Redes de Computadores: Uma visão geral

Michelli Malagoli

Uberlândia, Dezembro/1998.

Redes de Computadores: Uma visão geral

Michelli Malagoli

Monografia apresentada ao Curso de Ciência da Computação do Centro Universitário do Triângulo - Unit, como requisito básico à obtenção do grau de Bacharel em Ciência da Computação, sob a orientação do Prof. Alfen Ferreira de Souza Jr.

Uberlândia, Dezembro/1998.

Redes de Computadores: Uma visão geral

Michelli Malagoli

Monografia apresentada ao Curso de Ciência da Computação do Centro Universitário do Triângulo - Unit, como requisito básico à obtenção do grau de Bacharel em Ciência da Computação.

Alfen Ferreira de Souza Jr, Msc.	Marcos Ferreira Rezende, Msc.
Orientador	Coordenador
Mônica Rocha Ferreira, Msc.	Alex Dias, Msc.
Avaliador	Avaliador

Uberlândia, Dezembro/1998.

Aos amigos e família pela compreensão nos momentos de ausência.

“Cérebro eletrônico faz tudo, faz quase tudo, mas ele é mudo. Cérebro eletrônico comanda, manda e desmanda, ele é quem manda, mas ele não anda.”

Gilberto Gil - 1969

Agradecimentos ao orientador Alfen Ferreira de Souza Junior, à professora Sílvia FernandaM. Brandão e a Rosimeire Silva Souza que contribuíram de forma decisiva para o resultado final desse trabalho.

RESUMO

Neste trabalho, será abordado os requisitos necessários para a Implantação de Redes. As redes de computadores são formadas por um conjunto de módulos processadores capazes de trocar informações e compartilhar recursos, interligados por um meio de comunicação e um conjunto de camadas hierárquicas, cada uma sendo construída utilizando as funções e serviços oferecidos pelas camadas anteriores. As camadas se comunicam através de meios de transmissão e através de protocolos que organizam a comunicação. Para se escolher um sistema de comunicação é necessário usar um tipo de topologia adequado. Na implantação de uma rede ideal devem ser analisados diversos aspectos. Por isso a escolha de um tipo particular de rede é uma tarefa bastante complicada.

SUMÁRIO

1 - INTRODUÇÃO

Hoje em dia a informação é fundamental e para obtê-la, conexão é a palavra-chave. Num mundo em constante e rápida transformação é preciso estar sempre plugado para não ficar para trás, pois o tempo não espera. Por isso, este trabalho é dedicado ao estudo sobre os princípios básicos das redes de computadores bem como as principais técnicas de implantação.

No início da história do processamento, os computadores eram máquinas de custo bastante elevados que centralizavam em um único ponto o processamento das aplicações de vários usuários e muitas vezes de toda uma organização. Devido aos custos muito elevados, tornou-se necessário o compartilhamento da CPU (Unidade Central de Processamento) e seus periféricos, começando assim os primeiros sistemas multiusuários, chamados *mainframes*.

Mais tarde, com a diminuição do custo da tecnologia digital, surgiram os computadores de médio porte, os minicomputadores e os microcomputadores ou computadores pessoais. Contudo, isso não resolveu o problema da interconexão entre as máquinas. Os dados eram transferidos através de discos ou fitas magnéticas quando era necessário o compartilhamento.

O problema foi solucionado através da interconexão das CPU's entre si. É a isso que se propõe as redes de computadores.

O objetivo desse trabalho é mostrar as características da implantação de uma rede, enfocando as principais facilidades e dificuldades na instalação das mesmas e fazendo uma avaliação onde é viável a utilização de cada uma, levando em consideração os objetivos da organização e a performance esperada.

No capítulo 2 é mostrado os principais tipos de rede, o tipo de compartilhamento dando uma idéia geral sobre os fundamentos de uma rede.

No capítulo 3 é mostrado os meios de transmissão, os segmentos de uma rede, os tipos de cabos e a melhor forma de utilizá-los.

O capítulo 4 trata-se dos protocolos, definindo as características dos principais tipos e onde é viável a utilização de cada um.

No capítulo 5 é mostrado a arquitetura de redes, o modelo OSI (Open System Interconection) e as sete camadas do modelo OSI.

O capítulo 6 trata-se das topologias de rede, mostrando os principais tipos e qual a melhor forma de utilização de cada uma.

O capítulo 7 mostra as principais dificuldades e necessidades na implantação de uma rede mostrando a melhor forma de utilização de cada um dos itens propostos nos capítulos anteriores e tentando se aproximar de uma rede ideal.

2 - FUNDAMENTOS DE UMA REDE

2.1 - INTRODUÇÃO

Uma rede de computadores é formada por um número ilimitado mas finito de computadores autônomos interconectados através de um meio de comunicação. Elas são capazes de compartilhar todos os recursos e trocar informações.

O objetivo de uma rede é tornar disponível a qualquer usuário os programas, dados e outros recursos de qualquer máquina ligada ao sistema, independente de suas localizações físicas.

São considerados como recursos: *Hard Disk*, *drives de CD-ROM*, impressoras, *drives* de disquetes e *modems.*

Outro objetivo das redes de computadores é proporcionar uma maior disponibilidade e confiabilidade, dada a possibilidade de migração de dados e recursos para outro equipamento quando uma máquina sofre alguma falha.

Quanto a distância entre os módulos processadores, as redes foram divididas em:

- Confinadas: quando a distância entre os módulos processadores são menores que alguns poucos metros.

- Redes Locais: (LAN's ou *Local Area Networks*) são sistemas cujos módulos processadores se encaixam na faixa de alguns poucos metros a alguns poucos quilômetros.

- Redes Metropolitanas: (MAN's ou *Metropolitan Area Networks*) são sistemas cujos módulos processadores começam atingir distâncias metropolitanas.

- Redes geograficamente distribuídas: (WAN's *Wide Area Networks*) são sistemas cuja dispersão é maior e geralmente necessitam de recursos como: linha telefônica convencional ou privada, torres de transmissão, satélites, etc.

2.2 - REDES LOCAIS

Surgiram dos ambientes de institutos de pesquisa e universidades [7]. O enfoque dos sistemas de computação antigos levaram em direção à distribuição do poder computacional. Redes locais surgiram para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de *hardware* e *software*), preservando a independência das várias estações de processamento, e permitindo a integração em ambientes de trabalho cooperativo. Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região que são distâncias entre 100 m e 25 Km embora as limitações associadas às técnicas utilizadas em redes locais não imponham limites à essas distâncias. Outras características típicas encontradas e comumente associados à redes locais são as altas taxas de transmissão e baixas taxas de erros. Em geral esse tipo de rede são de propriedade privada.

2.3 - REDES METROPOLITANAS

Uma rede metropolitana apresenta características semelhantes às redes locais, sendo que as MAN's (*Metropolitan Area Networks*) em geral, cobrem distâncias maiores que as redes locais operando em velocidades maiores.

2.4 - REDES GEOGRAFICAMENTE DISTRIBUÍDAS

Sistemas cuja dispersão é maior que os outros tipos. Surgiram da necessidade de se compartilhar recursos especializados por uma maior comunidade de usuários geograficamente dispersos.

Por terem um custo de comunicação bastante elevado (circuitos para satélites e enlace de microondas),

tais redes são em geral públicas, isto é, o sistema de comunicação, chamado sub-rede de comunicação, é mantido gerenciado e de prioridade pública. Face a várias considerações em relação ao custo, a interligação entre os diversos módulos processadores em uma tal rede determinará a utilização de um arranjo topológico específico e diferente daqueles utilizados em redes locais. Ainda por problemas de custo, as velocidades de transmissão empregadas são baixas: da ordem de algumas dezenas de Kilobits/segundo (embora alguns enlaces cheguem hoje a velocidade de megabits/segundo [6]). Por questão de confiabilidade, caminhos alternativos devem ser oferecidos de uma forma a interligar os diversos módulos.

2.5 - TIPO DE COMPARTILHAMENTO

As redes também podem ser classificadas pelo tipo de compartilhamento de seus recursos.

2.5.1 - CLIENTE-SERVIDOR

Configuração usada em médias ou grandes corporações. Devido ao volume, as informações estão todas contidas num computador central, geralmente chamado de servidor e são compartilhados pela rede.

Na arquitetura cliente-servidor a entidade que solicita um serviço é chamada cliente e a que presta serviço é o servidor.

A arquitetura cliente-servidor possui duas variações, definidas pela forma como são utilizados os servidores [6]:

- Com servidor dedicado como por exemplo o servidor de banco de dados corporativo que necessita de segurança, por isso é indicado o servidor dedicado;

- Com servidor não-dedicado como por exemplo um servidor de impressão que não necessita de tanta segurança como o servidor de banco de dados.

A diferença é a possibilidade ou não de uso da estação servidora por usuários locais como sendo também uma estação cliente.

Em geral, o servidor é uma estação com elevada capacidade de processamento cuja função é disponibilizar serviços à rede. Esta máquina processa grandes volumes de dados, necessitando de CPU's rápidas e dispositivos de armazenamento (discos rígidos, discos óticos) de alta capacidade e de rápido acesso.

A arquitetura cliente-servidor geralmente é usada integrando-se diferentes plataformas, permitindo que compartilhem recursos enquanto aproveitam ao máximo as vantagens das plataformas e dispositivos diferentes. Essas plataformas podem ser um microcomputador (PC - Computador Pessoal), uma estação de trabalho, um minicomputador ou um *mainframe*.

Dentre as características de um ambiente cliente/servidor, pode-se destacar:

- Performance: Uma arquitetura cliente/servidor consiste em um processo de cliente e um de servidor, que possam interagir totalmente.
- Interoperabilidade: A parte cliente e a parte servidor podem operar em diferentes plataformas de computador.
- Modularidade: Tanto a plataforma do cliente como a do servidor podem ser atualizadas sem que se tenha a necessidade de atualizar a outra plataforma.
- Transparência: O servidor pode atender a vários clientes simultaneamente e em alguns sistemas cliente/servidor, os clientes podem acessar vários servidores.
- Conectividade: Os sistemas cliente/servidor incluem algum tipo de capacidade de operar em rede na empresa ou em locais fisicamente distantes (acesso remoto).

Os serviços que o servidor pode oferecer à rede são: Servidor de rede; servidor de aplicativos; servidor de arquivos; servidor de impressoras; servidor de banco de dados; Internet e Intranet; servidor de correio eletrônico e servidor de fax.

Caso a velocidade de processamento ou acesso a disco não atenda a demanda, provavelmente o sistema vai ficar muito lento devido ao enchimento provocado no servidor. Se a demanda for muito grande pode-se ter dois ou mais servidores.

O fato dos dados estarem todos no servidor pode se tornar bastante perigoso partindo do princípio que o mesmo pode falhar ou se danificar inesperadamente. Por isso, uma rotina de *backup* (cópia de segurança de dados) é de suma importância.

Os clientes são as estações que acessam os recursos oferecidos pelo servidor e executam tarefas locais. As aplicações cliente-servidor são compartilhadas: parte delas são executadas no servidor e parte delas no cliente.

2.5.2 - PONTO-A-PONTO

É um tipo de rede simples para poucos micros. Ideal para pequenas empresas e para uso doméstico. Na rede ponto-a-ponto não existe um servidor dedicado. Os recursos das estações podem ser compartilhadas entre si por toda a rede.

Na realidade, em uma rede ponto-a-ponto todas as estações podem ser configuradas como clientes e servidores ao mesmo tempo. Além disso, as necessidades de segurança e controle de dados geralmente são menores.

Assim, é possível ter duas ou mais estações como servidoras de disco, outra estação como servidora de impressora e assim por diante. A estação é servidora por compartilhar seu recurso pela rede , e é cliente, pois utiliza os recursos que são compartilhados por outras estações.

Portanto, o usuário de uma rede ponto-a-ponto precisa ter em mente que outros usuários podem estar usando determinado recurso em sua máquina, por isso deverá estar sempre atento ao operá-la.

2.6 - SEGURANÇA EM REDES

A segurança está relacionada à necessidade de proteção contra acesso ou manipulação de informações confidenciais de elementos não autorizados, e também a utilização não autorizada do computador e seus periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização.

Algumas das principais ameaças às redes de computadores são:

- Modificação ou deturpação da informação provocada por ruídos no meio de comunicação;
- Roubo, remoção ou perda de informação ou de outros recursos;
- Revelação de informação para pessoas não autorizadas;
- Interrupção de serviços provocada por pane na rede.

As ameaças podem ser acidentais ou intencionais. As ameaças acidentais são aquelas que não estão associadas a intenção premeditada e ameaças intencionais variam desde a observação de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema [1].

2.6.1 - FIREWALL

Firewall (parede de fogo) é um dispositivo de rede (pode ser um computador ou roteador específico) que filtra o acesso a uma rede de computadores.

Os *firewalls* permitem que o administrador proteja sua rede contra acessos de pessoas não autorizadas. Podem também ser usados no controle de acessos à rede para permitir que certas pessoas da organização tenha acesso aos dados à partir da Internet.

Embora sejam mais utilizados na proteção de redes públicas de acesso e na Internet, podem ser utilizados em grandes redes locais para a proteção de informações estratégicas (acesso a *mainframe*, por exemplo).

Para uma proteção eficaz, deve-se levar em consideração os seguintes requisitos básicos: Controle de acesso; privacidade; autenticação; integridade; gerenciamento; auditoria.

Para se evitar o acesso não autorizado à rede, os modernos *firewalls* se utilizam de modernas técnicas de criptografia.

- CRIPTOGRAFIA

É a transformação dos dados a partir de uma espécie de senha denominada chave. Isto é determinado na forma de que mesmo interceptada a mensagem não possa ser lida por alguém que não tenha a chave para descriptografar.

Existem dois tipos básicos de criptografia que são a chave pública e a chave privada.

Com a chave privada, a entidade remetente utiliza uma determinada chave para criptografar os dados, enquanto o destinatário, utilizará a chave para descriptografar. Este método também é chamado de criptografia de chave secreta.

A geração, transmissão e armazenamento de chaves é chamada de gerenciamento de chaves, característica fundamental de um bom sistema de criptografia.

Com a chave pública, cada pessoa obtém um par de chaves, uma pública e outra privada. Cada chave pública de cada pessoa é publicada enquanto a chave privada é mantida em segredo. Qualquer um pode enviar uma mensagem confidencial utilizando somente a informação pública, mas esta somente poderá ser lida (descriptografada) com a chave privada que está com o destinatário. Este tipo de criptografia pode ser usada tanto para assinaturas digitais como para privacidade.

O problema da criptografia está na possibilidade de um intruso descobrir o método utilizado, tendo então que ser substituído.

- SERVIDOR PROXY

Os proxies são principalmente usados para permitir acesso à Web através de um firewall. Um proxy é um servidor HTTP especial que tipicamente roda em um máquina firewall. O proxy espera por uma requisição de dentro do firewall, a repassa para o servidor remoto do outro lado do firewall, lê a resposta e envia de volta ao cliente[9].

Um nível de aplicação proxy faz um firewall seguramente permeável para os usuários na organização sem criar um furo de segurança onde hackers poderiam entrar na rede de organização.

2.7 - CONCLUSÃO

As redes diferem principalmente pelo tipo de compartilhamento e pela característica geográfica. Quanto ao compartilhamento uma rede pode ser do tipo cliente-servidor para médias ou grandes corporações ou ponto-a-ponto para uma rede de poucos micros.

A segurança é um fator de extrema importância também na implantação de uma rede. Ataques, modificação ou deturpação da informação, acesso de pessoas não autorizadas são fatos que devem ser levados em consideração. Por isso os mecanismos de segurança merecem uma atenção especial.

A escolha de um tipo de rede está diretamente ligada à característica geográfica dessa rede. Através da definição geográfica será definido os meios de transmissão, os protocolos e a topologia utilizada. Esses itens serão vistos nos próximos capítulos.

3 - MEIOS DE TRANSMISSÃO

3.1 - INTRODUÇÃO

Os meios de transmissão são utilizados em redes de computadores para ligar as estações ao meio físico.

Os principais meios de transmissão ou cabos estão descritos neste capítulo.

3.2 - PRINCIPAIS MEIOS DE TRANSMISSÃO

Antes de detalhar sobre os meios de transmissão existentes faz-se necessário definir o que é um cabo. Cabo em sua definição mais genérica é algo que conduz sinais entre nós de rede e de uma forma geral, a palavra fio se refere a fios de cobre individuais contidos em uma cobertura formada por um cabo.

O custo dos cabos de rede local está dividido entre os custos do material e da mão-de-obra. Os preços variam de acordo com a quantidade comprada, de modo que, quanto menor a quantidade de cabos comprada, maior será o preço por metro de cabo.

Três tipos de cabos são usados para conectar computadores entre si em uma rede: cabos coaxiais, de par trançado e de fibra ótica. Eles diferem significativamente em termos de custo, técnicas de instalação e características elétricas.

3.2.1 - CABOS COAXIAIS

Consiste em um condutor de cobre central (um fio sólido ou torcido), uma camada de isolamento flexível, uma blindagem com uma malha ou trança metálica e uma cobertura externa. O termo “coaxial” surgiu porque a malha de blindagem e o condutor central têm o mesmo eixo.

A malha externa do cabo coaxial forma metade do circuito elétrico, além de funcionar como uma blindagem para o condutor interno. Portanto, ela deve estabelecer uma sólida conexão elétrica em ambas as extremidades do cabo.

O cabo coaxial, ao contrário do par trançado, mantém uma capacitância constante e baixa, independente do comprimento do cabo.

Possui uma imunidade a ruído melhor e uma fuga eletromagnética mais baixa. Quanto ao custo, o cabo

coaxial é mais caro que o par trançado, assim como é mais elevado o custo das interfaces para ligação ao cabo.

O cabo coaxial teve uma importante função nas arquiteturas de rede ArcNet e Ethernet. Hoje em dia, não está sendo usado mais.

3.2.2 - PAR TRANÇADO

É composto por pares de fios, sendo que cada par é isolado do outro e todos são trançados juntos dentro de uma cobertura externa. A trança dos pares de fios produz um efeito de proteção mútua. Esse efeito diminui a absorção e a radiação de energia elétrica, mas não é tão eficiente quanto uma lâmina metálica ou uma malha externa.

Os UTPs (*Unshielded Twisted Pairs*) são cabos sem blindagem, eles obtém sua proteção do efeito de cancelamento dos pares trançados [1]. O efeito de cancelamento mútuo reduz a diafonia entre os pares de fios e diminui o nível de interferência eletromagnética de rádio freqüência. Os projetistas de rede variam o número de tranças nos fios contidos em cada cabo, a fim de reduzir o acoplamento elétrico e a diafonia entre os pares. O cabo UTP se baseia unicamente no efeito de cancelamento para reduzir a absorção e a radiação de energia elétrica. Eles podem ser usados com arquiteturas de rede (ArcNet, Ethernet).

Os pares trançados STP (*Shielded Twisted Pairs*) são com blindagem. Combinam as técnicas de blindagem e cancelamento. Os cabos STP projetados para redes têm dois tipos. O STP mais simples é chamado blindado de 100 ohms, pois tem uma impedância (característica elétrica específica de cada cabo proporcionadas pela distância entre os dois condutores, tipo de isolamento e outros fatores [7]) de 100 ohms e contém uma blindagem formada por uma folha de cobre ao redor de todos os seus fios. No entanto, o formato mais comum de STP, é conhecido como STP de 150 ohms devido à sua impedância de 150 ohms, não só o cabo todo é blindado para reduzir a interferência eletromagnética e a interferência de radio freqüência, como cada par de fios trançados é separado um do outro por uma blindagem, o que diminui a diafonia. Ao contrário do que acontece com os cabos coaxiais, a blindagem nos STPs de 150 ohms não faz parte do caminho percorrido pelo sinal, mas é aterrada nas duas extremidades.

Os cabos STPs de 150 ohms são mais utilizados no esquema Token-Ring da IBM, já os de 100 ohms na maioria das vezes são utilizados em instalações Ethernet.

3.2.3 - FIBRA ÓTICA

Esses cabos transportam luz, enquanto os de cobre transportam elétrons [6]. Possuem imunidade total contra diafonia e contra interferências eletromagnéticas e de rádio freqüência. A falta de ruídos internos e externos significa que os sinais têm um alcance maior e se movem mais rápido, o que proporciona uma velocidade e uma distância maiores do que as obtidas com os cabos de cobre.

Como não transporta eletricidade, a fibra é o meio mais adequado para conectar prédios com diferentes aterramentos elétricos. Além disso, os cabos de fibra não atraem raios como os cabos de cobre.

Cada metade do cabo de fibra ótica é composta de camadas de material. Na parte externa, uma cobertura plástica deve obedecer às normas de construção de prédio e aos códigos de proteção contra incêndio para que o cabo inteiro fique protegido. Sob a cobertura, uma camada de fibras tevlar, sob as fibras outra camada de plástico, denominada capa. Quando projetados para entrarem em contato com o solo devem conter fios de aço inoxidável ou de outro material que proporcione maior robustez. Todos esses materiais protegem o fio de fibra de vidro, que é tão fino quanto um fio de cabelo.

As redes de fibra deixaram de ser enigmas de alta tecnologia. Elas representam formas práticas de transportar dados com segurança e confiabilidade.

3.2.4 - OUTROS MEIOS DE TRANSMISSÃO

Além dos três meios de transmissão já mencionados, existem outros meios de transmissão, embora menos utilizados em redes locais. Um desses meios é o Rádio Difusão [2].

É adequado tanto para a ligações multipontos como para ligações ponto-a-ponto. Seu emprego é particularmente importante para comunicações entre computadores e o ambiente de rede local móvel.

Rádio Difusão também é utilizado em aplicações onde a confiabilidade é requisito básico. Essa confiabilidade seria no caso de um rompimento de um cabo, por exemplo.

Radiação infravermelha e microondas são outros meios possíveis de comunicação, mas raramente utilizados em redes locais.

3.2.5 – CABEAMENTO ESTRUTURADO

Um sistema de cabeamento estruturado fornece uma plataforma universal, sobre a qual é construída a estratégia de um sistema corporativo. Com uma infra-estrutura de cabeamento flexível, um sistema de cabeamento estruturado pode suportar múltiplos sistemas de voz, dados, vídeo e multimídia, independentemente de seus fabricantes. Ligada através de uma topologia do tipo estrela, cada estação de trabalho é conectada à um ponto central, o que facilita a interconexão e administração do sistema. Este tipo de proposição permite que haja realmente uma comunicação com qualquer dispositivo, em qualquer lugar, a qualquer hora. Um projeto de cabeamento bem elaborado pode incluir várias soluções independentes de cabeamento, de diferentes tipos de meios, instalados em cada estação de trabalho, com a finalidade de suportar as exigências de performance dos múltiplos sistemas[10].

3.3 - LIGAÇÕES AO MEIO

Quando utilizamos um meio de transmissão, conectamos a ele equipamentos transmissores e receptores [1]. A forma como essas conexões são efetuadas dependem da topologia, que definirá se as ligações físicas são ponto-a-ponto ou multiponto, e do próprio meio físico, que determinará como as ligações podem ser implementadas, respeitando-se as características físicas desse meio.

3.3.1 - PONTO-A-PONTO

As topologias como o anel, a estrela e a topologia parcialmente conectados se utilizam de ligações ponto a ponto.

A interface de uma estação com o anel contém um repetidor que tem dois propósitos principais. O primeiro é contribuir para o funcionamento correto do anel, deixando fluir todos os dados para eles recebidos, depois de regenerá-los. O segundo é fornecer um ponto de acesso para o envio e recebimento de dados por uma estação a ele conectada.

Na topologia estrela, tanto lógica quanto física, utilizam-se ligações ponto-a-ponto entre as estações e o elemento central.

Ligações ponto-a-ponto apresentam menos dificuldades que ligações multiponto, pois não têm os problemas de múltiplas reflexões nem a possibilidade de múltiplas transmissões simultâneas.

3.3.2 - MULTIPONTO

Em ligações multiponto, o meio de transmissão deve ser casado com seus extremos, terminando por sua impedância igual a sua impedância característica, de forma a impedir reflexões.

As ligações são feitas através de transceptores que possuem funções básicas de transmitir e receber sinais do meio, bem como reconhecer a presença desses sinais no meio.

A localização do transceptor fora da estação traz como principal vantagem uma flexibilidade maior para o sistema. As estações podem se situar afastadas do meio de comunicação, estando ligadas ao transceptor por uma linha de comunicação (par trançado). Assim, dentro dos limites estabelecidos pelas características de meio de transmissão entre o transceptor e a estação, esta pode estar localizada em qualquer ponto convenientemente distante do meio comum.

3.4 - INTERLIGANDO SEGMENTOS DE UMA REDE

As redes utilizam repetidores, pontes, roteadores e *gateways* para gerar e transmitir sinais transportados em longas distâncias e para estabelecer comunicações com outras redes locais e remotas através dos meios de transmissão.

3.4.1 - REPETIDORES

Fazem o que o próprio nome sugere: repetem sinais elétricos entre sessões de cabo da rede [9]. 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.

3.4.2 - PONTES

Permitem combinar duas redes locais, além de admitir que estações de uma rede acessem recursos de outra rede local. As pontes utilizam protocolos de acesso ao meio físico na camada física da rede. Através desse recurso, é possível ligar meios físicos diferentes entre si, como os cabos de fibra ótica e os cabos coaxiais, desde que partes utilizem o mesmo protocolo.

3.4.3 - ROTEADORES

Os roteadores operam na camada de rede do modelo OSI. Sua função é examinar a 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 à linhas telefônicas privativas de alta velocidade.

3.4.4 - 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. Em geral, nas redes baseadas em PC's, os *gateways* ligam os PC's a equipamentos, como *mainframes* IBM.

3.5 - CONCLUSÃO

Os meios de transmissão são diretamente ligados à característica geográfica de uma rede. Os principais meios utilizados são os cabos coaxiais, o par trançado e a fibra ótica. Os cabos coaxiais suportam velocidades mais altas que o par trançado e são mais caros. As fibras óticas possuem velocidades ainda maiores e consequentemente custos mais elevados. A maior vantagem da fibra ótica é o fato de não existir ruídos internos e externos obtendo maiores distâncias que os cabos de cobre.

Conectados ao meio de transmissão estão as ligações ao meio que podem ser multiponto ou ponto-a-ponto diferindo principalmente na possibilidade de mútiplas transmissões simultâneas da ligação ponto-a-ponto.

As redes utilizam também os repetidores, as pontes, os roteadores e os gateways que são responsáveis por fazer a comunicação entre redes locais e remotas através do meio de transmissão.

4 – PROTOCOLOS

4.1 – INTRODUÇÃO

Protocolo pode ser entendido como um conjunto de regras para estabelecer comunicação entre duas entidades [3]. Essas regras são compartilhadas sobre o gerenciamento do fluxo de informações, que interagindo com as camadas mais baixas da rede tem como finalidade garantir o intercâmbio de informações ordenado e sem erros.

As funções do protocolo são:

- Endereçamento: especificação clara do ponto de destino da mensagem;
- Numeração e seqüência: individualização de cada mensagem, através de número seqüencial;
- Estabelecimento da conexão: estabelecimento de um canal lógico fechado entre fonte e destino;
- Confirmação de recebimento: confirmação do destinatário, com ou sem erro, após cada segmento de mensagem;
- Controle de erro: detecção e correção de erros;
- Retransmissão: repetição da mensagem a cada recepção da mensagem;
- Conversão do código: adequação do código às características do destinatário;
- Controle de fluxo: manutenção de fluxos compatíveis com os recursos disponíveis.

Através do protocolo as fases de estabelecimento, controle, tráfego e encerramento, componentes da troca de informações são sistematizadas [7].

4.2 – PACOTES

Para que uma mensagem seja enviada via rede, é necessário dividi-la independentemente de seu tamanho original, em pequenos blocos de tamanho predeterminado denominado pacotes.

Como cada estação na rede tem um endereço específico, as comunicações na rede são organizadas em

pacotes contendo o endereço do destinatário, a mensagem propriamente dita e o endereço do remetente.

Portanto como viajam em pacotes, protocolos diferentes podem ser empilhados em várias camadas da rede.

4.3 – TIPOS

Os protocolos mais usados em redes são: o IPX/SPX, *NetBios, Apple Talk*, TCP/IP. Existem também os protocolos de alto nível e os protocolos de baixo nível que serão detalhados nesse capítulo.

4.3.1 – IPX/SPX

Baseado num conjunto criado pela Xerox. Padrão nas populares redes *Novell Netware*, o IPX/SPX também são robustos e muito seguros, porém menos complexos, e por isso indicado para redes locais [3].

A) IPX

O protocolo original de comunicação da *Netware* é chamado *Internetwork Packet Exchange* (IPX). Como ele é uma derivação do protocolo de comunicação Xerox, ele preserva o legado de orientação de bytes do *BIG ENDIAN*, embora os microprocessadores PC´s *Intel Corporation* observem a arquitetura do *LITTLE ENDIAN* .

Vagamente falando, isto significa que os pacotes e blocos de controle do Ipx contém valores, (por exemplo, inteiros, e longos) que são bytes trocados da ordem natural do PC. Consequentemente, você percebe freqüentes funções() dentro da programação de exemplos.

É um serviço de comunicação de baixa conexão e orientação de datagrama. Isso significa que pacotes de

Ipx podem chegar numa ordem diferente da seqüência em que foram enviados, o mesmo pacote pode chegar duas vezes ou um pacote pode nunca chegar. Assim como os serviços de baixa orientação e conexão de datagrama, esse serviço é uma ação de enviar e receber em alta escala.

Em nenhuma circunstância é da responsabilidade dos programas de documentação do Ipx classificar o impacto de nenhum desses desenvolvimentos. Na verdade o Ipx é usado como protocolo de comunicação subordinado. Se o suporte de sessão foi confiável, o Ipx, com programação apropriada, fornece suporte suficiente para adquirir trocas confiáveis de pacote [5].

B) SPX

As próximas versões do *Netware* contém outro protocolo de comunicação chamado *Sequenced Packed Exchange* (SPX). Ao contrário do Ipx, o Spx é um protocolo de sessão com orientação de conexão. Ele garante que as aplicações de recebimento recebam os pacotes na ordem em que foram enviados e pacotes duplicados sejam eliminados. Quando um módulo de recebimento do Spx detecta que está faltando um pacote, o módulo requisita uma nova transmissão do parceiro de comunicação e continua a fazê-lo até cansar seu programa específico de fazer tentativas. Spx também tem provisões para sentir quando o parceiro de comunicação some, permitindo ao módulo que aborte sessões.

Finalmente, o Spx usa amplamente os serviços do Ipx. O vínculo entre eles é tão forte que eles são implementados no mesmo módulo PC se eles estiverem presentes.

4.3.2 – NETBIOS

Criado pela IBM, é um protocolo simples e rápido. Mesmo não tendo a complexidade e segurança dos seus irmãos maiores, o *NetBios* pode ser usado sem problemas em pequenas e médias redes locais [4].

4.3.3 – APPLE TALK

Desenvolvido pela *Apple Computer* para redes de computadores padrão *Macintosh*. Por ser proprietário seu uso também é restrito somente a redes com esse tipo de computador.

4.3.4 – TCP/IP

Com raízes no Departamento de Defesa norte-americano, o TCP/IP é o protocolo usado na Internet é o mais usado no mundo hoje. Foi projetado para interligar computadores à longa distância, por isso é robusto, confiável e seguro. O TCP e o IP são apenas dois membros da família TCP/IP. O TCP (*Transmission Control Protocol*) tem por função o transporte confiável de dados entre os sistemas. O IP (*Internet Protocol*), por sua vez é responsável pelo encaminhamento de pacotes de dados desde a origem até o destino.

Somente os protocolos TCP/IP, o fundamento da Internet mundial, oferecem suporte a Web em redes de áreas locais e mais amplas, incluindo a Internet e a rede local. Para instalar uma Intranet é preciso rodar o TCP/IP na rede. Projetado desde o início para operar em diferentes meios de comunicação, o TCP/IP trabalha em redes Ethernet e Token Ring; ele opera até mesmo através de linhas telefônicas comuns com modems.

A) TCP

É um protocolo da camada de transporte da arquitetura TCP/IP. Ele é responsável por inserir as mensagens das aplicações dentro dos pacotes de transporte, reenviar pacotes perdidos e ordenar a chegada de pacotes enviados por outro micro, ou seja, o transporte confiável dos dados.

O protocolo TCP não exige um serviço de rede confiável para operar. Ele responsabiliza-se pela recuperação de dados corrompidos, perdidos, duplicados ou entregues fora de ordem [8]. Isto é feito anexando-se às mensagens um número de seqüência. O número de seqüência dos dados contidos em um segmento é transmitido junto com o mesmo e é denominado seqüência de segmento.

Na camada de rede são especificados vários protocolos: O ICMP (*Internet Control Message Protocol*) tem a função de transportar mensagens e controle dentro da rede Internet. O ARP (*Address Resolution Protocol*) tem como objetivo o mapeamento do endereço físico. O RARP (*Reverse Address Resolution Protocol*) destina-se a resolver o inverso, ou seja, o endereço das estações que não conhecem o seu endereço IP ou da outra estação, mas possui o endereço físico correspondente. O protocolo IP o que mais se destaca pois é o responsável pelo encaminhamento de pacotes de dados desde a origem até o destino.

B) IP

Sua função é transferir blocos de dados denominados datagramas da origem para o destino, onde a origem e o destino são identificados por endereços IP. Esse protocolo também fornece serviço de fragmentação e remontagem de datagramas longos, para que esses possam ser transportados em redes onde o tamanho máximo permitido para os pacotes é pequeno.

Cada datagrama é tratado como uma unidade independente que não possui nenhuma relação com qualquer outro datagrama. Aqui, a comunicação não é confiável pois não são empregados mecanismos de controle de fluxo ou erros (isso fica a cargo da TCP) [8]. Apenas uma conferência simples do cabeçalho é realizada, para garantir que as informações nele contidas estão corretas.

– OS ENDEREÇOS IP

É através do endereço IP que os *hosts* conseguem enviar e receber mensagens pela rede, em uma arquitetura Internet TCP/IP. Os endereços IP são números de 32 bits, representados por quatro números, cada um com um valor entre 0 e 255.

Como por exemplo: 200.236.143.1.

A primeira parte de endereço identifica uma rede específica na inter-rede, a segunda parte identifica um *host* dentro dessa rede. Este endereço, portanto, pode ser usado para nos referirmos tanto a redes quanto a um *host* individual.

O protocolo IP utiliza três classes diferentes de endereços:

- Na primeira classe, a classe A, é usada para redes de grande porte. Seus endereços variam de 1 a 126, e cada rede tem capacidade de endereçar cerca de 16 milhões de hosts.

- Na classe B os endereços variam na faixa de 128.1 até 191.255, e cada rede pode interligar cerca de 65 mil hosts.

- Já os endereços classe C situam-se na faixa de 192.1.1 até 223.254.254 (os endereços acima de 223 foram reservados para uso futuro), e cada rede pode endereçar 254 *hosts* [3].

– ENDEREÇOS IP E NOMES

Como todo dispositivo de uma rede TCP/IP é identificado por um prudente endereço IP, podemos atribuir um nome a qualquer um deles. Isto torna-se necessário pelo fato que para usuários é bem mais fácil lidar com nomes do que com números.

Uma vez que o software de rede trabalha apenas com números, a tradução dos mesmos para nomes é viabilizada por um grande banco de dados distribuído chamado de *Domain Name Service*.

Neste sistema não existe nenhum banco de dados central que contenha informações sobre todos os computadores ligados a Internet. Estas informações são distribuídas por milhares de computadores, denominados *Name Servers*.

C) CONFIABILIDADE

A confiabilidade torna o TCP/IP o protocolo escolhido para transmissões baseadas em sessão, aplicativos cliente-servidor e serviços críticos como o correio eletrônico. Porém, essa confiabilidade tem um preço. Os cabeçalhos do pacote TCP requerem o uso de bits adicionais para assegurar o correto sequenciamento da informação, bem como *checksun* obrigatório para garantir a integridade do cabeçalho e dos dados. Para garantir a integridade na entrega dos pacotes, o protocolo também requer que o destinatário informe o recebimento do pacote.

Essa informação de recebimento (ou ACK's de *acknowledgments*) geram tráfego de transferência de dados em favor da confiabilidade. Para reduzir o impacto na performance, a maioria dos servidores enviam Ack para todo o segmento de dados (ao invés de todo pacote) ou quando o Ack expira.

4.4 – OS PROTOCOLOS DE ALTO NÍVEL

Esses protocolos de alto nível definem e policiam a comunicação entre os usuários propriamente ditos, ou seja, os pontos finais da comunicação).

Alguns deles estão descritos abaixo:

- *Telnet*: É um protocolo que permite o logon em máquinas remotas. Você passa a utilizar a máquina remota para realizar o processamento. No Windows NT (New Techonology) existe o RAS (*Remote Access Service*, serviço de acesso remoto) que tem os mesmos objetivos do telnet.

- FTP: *File Transfer Protocol* (protocolo de transferência), como o próprio nome já diz é utilizado para transferência de arquivos.

- HTTP: *Hyper Text Protocol*: É o protocolo utilizado pela Web, ele transmite textos, gráficos e qualquer outro tipo de arquivo (substituindo o FTP) além de permitir a navegação através de hiper texto.

4.5. OS PROTOCOLOS DE BAIXO NÍVEL

Para que a troca de informação entre os vários componentes de uma rede local se dê de forma ordenada e/ou eficaz, estabelece-se um número de protocolos que definem as regras a serem usadas quando há comunicação entre os componentes.

Cada interface na sub-rede é geralmente responsável por implementar o protocolo de acesso ao meio que controla transmissões ao meio, o protocolo de enlace que regula a comunicação entre interfaces e o protocolo de acesso a rede que especifica e policia as interações entre a interface e seu usuário, esses protocolos da alçada da sub-rede de comunicação, são chamados protocolos de baixo nível.

4.5.1 – PROTOCOLOS DE ACESSO AO MEIO

Foram desenvolvidos na maioria dos casos para uma topologia particular de rede, no entanto, muitas das estratégias de controle podem ser usados em qualquer topologia, embora às vezes sejam mais adequados a uma topologia particular [1].

Na avaliação de protocolos de controle de acesso, atributos específicos podem ser usados, são eles: Capacidade, equidade ou justiça, prioridade, estabilidade sem sobrecarrega e retardo de transferência.

Capacidade é o máximo que o método de acesso pode tirar do meio, em percentagem da banda passante disponível. As variáveis que afetam a capacidade são: a taxa de transmissão, o comprimento da rede, o número de nós, o tamanho do quadro, o tamanho do cabeçalho e o retardo em cada estação (fila de espera, retransmissão, etc.)

Equidade ou justiça no acesso é desejável na maioria das redes, a fim de permitir às estações o acesso aos recursos compartilhados. Justiça não implica em ausência de prioridade de acesso. Implica simplesmente que a estação deverá ser tratada com igualdade dentro de sua classe de prioridade.

Prioridade: é desejável em várias aplicações, principalmente naquelas que evolvem controle de tempo real.

Estabilidade: é uma característica importante em aplicações onde o carregamento da rede é pesado. Protocolos de acesso que alocam intervalo separado para cada nó são bastante estáveis e exigem grandes variações de retardo. Esquemas baseados em contenção têm sua estabilidade bastante dependente da realização, exigindo sofisticações no tratamento de conflitos para tornar o protocolo mais estável.

Retardo de transferência é a soma dos retardos de acesso e transmissão. O retardo de transferência é na grande maioria dos casos, não em todos, uma variável aleatória.

Os métodos de acesso podem ser divididos em dois grandes grupos: os métodos baseados em contenção e os de acesso ordenado sem contenção.

A) ACESSO BASEADO EM CONTENÇÃO

Numa rede baseada em contenção não existe uma ordem de acesso e nada impede que dois ou mais nós transmitam simultaneamente provocando uma colisão, o que acarretará, geralmente, na perda das mensagens [6].

Alguns protocolos com acesso baseados em contenção:

- Aloha: Esse método foi desenvolvido para a rede Aloha, que lhe emprestou o nome. É uma rede de radiofusão via satélite que do estudo do seu protocolo resultaram grande parte dos protocolos de acesso baseado em contenção.

- CSMA (*Carrier Sense Multiple Access*): Nesse método quando se deseja transmitir, a estação ouve antes o meio para saber se existe alguma transmissão em progresso. Se na escuta ninguém controla o meio, a estação pode transmitir.

- REC-RING (*Resolvable Connection Ring*): Um nó começa a transmissão quando sente que o anel está desocupado. O quadro transmitido propaga-se em uma única direção e é removido do anel pelo nó de origem depois de dar uma volta completa no anel.

B) ACESSO ORDENADO SEM CONTENÇÃO

Ao contrário dos esquemas anteriormente apresentados, vários protocolos são baseados no acesso ordenado ao meio de comunicação, evitando o problema de colisão. Cada método é mais adequado a um determinado tipo de topologia, embora nada impeça seu uso em outras arquiteturas. Os métodos mais usuais são por *polling* e por *slot*.

Polling: É geralmente usado na topologia barra comum. Nesse método as estações conectadas à rede só transmitem quando interrogadas pelo controlador de rede, que é uma estação centralizadora. Se não tiver quadro para transmitir, o nó interrogado envia um quadro de status , simplesmente avisando ao controlador que está em operação.

Slot: Desenvolvido pela primeira vez por Pierce para a topologia em anel, este esquema é algumas vezes conhecido como anel de Pierce ou anel segmentado. O método divide o espaço de comunicação em um número pequeno de segmentos (*slots*) dentro dos quais a mensagem pode ser ordenada [6].

C) PROTOCOLOS DE ACESSO EM REDES ÓTICAS

As redes óticas atualmente disponíveis desdobram a enorme banda passante do meio de transmissão ótico através de multiplexação por divisão de comprimento de onda. Utilizando os novos dispositivos óticos, é possível multiplexar e demultiplexar dezenas ou mesmo centenas de canais de alta velocidade, com comprimentos de onda diferentes, em uma única fibra ótica.

D) ACESSO COM PRIORIDADE

A proliferação de redes locais induziu um grande número de aplicações que exigem requisitos bem diferentes do sistema de comunicação. Os requisitos de tempo e acesso desempenhados podem variar de tal modo que a otimização de acesso para uma dada aplicação pode resultar em uma degradação de acesso, até um ponto insustentável.

A necessidade de funções de prioridade em ambientes de multiacesso é evidente. Uma vez que diferentes aplicações impõem diversos requisitos ao sistema, é importante que o método de acesso seja capaz de responder às exigências particulares de cada uma dessas aplicações. Funções de prioridade oferecem a solução para esse problema.

4.6 - CONCLUSÃO

Os protocolos estabelecem a comunicação entre duas entidades. A comunicação feita pelos protocolos é vertical nas camadas do modelo OSI que será visto no próximo capítulo. Existem vários tipos de protocolos, destacando entre eles o conjunto TCP/IP que é o protocolo da Internet e o mais usado no mundo hoje. Ele é responsável por ligar redes de longa distância, com isso é seguro, confiável e forte.

Os protocolos também se dividem em protocolos de alto nível que definem a comunicação entre os pontos finais (usuários) e os protocolos de baixo nível que são responsáveis pela troca de informação de forma ordenada e eficaz.

5 - ARQUITETURA DE REDES – O MODELO OSI

5.1 - INTRODUÇÃO

A arquitetura de rede é formada por níveis ou camadas. Cada nível executa um conjunto de serviços oferecidos pelo nível inferior a ele [1]. O número de níveis, o nome, o conteúdo e a função de cada nível diferem de uma rede para outra. No entanto, em todas as redes, o propósito de cada nível é oferecer certos serviços aos níveis superiores, protegendo esses dos detalhes de como os serviços oferecidos são de fato implementados.

A camada n em uma máquina se comunica com a camada n em outra máquina, as regras e convenções utilizadas nessa conversação são chamadas de protocolo da camada n. Essa comunicação é horizontal. A comunicação vertical é de uma camada n para uma camada n-1 e n+1.

Os dados transferidos em uma comunicação de um dado nível não são enviados diretamente (horizontalmente) ao processo do mesmo nível em outra estação, mas "descem" verticalmente através de cada nível adjacente da máquina transmissora até o nível físico (onde na realidade há a única comunicação horizontal entre as máquinas), para depois "subir" através de cada nível adjacente da máquina receptora até o nível de destino.

Os serviços executados em uma máquina n só são vistos pela camada n-1 que os enviou. Essa camada n manda serviços para a camada n+1 que manda serviços para a camada n+2 e assim por diante.

5.2 - O MODELO OSI

A ISO (*International Organization for Standartization*) é uma organização internacional que estabelece padrões de comunicação.

Com o objetivo de padronizar as redes de dados remotas de maneira flexível e utilizando facilidades de comunicação de dados, foi criado um modelo aberto (*Reference Model for Open Systems Interconection* - RM OSI), baseado no OSI (*Open System Interconection*).

Este modelo não propõe um padrão propriamente dito, mas um modelo de referência para interconexão de sistemas abertos. Por isso é pouca implementada em sua totalidade [1].

O modelo OSI diz respeito à interconexão de sistemas - o modo como eles trocam informações - e não às funções internas que são executadas por um dado sistema. Ele oferece uma visão generalizada de uma arquitetura estratificada e organizada em camadas. Pela definição que foi dada a sistemas muito simples, como a conexão de um terminal a um computador, e a sistemas muito complexos, como a interconexão de duas redes completas de computadores OSI também pode ser usado como modelo para a arquitetura de rede. O desenvolvimento deste modelo está constantemente sofrendo alterações para poder adaptar-se aos diversos sistemas existentes.

O modelo OSI utiliza uma abordagem estratificada com certos conjuntos de funções alocadas às diversas camadas.

Uma entidade é um elemento ativo em uma camada. Duas entidades em uma mesma camada são denominadas entidades pares. As entidades de uma camada imediatamente acima e, por sua vez, recebem serviços da camada imediatamente abaixo. Por exemplo, as entidades da camada de apresentação prestam serviços à camada de aplicação e recebem serviços da camada de sessão.

As sete camadas sugeridas pelo modelo OSI são: Camada Física, Camada de Enlace de Dados, Camada

de Rede, Camada de Transporte, Camada de Sessão, Camada de Apresentação e Camada de Aplicação.

Na figura 5.2.1 é mostrada a hierarquia das camadas

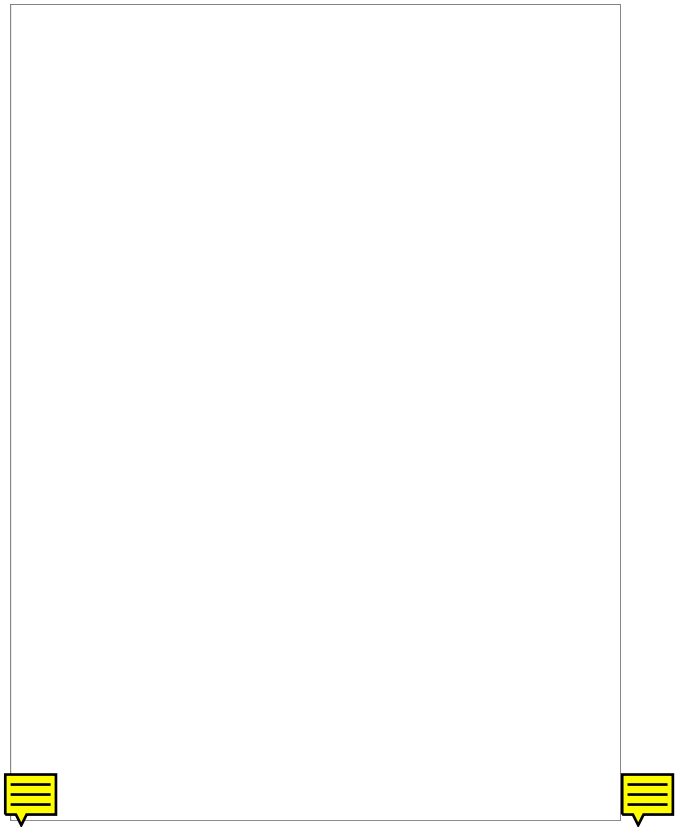

Figura 5.2.1 - Hierarquia das camadas

5.2.1 - CAMADA FÍSICA

A camada física define as características elétricas (níveis de tensão), as características mecânicas (tipo de conectores, dimensões do suporte físico de transmissão, etc) e as características funcionais e de procedimentos das conexões físicas, tratamento das atividades de gerência da camada física, inclusive a

ativação e o controle de erros. Essas funções são solicitadas pela camada de enlace de dados.

A função da camada física é permitir uma cadeia de bits pela rede sem se preocupar com o seu significado ou com a forma como esses bits são agrupados.

É a camada mais importante, ela transporta os sinais das camadas mais altas. Se você interromper a ligação entre a camada física e as outras camadas, não haverá comunicação. Sem as camadas mais altas nada você terá para dizer. Quanto mais alto for no modelo OSI, mais significativa será a comunicação para o usuário final.

São considerados como equipamentos do nível físico os repetidores, os hubs, os modems e os multiplexadores.

5.2.2 - CAMADA DE ENLACE DE DADOS

A camada de Enlace de Dados organiza os bits da camada física em unidades lógicas de informação denominados quadros. Seu objetivo é controlar o fluxo de dados no meio físico, corrigir os erros causados por um meio físico não confiável e fazer o endereçamento físico para identificação dos nós na rede.

São considerados como equipamentos da camada Enlace de Dados as *bridges* e os *switches*.

5.2.3 - CAMADA DE REDE

Nesta camada, os procedimentos decorrentes da interconexão de redes começam a ser considerados de uma forma mais abrangente: endereçamento, tamanho de mensagens, protocolos diferentes, etc. Sua principal função é providenciar a transparência dos dados pelo nível de transporte, permitindo a independência para as camadas mais altas rotear e comutar operações de uma conexão.

São exemplos de padrões definidos para a camada de rede o IP (*Internet Protocol*), o IPX (*Internetwork Packet eXcahnge*) e o CLNP (*Connection Less Network Protocol*).

5.2.4 - CAMADA DE TRANSPORTE

O nível de transporte garante que a cadeia de bits chegue ao seu destino. Pacotes podem ser perdidos ou mesmo reordenados. Para fornecer uma comunicação confiável é necessário o nível de transporte. Esse nível isola a parte de transmissão de rede dos níveis superiores.

As principais funções desse nível é o gerenciamento do estabelecimento e desativação de uma conexão, o controle de fluxo e a multiplexação das conexões. Além dessas funções, ela tem o controle de seqüência, a detecção e recuperação de erros, a segmentação e blocagem de mensagem, entre outras.

Faz parte da camada de transporte controlar a capacidade de *buffers* de recepção e sinalizar aos elementos da rede a existência de problemas.

5.2.5 - CAMADA DE SESSÃO

Essa camada organiza e sincroniza o diálogo e gerência na troca de dados entre entidades de apresentação permitindo que usuários, em máquinas diferentes, estabeleçam sessões entre eles. Uma sessão pode ser usada para permitir que um usuário se conecte a um sistema *time-sharing* ou para transferir um arquivo entre duas máquinas.

5.2.6 - CAMADA DE APRESENTAÇÃO

A camada de apresentação é responsável por fazer a codificação dos dados de modo que a aplicação os receba em um formato reconhecível. Além de negociar a sintaxe dos dados na rede, o nível de apresentação, se necessário, fará a tradução entre os diversos formatos de representação de dados (EBCDIC para ASCII, por exemplo).

Também é função deste nível o suporte aos diversos formatos de compressão de imagem (GIF, JPEG), sons (MIDI, WAV) e vídeo (MPEG, AVI).

A criptografia pode ser utilizada nessa camada para prover privacidade no tráfego da informação.

5.2.7 - CAMADA DE APLICAÇÃO

O nível de aplicação provê os serviços da rede de forma transparente para o usuário final. Uma aplicação tem que ter algum módulo de comunicação para ser enquadrado dentro do modelo OSI. Por exemplo, um processador de texto pode incorporar componentes de comunicação e permitir a transferência eletrônica do documento para o nó da rede.

5.3 - CONCLUSÃO

A arquitetura de rede é formada por níveis. Cada nível oferece os serviços ao nível superior a ele. O número de níveis, a função de cada um e o nome diferem de uma rede prá outra.

Com a intensão de padronizar as redes foi criado o modelo OSI que definiu sete camadas que são: a camada de aplicação, apresentação, sessão, transporte, rede, enlace de dados e a camada física sendo que cada uma tem sua função específica oferecida pela anterior.

6 - TOPOLOGIA

6.1 - INTRODUÇÃO

É uma das questões mais vitais na escolha de qualquer tipo de sistema de comunicação. É considerado o mapa ou o plano de rede [8].

A topologia de uma rede de comunicação irá, muitas vezes caracterizar seu tipo, eficiência e velocidade. A topologia refere-se a 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.

6.2 - TIPOS DE TOPOLOGIA

Os principais tipos de topologia estão descritos abaixo:

6.2.1 - ESTRELA

Nesse tipo de topologia cada nó é interligado a um nó central (mestre) do qual as mensagens devem passar [9]. Este nó age assim, como centro de controle da rede, interligando os demais nós (escravos) que usualmente podem se comunicar apenas com um ou outro nó de cada vez. Isto não impede que as comunicações 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. Em outras redes o nó central tem como única função o gerenciamento das comunicações. O nó central cuja função é o chaveamento (ou comutação) entre as estações que desejam se comunicar é denominado comutador ou *switch*. A comunicação pode ser por chaveamento ou por 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 o nó 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. Como as mensagens se concentram no nó central, esta topologia não necessita de roteamento.

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

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

Outro problema de 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 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 a substituição do nó central.

A figura 6.2.1.1 mostra como os computadores estão ligados ao HUB em uma topologia em estrela.

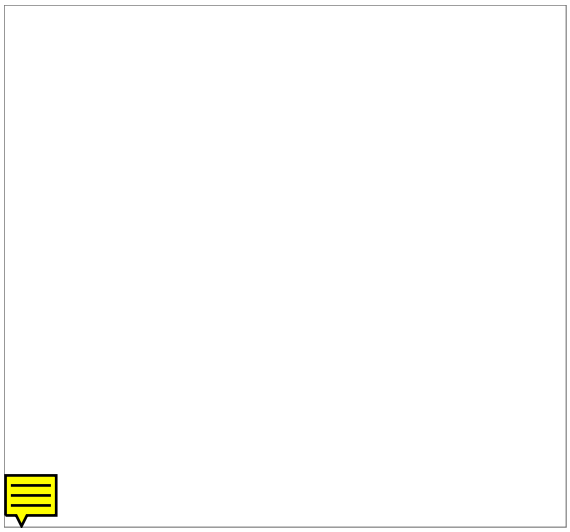

Figura 6.2.1.1 - Topologia em estrela

* HUB - Dispositivo que controla entrada e saída de dados em uma rede de computadores.

6.2.2 - ANEL

A rede em anel é formada de estações conectadas através de um caminho fechado, evitando assim, os

problemas de confiabilidade de uma rede em estrela. O anel não interliga as estações diretamente, mas existe um meio físico, sendo cada estação ligada a esses repetidores.

A transmissão de dados através de uma rede em anel é feita em qualquer direção. São mais usadas as comunicações unidirecionais pois simplificam o projeto dos repetidores de comunicação assegurando a entrega da mensagem ao destino corretamente e em seqüência, pois, sendo unidirecionais evitam o problema de roteamento. Os repetidores são em geral projetados de forma a transmitir e receber dados simultaneamente, diminuindo assim o retardo da transmissão.

As redes onde a mensagem é retirada pelo nó de origem também permitem a difusão onde um pacote é enviado para múltiplas estações simultaneamente. Essas redes também possibilitam a determinadas estações receberem mensagens enviadas por qualquer outra estação de rede.

Topologia em anel requer que cada nó seja capaz de remover mensagens da rede ou passá-las para o próximo nó. Para isso, é necessário um repetidor ativo em cada nó e a rede poderá ser mais confiável do que esses repetidores pois, se houver uma quebra em qualquer dos enlaces entre os repetidores vai parar toda a rede até que o problema seja isolado e um novo cabo instalado. Falhas no repetidor ativo também podem causar a parada total do sistema.

Os repetidores são alimentados e mantidos separados do hardware da estação, pois assim eles estão menos susceptíveis a falha no equipamento ou a própria falta de alimentação elétrica da estação. Uma solução parcial do problema de falha do repetidor consta em prover cada um deles de um relé que pode removê-lo mecanicamente em caso de falha. Essa remoção pode ser impossível se os repetidores imediatamente posterior e anterior ao repetidor com falha estiverem a uma distância maior que o limite exigido pelo meio de transmissão para a interconexão de dois nós.

A topologia pode ser feita suficientemente confiável de forma que a possibilidade de falhas possa ser praticamente ignorada. Existem algumas melhorias, tais como:

A introdução de concentradores, também denominados *hubs*. Inicialmente esses concentradores eram elementos passivos que permitiam a concentração de todo o cabeamento utilizado e possuíam um

mecanismo de relés, acionado externamente, permitia o isolamento de estações em falha. Mais tarde eles passaram a ser utilizados como concentradores do anel. Tal técnica tem várias vantagens. O isolamento de falhas se torna mais simples porque existe um ponto de acesso central para o sinal. Sem o concentrador, quando um repetidor ou enlace falha, a localização da falha requer um busca através de todo o anel, exigindo o acesso a todos os locais que contêm repetidores e cabos. Outra vantagem do concentrador é a possibilidade de adição de novas estações sem a parada total da rede, um vez que novos repetidores podem ser ativados no concentrador sem parar a rede, por meio da utilização de relés. Pode-se fazer também um anel formado pela interconexão de concentradores. A distância entre dois concentradores não deverá ultrapassar o limite máximo permitido sem regeneração do sinal. Embora a utilização de relés permita a rápida recuperação de algumas falhas nos repetidores, existem outras falhas nos repetidores, falhas que podem temporariamente parar toda a rede , como por exemplo, falhas nos segmentos entre os concentradores. Uma solução para o problema seria utilização de caminhos alternativos: duplo anel, triplo anel, etc.

No duplo anel, um dos anéis é o principal e o outro (secundário) é usado só em caso de falha. Esse anel tem sua orientação definida no sentido contrário ao do anel principal.

Para aumentar a confiabilidade de uma rede em anel, uma outra solução seria considerar a rede local como constituindo de vários anéis e o conjunto dos anéis conectados por pontes. A ponte encaminha os pacotes de dados de uma sub-rede a outra com base nas informações de endereçamento. Fisicamente cada anel operaria independentemente, uma falha em um anel vai para somente àquela porção da rede. Uma falha na ponte não impede o tráfego intra-rede, múltiplos anéis podem ser empregados para a obtenção de um maior nível de desempenho.

Os maiores problemas com topologia em anel são sua vulnerabilidade a erros e pouca tolerância à falhas. Qualquer que seja o controle de acesso empregado, ele pode ser perdido por falhas e pode ser difícil determinar com certeza se esse controle foi perdido ou decidir qual nó deve recriá-lo. Erros de transmissão e processamento podem fazer com que uma mensagem continue eternamente a circular no anel.

A figura 6.2.2.1 mostra como os computadores estão ligados em uma topologia em anel

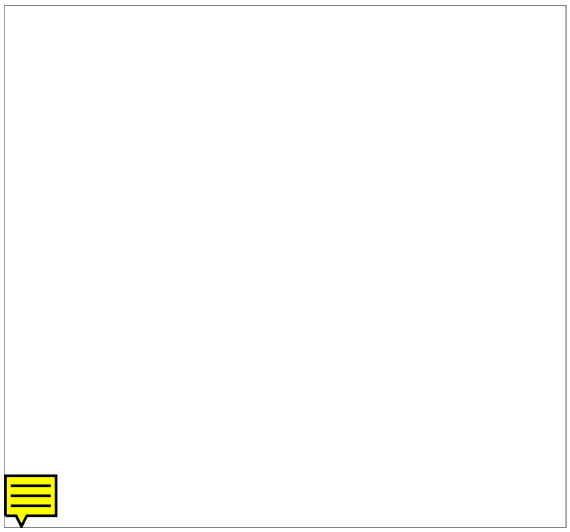

Figura 6.2.2.1 - Topologia em anel

6.2.3 - BARRA

A topologia em barra comum se caracteriza pela ligação de estações (nós) ao mesmo meio de transmissão. A barra geralmente é compartilhada no tempo ou na frequência, permitindo a transmissão de informação. Ao contrário das outras topologia que são configurações ponto a ponto (isto é, cada enlace físico de transmissão conecta apenas dois dispositivos), a topologia em barra tem uma configuração multiponto (isto é, mais que dois dispositivos estão conectados ao meio de comunicação).

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

Existe uma variedade de mecanismos para o controle de acesso à barra, que pode ser centralizado ou descentralizado. A técnica adotada para cada acesso à rede é a multiplexação no tempo. Em um controle centralizado, o direito de acesso é determinado por uma estação especial. Em um ambiente de controle descentralizado, a responsabilidade é distribuída entre os nós.

Diferente da topologia em anel, a topologia em barra pode empregar interfaces passivas, nas quais falhas não causam parada total do sistema. A confiabilidade desse 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 só que aqui a redundância de um nó pode ser outro nó comum da rede. Mecanismos de controle descentralizados são semelhantes aos empregados nesse 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 em barra comum. 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 à sua característica, de forma a evitar reflexões exporias que interfiram com o sinal transmitido. O poder de crescimento, tanto no que diz respeito à distância máxima entre dois nós da rede quanto no número de nós que a rede pode suportar, vai depender do meio de transmissão utilizado, da taxa de transmissão e da quantidade das ligações ao meio. Conforme se queira chegar à distâncias maiores que a máxima permitida em segmento de cabo, esses 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 sistema em barra comum é determinado pelo meio de transmissão, número de nós conectados, controle de acesso, tipo de tráfego e outros fatores. Por empregar interfaces passivas, a inexistência de retardos no repetidor não vão degradar o tempo de resposta, que contudo, pode ser altamente dependente do protocolo de acesso utilizado.

A figura 6.2.3.1 mostra como os computadores estão interligados em uma topologia em barra

Figura 6.2.3.1 - Topologia em barra

6.2.4 - OUTRAS TOPOLOGIAS

Dentre outras topologias podemos citar as topologias em árvore e a estrutura de grafos ou parcialmente ligadas [8].

A topologia em árvore é uma série de barras inter-conectadas. Geralmente existe uma barra 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 barra padrão.

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

A topologia mais geral de redes é a estrutura de grafos. Desta derivam as redes completamente ligadas, as redes parcialmente ligadas, as redes em estrela e as redes em anel.

Redes interligadas ponto-a-ponto crescem em complexidade com o aumento do número de estações conectadas. Neste sistema não é necessário que cada estação esteja ligada a todas as outras (sistema 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 são normalmente baseados no tráfego da rede.

A generalidade introduzida nesse tipo de topologia visa a otimização do custo do meio de transmissão. Devido a isto a topologia é normalmente empregada em redes de longas distâncias (geograficamente distribuídas).

Em redes locais, meios de transmissão de alta veleocidade e privados podem ser utilizados, pois têm um custo menor. Devido a isto 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 tornaria 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 aqui atenuado devido a 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 ligaria possam suportar o aumento de carregamento.

Na tabela 6.3.1 é mostrado um quadro comparativo das topologias e suas características

6.3 - QUADRO COMPARATIVO DE DIVERSAS TOPOLOGIAS

TOPOLOGIA / CARACTERÍSTICAS	ESTRELA	ANEL	BARRA COMUM	GRAFOS
SIMPLICIDADE FUNCIONAL	A melhor de todas	Razoável	Razoável, um pouco melhor que o anel	Extremamente complexa
ROTEAMENTO	Inexistente	Inexistente no anel unidirecional, simples nos outros tipos	Inexistente	Bastante complexo
CUSTO DE CONEXÃO	Alto(incluindo o custo do nó central)	Baixo para médio	Baixo	Muito alto
CRESCIMENTO INCREMENTAL	Limitado a capaci-dade do nó central	Teoricamente infinito	Alto	Alto
APLICAÇÃO ADEQUADA	Aquela envolvendo o processamento central de todas as mensagens	Sem limitação	Sem limitação	Sem limitação
DESEMPENHO	Baixo, todas as	Alto, possibilidade de	Médio	Alto, pode se adaptar

	mensagens tem que passar pelo nó central	mais de uma mensagem ser processada ao mesmo tempo		ao volume de tráfego existente
CONFIABILIDADE	Pouca confiabilidade	Boa, desde que sejam tomados cuidados adicionais	A melhor de todas, interface passiva com o meio	Boa, devido a existência de caminhos alternativos
RETARDO DE TRANSMISSÃO	Médio	Baixo, podendo chegar a não mais que um bit por nó	O mais baixo de todas	Alto
LIMITAÇÃO QUANTO AO MEIO DE TRANSMISSÃO	Nenhuma, ligação ponto a ponto	Nenhuma, ligação ponto a ponto	Pode ter a ligação multiponto. Sua ligação ao meio de transmissão pode ser de custo elevado, como é o caso da fibra ótica	Nenhuma, ligação ponto a ponto

Tabela 6.3.1 Quadro comparativo de diversas topologias

6.4 - CONCLUSÃO

Pode-se interpretar a topologia como sendo o layout, ou seja, a configuração física de como os computadores estão interligados. Elas são divididas em estrela, anel e barra. A topologia em estrela tem a mais simples funcionalidade e o custo alto incluindo o custo do nó central. Seu maior problema é a confiabilidade. O anel possui um custo menor que a estrela e melhor confiabilidade. A barra comum tem o custo menor de todas, possui a melhor confiabilidade, mas a simplicidade funcional é inferior à estrela e superior ao anel.

Existem também os grafos que são muito complexos e possuem custos bastante elevados e as árvores que são uma série de barras interconectadas.

7 - NECESSIDADES E DIFICULDADES NA IMPLANTAÇÃO DE REDES

7.1 - INTRODUÇÃO

A escolha de um tipo particular de rede para suporte a um dado conjunto de aplicação é uma tarefa difícil. Cada arquitetura possui certas características que afetam sua adequação a uma aplicação em particular. Nenhuma solução pode chamar para si a classificação de ótima quando analisada em um contexto geral, e até mesmo em particular [8]. Muitos atributos entram em jogo, o que torna qualquer comparação bastante complexa. Esses atributos dizem respeito ao custo, à confiabilidade, ao tempo de resposta, à velocidade, ao desempenho, à facilidade de desenvolvimento, à disponibilidade, à facilidade de uso, à facilidade de manutenção, etc.

7.2 - ATRIBUTOS ESSENCIAIS NA ESCOLHA DE UMA REDE

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 [6]. 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 às suas 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.

Várias são as medidas que caracterizam o desempenho de um sistema, com isso faz-se necessário definir o que é retardo de transferência, retardo de acesso e retardo de transmissão [1].

Retardo de acesso é o intervalo de tempo decorrido desde que uma mensagem à transmitir é gerada pela 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 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 deve 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 tráfego 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.

A utilização efetiva do sistema de comunicação é apenas uma porcentagem da capacidade total que ela oferece. Uma rede deve proporcionar capacidade suficiente para viabilizar à que é destinada, e certos critérios devem ser levados em conta, a escolha adequada de arquitetura [2], incluindo a estrutura de conexão, o protocolo de comunicação, o meio de transmissão, velocidade e retardo de transferência de uma rede são essenciais para um bom desempenho de uma rede local.

A confiabilidade de um sistema em rede pode ser avaliada em termos de tempo médio entre falhas, tolerância a falhas, degradação amena, tempo de reconfiguração após falhas e tempo médio de reparo.

O tempo médio entre falhas é geralmente medido em horas, estando relacionado com a confiabilidade de

componentes e nível de redundância.

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

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 sem recursos de redundância, mecanismos de autoteste, diagnóstico e manutenção eficiente [2].

Modularidade pode ser caracterizada como grau de alteração de desempenho e funcionalidade que uma rede pode sofrer em mudar seu projeto original. Os três maiores benefícios de uma arquitetura modular são a facilidade para modificação que é simplicidade com funções lógicas ou elementos de hardware podem ser substituídos, a respeito da relação íntima com os outros elementos; a facilidade para crescimento diz respeito à configurações de baixo custo de expansão; e a facilidade para o uso de um conjunto de componentes básicos será melhor para viabilizar um projeto, adicionar equipamentos à rede, manutenção do sistema como um todo.

Uma rede bem projetada deve se adaptar modularmente às várias aplicações que é dedicada, como prever futuras instalações.

De fundamental importância a compatibilidade será aqui utilizada como a capacidade que a rede possui para se ligar a dispositivos de vários fabricantes, que a nível de hardware quer a nível de software. Essa característica é extremamente importante na economia de custo de equipamentos já existentes.

7.3 - SISTEMAS OPERACIONAIS

Os sistemas operacionais de redes (ou NOS), são uma extensão dos sistemas operacionais locais complementando-os com um conjunto de funções básicas possibilitando o compartilhamento através de rede [6].

Como o NOS é o coração da rede, deve-se fazer um criterioso estudo visando a escolha do NOS mais adequado às necessidades diversas.

Deve-se considerar diversos aspectos como: quantidade de estações de trabalho, desempenho, compatibilidade com as aplicações, necessidade de interface com outros NOS, sistemas operacionais das estações de trabalho, etc.

Existem sistemas para rede cliente-servidor e sistemas para redes ponto-a-ponto. Os sistemas operacionais mais conhecidos são Windows NT, Unix, Novel Netware e OS/2 Server.

7.3.1 - WINDOWS NT

O windows NT (New Technology) é um ramo separado da família windows. O NT possui recursos multitarefas integrais que faltam ao windows. Isso significa que o computador pode executar diversas tarefas, incluindo comunicações, de uma só vez sem falha. O pacote do servidor NT também oferece mais segurança que o windows [7]. Tanto o windows como o windows NT fazem uso extensivo das operações em 32 bits para mover rapidamente os dados dentro do computador.

O windows NT possui a capacidade de utilizar multiprocessamento simétrico que significa a alocação de tarefas para duas ou mais CPU’s simultaneamente em hardware, e inclui drivers de rede TCP/IP. No entanto, se a necessidade não é segurança máxima, confiabilidade total, ou multiprocessamento simétrico do windows NT, é melhor escolher o windows 95 ou uma versão mais avançada para executar aplicativos mais modernos e integrar necessidades de redes, já que o custo geral dos equipamentos e softwares são bem menores.

7.3.2 - UNIX

O sistema operacional unix controla os recursos do computador, faz sua distribuição entre os vários usuários concorrentes, executa o escalonamento de tarefas, controla os dispositivos periféricos conectados ao sistema, fornece funções de gerenciamento dos sistemas e, de um modo geral, oculta do usuário final a arquitetura interna da máquina . Isso é realizado através de uma arquitetura que usa camadas de software projetada para diferentes finalidades[7].

O unix executa multiprogramação, na qual diversos programas podem ser executados e multiusuário no qual várias pessoas o utilizam simultaneamente arbitrando as várias solicitações para distribuir os recursos do computador justa e eficazmente.

- UNIX/WINDOWS NT

O unix e o NT são surpreendentemente iguais no projeto e nas capacidades mas suas diferenças são significativas. Ambos oferecem textos e aplicativos básicos. Ambos dão aos aplicativos um espaço de endereçamento virtual no qual rodam. Os dois dão suporte a CPU's múltiplas e a processos leves. Rodam em uma variedade de plataformas, embora o unix faça com muito mais delas. Suportam sistemas de arquivos avançados com longos nomes. Ambos oferecem um poderoso compartilhamento de arquivo e outros serviços de redes similares[8].

O unix é uma escolha bem respeitável para servidores de banco de dados. Porém o NT ganhou reputação pela implementação e gerenciamento mais fáceis, além de ser uma ótima escolha para o compartilhamento de arquivos e impressoras.

7.3.3 - NOVELL NETWARE

Poderoso, extremamente confiável e robusto, o netware é uma excelente opção para redes médias e grandes.

7.3.4 - OS/2 SERVER

Robusto, confiável e estável, o OS/2 Server da IBM conta com uma boa base instalada nos Estados Unidos, principalmente na área de serviços públicos.

- A ESCOLHA CERTA

Em ambiente cliente-servidor, a escolha do NOS é crítica, por isso deve-se observar atentamente os seguintes aspectos:

- Gerenciamento: quanto maior a rede, mais complexo é o seu gerenciamento. Um bom NOS deve fornecer uma completa infra-estrutura para acessar, gerenciar e controlar recursos da rede à partir de um único ponto.

- Escalabilidade: acompanhar o crescimento da rede é de importância capital. As redes crescem rapidamente, ao passo que empresas e departamentos se conectam para formar redes corporativas e inter empresariais.

- Desempenho: a escalabilidade só é possibilitada se houver um bom desempenho. O número de usuários, aplicações e operações que um NOS pode suportar rápida e simultaneamente é também muito importante.

- Segurança: a segurança para arquivos, usuários, níveis de conexão, controle e rastreamento de atividades do usuário é fundamental nas redes atuais.

- Tolerância à falhas: a tolerância completa à falhas é necessária em serviços de missão crítica da empresa. Um bom NOS deve dispor de recursos como espelhamento de disco, de servidor e de possibilidade de recuperação de dados após um "*crash*".

- Custo benefício: o NOS deve não só dispor de boas qualidades técnicas mas ter um custo compatível. Hardware, software, administração e suporte juntos determinam o custo de uma rede.

- Ferramentas para a Internet: a Internet está rapidamente se incorporando à redes de todos os tamanhos. É muito importante que o NOS disponha de boas e fáceis ferramentas para a conexão da Internet.

- Suporte ao usuário: os usuários da rede devem ter a possibilidade de acesso à detalhada documentação *on-line*, em manuais e pronto atendimento via telefone ou fax.

7.4 - CONCLUSÃO

Uma rede deve suportar todas as aplicações para a qual foi elaborada e mais aquelas que o futuro requer. Quando possível, não deve ser vulnerável à tecnologia, prevendo a utilização de futuros desenvolvimentos, quer sejam novas

estações, novos padrões de transmissão ou novas tecnologias de transmissão.

8 - CONCLUSÃO

As características geográficas das redes locais e metropolitanas são bastante diferentes das redes de longa distância, principalmente considerando os custos e a tecnologia. Em redes locais e metropolitanas são usados meios de transmissão de alta velocidade, baixa taxa de erro, baixo custo e de propriedade privada, enquanto que em redes de longa distância a velocidade é menor, os custos são bem mais elevados e elas são em geral de propriedade pública.

A dispersão geográfica é fundamental também na escolha da topologia. Em alguns tipos de topologia a ligação ao meio de transmissão limita-se ao número de nós que a rede pode suportar. Com isso o número máximo de nós, a distância máxima e mínima entre eles e a taxa máxima de informações transmitidas influenciam tanto no meio de transmissão utilizado quanto na topologia de rede.

Influenciados também pela dispersão geográfica e automaticamente pelo meio de transmissão, os protocolos são responsáveis por mecanismos de detecção de erros e recuperação de dados quando são escolhidos ambientes ruidosos e com problemas de segurança na implantação de redes. A escolha do protocolo de acesso depende do tempo de resposta esperado. Para aplicações em tempo real, a garantia de uma resposta rápida é uma característica bastante desejável. Em qualquer aplicação existe sempre uma possibilidade de erro de transmissão, que causará um retardo no tempo de resposta. Por isso é importante que esse problema não seja causado pelo protocolo utilizado.

A arquitetura é fundamental na implantação de uma rede por ser formada por níveis, interfaces e protocolos que delimitam e isolam funções de comunicação entre as camadas.

Uma das maiores dificuldades em redes é sem dúvida a parte física, ou seja, o cabeamento. É complicado ter que trocar um cabeamento velho e obsoleto porque envolve uma imensa mão-de-obra e enormes transtornos ao estabelecimento onde se encontra. Pode-se trocar as máquinas, o sistema operacional, o software com relativa facilidade (o trabalho é quase todo a nível operacional), mas os cabos não. Nenhum outro componente da rede possui um ciclo de vida mais longo ou requer uma atenção tão profunda. Uma solução para se contornar esse problema seria o cabeamento estruturado que integra sistemas de dados, voz e vídeo.

A escolha de um tipo de rede é uma tarefa complicada. Nenhuma solução pode ser chamada de ótima se analisada em um contexto geral. Para se ter uma rede ideal antes de mais nada é imperativo definir o tipo de tecnologia de cabeamento a ser empregado levando-se em consideração todos os demais fatores como o tamanho da rede, o tráfego e também o futuro como ampliações de rede e as mais novas tecnologias de transmissão. Portanto ela deve ter a capacidade de suportar todas as aplicações para a qual foi dedicada e mais aquelas que o futuro possa requerer.

Importante também na implantação de qualquer rede é a segurança. Controlar o acesso, assegurar os dados ou até mesmo a utilização do computador e seus periféricos é uma questão de proteção e não há quem queira estar desprotegido, por isso segurança é um tema com vasto campo de pesquisa, haja visto que o mundo gira em torno da tecnologia. Desenvolver projetos para segurança em rede pode resultar em boas oportunidades profissionais.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] TANENBAUM, Andrew S., 1944 - ; Redes de Computadores/ Andrew S. Tanenbaum; tradução de publiCare Serviços de Informática - Rio de Janeiro, 1994.

[2] DERFLER, Frank J. ; Guia de Conectividade; Frank J. Derfler Jr.; tradução , Insight Serviços de Informática - Rio de Janeiro: Campus 1993.

[3] SCHWADERER, W. David; C Programmer's Guide to NETBIOS, IPX and SPX/ W. David Schwaderer; criação de 3Com Corporation, Editora Infoworld Magazine - 1992.

[4] HAUGDAHL, J. Scott; Inside Netbios 3rd Edition/ J. Scott Haugdahl; Editora Architecture Technology Corporation - 1990.

[5] EVANS, Tim; Construindo uma Intranet; tradução: Eduardo Nunes, título original assunto: Intranet e Redes - 1998.

[6] SOARES, Luiz Fernando Gomes; Redes de Computadores: das LAN's, MAN's e WAN's às redes ATM/ Luiz Fernando Gomes Soares, Guido Lemos e Sérgio Colcher - 2.ed.rev.e.ampliada. - Rio de Janeiro: Campus, 1995

[7] HTTP:/ www.geocities.com/capecanaveral/3427

[8] HTTP:/ www.angelfire.com/nh/fbdias

[9] HTTP:/www.penta.ufrgs.br/redes296/proxy/proxy.htm

[10] HTTP:/www.anixter.com/la/solution/cabling/x3084100.htm