

DISPOSITIVOS DE INTERCONEXÃO

Visando a interligação das redes geograficamente distribuídas, existem vários dispositivos cujas facilidades de operação possibilitam efetuar de maneira transparente a ligação dos usuários e suas aplicações, considerando uma grande dispersão geográfica.

A tarefa de compreender o funcionamento de qualquer protocolo em termos de rede é precedida pela necessidade de um conhecimento adicional de como as redes podem ser interligadas em diferentes situações. A ligação denominada de inter-rede é um tópico essencial para que possamos trabalhar com os princípios de qualquer configuração de rede e eventuais problemas possam ser tratados.

**Dispositivos
de interconexão
compreendem:**

- **CONCENTRADORES**
- **REPETIDORES**
- **PONTES**
- **SWITCHES**
- **ROTEADORES**
- **GATEWAYS**

1. **CONCENTRADORES (HUBS):** Neste dispositivo só existem sinais do próprio segmento de rede. Compartilham os dados entre todos os elementos da rede (*broadcast*).
2. **REPETIDORES:** Interligam redes com mídia compartilhada e arquiteturas idênticas. Recebem dados de um segmento e transmitem para outro segmento. Não tratam o pacote.
3. **PONTES (BRIDGES):** Armazenam e encaminham segmentos de dados entre redes de mesma tecnologia. Conseguem interligar segmentos de redes diferentes, contanto que as redes usem *softwares* baseados no mesmo protocolo de comunicações.
4. **SWITCHES:** São equipamentos utilizados para conectar segmentos de redes locais. São similares a uma ponte com múltiplas portas, em que os pacotes são enviados para a porta de saída apropriada. O *switch* permite que estações em segmentos separados transmitam simultaneamente, já que comuta pacotes utilizando caminhos dedicados.
5. **ROTEADORES:** Encaminham pacotes entre redes dissimilares. Os roteadores lêem informações complexas de endereçamento e tomam decisões sobre como encaminhar os dados através dos diversos *links* que interligam as redes.
6. **GATEWAYS:** Qualquer dispositivo que conecta duas ou mais redes dissimilares, possibilitando *internetworking*.

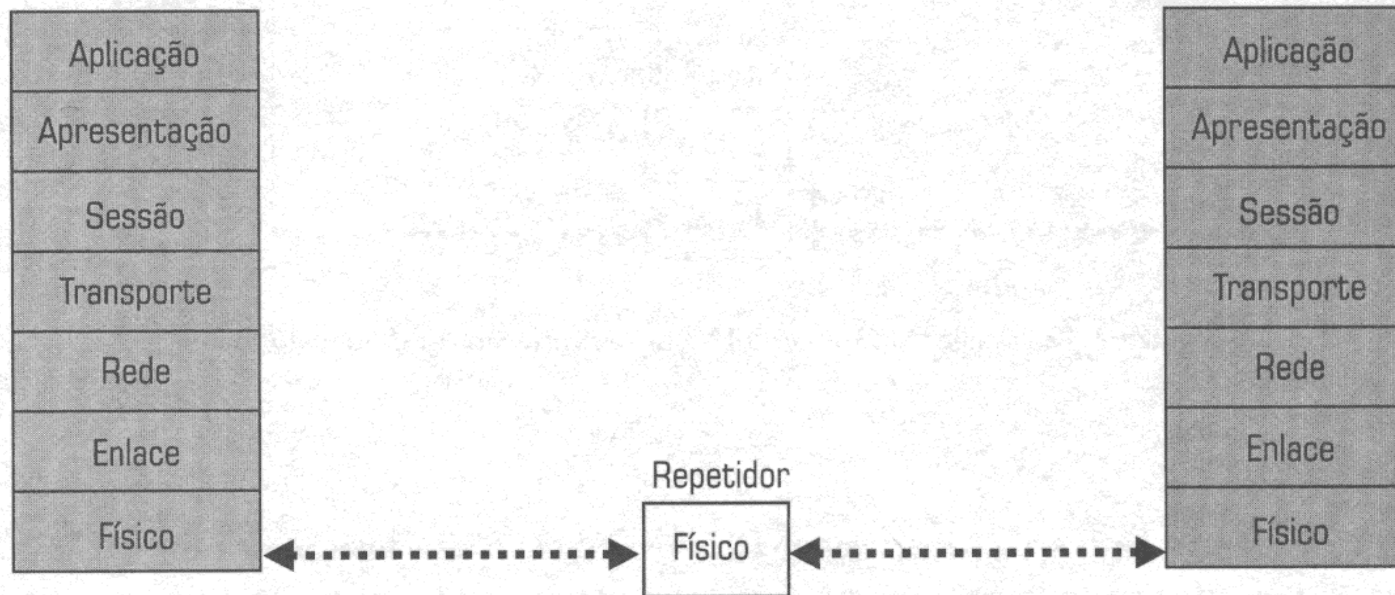
CONCENTRADORES

Os concentradores (hubs) são dispositivos de rede que podem ser classificados como:

- Passivos: nestes equipamentos só existem sinais do segmento de rede, não existindo a regeneração do sinal.
- Ativos: nestes dispositivos existe a regeneração do sinal, o que significa que a rede pode abranger distâncias maiores em termos de cabeamento.
- Inteligentes: além de regenerar os sinais, estes dispositivos podem fazer gerência e seleção de conexões.

REPETIDORES

São equipamentos empregados para a interligação de redes com mídia compartilhada e de idênticas arquiteturas. A função de um repetidor é receber os pacotes de um segmento de rede e repetir este pacote para o outro segmento de rede. Não é efetuado nenhum tratamento sobre o pacote. A Figura apresenta a situação de um repetidor considerando o modelo RM-OSI.



Localização funcional de um repetidor no modelo RM-OSI.

PONTES

As pontes (bridges) são dispositivos que interligam segmentos de redes. Ao contrário de um repetidor, deseja-se que, com o uso de uma ponte, as seguintes funções sejam satisfeitas:

- Transmissão de pacotes entre dois segmentos de rede.
- Filtro na transmissão entre os dois segmentos.
- Facilidade de armazenamento para a transmissão entre os segmentos.
- Melhorar o desempenho de uma rede que começa a crescer.
- Que numa eventual falha de um dos segmentos, o outro não seja afetado.

Pontes

As pontes convencionais conectam segmentos de uma mesma tecnologia de rede. As *bridges* são usadas para melhorar o desempenho da rede, pois, diferente dos repetidores, selecionam/filtram os sinais entre os segmentos. Quando uma mensagem de um computador é, por exemplo, de um segmento A, esta não é propagada para um outro segmento B.

- Pontes são utilizadas quando precisamos interligar LANs, local ou remotamente, e não queremos sobrecarregar cada segmento da rede com tráfego desnecessário.
- As pontes conseguem analisar os quadros, só permitindo a passagem dos quadros endereçados aos nós de um dado segmento de rede.
- Pontes remotas: são necessários dois dispositivos para fazer a tradução entre os circuitos lentos, de longa distância, que interligam as redes, e os cabos rápidos de redes locais.
- Ponte local (entre dois segmentos da rede): apenas um dispositivo.

Pontes

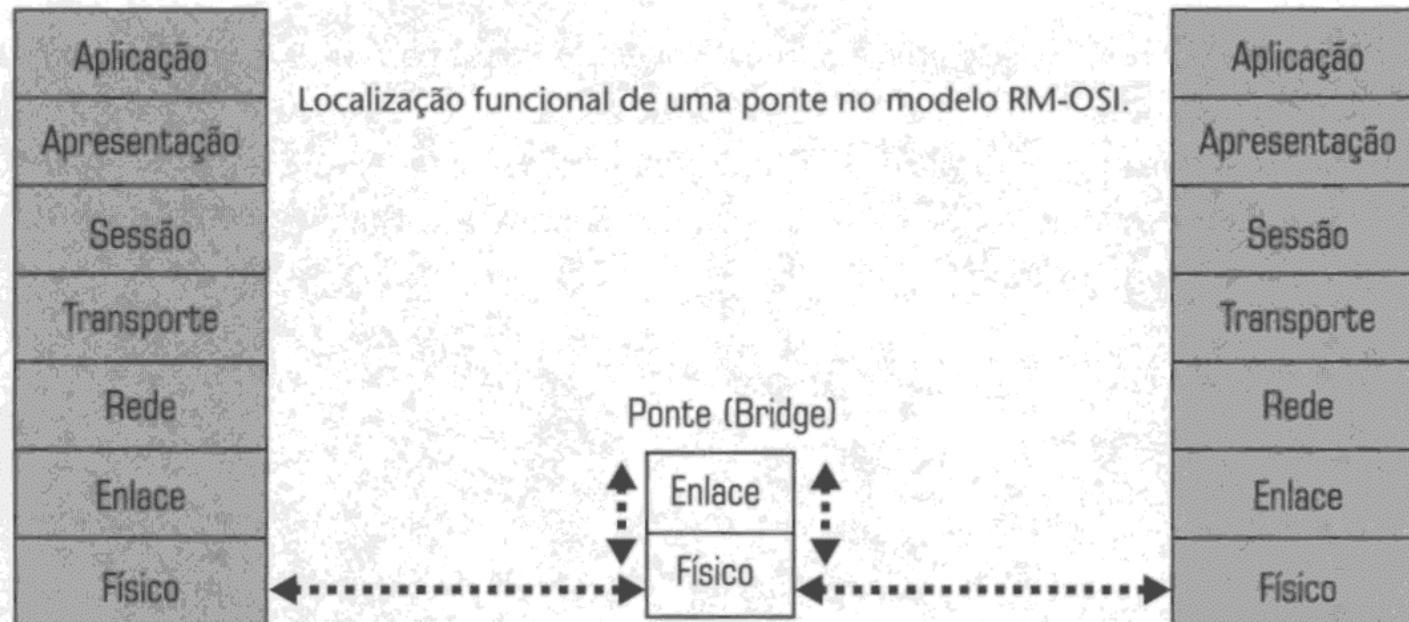
As pontes de tradução têm a função de resolver as diferenças e formatos dos quadros das diferentes LANs na camada de enlace (MAC). Uma outra função destes equipamentos é, por exemplo, tratar das diferenças de taxas de transmissão entre redes com idênticos protocolos de acesso (exemplo: *Token-Ring* a 4 Mbps e 16 Mbps).

(As pontes conseguem interligar um segmento Ethernet a um Segmento Token-Ring, por exemplo, contanto que as redes usem *softwares* baseados no mesmo protocolo de comunicações (IP com IP, ...)).

- As pontes conseguem transferir quadros entre meios diferentes, sendo este procedimento invisível para os usuários da rede.
- Os PCs clientes não necessitam de nenhum *software* ou *hardware* especial para aproveitar os benefícios das pontes.

Pontes

A Figura apresenta a localização funcional de uma ponte segundo o modelo RM-OSI.



Pontes

- ◆ Pontes são inteligentes. Seus programas enviam mensagens a todos os nós, provocando respostas de todos eles.
- ◆ Os programas lêem o endereço de origem de cada quadro e associam os endereços de origem aos segmentos correspondentes da rede. Isso limita o tráfego que cruza os segmentos das redes.
- ◆ Se a ponte receber um pacote ou quadro dirigido a um nó de destino ainda não identificado, o pacote ou quadro será encaminhado (*broadcast*) e aguardará uma resposta do destino. Chama-se a isso de lógica **forward-if-not-local** (encaminha quando não é local).
- ◆ As pontes modernas são importantes recursos de gerenciamento, pois monitoram de perto o tráfego da rede.
- ◆ Assim, a inclusão de *softwares* especiais (ditos agentes) nas pontes pode oferecer informações de volume de tráfego e erros da rede.
- ◆ No entanto, como as pontes são dispositivos ocupados (precisam avaliar os pacotes instantaneamente) se associarmos a atividade das pontes com um excesso de relatórios acabaremos impedindo que a carga de transmissão seja tratada com eficiência.

Pontes

- As pontes inteligentes são adequadas para interligar dois Segmentos de rede, mas o processo se torna mais complexo quando diversos segmentos de rede são interligados entre si, quer diretamente, em conexões locais, quer remotamente, através de circuitos de longa distância.
- Se diversos segmentos de rede forem conectados por meio de pontes, haverá a passagem de tráfego estranho de um ou mais segmentos, a caminho dos endereços de destino. Esta operação aumenta desnecessariamente a carga dos segmentos intermediários.
- Sempre existe a possibilidade de que, de alguma forma, diversos segmentos da rede sejam conectados por mais de uma via.
- Quando isso ocorre, é possível que os Quadros circulem continuamente entre os segmentos da rede, uma situação chamada, às vezes, de ***data storm***.

Pontes

- São várias as técnicas utilizadas para lidar com esse problema (***data storm***): a mais comum chama-se ***Spanning Tree Algorithm***.
- Os *softwares* que obedecem a esse algoritmo conseguem detectar a existência de diversas vias e efetuar bloqueios.
- Os produtos que suportam este algoritmo são, principalmente, pontes locais.
- Os recursos do ***Spanning Tree Algorithm*** não têm a mesma utilidade nas pontes remotas, pois conflitam com as técnicas utilizadas para a transferência de dados através de mais de um dos circuitos lentos de longa distância.

Pontes

As pontes remotas utilizam técnicas denominadas:
Source-Level Routing ("roteamento" ao nível da origem) e
Protocol-Transparent Routing ("roteamento" transparente aos protocolos).

Source-Level Routing: No roteamento ao nível de origem, usado principalmente nas redes *Token-Ring*, a ponte envia uma mensagem de teste a uma estação de destino.

As pontes que usam essa técnica, dispersas ao longo do caminho, acrescentam seus próprios endereços.

A estação de destino, por sua vez, envia uma mensagem de volta à estação de origem, produzindo uma listagem completa de todas as pontes intermediárias.

A ponte que atende a estação de origem usa essas informações para construir um **mapa da rede de interconexões** e determinar o caminho mais rápido entre os nós de origem e destino.

Protocol-Transparent Routing: O roteamento transparente aos protocolos utiliza a lógica **forward-if-not-local** (se a ponte receber um pacote ou quadro dirigido a um nó de destino ainda não identificado, o pacote ou quadro será encaminhado em *broadcast* e aguardará uma resposta do destino).

SWITCHES

- Os *switches* são equipamentos utilizados para conectar segmentos de redes locais.
- Um *switch* de uma LAN é similar a uma ponte com múltiplas portas, em que os pacotes são enviados para a porta de saída apropriada.
- O *switch* permite que estações em segmentos separados transmitam simultaneamente, já que comuta pacotes utilizando caminhos dedicados.
- Colisões não ocorrerão, porém poderá ser experimentada a contenção de dois ou mais quadros que necessitem do mesmo caminho ao mesmo tempo.
- *Buffers* de entrada e saída das portas são utilizados para a posterior transmissão.
- *Switches* podem suportar somente uma estação ligada por porta, ou segmentos com múltiplas estações podem ser ligados a cada porta.

- ◆ O endereçamento dos *switches* é realizado utilizando uma tabela com endereços, similar às pontes transparentes.
- ◆ Cada porta possui uma tabela de transmissão que relaciona os números das portas do equipamento com o endereço dos nós de destino.
- ◆ Quando o quadro é recebido por uma porta, seu endereço de destino é comparado com os endereços da tabela de transmissão, a fim de encontrar a porta de destino correta, sendo então estabelecida uma conexão virtual com a porta de destino.
- ◆ O aprendizado e atualização da tabela é realizado por um processador central no *switch*, que pode também proporcionar tarefas de gerenciamento e manter tabelas de redes locais virtuais .

Switch modo de operação *cut-through*: os quadros são enviados adiante diretamente. Assim que o quadro chega, seu endereço destino é comparado na tabela, a fim de verificar a porta de saída. Desde que esta porta esteja disponível, o quadro começa a ser imediatamente enviado. Esta transmissão ocorre em paralelo com o recebimento do restante do quadro pela porta de entrada.

Switch modo de operação *store-and-forward*: o quadro deve ser recebido completamente antes de ser iniciada a transmissão para o endereço destino.

- ⦿ *Switches* no modo ***cut-through*** reverterem para o modo ***store-and-forward*** quando a porta destino de um quadro recebido está ocupada.
- ⦿ Neste caso, o quadro recebido é armazenado em um *buffer* até que seja possível utilizar a porta ocupada.
- ⦿ Uma vantagem deste modo é que, uma vez que os quadros foram recebidos inteiros, é possível realizar um controle de erros e descartar os pacotes com problemas, o que não é possível no modo ***cut-through***, que transmite os quadros sem verificar erros.

ROTEADORES

Os roteadores (*routers*) são os dispositivos que permitem a interligação de redes distintas, formando-se um verdadeiro ambiente de inter-rede.

De uma maneira mais específica, os roteadores são responsáveis pelo recebimento dos pacotes do nível inferior, pelo tratamento do cabeçalho de inter-rede destes pacotes, descobrindo qual o roteamento necessário, pela construção de um novo pacote com um novo cabeçalho de inter-rede e, quando necessário, pelo envio do novo pacote para o novo destino.

Roteadores

Como uma determinada rede pode ser composta por um conjunto de redes internas independentes administradas por um único grupo da empresa, denomina-se este ambiente como um sistema autônomo (SA).

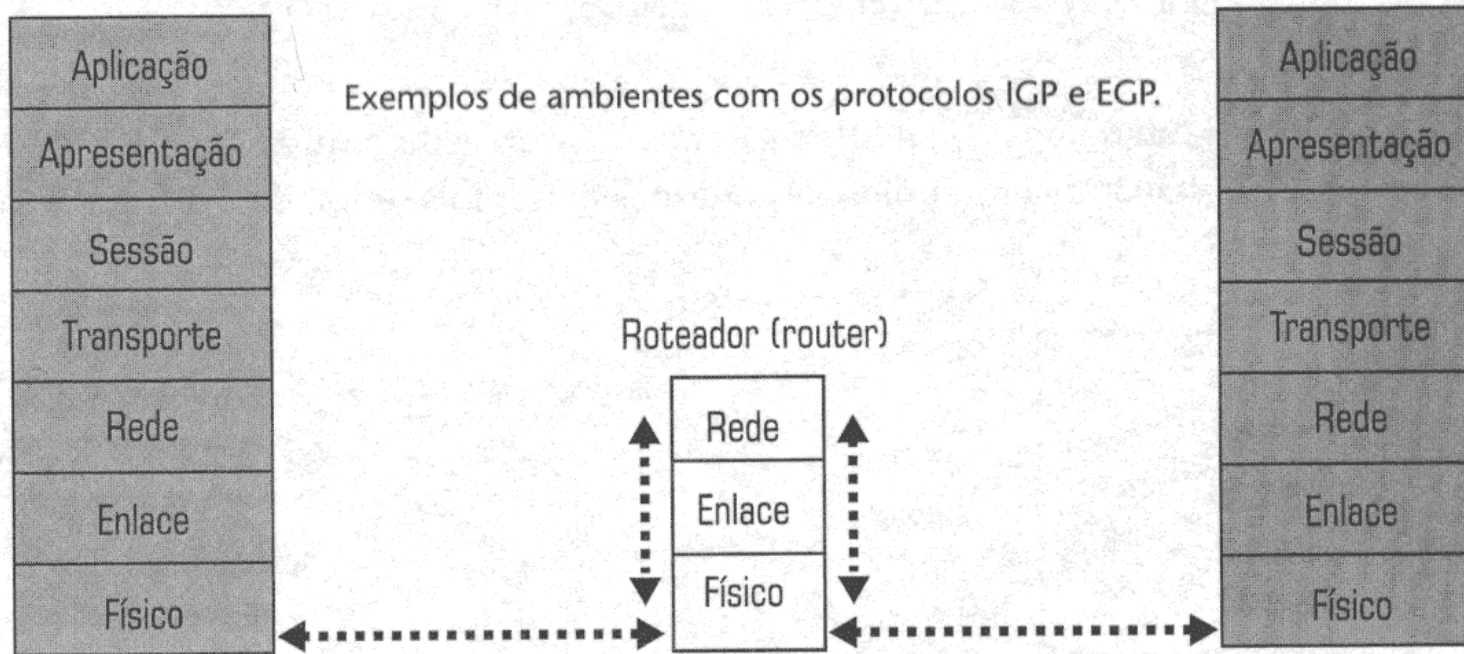
Os protocolos que efetuam as funções de roteamento, dentro de um sistemas autônomo, são denominados de *IGP (Interior Gateway Protocol)*. O protocolo *OSPF (Open Shortest Path First)* é um exemplo de protocolo de roteamento interno num sistema autônomo em redes com arquitetura TCP/IP.

Roteadores

Por outro lado, aqueles protocolos empregados para interligar sistemas autônomos distintos são conhecidos como *EGP* (*Exterior Gateway Protocol*). O protocolo *BGP* (*Border Gateway Protocol*) é o protocolo de roteamento externo mais utilizado na Internet. A Figura mostra dois sistemas autônomos e um exemplo de ligação dos ambientes.

As nomenclaturas IGP e EGP são intrínsecas a ambientes TCP/IP. A melhor forma de expressar estes ambientes, genericamente, seria IRP (Interior Router Protocol) e ERP (Exterior Router Protocol).

Roteadores



ROTEADORES ESTÁTICOS E DINÂMICOS

➤ Roteadores Estáticos:

- ◆ Roteadores cujos programas sempre selecionam o caminho mais curto entre dois pontos.**
- ◆ Como as informações de roteamento são registradas manualmente, os roteadores estáticos exigem a atenção cuidadosa de administradores experientes.**

➤ Roteadores Dinâmicos:

- ◆ São produtos mais sofisticados, que tomam decisões ao nível de cada pacote com base nas informações obtidas de outros roteadores e dispositivos da rede.**
- ◆ Tais decisões dizem respeito à eficiência e confiabilidade das diversas vias entre os nós de origem e destino.**

Roteadores filtram tráfego baseado nos campos de endereçamento contidos dentro do cabeçalho do protocolo de rede.

Sub-campos destes endereços identificam o segmento da LAN onde estão localizadas a estação origem e destino.

Protocolos em que os campos de endereçamento não possuem sub-campos identificadores da localização da estação destino não podem ser roteados, podendo, porém, ter seus pacotes filtrados por pontes.

Nestes casos, a fim de repassar pacotes, o roteador é freqüentemente usado como uma ponte.

COMPARAÇÕES ENTRE PONTES, ROTEADORES E SWITCHES

- As pontes são inteligentes, mas relativamente simples. Elas permitem a passagem do tráfego ou ignoram a existência, e só conseguem tratar dados em pacotes homogêneos.
- Os roteadores são mais inteligentes e mais sofisticados. Os programas dos roteadores lêem informações complexas de endereçamento e tomam decisões sobre como encaminhar os dados através dos diversos *links* que interligam as redes.
- Em comparação com as pontes, como os roteadores só lêem os pacotes da rede especialmente endereçados a eles, sua carga de trabalho é menor que a das pontes. Sendo assim, os roteadores impõem um esforço menor à CPU do *host*.

- ◆ As pontes utilizam a lógica ***forward if-not-local*** (encaminha-se-não-é-local).
- ◆ Os roteadores usam uma lógica descrita como ***forward-only-if-known-remote*** (encaminha-só-se-certamente-remoto). Ou seja:
 - Os roteadores só transferem o tráfego ao *link* entre as redes quando o endereço é conhecido e não pertence a um nó local.
 - Os *links* de redes locais à longa distância são caros e, portanto, vale ressaltar que os roteadores usam os *links* com mais eficiência do que as pontes.
 - Isso ocorre porque os roteadores retiram as informações de endereço da camada MAC antes de enviarem os pacotes através dos *links*.

Comparações entre Pontes e Roteadores e *Switches*

- ◆ Se uma série de pacotes curtos for transmitida através do *link* entre duas redes - toques no teclado, por exemplo - os endereços podem consumir até 50% de cada pacote.
- ◆ Alguns roteadores usam um algoritmo de compressão em seus *softwares* para melhorar ainda mais o *throughput* (o parâmetro *throughput* é uma medida de qualidade de serviço, a qual mede o nº de bytes do usuário que são transferidos por segundo, sobre algum intervalo de tempo) .
- ◆ A compressão ***on-the-fly*** (no instante em que os dados são recebidos) é complicada. Em geral, considera-se que a compressão seja útil em circuitos de comunicações lentos ou muito congestionados, mas se os circuitos forem rápidos haverá uma perda maior de tempo na execução do *software* de compressão do que no envio dos dados sem compressão.
- ◆ Os roteadores não mantêm tabelas descrevendo cada nó e os segmentos a que pertencem, como acontece com as pontes. Só tomam conhecimento de outros roteadores identificados por endereços de sub-redes.

Comparações entre Pontes e Roteadores e *Switches*

- ◆ Os roteadores não se importam com o formato dos pacotes ou quadros, limitando-se a ler o endereço de sub-rede, decidir sobre o melhor caminho, e envolver o pacote ou quadro no envelope apropriado, que pode ser um pacote de X.25 ou quadro de *frame relay*, por exemplo.
- As redes conectadas por pontes possuem segmentos físicos separados, porém logicamente são consideradas uma grande rede.
- As pontes assumem que o destino de um quadro é atingível diretamente, sem nós (nodos) intermediários, uma vez que não têm conhecimento de inter-redes ou de roteamento através de redes locais conectadas em série.
- Assim, as pontes não oferecem a possibilidade de isolar nodos entre grupos lógicos, o que seria útil em situações onde mensagens *broadcast* são destinadas a apenas alguns nodos específicos.
- Já os roteadores oferecem muito mais flexibilidade no tráfego do fluxo, dividindo as redes em grupos lógicos distintos, por meio de convenções de endereçamento.

Comparações entre Pontes e Roteadores e *Switches*

Roteadores diferem das pontes:

- na forma de filtrar o tráfego,
- pelo controle do congestionamento,
- por filtrar quadros de *broadcast*,
- pela determinação da melhor rota na rede visando minimizar seu tráfego (a melhora no uso dos *links* também é oferecida pelas pontes com roteamento na origem, porém de forma muito menos eficiente que pelos roteadores).

Comparações entre Pontes e Roteadores e *Switches*

- Roteamento é uma técnica que deve ser usada quando é necessária a conversão de protocolos, o que não é possível utilizando *switching*.
- ◆ A instalação de pontes, assim como acrescentar novos nodos, é simples, especialmente para pontes transparentes, que descobrem novos nodos sem intervenção manual. Para os *switches*, a menos que tenham a função de aprendizado desabilitada, isto também é válido, requerendo pouca configuração.
- Pontes e *switches*, no entanto, impõem limitações quando conectam duas redes diferentes, limitando frequentemente o tamanho dos pacotes de uma rede para o tamanho dos pacotes de outra rede.
- ◆ Os roteadores, por sua vez, exigem muito mais configuração, pois deve ser selecionado um protocolo de roteamento e numeradas as redes com identificadores únicos.
Porém, uma vez instalados e propriamente configurados, os roteadores são capazes de descobrir o melhor caminho para uma estação destino, otimizando o tráfego das redes, o que não é oferecido por pontes e *switches*.

- Em determinados casos, as facilidades de controle de fluxo dos roteadores determina sua escolha para interconexão.
- ◆ Roteadores possuem também a propriedade de criar redes lógicas e grupos de trabalho, o que representa uma vantagem pois permitem direcionar mensagens para apenas um grupo determinado, filtrando mensagens *broadcast*, o que não é desempenhado pelas pontes, que repassam estes pacotes para todos os segmentos conectados. Quando são utilizados pacotes deste tipo para, por exemplo, resolver endereços, a capacidade de filtrar quadros *broadcast* pode ser extremamente vantajosa.
- Em relação a roteadores, pontes e *switches* apresentam maiores dificuldades para isolar problemas: erros de configuração ou falhas em um equipamento que causam erro em uma localização podem afetar grande parte ou mesmo toda a rede. Já os roteadores fornecem uma ferramenta para gerência complexa e diagnóstico de falhas que as pontes não possuem, detectando violações facilmente.

⊙ Assim, utilizar **switches** e **pontes** é uma boa escolha para redes homogêneas (por dificuldades como limitação de tamanho de pacotes) com baixo grau de interoperabilidade e onde existam ferramentas de diagnóstico de falhas excelentes.

⊙ **Roteamento**, por sua vez, é boa escolha para redes distribuídas, heterogêneas, em que o custo de largura de banda deve ser cuidadosamente gerenciado, com diagnóstico de falhas difícil, e onde confiabilidade e disponibilidade são considerações importantes.

Comparações entre Pontes e Roteadores e *Switches*

CONCEITO OPERACIONAL DE ROTEADORES

- Se considerarmos o roteador como um PC conectado à rede, além de sua placa de rede, este PC possui adaptadores de comunicações que lhe dão a capacidade de enviar e receber dados através de duas linhas telefônicas privadas simultaneamente.
- Além disso, o PC executa *softwares* especiais que inspecionam os pacotes de dados recebidos através das linhas telefônicas e da rede.
- Os circuitos privados se ligam a roteadores em duas outras redes e essas redes, por sua vez, estão conectadas entre si.
- Poderíamos descrever esse sistema de redes interligadas como três roteadores remotos internos conectados em anel.
- Muitas empresas possuem redes interligadas com dezenas ou centenas de roteadores e circuitos de conexão.

- Em geral, os roteadores conectam vários segmentos de rede e vários circuitos de interligação de redes simultaneamente.
- A capacidade de selecionar uma entre as diversas vias de conexão disponíveis e limitar o tráfego que flui por algumas delas é uma vantagem clara dos roteadores sobre as pontes.
- Os computadores existentes em cada segmento da rede endereçam quadros ao roteador quando os quadros contêm pacotes destinados a endereços pertencentes a segmentos distantes.
- Os protocolos de roteamento conseguem chegar a níveis de detalhe tais que são capazes de direcionar um pacote de informações a um programa específico que esteja sendo executado num determinado computador, não se limitando a enviá-lo apenas ao computador.

Conceito Operacional de Roteadores

- Os roteadores filtram pacotes com base (entre outros fatores) numa lista específica de endereços de origem e, assim, podem se tornar um componente fundamental de segurança da rede.
- Quando o roteador recebe um quadro, ele verifica os dados contidos dentro do quadro, para determinar o tipo de protocolo obedecido na formatação dos dados.
- O protocolo de roteamento é implementado sob a forma de um tipo especial de pacote contido e identificado dentro do pacote da camada de transporte.
- Um pacote formatado de acordo com o padrão IP do protocolo TCP/IP poderia conter qualquer um dos protocolos de roteamento IP.
- Há roteadores capazes de tratar dados formatados de acordo com apenas um protocolo de transporte, embora roteadores de diversos protocolos sejam comuns.

Conceito Operacional de Roteadores

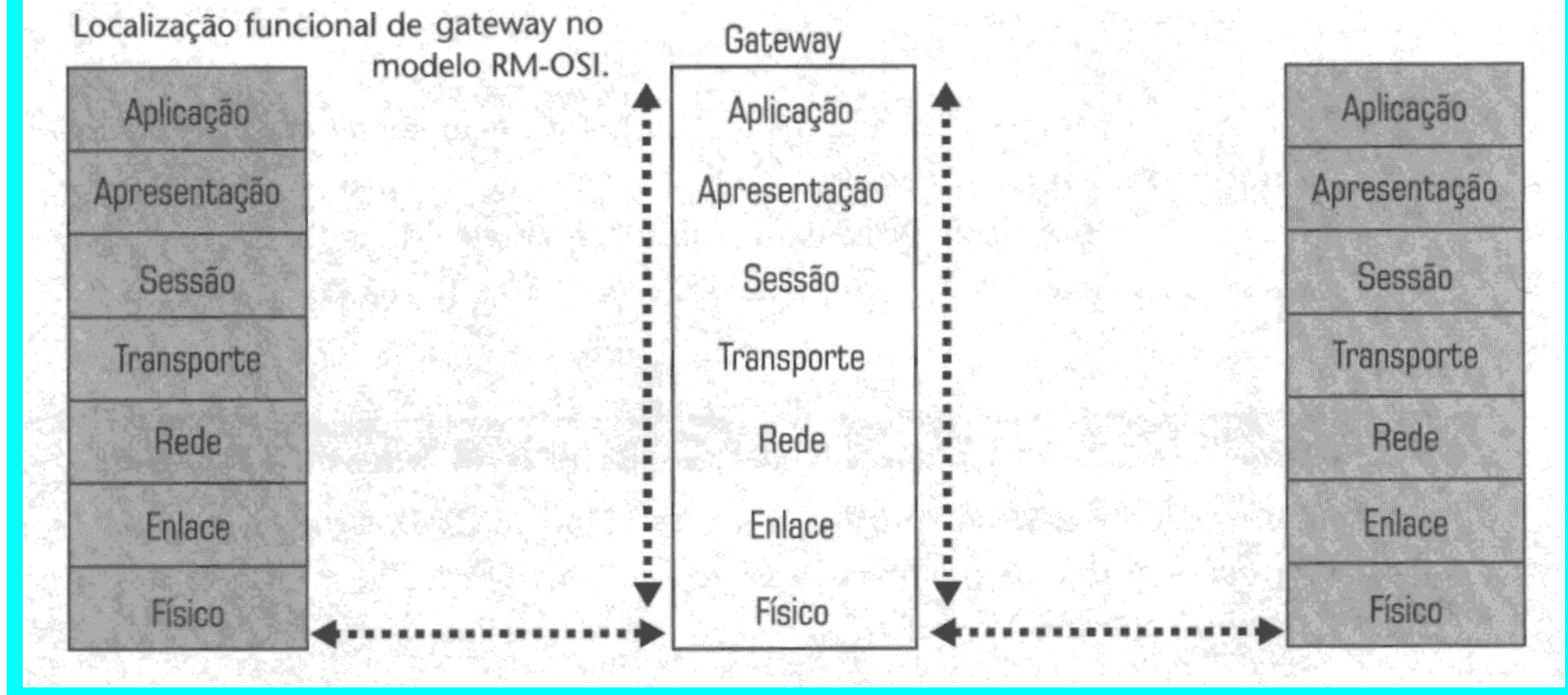
GATEWAYS

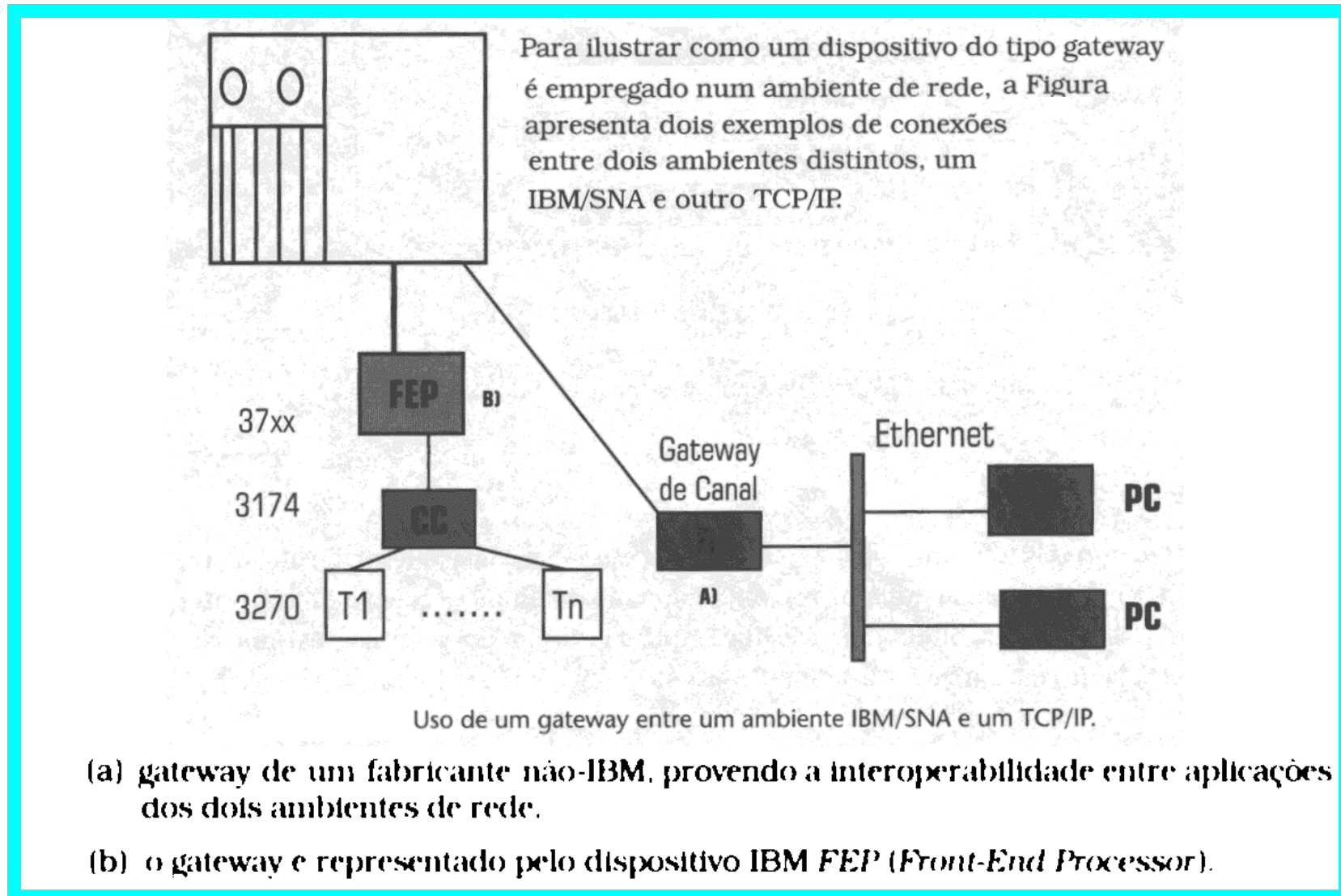
Os *gateways* são um tipo especial de roteador empregado para fazer o roteamento de pacotes em redes com arquiteturas completamente distintas. A função de um *gateway* é prover a interoperabilidade entre duas aplicações em dois ambientes, apesar das diferenças entre as arquiteturas de redes existentes nos computadores.

Uma situação clássica, que ilustra como o uso dos *gateways* é eficaz, é aquela na qual um computador de uma rede TCP/IP deseja fazer uma conexão e se interoperar com um ambiente IBM/SNA. Nenhuma dessas duas arquiteturas tem alguma similaridade então, o roteamento ocorre não só em nível de rede, mas também entre todas as diferentes camadas superiores em nível de inter-rede.

Na Figura a localização funcional de um *gateway* considerando o modelo RM-OSI.

Gateways





PROCOLOS E ALGORITMOS DE ROTEAMENTO

Conduzir os pacotes desde a fonte até o destino (*end-to-end transmission*) é uma tarefa que, em geral, pode requer muitos *hops* (saltos ou trocas de rota) em roteadores intermediários ao longo do caminho.

Para atingir este objetivo é necessário:

- ◆ conhecimento da topologia da sub-rede de comunicação (conjunto de roteadores);
- ◆ escolha de caminhos apropriados ao longo da sub-rede e
- ◆ escolha de rotas que evitem desequilíbrio de fluxo na rede, sobrecarregando algumas linhas de comunicação e roteadores, enquanto outras resultam desocupadas.

Quando fonte e destino encontram-se em diferentes redes, duas filosofias básicas podem ser adotadas para organizar a *sub-net*:

- I. abordagem que utiliza conexões (*connection - oriented service*) e
- II. abordagem que não utiliza conexões (*connectionless service*).

CIRCUITOS VIRTUAIS (VCs)

- ◆ No contexto de operação interna de uma sub-rede, uma conexão é usualmente chamada de **circuito virtual** (em analogia com o conjunto de circuitos físicos estabelecidos pelos sistemas telefônicos).
- ◆ Circuitos virtuais são geralmente usados em sub-redes cujo **serviço é orientado à conexão**.
- ◆ Um circuito virtual evita a escolha de uma nova rota para cada pacote ou célula a ser enviado.
 - Quando uma conexão é estabelecida, é escolhida uma rota partindo da máquina fonte até a máquina destino.
 - Esta rota é usada para todo o tráfego que irá fluir pela conexão (da mesma forma que ocorre em sistemas telefônicos).
 - Quando a conexão é terminada (desestabelecida) o circuito virtual é também terminado.

- ◆ Pacotes que fluem sobre um dado **circuito virtual** sempre tomam a mesma rota através da *sub-net*.
- ◆ Cada roteador deve, portanto, saber para onde propagar os pacotes ao longo de cada um dos circuitos virtuais correntemente abertos.
- ◆ Cada roteador deve manter uma tabela com uma entrada para cada circuito virtual aberto.
- ◆ Cada pacote viajando através da sub-rede deve conter, em seu cabeçalho, um campo para ser ocupado com o número do circuito virtual pelo qual deverá trafegar.
- ◆ Quando um pacote chega no roteador, o roteador sabe de qual linha de transmissão o pacote chegou e qual é o número do circuito virtual pelo qual está trafegando.
- ◆ Baseado nesta informação, o pacote deve ser progressivamente enviado sobre a linha de transmissão de saída correta.

- ◆ Quando uma conexão de rede é estabelecida, um número de circuito virtual ainda não em uso naquela máquina é escolhido como o identificador daquela conexão.
- ◆ Cada máquina escolhe circuitos virtuais de forma independente, desta forma, estes números possuem significação apenas local.
- ◆ No caso do estabelecimento de circuitos *full-duplex*, se os números tivessem significado global (sobre toda a rede), poderia ocorrer que dois circuitos virtuais de mesmo número global de circuito virtual pudessem passar através de algum roteador intermediário, conduzindo a **ambigüidades**.
- ◆ Em caso de estabelecimento de circuitos *simplex*, não ocorrerá ambigüidade.

- **Circuitos virtuais podem ser propagados em ambas direções (podem ser iniciados em ambos os fins da conexão *end-to-end*) ao mesmo tempo, ao longo de uma cadeia de roteadores, constituindo circuitos *full-duplex*.**
- **Quando chamadas estabelecidas (que estão se propagando) chegam, em algum ponto, a roteadores adjacentes, cada roteador deverá, então, escolher um número de circuito virtual para usar para o circuito *full-duplex* que está tentando estabelecer.**
- **Se os roteadores foram programados para escolher o menor número ainda não utilizado no *link*, ambos irão escolher o mesmo número, levando ao estabelecimento de dois circuitos virtuais não relacionados, de mesmo número, trafegando sobre a mesma linha física.**
- **Quando um novo pacote de dados chega, o roteador que o recebe não tem como dizer se é um pacote que está sendo propagado em uma direção sobre um circuito ou se é um pacote que está se propagando reversamente sobre o outro circuito.**

- ⇒ Cada processo que utiliza um circuito virtual deve indicar quando é finalizado, para que o circuito virtual possa ser excluído das tabelas de roteamento, visando a recuperação do espaço.
- ⇒ Em redes públicas, a estratégia para resolver este problema é cobrar os usuários por tempo de conexão e por dados transportados.
- ⇒ Além desta providência, algum outro tipo de "punição" deve ser aplicado a máquinas que interrompem seus circuitos virtuais bruscamente, sem polidamente avisar da liberação do circuito quando não mais o estão utilizando.

DATAGRAMAS

- ◆ Os pacotes independentes de uma organização **sem conexão** são chamados **datagramas**, em analogia com telegramas.
- ◆ Em contraste com os circuitos virtuais, em uma sub-rede que utiliza datagramas nenhuma rota é estabelecida antecipadamente.
- ◆ Cada pacote enviado pela rede é roteado independentemente de seus predecessores.
- ◆ Desta forma, pacotes sucessivos podem seguir rotas diferentes.
- ◆ O envio de pacotes por sub-redes que utilizam datagramas exige a execução de mais tarefas.
- ◆ No entanto, estas redes são geralmente mais robustas, podendo se adaptar a falhas e ao congestionamento mais facilmente do que sub-redes que utilizam circuitos virtuais.

- ◆ **Usando datagramas internamente, os roteadores não terão uma tabela com uma entrada para cada VC aberto.**
- ◆ **Ao invés disto, terão uma tabela que indicará qual a linha de saída a ser usada para cada possível roteador de destino.**
- ◆ **Estas tabelas são também necessárias quando circuitos virtuais são usados internamente, para determinar a rota para um pacote.**
- ◆ **Cada datagrama deve conter o endereço de destino completo.**
- ◆ **Para uma rede grande, estes endereços podem ser um tanto longos (uma dúzia de bytes ou mais).**
- ◆ **Quando um pacote chega, o roteador procura a linha de saída que irá usar e envia o pacote.**
- ◆ **Ainda, o estabelecimento e a liberação da rede para cada roteador não requerem qualquer particular tarefa de parte dos roteadores.**

COMPARAÇÃO ENTRE CIRCUITOS VIRTUAIS E SUB-REDES DATAGRAMAS

ASPECTO	SUB-REDE DATAGRAMA	SUB-REDE VC
Estabelecimento do circuito	Não necessário	Requerido
Endereçamento	Cada pacote contém os endereços completos de fonte e destinatário	Cada pacote contém um número VC curto
Informação de Estado	Sub-rede não retém informação de estado	Cada VC requer espaço na tabela de sub-rede
Roteamento	Cada pacote é roteado independentemente	A rota é escolhida quando o VC é estabelecido, todos os pacotes seguem esta rota.
Efeito de falhas em roteadores	Nenhuma, exceto para pacotes perdidos durante a falha	Todos os VC que passam pelo roteador em falha são terminados
Controle de Congestão	Difícil	Fácil se <i>buffers</i> suficientes forem alocados para cada VC antecipadamente

Dentro de uma sub-rede existem muitos compromissos a serem considerados entre o uso de VCs e datagramas:

1. Um destes compromissos diz respeito ao espaço na memória do roteador e à largura de banda.

- VCs permitem que pacotes contenham números de circuitos, ao invés de endereços de destino completos, o que economiza banda.
- Como os pacotes tendem a ser razoavelmente curtos, um endereço completo de destino em cada pacote poderia representar uma significativa quantidade de cabeçalho, e um conseqüente desperdício de largura de banda.
- No entanto, o preço pago por usar VCs internamente está relacionado à ocupação de memória do roteador, já que necessitam ocupar um espaço na tabela dentro dos roteadores.
- A decisão irá depender da relação entre o custo dos circuitos de comunicação (largura de banda) e o custo associado à memória do roteador.

2. Outro compromisso diz respeito ao tempo de estabelecimento (*setup time*) versus o tempo de "divisão de código" de endereçamento (*address parsing time*).

- A utilização de VCs requer uma fase de *setup*, a qual toma tempo e consome recursos.
- Entretanto, após o *setup*, decidir o que fazer com um pacote de dados em uma sub-rede VC é fácil: o roteador apenas tem que utilizar o n° do circuito como índice em uma tabela para saber para onde o pacote irá.
- Em uma sub-rede datagrama é requerido um procedimento mais complicado para determinar para onde os pacotes irão.

3. VCs têm algumas vantagens ao evitar congestionamento dentro da sub-rede, porque os recursos podem ser reservados antecipadamente, quando a conexão é estabelecida.

- Uma vez que os pacotes começam a chegar, a largura de banda necessária e a capacidade de roteamento estarão garantidas.
- Com redes datagrama, evitar congestionamento é mais difícil.

4. VCs têm problemas de vulnerabilidade.

- Se um roteador tem problemas e perde sua memória, mesmo que retorne segundos mais tarde, todos os circuitos virtuais que passam por ele terão de ser abortados.

5. Em contraste, se um roteador datagrama tem problemas, apenas aqueles usuários cujos pacotes estão na fila do roteador, naquele momento, irão sofrer.

6. A perda de uma linha de comunicação é fatal para os VCs que a utilizam, mas pode ser facilmente compensada se datagramas são usados.

7. Datagramas permitem que os roteadores possam fazer um balanço do tráfego através da sub-rede, já que as rotas podem ser mudadas no meio do caminho por meio de uma conexão.

REDES BASEADAS EM DATAGRAMAS:

- **Exemplo: Internet**
- **Não-orientadas à conexão.**
- **Modelo: Sistema Postal.**
- **Baseadas em Datagramas.**
- **Cada pacote precisa transportar o endereço do destino completo.**
- **Cada pacote é enviado independente do predecessor, se houver.**
- **Os controles de erro e de fluxo ficam a cargo do *host* (a rede não ordena pacotes ou controla fluxo).**
- **Consideradas (principalmente pelos defensores de redes baseadas em VCs) como redes não confiáveis, não importa quão bom seja o projeto.**

REDES BASEADAS EM CIRCUITOS VIRTUAIS:

- **Exemplo: ATM**
- **Baseadas no estabelecimento de Circuitos Virtuais (VCs).**
- **Confiáveis.**
- **Modelo: Companhias Telefônicas.**
- **Orientadas à conexão (necessitam tempo de *setup*):**
 1. Antes de enviar os dados, a camada de rede processa do lado do TX para estabelecer conexão para o RX.
 2. A conexão recebe identificador especial (nº do circuito virtual) e é usada até que todos os dados sejam enviados quando, então, é liberada.
 3. Quando a conexão é estabelecida os dois processos negociam os parâmetros, a qualidade e o custo do serviço a ser provido.
 4. A comunicação estabelecida é bi-direcional.
 5. Os pacotes são entregues em seqüência.
 6. O controle de fluxo é provido automaticamente para prevenir que sejam transmitidos pacotes a taxas maiores do que aquela com que o receptor possa receber (\Rightarrow *overflow!!*).
- **Entrega dos pacotes é garantida.**
- **Provê confirmação de entrega e priorização opcional de pacotes.**