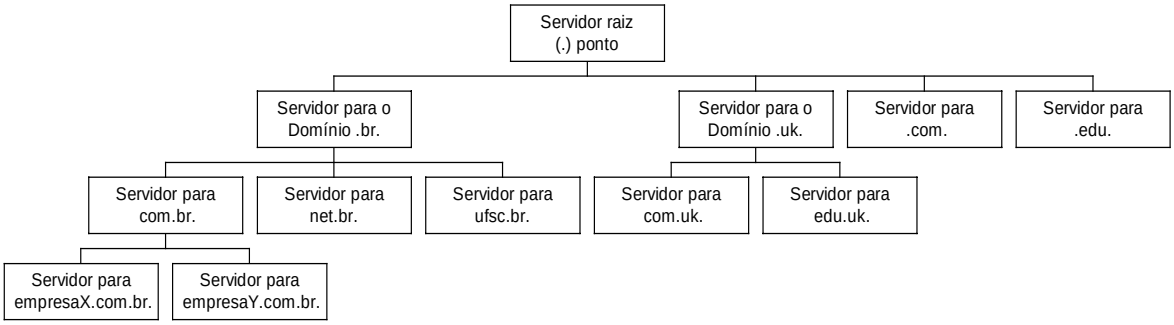


Figura 6.27 - Servidores DNS estruturados hierarquicamente

Os domínios principais genéricos, chamados de GTLDs (Generic Top Level Domain Names) que são .net, .com e .org são administrados pelo Internic (Internet Network Information Center) que também é responsável pela administração do espaço de endereçamento IP. Recentemente foram criados novos nomes de domínio genéricos que serão utilizado a partir de 98. São eles: .firm, .store, .web, .arts, .rec, .infor, .nom.

Os domínios são completamente independentes da estrutura de rede utilizada. Não existe, necessariamente, relacionamento entre eles. O DNS possui uma estrutura inversa para poder representar o endereçamento de rede, ou permitir que seja feita a associação do endereço IP correspondente a um nome. Esta estrutura possui como raiz principal a notação .ARPA e possui como único ramo o .in-addr. Abaixo deste são colocados em ordem os bytes do endereço IP.

6.6 - OUTROS EXEMPLOS DE ARQUITETURAS DE REDES.

Existe atualmente um número muito grande de redes em operação. Algumas são públicas, controladas por concessionárias de serviços de comunicação, outras são redes de pesquisa e outras ainda são redes corporativas ou comerciais. Todas elas apresentam diferenças em relação a sua história, administração, recursos oferecidos, projeto técnico e comunidade de usuários. A história e a administração de uma rede podem variar significativamente, de exemplos onde ela foi cuidadosamente planejada por uma organização até exemplos de redes cujas máquinas foram interconectadas no decorrer dos anos sem qualquer planejamento ou administração central. Os recursos disponíveis podem variar da arbitrária comunicação processo a processo até o correio eletrônico, à transferência de arquivos, ao *login* remoto e à execução remota. Os projetos técnicos podem diferir no tipo de meio de transmissão utilizado, nos algoritmos de roteamento e de denominação empregados, no número e no conteúdo das camadas presentes e nos protocolos usados. Por fim, a comunidade de usuários pode variar dos funcionários de uma empresa até todas as pessoas interessadas no mundo.

Muitos são os exemplos de redes disponíveis no mercado, principalmente para redes locais. Ainda podemos analisar algumas experiências de grandes redes tais como a ARPANET e a NSFNET, precursoras da Internet mundial, assim como das primeiras experiências até a gigabit. Um bom exemplo de rede local bastante popular é a Novel NetWare. Ela foi projetada para ser usada para empresas que estavam fazendo downsizing de mainframe para rede de PCs. Ela utiliza a filosofia cliente/servidor e está baseada numa pilha de protocolos proprietária ilustrada na figura 6.28. Ela é baseada na antiga XNS (Xerox Network System) com várias modificações. Esta arquitetura antecede o RM-OSI e se parece mais com a arquitetura TCP/IP.

As camadas física e de enlace podem ser escolhidas dentre vários padrões industriais. O IPX é um protocolo sem conexão não confiável e é funcionalmente semelhante ao IP, com diferenças no endereçamento, que é de 10 bytes.

O NCP (Network Core Protocol) é um protocolo de transporte orientado a conexão e não está restrito ao transporte de dados do usuário, sendo considerado o coração do Netware. O SPX (Sequence Packet Exchange) oferece apenas o transporte de mensagens. Ainda há a opção do TCP, que também pode ser utilizado. Por exemplo, o sistema de arquivos utiliza o NCP e o Lotus Notes utiliza o SPX.

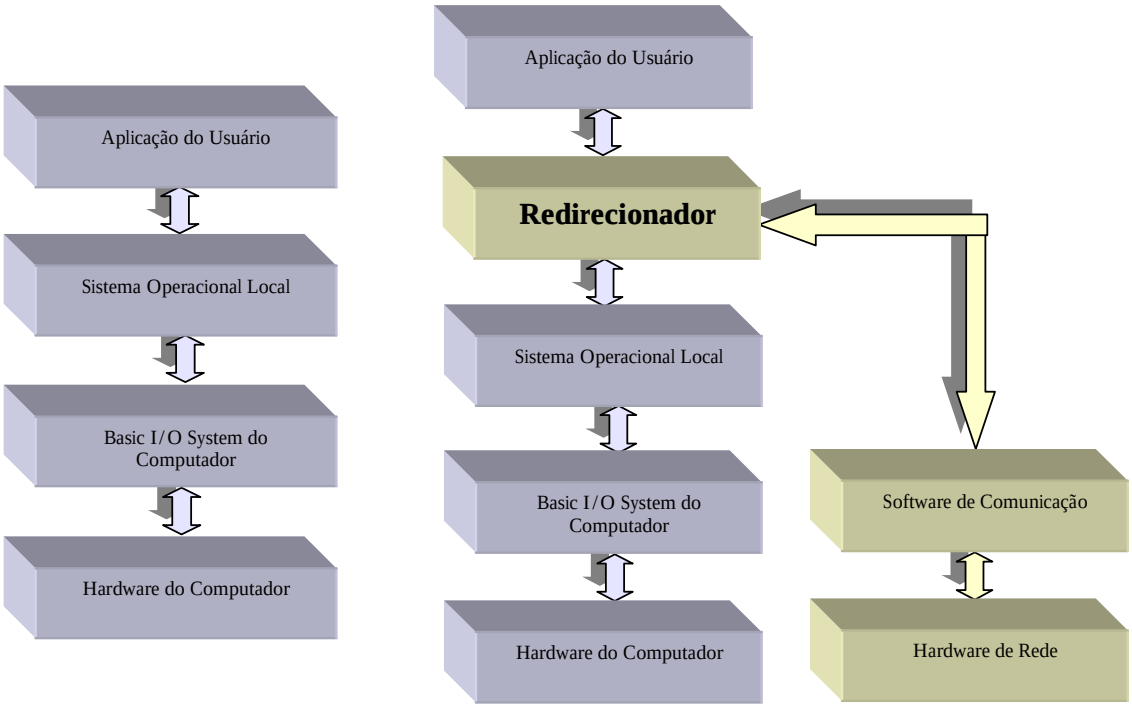
Figura 6.28 – O modelo de referência da Novel NetWare.

Com o surgimento das redes de computadores, um sistema de comunicação foi inserido interligar os computadores, que até então operavam de forma isolada, para permitir o compartilhamento de recursos. No hardware dos computadores, a modificação necessária foi a introdução de um dispositivo de entrada e saída adicional, responsável pela interface do computador com o sistema de comunicação, mais conhecida como **interface de rede**.

A modificação no hardware gerou a necessidade de modificações nos sistemas operacionais para o novo ambiente de processamento, onde se tornou possível utilizar recursos de hardware e software remotos. Como os sistemas operacionais até então tratavam os recursos locais, tornou-se necessário adicionar um conjunto de programas para dota-los da capacidade de comunicação e de reconhecimento dos recursos compartilhados.

Considerando que as modificações nos sistemas operacionais locais não deveriam alterar a forma de operação dos computadores para gerar o menor impacto possível nos usuários, os **sistemas operacionais de rede** (N.O.S. – Network Operational System) surgiram como uma extensão dos sistemas operacionais locais existentes.

Para atender à necessidade de transparência na operação de recursos da rede do ponto de vista dos usuários, foi introduzido um **redirecionador** no sistema operacional. Este redirecionador funciona interceptando as chamadas feitas pelas aplicações ao sistema operacional local, desviando para o módulo de comunicação aquelas que dizem respeito aos recursos remotos . A figura 7.1 ilustra o esquema geral de funcionamento do redirecionador.



(a) Sistema Operacional Local

(b) Sistema Operacional Local com Redirecionador para comunicação em rede

Figura 7.1 – Inclusão do Redirecionador em um Sistema Operacional

Para as aplicações dos usuários, a instalação de um sistema operacional de rede é percebida apenas pela adição de novos recursos aos que elas possuíam anteriormente. A interface utilizada pelas aplicações para ter acesso aos recursos locais ou remotos permanece inalterada.

A interface entre as aplicações e o sistema operacional baseia-se em interações do tipo solicitação/resposta onde a aplicação solicita um serviço (abertura de um arquivo, impressão de dados, etc.) através de chamadas ao sistema operacional. O S.O., em resposta, executa o serviço, informa o resultado da operação (execução com sucesso, erro, etc.) e devolve dados para a aplicação, quando é o caso.

7.1 – SISTEMAS CLIENTE/SERVIDOR E PEER-TO-PEER.

O conceito de **Cliente/Servidor** utiliza-se desta forma de interação. O Cliente/Servidor é o modo de interação básico nas redes de computadores. Nele, o **Cliente** é a entidade que solicita o serviço e o **Servidor** é a entidade que presta o serviço. Os computadores que disponibilizam recursos através da rede devem possuir a entidade *servidor* enquanto os computadores que permitem que suas aplicações utilizem recursos compartilhados por outros computadores devem possuir a entidade *cliente*.

As funções necessárias ao NOS na entidade Cliente são diferentes das funções nas entidades Servidor. No Cliente, o NOS restringe-se a fornecer comunicação de requisições para o Servidor e entregar as respostas às aplicações. No Servidor, além da comunicação, devem ser executadas tarefas como: controle de acesso aos recursos, suporte para impressão, armazenamento de arquivos compartilhados, etc.

Nas redes do tipo ***Peer-to-Peer*** (ou **redes homogêneas** para alguns autores) as entidades Cliente e Servidor estão presentes em cada computador da rede. Assim, todos os computadores da têm a capacidade de prover recursos e requisitar serviços.

Nas redes do tipo **Cliente-Servidor**, os computadores se dividem em estações clientes, que possuem funções da entidade Cliente e estações servidoras ou Servidores, que possuem funções da entidade Servidor. Nas redes Cliente-Servidor, os computadores Servidores podem ser utilizados de maneira dedicada (Servidores Dedicados), não permitindo o uso de aplicação através do sistema operacional local (como é o caso do NOS Novell 5.0), ou podem ser utilizados de maneira não dedicada (Servidores não Dedicados), onde o sistema operacional local interage com a rede permitindo o uso de aplicações no computador local. A figura 7.2 apresenta a estrutura de uma estação Cliente e um Servidor Dedicado em uma rede Cliente-Servidor.

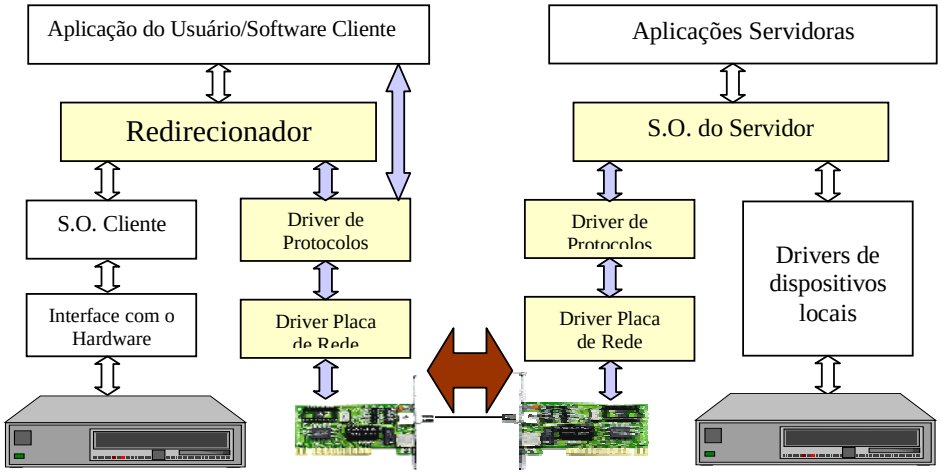


Figura 7.2 – Estrutura de um computador Cliente e de um Servidor Dedicado.

Na figura 7.2, as setas que partem do computador (cor branca) representam o fluxo entre o software e o hardware local e as setas que partem do adaptador de rede (cor azul) representam o fluxo entre o software local, o software de rede e o sistema de comunicação que possibilita a conexão da rede. A seta entre os adaptadores representa o trafego no meio de transmissão.

Como vimos, para que um computador possa operar como uma estação (um host) em uma rede de computadores, devem ser instalados recursos de hardware e software que complementam seus dispositivos e o seu sistema operacional local. Em uma rede local (LAN) o hardware adicional necessário se constitui, em geral, de uma placa de interface de rede e do *driver* de dispositivo correspondente que controla seu funcionamento. O software adicional, definido como Sistema Operacional de Rede (NOS), engloba os seguintes componentes:

1. Um conjunto de módulos que implementam os protocolos e aplicações cliente-servidor;
2. Um conjunto de drivers com implementações de protocolos de comunicação.

Os componentes do NOS devem se posicionar no nível do modelo de referência OSI (RM-OSI) correspondente às funções que implementa. A figura 7.3 apresenta a relação entre os componentes de um NOS típico e o RM-OSI.

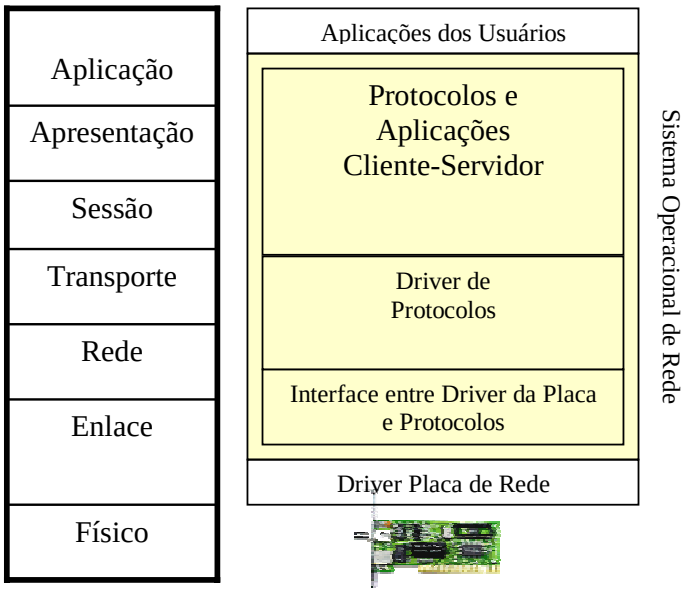


Figura 7.3 – Relação entre os componentes de um NOS típico e o RM-OSI.

7.2 – SERVIDORES DEDICADOS.

Uma das funções básicas das redes locais é o compartilhamento de recursos caros e especializados (quer equipamentos, programas, base de dados, ou vias de comunicação), isto é: serviços, entre os vários usuários da rede.

Qualquer estação de uma rede local com a entidade Servidor instalada pode oferecer serviços para outras estações (clientes). Vários serviços são típicos para cada aplicação e Servidores são projetados de forma a melhor oferecê-los. Tais servidores são distinguidos das outras estações apenas pelo software que os suportam e hardware especial que contenham. Entre os serviços mais oferecidos podemos citar: o armazenamento de arquivos, a gerência de banco de dados, o suporte para impressão, a tradução de nomes simbólicos em endereços físicos, a monitoração de redes, a criptografia, o correio eletrônico, o serviço de gateway para outras redes e outras funções de hardware e software.

Servidores podem ser também clientes de outros servidores da rede. Por exemplo, o servidor de impressão pode ser cliente de um servidor de arquivos ao fornecer serviços aos seus próprios clientes. O serviço de correio eletrônico é um outro exemplo de servidor que muitas vezes é realizado utilizando os serviços de armazenamento de arquivos de um outro servidor.

7.1.1 - SERVIDORES DE ARQUIVOS.

O Servidor de Arquivo tem como função oferecer aos seus clientes o serviço de armazenamento e acesso a informações e de compartilhamento de disco. Controlam unidades de disco ou outras unidades de armazenamento, sendo capazes de aceitar pedidos de transações das estações clientes e atendê-los utilizando os seus dispositivos de armazenamento.

Um Servidor de Arquivo Geral é aquele que é capaz de aceitar transações, independente do sistema operacional do cliente, ou seja, independente da estrutura de arquivos da estação cliente. Neste caso, existe um sistema de arquivo padrão da rede, utilizado pelo servidor de arquivos, nos quais os vários arquivos das demais estações da rede devem ser convertidos (pelos protocolos, no nível de apresentação) para comunicação com o Servidor. Sendo adotada esta solução, todos os arquivos da rede são potencialmente acessíveis a todas as estações, independente das estruturas de arquivos individuais.

7.1.2 - SERVIDORES DE IMPRESSÃO.

O Servidor de Impressão tem como finalidade oferecer serviços de impressão a seus clientes. Um Servidor de Impressão típico tem vários tipos de impressoras acoplados, cada um adequado à qualidade ou rapidez de uma aplicação particular.

Existem vária formas de se implementar um Servidor de Impressão. A forma mais simples é baseada na pré-alocação da impressora. Neste caso uma estação cliente envia um pedido ao Servidor, manifestando o desejo de uso de uma impressora específica. Caso esta impressora esteja disponível, ela então é alocada ao cliente até que este a libere (ou, então, até que se esgote o tempo máximo da utilização, conforme negociação na alocação). Caso a impressora não esteja disponível o cliente é avisado e colocado, se é de seu desejo em uma fila de espera.

Uma outra forma de implementarmos um Servidor de Impressão é utilizando a técnica de "*spooling*". Neste caso a estação ao invés de pedir a alocação de uma impressora, envia diretamente ao Servidor o texto a ser impresso. Este texto é colocado em uma fila de espera, sendo impresso quando a impressora estiver disponível.

7.1.3 - SERVIDORES DE COMUNICAÇÃO.

Consiste em uma estação especial que será responsável pela realização de todos os procedimentos de acesso à rede, bem como da interface com os dispositivos usuários, de forma a permitir o uso da rede por estes.

7.1.4 - SERVIDORES GATEWAY.

São estações da rede que oferecem serviço de comunicação com outras redes para seus clientes. A ligação entre redes pode ser realizada através de repetidores ou pontes, mas quando e trata de interligação de redes distintas o uso de Gateway se torna indispensável.

7.1.4 - SERVIDORES DE MONITORAMENTO.

Monitoramento do tráfego, do estado do sistema, do desempenho de uma estação da rede, assim como o monitoramento do meio de transmissão e de outros sinais é necessário para o gerenciamento da rede de forma a possibilitar a detecção de erros, diagnose e resoluções de problemas da rede, tais como falhas, desempenho e etc.

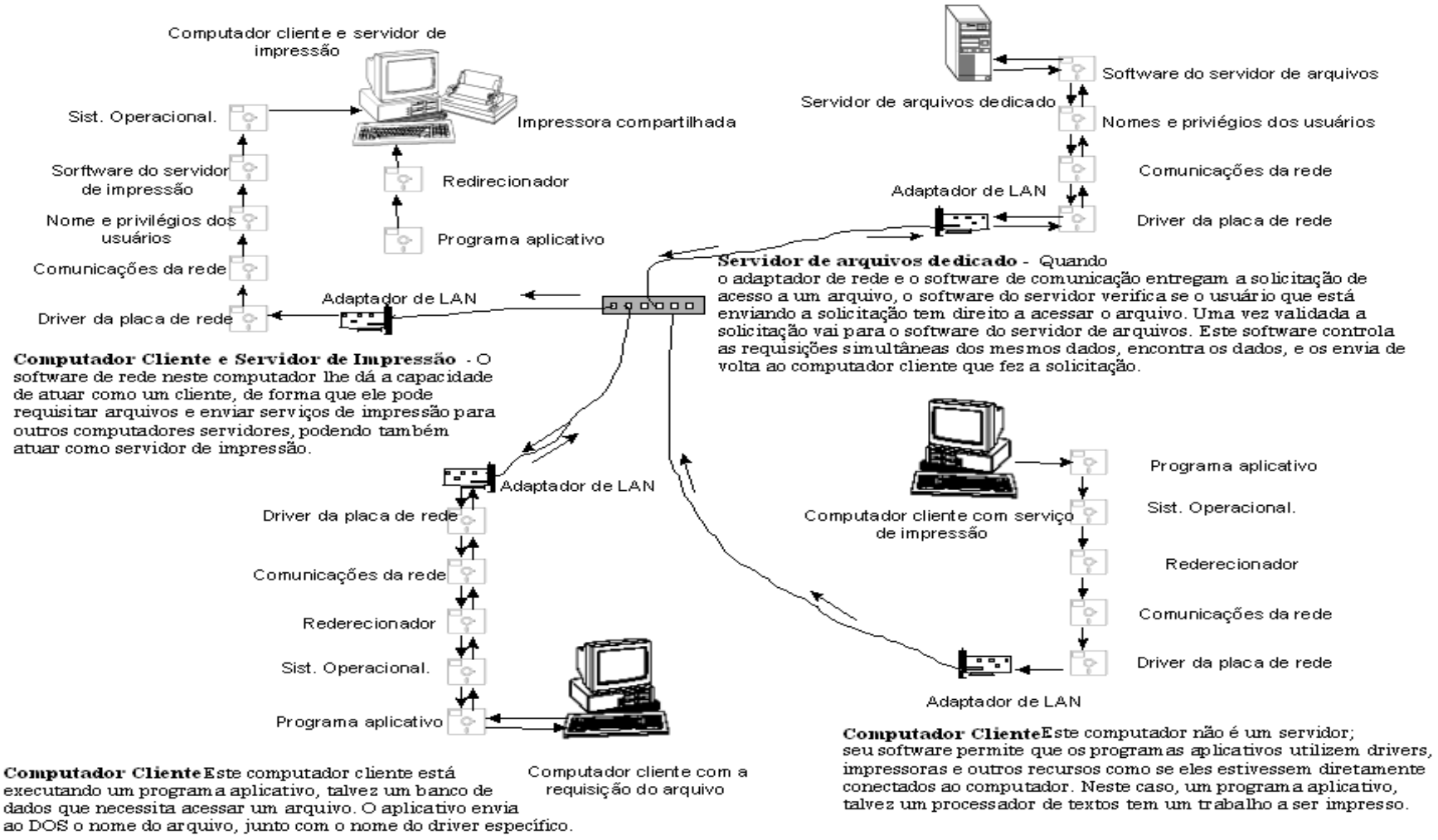


Figura 7.4 - Exemplo de Rede Local Elementar

[APA99] APARICI, Roberto et al. Nuevas Tecnologías, Comunicación y Educación. Madrid, Espanha. UNED, 1999. [CD-ROM]

[ARN97] ARNETT, Matthew Flint at al. Desvendando o TCP/IP. Rio de Janeiro. Editora Campus, 1997.

[BAR00] BARETTO, Marcelo L. Redes de Computadores. Departamento de Engenharia Elétrica. UFPA, 2000. Disponível no endereço URL: http://www.prodepa.gov.br/marcelo/

[COM98a] COMER, D. E. Interligação em Redes com TCP/IP - Volume 1. Ed. Campus, 1998.

[COM98b] COMER, D. E. et al. Interligação em Redes com TCP/IP - Volume 2. Ed. Campus, 1998.

[COS00] COSTA, Maurílio Alves. Martins. Avaliação Analítica de Desempenho do Uso do Ipv6. Florianópolis, SC, 2000. Dissertação (Mestrado em Ciência da Computação) – Programa de Pós-graduação em Ciência da Computação, UFSC, 2000.

[CYC97] CYCLADES Brasil. Guia Internet de Conectividade. São Paulo. 1997.

[KIR99] KIRCH, Olaf. Guia do Administrador de Redes Linux. Tradução de Conectiva Inf. Ltda. Conectiva, 1999. Disponível no endereço URL: : http://www.conectiva.com.br

[MAR97] MARTINS, Marcelo P. Redes Locais, UNIX x WindowsNT. Universidade Veiga de Oliveira. 1997. Disponível no endereço URL: http://www.tol.pro.br (Tutorial On-Line Home Page)

[SEM96] SEMERIA,C. Understanding IP Addressing:Everything You Ever Wanted To Know. 3COM Corporation. 1996. (mimeo)

[SOA96] SOARES, Luiz Fernando Gomes e outros: Redes de Computadores: Das LANs, MANs e WANs, às Redes ATM.2ª ed. Editora Campus, 1995/1996.

[SPE00] SPECIALSKI, Elizabeth S. Arquiteturas de Redes de Computadores. Departamento de Informática e Estatística. UFSC. Florianópolis, 2000. (mimeo)

[TAM96] TANENBAUM, Andrew S. Redes de Computadores. 3a. ed. Editora Campus, 1996.

[TOR99] TORRES Gabriel. Redes Locais, Placas e Cabos. Clube do Hardware. 1999. Disponível no endereço URL:http://www.clubedohardware.com.br/

[WER98] WERNER, José Alberto V. Apostila de Internet e Arquitetura TCP/IP. PUC-RIO. 1998. Disponível no Endereço URL: http://www.tol.pro.br (Tutorial On-Line Home Page)

CITAÇÔES:

[APA99]
Conceito de Comunicação. Figuras 2.2, 2.3, 6.1 e 6.2.

[ARN97]
Protocolos da camada de aplicação.

[BAR00]
Figura 4.6, 4.11 a 4.15.
Quadro Comparativo Entre Os Padrões Ethernet / Fast Ethernet / Gigabit Ethernet
Parte dos Componentes de Conexão.

[CYC97]
Figura 6.13. Classes IP.

[COS00]
Arquitetura TCP/IP - Internet. Protocolo Ipv4.

[KIR99]
Endereçamento IP. Sub-Redes IP.

[MAR97]
Parte dos Componentes de Conexão.
Parte dos Servidores Dedicados.
Quadro Comparativo Dos Meios De Transmissão.

[SEM96]
Sub-Redes IP. Figura 6.12.

[SOA96]
Evolução dos Sistemas de Computação.
Objetivos de uma Rede de Computadores.
Parâmetros de Comparação entre Redes de Computadores.
Sistemas Operacionais de Rede. Figuras 7.1 e 7.2.

[SPE00]
Hardware De Rede: Tecnologia de Transmissão, Arranjos Topológicos, Categorias, Partes do Suporte à transmissão. Figuras 4.1 a 4.4, Figura 4.5.
Software de Rede: Capítulo completo incluindo todas as figuras.
Arquiteturas de Redes: Arquitetura RM-OSI incluindo figuras. Camadas do RM-OSI incluindo figuras.Padrão IEEE 802. Interconexão de redes Locais. Partes da Arquitetura TCP/IP incluindo figuras 6.9 e 6.10. Outros exemplos de arquiteturas de redes.

[TOR99] Figuras 4.9 e 4.10.

[WER98]
Resolução de Endereços IP, incluindo Figuras 6.15 a 6.17.
Roteamento IP, incluindo Figuras 6.18 e 6.19.
Fragmentação IP, incluindo Figuras 6.20 e 6.21.
Protocolos da camada de transporte, incluindo Figuras 6.22 a 6.26.