

1. INTERCONECTIVIDADE

Para entender a forma com que diversas redes podem ser interconectadas, deve-se procurar compreender o modelo OSI, pois torna-se bem mais fácil o entendimento quando se visualiza a independência entre os sete níveis do modelo. Dessa forma, quando sistemas operacionais diferentes ou sistemas de rede diferentes devem ser interconectados, existe a necessidade de um padrão único de comunicação, onde qualquer máquina de qualquer fabricante deverá falar a mesma linguagem ou padrão. Assim, por exemplo, todas as máquinas independentemente do sistema operacional ou fabricante, podem se comunicar via um padrão único, como é feito atualmente na Internet através dos protocolos TCP/IP

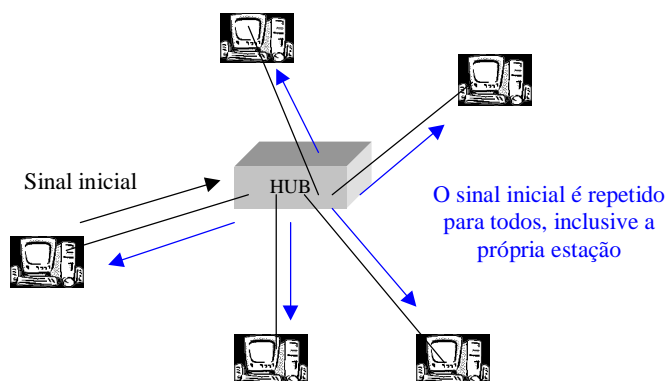
Algumas situações exigem a interconexão de redes iguais divididas para balancear a carga (Ethernet-Ethernet, por exemplo), outras em redes que utilizam protocolos diferentes, tais como Ethernet e Token-Ring. Outras situações requerem a conexão de redes locais com redes de longa distância, tais como Ethernet com X.25. Para executar tais interconexões, é necessária a utilização de determinados equipamentos, que serão estudados neste capítulo.

Os principais equipamentos que fazem a interconexão entre segmentos de rede, alguns modificando os protocolos de rede para manter a compatibilidade com o outro segmento, são os **Repetidores**, as **Pontes**, os **Switches** e os **Roteadores**, que serão analisados a seguir. A figura abaixo ilustra a interconexão de redes heterogêneas utilizando esses equipamentos.

1.1 Repetidores e hubs

Repetidores são equipamentos cuja principal função é amplificar sinais elétricos, sem dar tratamento algum à informação que passa através dele. Sua necessidade surge quando tem-se cabos longos e a potência do sinal não é suficiente para fornecer a corrente necessária por toda a extensão do cabo, ou para difundir o sinal em uma rede local.

A principal utilização dos repetidores é através dos equipamentos conhecidos como hubs (concentradores), que interligam uma rede local no nível físico. A figura a seguir mostra seu funcionamento.



Outra utilização é como amplificador, como nas redes Ethernet, cuja distância máxima (com cabo coaxial grosso) é de 2.500 m, mas os *chips* dos *tranceivers* só tem

potência para 500 m. Uma das soluções é utilizar repetidores para poder aumentar a distância.

Assim, conecta-se o repetidor entre dois segmentos de cabo da rede. Este repetidor vai retemporizar e regenerar os sinais digitais de uma ponta, recolocando-os em sua rota novamente. Ele tem capacidade de movimentar tráfego nos dois sentidos de um cabo de rede, sendo utilizado principalmente em redes locais e de longa distância.

Como os repetidores trabalham diretamente no meio físico, amplificando os sinais, pode-se dizer que eles estão situados no nível 1 do modelo OSI, dessa forma, eles podem ser utilizados somente em redes iguais, ou seja, Ethernet-Ethernet, RS232-RS232, etc.

/**/ domínio de colisão e broadcast - hubs

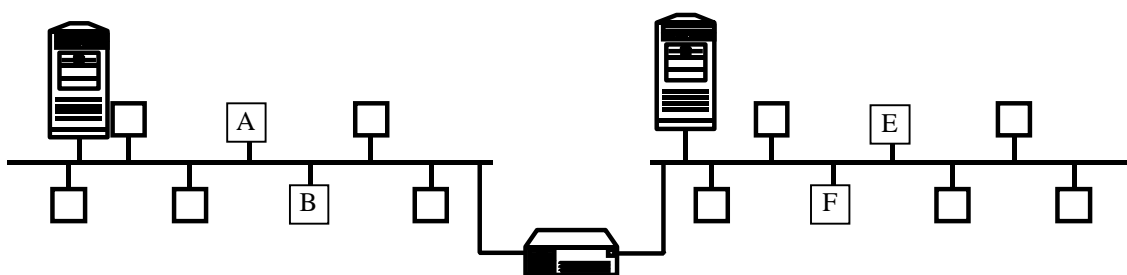
/**/ conectando mais de um hub entre si

/**/ cabo cross para ligar diretamente dois PCs

1.2 Pontes (Bridges)

Pontes são equipamentos que trabalham no nível de enlace (nível 2) do modelo OSI, portanto, uma ponte pode interligar duas redes que utilizem protocolos de nível de enlace diferentes, como por exemplo Ethernet e Token Ring, ou Token Ring e FDDI. **OBS:** Na prática se utilizam roteadores para isso.

As pontes possuem uma certa inteligência, armazenando o quadro e transmitindo para o outro segmento somente se o quadro for destinado a ele, e ignorando-o caso seja destinado ao mesmo segmento. Isso permite uma carga menor na rede como um todo, já que os quadros do mesmo segmento não vão "poluir" os outros segmentos. Para ilustrar esse fato, pode-se ver pela figura abaixo que pode acontecer uma comunicação entre as estações A e B ao mesmo tempo que acontece outra comunicação entre as estações E e F. Com a utilização de uma ponte, o quadro só vai para o outro segmento se for destinado a ele, ou seja, uma comunicação entre as estações A e F, por exemplo.



Devido a essa característica, muitas vezes utiliza-se pontes para conectar segmentos da mesma rede. Por exemplo, interligando dois segmentos de rede Ethernet através de pontes vai diminuir o número de colisões da rede, diminuindo a carga total da rede e melhorando o desempenho das aplicações.

Para saber se o destino do quadro está localizado no mesmo segmento da estação origem ou deve ser retransmitido para o outro segmento, as pontes utilizam um algoritmo simples, criando tabelas baseando-se no endereço fonte do pacote à medida que eles vão passando pela rede.

Assim, inicialmente, quando uma estação **A** transmite um pacote de dados à uma estação **B**, a ponte sabe o segmento da estação **A** (pois foi de onde partiu o pacote), mas não sabe o segmento da estação **B**. Portanto, envia o pacote para o outro segmento e armazena em sua tabela que a estação **A** está no **segmento 1**, por exemplo. Entretanto, quando a estação **B** responde à consulta de **A**, a ponte descobre qual o segmento de **B** (**segmento 1**). Consultando sua tabela, descobre que já tem o endereço de **A**, e fica no mesmo segmento de **B**. Assim, não redireciona o pacote ao segmento 2 e já cadastra a estação **B** na tabela.

Após esses dois pacotes, a tabela da ponte deve conter algo semelhante ao seguinte esquema:

Estação	Segmento
A	1
B	1

A seguir serão descritas algumas situações comuns onde são utilizadas pontes para conectar segmentos de redes. As mesmas funções podem ser efetuadas por switches, como será visto adiante.

- Em uma grande empresa ou universidade, podem existir diferentes departamentos com diferentes interesses, cada um com seus próprios computadores, estações de trabalho e rede local. Em algum momento pode existir a necessidade de conectar esses departamentos entre si, e uma das formas é através de pontes (caso as redes sejam compatíveis no subnível LLC do nível de enlace);
- Pode ser necessário dividir a carga de uma rede de mesmo protocolo para diminuir a carga. Por exemplo, uma empresa com 30 máquinas pode decidir dividir sua rede em dois segmentos de 15 máquinas separados por pontes, com cada segmento possuindo seu próprio servidor. Isso resulta numa diminuição da carga total do sistema e também no número de colisões;
- Em algumas situações, a carga pode ser adequada para uma única LAN, mas a distância entre a primeira e última estação é muito grande, passando do limite suportável pela rede (por exemplo, a máxima distância de uma rede Ethernet é 2,5 Km com repetidores);
- Por questões de segurança, podem ser inseridas pontes em locais críticos em que vai passar o cabo (como portas corta fogo). Assim, caso o cabo seja rompido por alguma razão, somente um segmento será afetado;
- Muitas interfaces de rede local possuem o modo promíscuo, na qual todos quadros são recebidos pelo computador, e não apenas os endereçados a ele. Espiões utilizam esse artifício para obter informações ilicitamente. Inserindo pontes em alguns locais estratégicos pode isolar determinadas comunicações sigilosas.

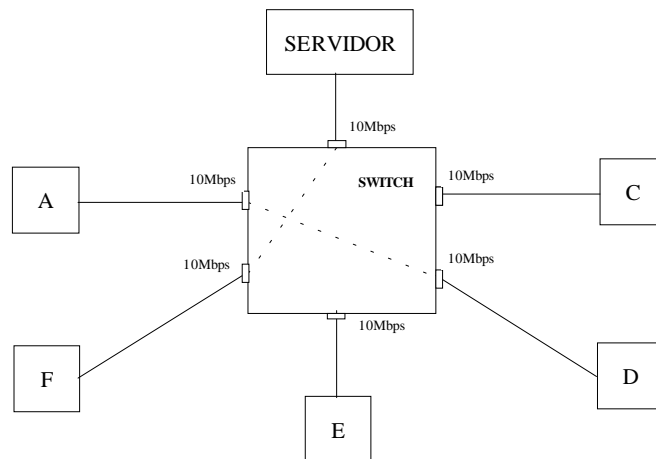
/**/ domínio de colisão e broadcast - pontes

1.3 Switches

Os *switches* podem ser considerados como uma evolução das pontes, porém, com múltiplas portas. Eles são equipamentos que trabalham no nível 2 do modelo OSI e permitem a interconexão entre máquinas diretamente, ou seja, simulando uma conexão **ponto a ponto**. Essa é uma grande vantagem em relação aos *hubs*, pois estes somente conseguem fazer uma conexão do tipo *broadcast*.

Assim, em uma rede local com *hub* central, os 10Mbps da Ethernet são compartilhados por todas as estações, provocando colisões e queda de desempenho. Como se sabe, uma rede Ethernet deve ser projetada com tráfego médio de, no máximo, 40% de sua capacidade nominal.

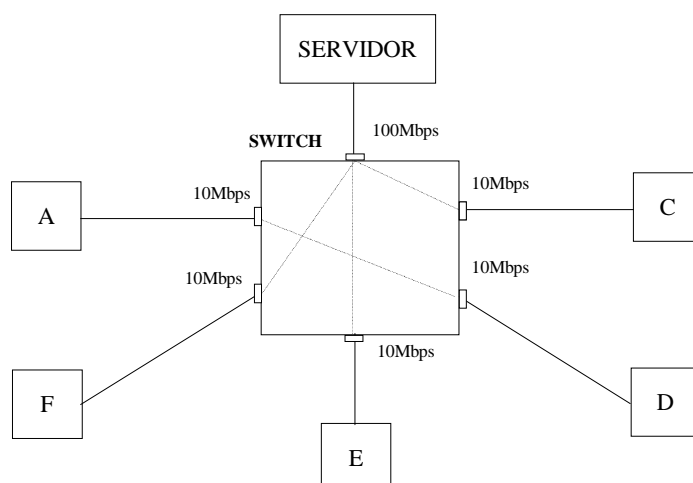
Já no *switch*, a largura de banda é dedicada entre as estações, eliminando as colisões e provocando um aumento de desempenho. A figura a seguir ilustra várias estações se comunicando simultaneamente.



Com a eliminação das colisões, as estações não precisariam mais ouvir a informação à medida que transmitissem o pacote (característica do CSMA/CD). Dessa forma, sobra um par de fios no esquema Ethernet. Aproveitando-se disso, os fabricantes já lançaram no mercado o Ethernet *full-duplex*, onde as estações falam por um par de fios e ouvem por outro, duplicando a velocidade da rede, ou seja, as estações falam entre si a 20Mbps (ou 200Mbps no caso de redes Fast-Ethernet).

Entretanto, caso se utilizem placas *full-duplex*, é necessário a utilização de *switches* que suportem esse protocolo.

Mesmo assim, num segmento de rede, normalmente a comunicação não é como foi ilustrado na figura acima, e sim entre estações clientes e servidor. Dessa forma, existiria um “gargalo” para acesso ao servidor. Para resolver isso, existem *switches* com portas de diferentes velocidades, ou seja, várias portas **Ethernet** de 10Mbps e uma **Fast-Ethernet** de 100Mbps, onde fica o servidor. A figura a seguir ilustra o que foi dito.



Um cuidado que deve-se levar na hora de escolher as placas de rede para operar nessa arquitetura é a forma com que são resolvidas grandes transferências de dados entre o servidor e o cliente. Caso o servidor (operando a 100Mbps) transmita um arquivo de 10Mbps ao cliente (operando a 10Mbps), pode acontecer um estouro de *buffer*, já que o servidor vai enviar a 100M e o cliente vai receber a 10M, criando-se rapidamente uma fila na porta associada ao cliente. Para resolver esse problema, existem estudos para compatibilizar melhor essa diferença de velocidade. Uma forma de resolver esse problema é a placa do servidor saber que as outras portas são de 10Mbps e enviar a informação no máximo a 10Mbps.

Existem duas formas de operação do *switch* para transmitir os pacotes entre as estações ou os segmentos: *Store and Forward switching* e *Cut-Through switching*.

1.3.1 Switches Store and Forward

A operação *Store and Forward* caracteriza-se exatamente pelo que o nome diz, ou seja, o *switch* armazena todo o pacote de nível 2, analisa o CRC, e envia o pacote ao outro segmento somente se tudo correu bem. Essa técnica é mais lenta devido ao tempo que leva para analisar o pacote recebido. Normalmente é necessário a fim de converter um pacote entre tipos diferentes de redes, como Ethernet e FDDI.

Essa técnica também é obrigatória quando se utilizam *switches* de nível 3, pois eles devem analisar o pacote para fazer funções de roteamento.

1.3.2 Switches Cut-Through

A operação *Cut-Through* caracteriza-se pelo fato do *switch* enviar o pacote ao outro segmento tão logo descubra a porta destino, ou seja, assim que examina o endereço MAC de destino. Essa técnica é mais rápida, e o controle de erros é deixado para tratamento nas estações finais.

Um problema dessa técnica é quando a porta do *switch* está conectada a um segmento de rede baseado em Ethernet, ou seja, com colisões (utilizado quando o *switch* está interligando segmentos de redes locais). O problema é que, quando uma colisão ocorre, o que circula na rede local é um quadro “rotten”. Caso a colisão tenha acontecido após a transmissão do endereço destino, o *switch* já vai retransmitir o quadro

para o destino, provocando a existência de um quadro “rotten” circulando pela rede desnecessariamente. Esse tipo de problema não ocorre se toda rede é baseada em *switches* ou em redes locais sem colisão, pois nesse caso não existem colisões.

Os *switches* livres de fragmentos (*Fragment Free*) melhoram esse tipo de problema, como pode ser visto a seguir.

1.3.3 Switches *Fragment Free*

Os *switches* livres de fragmento utilizam a técnica de retransmissão *Cut-Through*, porém, somente repassam o quadro se ele contiver mais do que 64 bytes, que é o tamanho mínimo nas redes Ethernet. Dessa forma, eliminam a passagem de pacotes “rotten” pela rede, sendo, entretanto, um pouco mais lentos que o *Cut-Through* puro.

1.3.4 Gerência de memória no *switch*

E o que faz o *switch* quando tem duas ou mais comunicações para o mesmo endereço? A solução comumente utilizada é que ele mantenha um *buffer* interno para cada porta existente. Dessa forma, ele armazena temporariamente o quadro até poder transmiti-lo. A diferença entre os *switches* do mercado está na forma com que eles gerenciam essa memória. Alguns possuem um *buffer* dedicado para cada porta. Caso tenha muitas comunicações para essa porta, pode acontecer do *buffer* terminar, fazendo com que sejam perdidas informações (mesmo que os *buffers* das outras portas estejam livres). Outra solução é utilizar uma gerência para a memória. Assim, tem-se uma memória para cada porta do *switch* e uma memória global. Caso o *buffer* da porta estoure, automaticamente os quadros passam a ser guardados na memória global. Nessa última forma, com o mesmo tamanho de memória, consegue-se um melhor aproveitamento e menos perda de informação.

/**/ domínio de colisão e broadcast - switches

/**/ placas full duplex

1.4 Roteadores

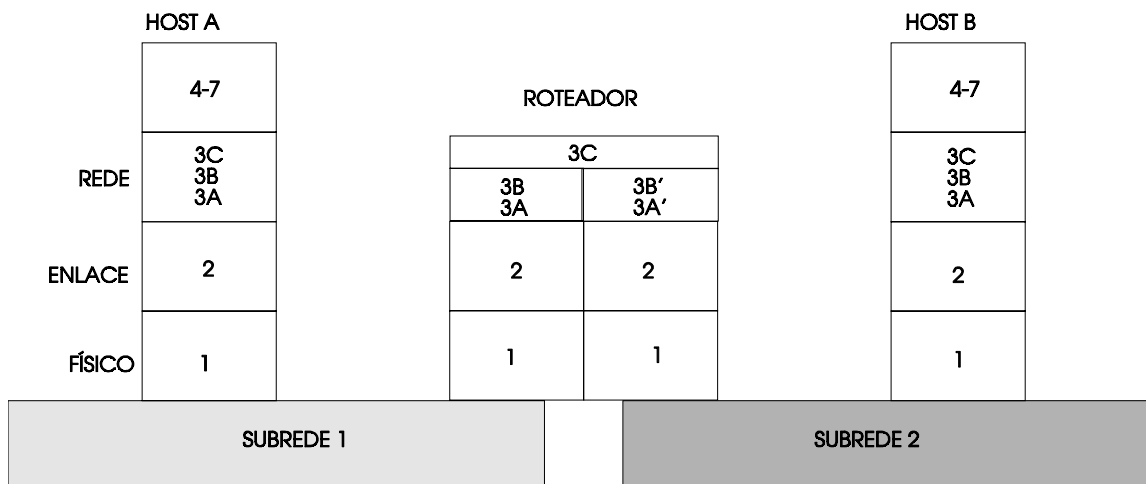
Roteadores são conceitualmente similares às pontes, porém, trabalham no nível de rede do modelo OSI. Dessa forma, as redes interligadas através de roteadores podem diferir muito mais que as redes conectadas através de pontes. Os roteadores normalmente são necessários quando existe a necessidade de interligar redes locais com redes de longa distância, ou quando se deseja dar uma independência maior aos diferentes segmentos de uma rede local, pois dois segmentos de rede local conectados através de um roteador possuem endereços de rede diferentes.

A figura a seguir ilustra o funcionamento de um roteador. O *host* A tem um pacote a transmitir. O pacote desce através dos níveis 7 a 4, chegando ao nível de rede (nível 3). O nível de rede pode ser dividido nos três seguintes subníveis:

- **Subnet access sublayer (3A)** - trabalha com o protocolo de nível 3 para sua própria subrede, gerando e recebendo dados e pacotes de controle, e fazendo as funções próprias do nível de rede;

- **Subnet enhancement sublayer (3B)** - tem o objetivo de harmonizar subredes que oferecem diferentes serviços;
- **Internet sublayer (3C)** - todas as subredes utilizam o mesmo esquema de endereçamento, homogêneo no subnível internet.

Da mesma forma que as pontes, o pacote é tratado e os protocolos referentes a cada subrede são modificados a fim de serem entendidos pela outra subrede.



Devido à maior complexidade dos protocolos utilizados pelos roteadores, eles são mais lentos se comparados às pontes. Além disso, são mais caros e requerem um esforço maior para instalação e utilização.

O roteador não é transparente como a ponte. As estações de um determinado segmento de rede local devem endereçar especificamente o roteador, já que este trabalha no nível de rede.

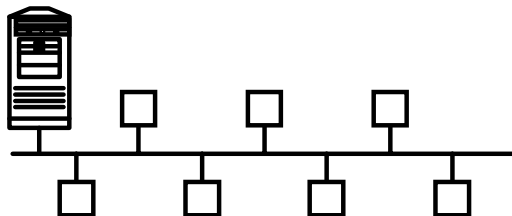
Para encontrar o destino, o roteador não conhece a posição exata de cada nó existente, mas sim os endereços das várias subredes. Assim, eles lêem as informações de nível 3 contidas em cada pacote, utilizam determinados algoritmos de endereçamento e roteamento para determinar o destino adequado, reestruturam os dados em pacotes e os retransmitem.

Alguns roteadores sempre escolhem uma rota determinada. São conhecidos como **roteadores estáticos**, e a informação da rota é entrada manualmente pelo gerente do sistema, que deve possuir um bom conhecimento da estrutura da rede. Outros produtos mais sofisticados, conhecidos como **roteadores dinâmicos**, avaliam determinados fatores antes de decidirem pela rota, tais como o custo da linha e o volume de tráfego atual. É claro que quanto maior o número de avaliações feitas, maior será o tempo de processamento necessário para chegar a uma conclusão, diminuindo seu desempenho como um todo.

/**/ domínio de colisão e broadcast – roteadores

1.5 A evolução das redes

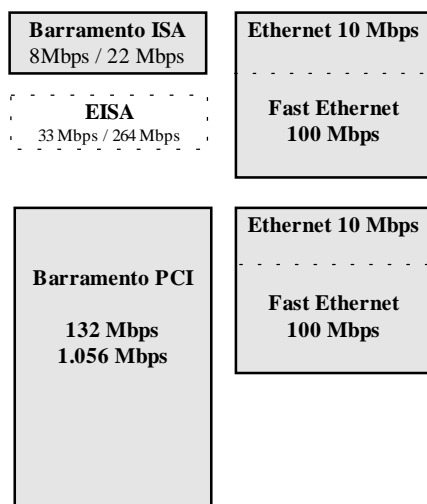
A figura a seguir representa um segmento de uma rede local com baixo tráfego.



Conforme aumenta a utilização (tráfego) de uma rede local do tipo Ethernet, esta torna-se mais lenta, pois existem mais pacotes sendo trocados entre estações clientes e o servidor, provocando um aumento no número de colisões e conseqüente queda de desempenho. O problema básico pode ser o excesso de requisições por minuto para um determinado servidor. Existem três alternativas básicas para solucionar o problema [KNU 96]:

Alternativa 1: Acrescentar um servidor de arquivos maior e mais veloz. É uma solução de curto prazo; o problema reaparecerá em oito meses, mantidas as atuais taxas de crescimento da rede [KNU 96]. Isso se o problema for realmente o servidor (o problema pode ser a rede muito lenta).

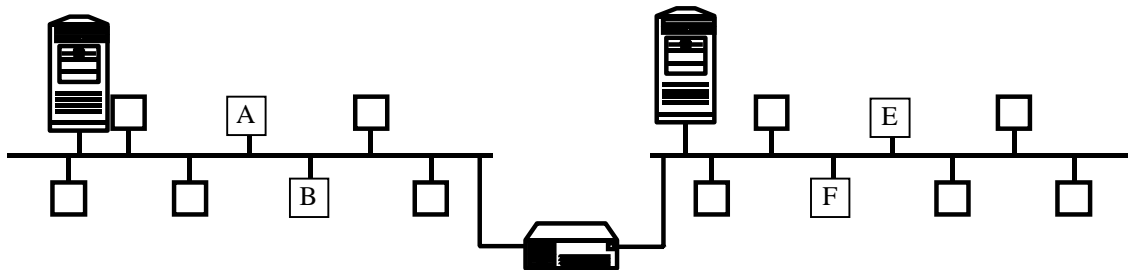
Alternativa 2: Usar conexões de maior velocidade: tem boas chances de resolver o problema, mas é necessário atualizar todas as placas de rede, e talvez o meio físico também, podendo tornar-se uma solução cara. Um dado importante nesse cenário é se o barramento do computador vai suportar o aumento de velocidade da rede. A figura a seguir mostra um comparativo entre os diversos tipos de barramento existentes.



Alternativa 3: Dividir a rede em segmentos menores. Normalmente soluciona o problema e ainda proporciona escalabilidade.

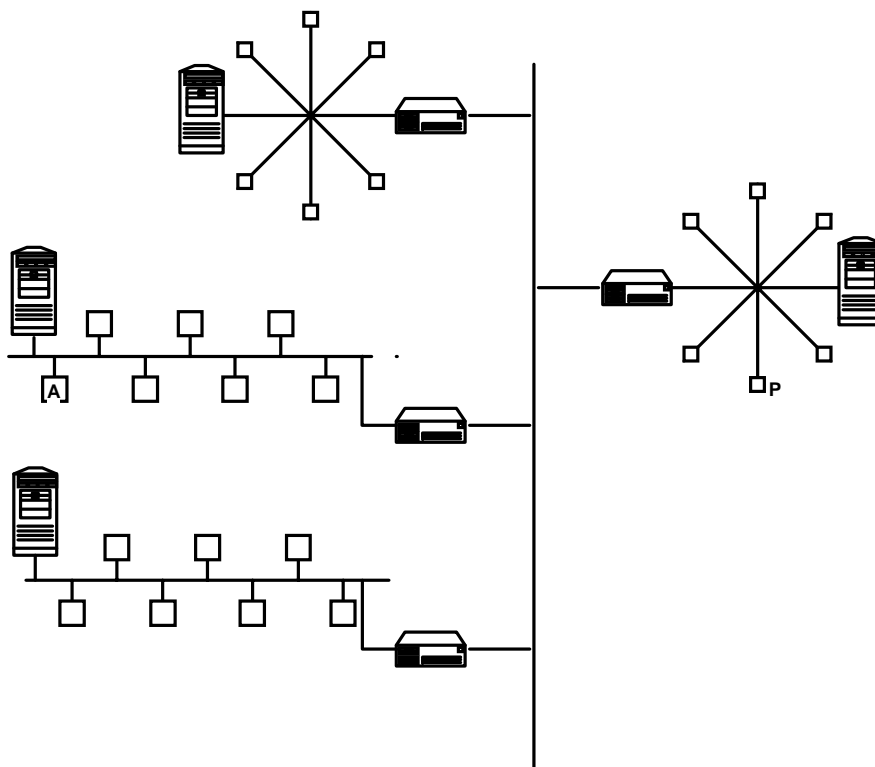
1.5.1 Segmentação das redes

A figura a seguir mostra uma rede local com dois segmentos, conectados através de um equipamento.



Essa forma de interconexão é bastante simples, já que a ponte ou switch aprende automaticamente o destino dos pacotes que estão circulando na rede, direcionando para o outro segmento somente se o pacote for destinado a ele, conforme foi explicado no item anterior.

Entretanto, não dá para ir aumentando o número de equipamentos aleatoriamente à medida que a rede fica lenta. Com várias pontes/switches, um pacote gerado no primeiro segmento teria que passar por todos os outros para chegar no último, gerando um tráfego desnecessário. Uma alternativa é criar um *backbone* para os diversos segmentos, como mostra a figura a seguir.



O problema que começa a se delinear é a velocidade do *backbone* corporativo. Caso tenha a mesma velocidade dos segmentos de rede local, vai criar um “gargalo” para comunicação entre segmentos. Uma solução, nessa situação, é utilizar um *backbone* corporativo de alta velocidade.

Existe atualmente uma tendência a manter o maior número de servidores centralizados num ambiente único, com o objetivo de facilitar o acesso e gerência pelo administrador. Além disso, existem situações onde o cliente está num segmento e o servidor ideal para ele se encontra em outro. Para resolver esses problemas, é necessário um grande tráfego de dados (que poderiam ficar confinados localmente) através do *backbone* empresarial.

1.5.2 Segmentação com *switches* ou roteadores

Os *backbones* distribuídos podem ser implementados concentrados em roteadores ou *switches*, baseado no interesse do usuário em querer um maior confinamento de tráfego broadcast ou não.

Existe atualmente uma vasta gama de equipamentos no mercado, e são cada vez mais rápidos. Hoje em dia não dá para dizer que o roteador é mais lento que o *switch*, visto que existem roteadores que passam milhões de pacotes por segundo.

Porém, para acesso a redes de longa distância é obrigatório o uso de roteadores, pois os *switches*, em virtude da camada do modelo OSI em que se encontram, não tem condições de fazer esse tipo de tratamento.

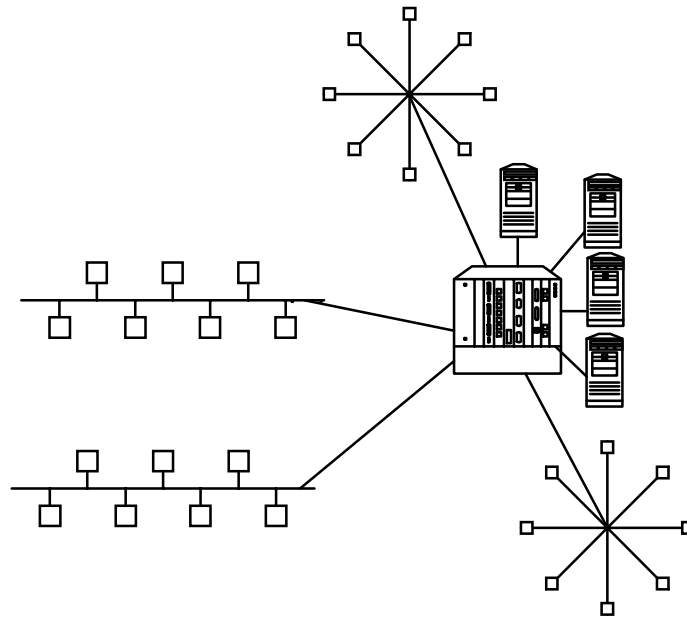
Uma outra característica dos *switches* são os *broadcasts*. Quando uma estação com *boot* remoto necessita ser inicializada, ela envia uma mensagem *broadcast* a fim de descobrir quem vai ser seu servidor. Quando o *switch* recebe um quadro desse tipo, ele o retransmite para todas as suas portas, e assim esse quadro se espalha (normalmente desnecessariamente) por toda a empresa. Duas coisas ruins podem acontecer no caso acima: a) o servidor errado assume controle da máquina cliente; b) gera tráfego desnecessário na rede. Para resolver esse tipo de problema, e ainda oferecer diversas vantagens, os *switches* podem ser configurados para utilizar redes virtuais (VLANs), que serão analisadas adiante.

Outra limitação do *switch* em redes maiores é para conectar diferentes redes virtuais (VLANs) entre si. É necessário a inclusão de um roteador para fazer essa trabalho. É por esse motivo que existem alguns *switches* que fazem papel de roteador, mantendo tudo em um único equipamento.

A tabela a seguir mostra uma comparação entre as funções de *hubs*, *switches* e roteadores.

	Conectividade	Controle de colisões	Controle de <i>Broadcasts</i>
Hub	SIM	NÃO	NÃO
Switch	SIM	SIM	NÃO
Roteador	SIM	SIM	SIM

A figura a seguir mostra a utilização de um *switch* ou roteador para interconectar diferentes redes, formando um *backbone* centralizado.



1.5.3 Redes virtuais ou virtual LANs

Uma solução para o problema do cliente ser inicializado através do servidor errado é programar o *switch* para que todo o quadro *broadcast* enviado por determinada estação seja redirecionado somente para a porta do seu servidor verdadeiro. Assim, cria-se um controle de *broadcasts* e a estação fica associada corretamente. Esta alternativa é uma das vantagens na utilização de redes virtuais. Uma outra está relacionada com a distribuição física *versus* distribuição lógica das pessoas, sendo descrito a seguir.

Algumas pesquisas realizadas nos Estados Unidos no ano de 1994 [MAR 95] mostraram que aproximadamente 75% dos custos associados à operação de uma rede local estão relacionados com o suporte aos usuários. Desses 75%, o maior problema está associado com os custos para administração de mudanças e movimentação de usuários pela companhia.

O termo Rede Virtual refere-se a um ambiente onde estações podem ser agrupadas independente de sua posição física na rede, formando redes locais isoladas, mesmo que não pertençam ao mesmo segmento físico [MAR 95].

Em outras palavras, uma Rede Virtual é uma rede local formada por um grupo de usuários que possuem alguma afinidade entre si, como trabalhar em um mesmo departamento ou participar de um mesmo projeto, dividindo o mesmo servidor, sem que para isso precisem estar em um mesmo segmento físico da rede. É nesse ponto que entram os *switches*. Eles formam uma peça fundamental para a implementação de Redes Virtuais. Agregando um “número de rede virtual” às suas tabelas de endereçamento, um *switch* pode decidir quando um quadro deve ou não ser transmitido a um determinado grupo de portas, isolando-as umas das outras.

Como esse processo decisório normalmente leva em consideração o endereço MAC contido no quadro de informação, essas redes virtuais são conhecidas como Redes Virtuais de nível 2. Todo esse processo é tipicamente uma função de *switching*.



Para redes corporativas de maior porte, a situação descrita acima tem um problema. Por não olhar informações do nível 3, as Redes Virtuais de nível 2 não são capazes de criar *firewalls* que impeçam, por exemplo, que pacotes em *broadcast* não confinados se espalhem pela rede.

Para resolver esse problema, surgiram no mercado os *switches* que implementam redes virtuais de nível 3, que olham o endereço da camada superior antes de tomar a decisão de retransmissão do pacote, ficando bastante parecido com um roteador, entretanto, mais caros e mais lentos que um *switch* de nível 2.

Como benefícios das Redes Virtuais pode-se citar [NET 96]:

- Redução de custos administrativos;
- Possibilidade de usuários pertencerem à mesma rede e ficarem fisicamente dispersos;
- Facilidade de implementação de políticas de segurança;
- Servidores podem pertencer a mais de uma Rede Virtual.