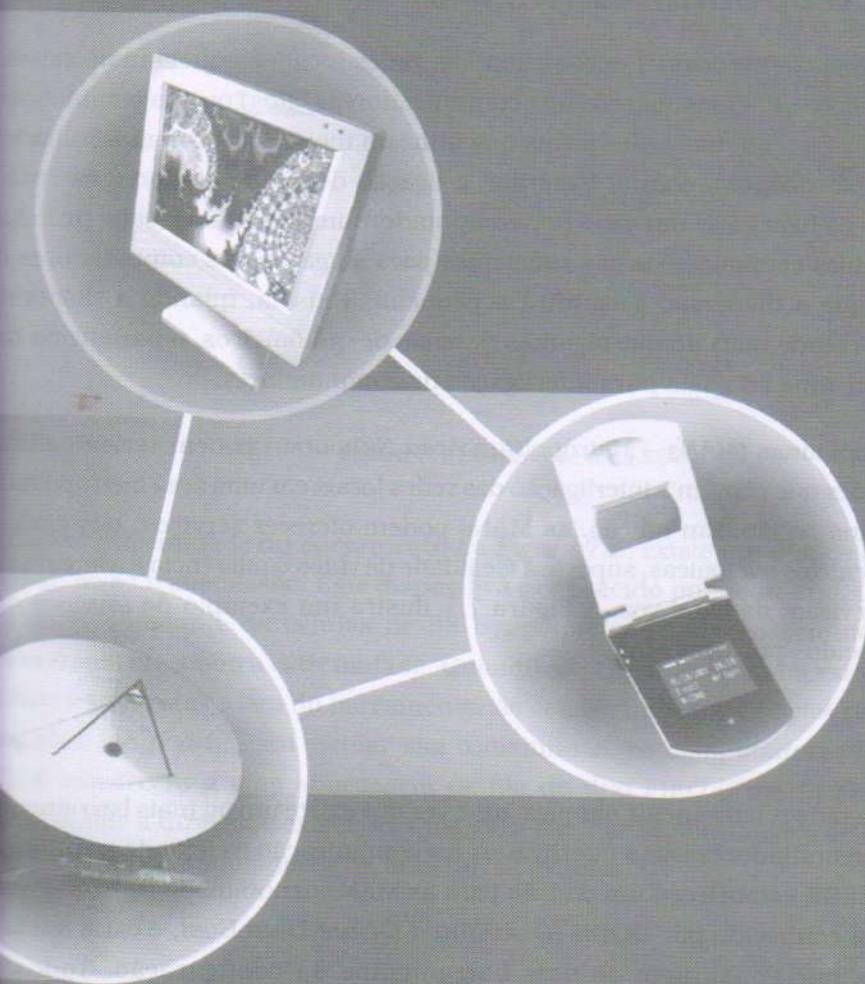


Capítulo

7

MANs e WANs



Introdução

No capítulo anterior, nosso foco foi abordar as tecnologias das redes locais e SANs. Estes ambientes de redes provêm uma série de facilidades para os usuários de um ambiente computacional distribuído em qualquer organização. Em adição, estas configurações de rede podem ser agrupadas considerando-se áreas geograficamente distribuídas. O objetivo principal da formação de uma configuração geograficamente distribuída numa corporação é a obtenção de um ambiente melhor e com maior poder computacional.

Desta forma, neste capítulo vamos abordar alguns dos elementos necessários que constituem a espinha dorsal das redes metropolitanas (MANs) e geograficamente distribuídas (WANs). Em outras palavras, vamos estudar os ambientes levando em consideração os diversos dispositivos que auxiliam a conexão das LANs e, ainda, vamos conhecer os protocolos que provêm a transparência necessária para a utilização das redes MANs e WANs.

Redes Metropolitanas (MANs)

A configuração mais convencional encontrada nas redes locais é aquela onde existe a interligação dos computadores da rede aos concentradores (*hubs*) ou aos comutadores (*switches*). Por outro lado, nas redes locais que utilizam meios físicos compartilhados, como por exemplo um cabo coaxial Ethernet, a ligação dos computadores na rede é efetuada através da ligação de um cabo por computador interceptando o cabo principal da rede. Essas duas configurações são suficientes para a ligação dos computadores na rede, uma vez que a dispersão geográfica é pequena. Todavia, quando a dispersão geográfica compreende mais do que algumas dezenas de quilômetros, o paradigma das LANs não fornece uma resposta para interligação de computadores.

As redes metropolitanas (MANs – *Metropolitan Area Networks*) podem ser entendidas como aquelas redes que provêm a interligação das redes locais em uma área metropolitana de uma determina região. Em adição, as MANs podem oferecer serviços, tais como a interligação de centrais telefônicas, suporte a facilidade de vídeo conferência e transmissão de sinais de televisão, dados e voz. A Figura 7.1 ilustra um exemplo de serviços que podem ser oferecidos por uma MAN.

DQDB

Uma MAN é uma rede relativamente simples, uma vez que existe um ou mais barramentos onde todos os computadores estão interligados e a comunicação é efetuada por difusão (*broadcast*). O IEEE estabeleceu um padrão para as MANs denominado de 802.6. Esse padrão, também conhecido por DQDB (*Distributed Queue Dual Bus*), é caracterizado por dois cabos que constituem os dois barramentos da configuração. Todos os

computadores estão interligados aos dois barramentos através de dois cabos. Um primeiro efetua a transmissão num determinado sentido do barramento da MAN. O outro cabo de ligação do computador faz a transmissão no sentido oposto ao primeiro. A Figura 7.2 apresenta um exemplo de uma rede MAN baseada no padrão 802.6.

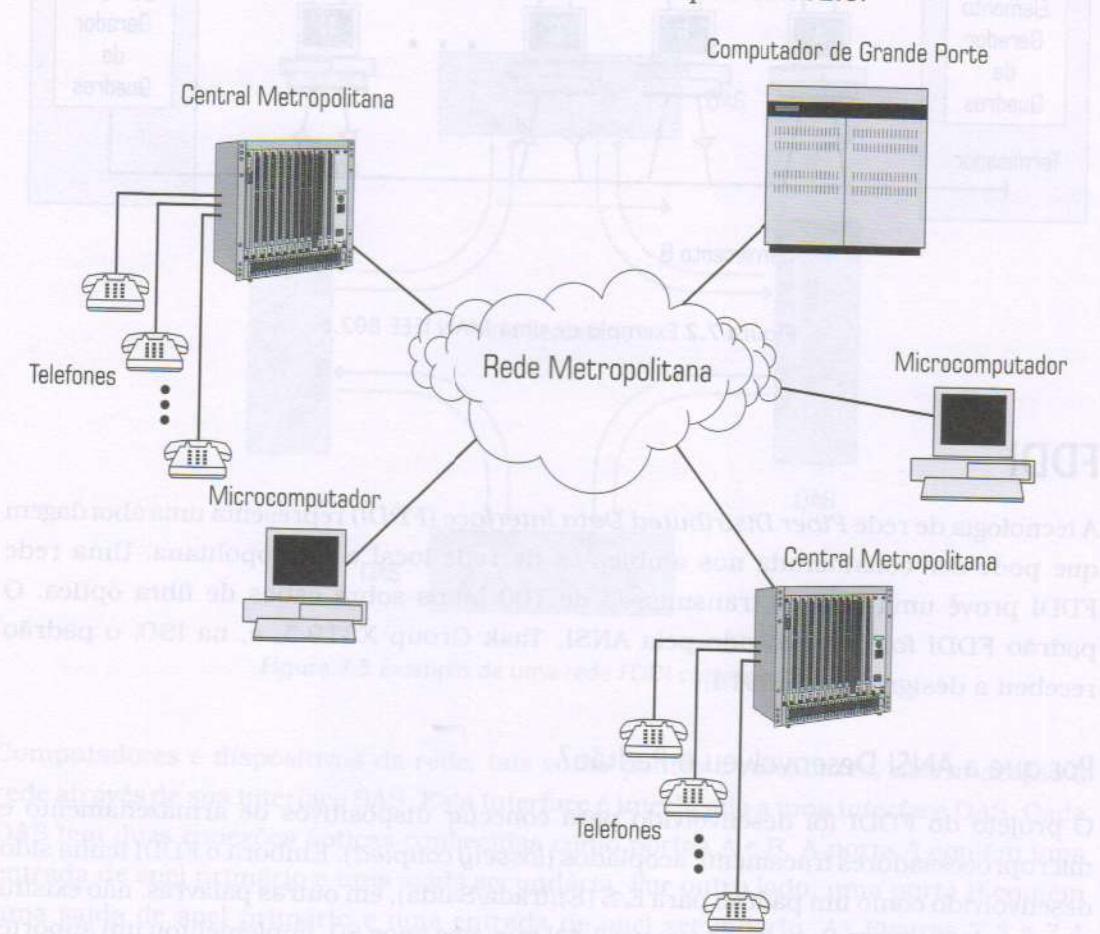


Figura 7.1 Exemplo de uma MAN.

Em cada extremidade do barramento da Figura 7.2, existe um dispositivo responsável pelo início da transmissão. Este dispositivo é conhecido por *head-end*. O *head-end* gera um fluxo constante de células de 53 bytes que trafegam no sentido horizontal do barramento até a outra extremidade. Quando as células chegam na extremidade oposta ao *head-end*, estas saem do barramento. As células utilizam 44 bytes para o transporte de dados (*payload*). Para efetuar sua transmissão, os computadores de um ambiente DQDB obedecem a uma abordagem de fila do tipo FIFO (*First In First Out*). O que corresponde a dizer que existe uma fila para atender às solicitações de transmissão em seqüência dos computadores de uma forma ordenada.

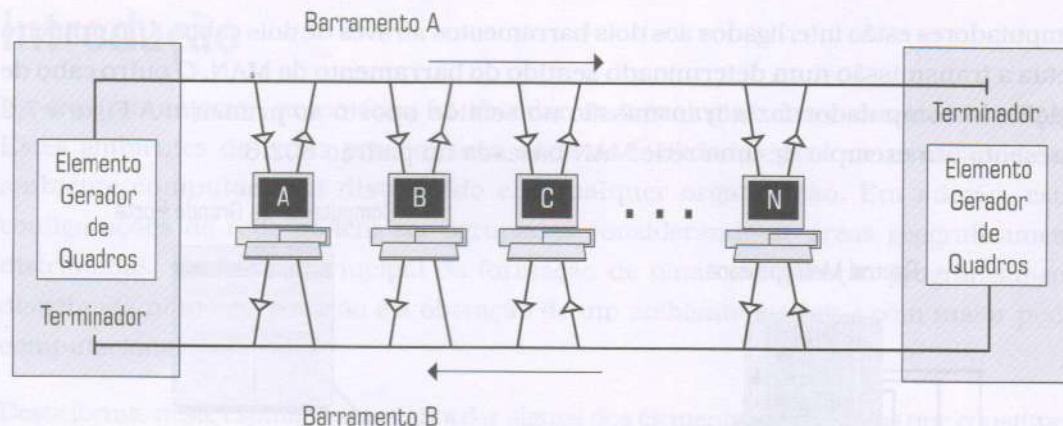


Figura 7.2 Exemplo de uma MAN IEEE 802.6.

FDDI

A tecnologia de rede *Fiber Distributed Data Interface* (FDDI) representa uma abordagem que pode ser considerada nos ambientes de rede local e metropolitana. Uma rede FDDI provê uma taxa de transmissão de 100 Mbps sobre cabos de fibra óptica. O padrão FDDI foi desenvolvido pela ANSI, Task Group X3T9.5, e, na ISO, o padrão recebeu a designação de 9314.

Por que a ANSI Desenvolveu o Padrão?

O projeto do FDDI foi desenvolvido para conectar dispositivos de armazenamento e microprocessadores fracamente acoplados (*loosely coupled*). Embora o FDDI tenha sido desenvolvido como um padrão para E/S (Entrada/Saída), em outras palavras, não existiu um comitê do IEEE; esta foi a primeira LAN que, nos anos 80, implementou um suporte de transmissão de rede a 100 Mbps.

NOTA

Um ambiente fracamente acoplado (*loosely coupled*) é aquele no qual cada processador tem sua memória local e a comunicação entre estes é efetuada através do envio de mensagens numa rede de comunicação.

Como Você Imagina a Topologia de uma LAN FDDI?

O FDDI usa dois anéis como backbone de transmissão denominados de primário e secundário. O anel primário é empregado como meio para circular a informação. No caso de ocorrer um defeito, o anel secundário entra em ação. Este mecanismo é conhecido como *self-healing* (autocura). A topologia do FDDI é conhecida como *counter-rotating*

ring. De forma semelhante a uma rede *Token-Ring*, a LAN FDDI usa um *token* para prover acesso à rede. A rede tem três tipos de dispositivos de comutação. Estes equipamentos são chamados de *stations*, sendo um do tipo *SAS* (*Single Attached Station*) e os outros dois do tipo *DAS* (*Dual Attached Station*).

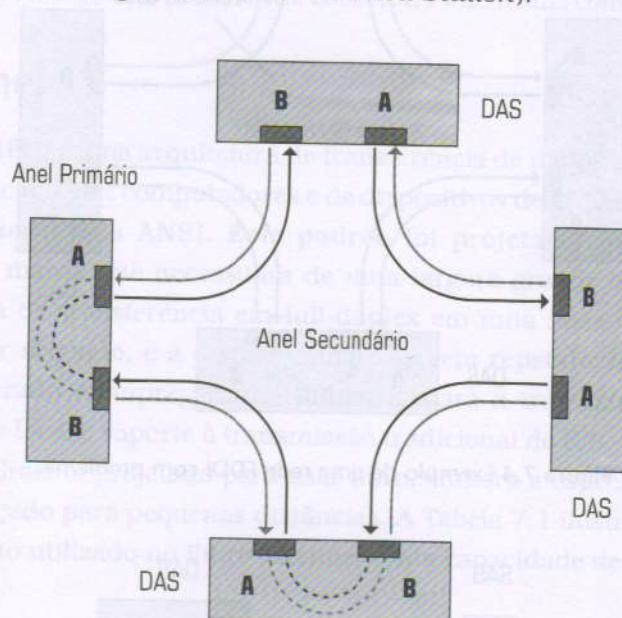


Figura 7.3 Exemplo de uma rede FDDI convencional.

Computadores e dispositivos de rede, tais como pontes e roteadores, obtêm acesso à rede através de sua interface *SAS*. Esta interface é interligada a uma interface *DAS*. Cada *DAS* tem duas conexões ópticas conhecidas como portas *A* e *B*. A porta *A* contém uma entrada de anel primário e uma saída secundária. Por outro lado, uma porta *B* contém uma saída de anel primário e uma entrada de anel secundário. As Figuras 7.3 e 7.4 ilustram, respectivamente, uma configuração de uma rede FDDI convencional e um exemplo de uma rede que apresentou um problema.

Um segundo tipo de interface do tipo *DAS*, cuja função é a de concentrador, contém um conjunto de interfaces denominadas de *M*, em adição às interfaces *A* e *B*. As interfaces *M* (*master ports*) são usadas para prover conectividade com interfaces *SAS* ou com outras interfaces do tipo *DAS*. Com o uso dessa extensão, é aumentada a capacidade de acesso ao anel primário. A Figura 7.5 apresenta um exemplo do segundo tipo de interface *DAS* e suas conexões.

- Outro ambiente de uso do FDDI foi como interface em dispositivos comutados (*switches*) para prover acesso de 100 Mbps para servidores.
- Elevado custo da fibra levou ao desenvolvimento do *CDDI* (Copper Distributed Data Interface). Todavia, o sucesso do Ethernet 100BASET inibiu uma competitividade do CDDI.

Fibre Channel

O *Fibre Channel* (FC) é uma arquitetura de transferência de dados desenvolvida por um consórcio de fabricantes de computadores e de dispositivos de armazenamento de massa que foi padronizado pela ANSI. Este padrão foi projetado para dispositivos de armazenagem de massa que necessitam de uma largura grande de banda. O padrão suporta uma taxa de transferência em full-duplex em uma faixa que vai de 12.5 até dezenas Gbps por segundo, e a distância máxima sem repetidores é de 10 Km. Este padrão é considerado e empregado na indústria para a transmissão como rede de interconexão, rede local e suporte à transmissão tradicional de E/S. Como o nome diz, o padrão foi originalmente projetado para usar fibra, embora a especificação inclua cabo coaxial e par trançado para pequenas distâncias. A Tabela 7.1 ilustra uma comparação entre o cabeamento utilizado no Fibre Channel e sua capacidade de transmissão.

Tabela 7.1: Cabeamento e Taxa de Transmissão do Padrão Fibre Channel.

Tipo de mídia	Taxa de Transmissão			
	800 Mbps	400 Mbps	200 Mbps	100 Mbps
Fibra monomodo	10 Km	10 Km	10 Km	10 Km
Fibra Multimodo 50 µm	0.5 Km	1 Km	2 Km	10 Km
Fibra Multimodo 62.5 µm	175 m	350 m	1.5 m	1.5 m
Cabo coaxial de vídeo	25 m	50 m	75 m	100 m
Cabo de par trançado	–	–	50 m	100 m

A sinalização usada pelo Fibre Channel é a de 8B10B, a qual codifica cada 8 bits de dados em 10 bits de código. Ainda são incorporados bits adicionais para conferência de erro. A codificação do Fibre Channel foi adotada como padrão de sinalização para as redes de Gbps. O padrão 8B10B, reconhecidamente eficiente, foi aceito pelo comitê do *Gigabit Ethernet* que resolveu adotar o sistema utilizado pelo padrão ANSI X3 (Fibre Channel). O padrão FC suporta protocolos de mais alto nível, tais como SCSI, HIPPI-FR (Framing Protocol), IP e IBM System/390 I/O. O FC é dividido em cinco níveis funcionais, denominados de FC – 0 até FC – 4, como ilustrado na Figura 7.6, e têm as seguintes funções:

- FC – 0: define o nível físico – cabos, conectores, velocidade de bits, especificação óptica e elétrica, especificação de jitter e distância sem repetição.
- FC – 1: neste nível é definida a codificação dos dados e controle de sincronização de bit/byte e palavras, controle de erros.

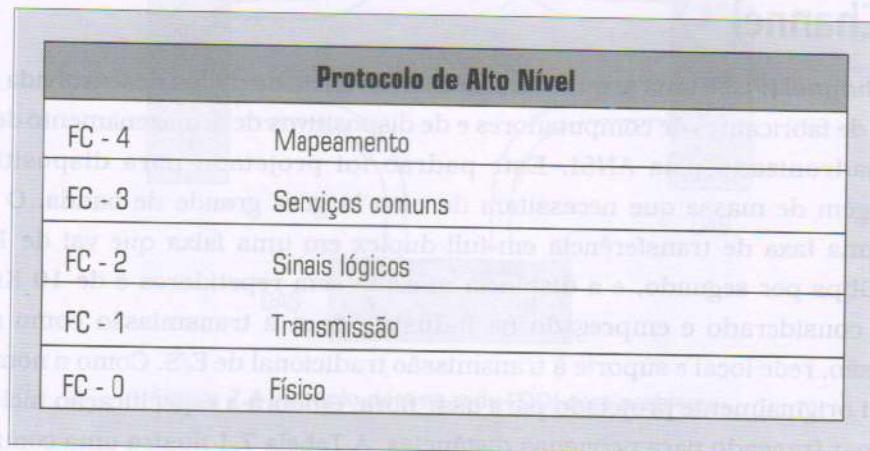


Figura 7.6 Modelo de referência Fibre Channel.

- FC – 2: define a forma do protocolo de sinalização; é semelhante ao enlace nos protocolos convencionais. Todavia, com o atual hardware, o enlace é efetuado ponto-a-ponto.
- FC – 3: define o nível de serviço entre nós.
- FC – 4: faz a interface entre os protocolos de mais alto nível e as camadas FC – 2 e FC – 3. Um exemplo é a transmissão de um pacote IP, ou seja, esta camada auxilia a transmissão utilizando os serviços da camada FC – 2. Quanto a exemplos de interfaces de canais de E/S (Entrada/Saída) definidos pelos FC-4, podemos citar:
 - O HIPPI (*High-Performance Parallel Interface*) que é um padrão que visa a transferência direta entre memória de computadores *mainframes* e supercomputadores, com taxas de transferência entre 800 Mbps e 1.600 Mbps.
 - O SCSI (*Small Computer System Interface*) que é uma interface largamente utilizada em ambientes de computadores pessoais, servidores e workstations visando o suporte de altas taxas de transferência de dispositivos como discos, equipamentos gráficos e de vídeo.

WANs

Quando as distâncias envolvidas na interligação dos computadores é superior a uma região metropolitana, podendo ser a dispersão geográfica tão grande quanto a distância entre continentes, a abordagem correta é a *rede geograficamente distribuída* (WAN). Em uma WAN, existe o roteamento dos datagramas ao longo de várias redes diferentes.

Geralmente, as redes geograficamente distribuídas têm uma taxa de transmissão menor e uma taxa de ocorrência de erros maior quando comparadas com as LANs.

NOTA

Uma observação interessante nesse ponto é que os dispositivos denominados de switches do nível 3 também podem ser considerados ambientes geograficamente distribuídos. Embora um switch seja uma caixa situada em um local, é possível o estabelecimento de várias redes com diferentes endereços. O roteamento é efetuado dentro do switch de nível 3.

As WANs, para efetuar a interligação das redes dispersas geograficamente, empregam dispositivos para efetuar o roteamento dos datagramas e a ligação à rede de comunicação. Assim, neste capítulo, vamos estudar também os equipamentos usados nos ambientes de inter-redes.

ATM

O ATM (Asynchronous Transfer Mode) é uma tecnologia de comutação (switching) baseada em células de tamanho fixo (53 bytes) para transporte da informação. A filosofia da rede é a transferência da informação numa simples LAN, MAN ou WAN. Outro objetivo da tecnologia ATM é a de ser uma ponte entre antigos diferentes legados de redes e a manutenção da oferta de uma qualidade de serviço (QoS). O desenvolvimento da tecnologia ATM é observado nos segmentos de desktop (placas e conexões), LAN, backbone e WAN. Por esta razão, consideramos interessante abordar a tecnologia de ATM no capítulo das redes geograficamente distribuídas.

Na terminologia de redes com grande disponibilidade de largura de banda, dois conceitos de gerenciamento da largura de banda são geralmente confundidos. Estes são a classe de serviços (CoS – Class of Service) e a qualidade de serviços (QoS – Quality of Service).

A classe de serviço (CoS) determina os limites de serviços (de forma discreta) que uma rede deve oferecer aos datagramas através da classificação do tráfego. Por outro lado, a qualidade de serviço (QoS) permite a negociação de um determinado serviço de forma dinâmica através da reserva de largura de banda.

Várias organizações têm trabalhado com os padrões CoS e QoS. O modelo CoS inclui o Differentiated Services (DiffServ) do IETF, as extensões do IEEE 802.1D, conhecidas como 802.1p/Q, e o user-network interface (LUNI 2.0) do ATM Forum. Por outro lado, os modelos de QoS incluem Integrated Services (IntServ) do IETF e ATM Forum's QoS.

No paradigma de classe de serviço (*CoS*), a sinalização reside em cada pacote dos dados. Assim, esta informação diz ao dispositivo que vai tratar a qual classe o datagrama pertence. Num ambiente de *CoS*, o tráfego pode ser classificado, como por exemplo, por melhor esforço (*best-effort*) ou multimídia. Outra possível classificação seria para descarte ou alto grau de segurança.

Uma prioridade bem definida dos tipos de tráfegos numa rede é um fator importante para aqueles pontos onde ocorrem os congestionamentos. Nestes locais, decisões sobre o retardo de envio ou descarte de pacotes devem ser priorizados por *switches* e *routers*. Exemplos de aplicações que necessitam de uma prioridade diferencial são o processamento de transações, aplicações de tempo real e vídeo, entre outras aplicações. A qualidade de serviço (*QoS*) implica não só na prioridade do tráfego, mas também:

- A garantia de largura de banda.
- As características de latência e o jitter da rede.

NOTA

O termo congestionamento pode ser interpretado de forma semelhante ao engarramento de tráfego dos carros.

As LANs, que utilizam o protocolo TCP/IP, já utilizam a prioridade há algum tempo através do parâmetro Type of Service (ToS) do datagrama IP. Por outro lado, nas WANs, os roteadores empregam uma política de prioridade na fila de saída para aqueles pacotes que devem seguir em frente. A qualidade de serviço pode ser implementada através de protocolos, tais como o ReSerVation Protocol (RSVP). O RSVP é um protocolo fim-a-fim que permite que um nó requisite uma certa reserva de garantia de largura de banda na rede. O RSVP opera no nível 3 para fluxo de dados baseados em IP. O protocolo permite que *switches* do nível 3 e roteadores mantenham filas com prioridades múltiplas.

O protocolo RSVP foi projetado para permitir que, numa ligação qualquer, o remetente, o destinatário e os roteadores pudessem se comunicar a fim de estabelecer o estado da rota para suportar os serviços que exijam *QoS*. Um nó emprega o protocolo RSVP para solicitar um serviço específico de qualidade à rede, segundo a necessidade de uma dada aplicação. Assim, esta solicitação vai desde o nó de origem, passando pelos roteadores até chegar ao nó destinatário.

Nos roteadores, dois mecanismos são utilizados para controle da solicitação da qualidade de serviços. Estes mecanismos são o da *admissão* e *policimento*. A técnica de admissão determina se o roteador tem recursos suficientes para atender à solicitação do serviço *QoS*. Por outro lado, o policimento caracteriza se o usuário possui permissão administrativa para solicitar o serviço. Em caso positivo das políticas de admissão e policimento, os parâmetros necessários ao atendimento do *QoS* são configurados no

quadro do RSVP. O protocolo RSVP identifica uma sessão de comunicação através do endereço do destinatário, do tipo de protocolo de transporte e do número da porta do destino. As operações do protocolo de reserva somente se aplicam aos pacotes de uma sessão. Outras características do protocolo são:

- Permitir o uso de multicast.
- Fácil implementação em computadores, switches e roteadores.
- Não é um protocolo de roteamento.

Retornando a características de uma rede ATM, é importante saber que:

- O ATM não transfere as células de maneira assíncrona, como o nome sugere. A forma assíncrona se refere à falta de sincronismo de quando uma solicitação de transmissão será efetuada.
- As células são transmitidas de uma forma contínua e síncrona, sem interrupção entre as mesmas.
- Quando não existe transmissão por parte do usuário, a célula ATM é preenchida com uma seqüência de bits para indicar que está vazia (ou livre).
- A natureza assíncrona do ATM, conforme comentamos no primeiro tópico, vem do tempo indeterminado quando a próxima unidade de informação lógica de conexão será iniciada.
- O tempo não utilizado por uma conexão lógica é cedido para outra conexão ou usado por células livres.
- O significado do tempo não utilizado pode ser traduzido como células para uma determinada conexão que podem chegar de maneira assíncrona.
- O roteamento de cada célula é efetuado através do endereço dentro da própria célula.

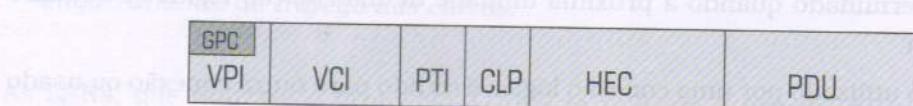
A utilização de células pequenas e de tamanho fixo nas redes ATM resulta num conjunto de vantagens:

- Implementação em hardware de alto desempenho para os *switches* ATM. Estes são mais simples e mais eficientes.
- Em 622 Mbps, as células ATM podem ser comutadas em apenas 0,68 ms.
- O desempenho do ATM é uma importante consideração a ser observada por causa do fluxo orientado das células e a comutação rápida em hardware que permite que tenhamos um tamanho fixo para a célula.
- Com o tamanho da célula fixo, é possível fazer alocação de memória sem desperdício, uma vez que o incremento de memória será conhecido previamente.
- O armazenamento das células não só é eficiente na memória como também no momento da busca.
- Outro fator importante de células de tamanho pequeno e fixo é o transporte eficiente de informação constante com baixa velocidade, como a voz.

Diferente de outros protocolos quanto à capacidade de transferência, o ATM pode transportar voz, vídeo, dados, imagem e gráficos separadamente ou simultaneamente, empregando o mesmo enlace. A característica de transporte de múltiplos tipos de informação no ATM deve-se ao fato do tamanho fixo das pequenas células do ATM e da qualidade de serviço (QoS).

Os primeiros 5 bytes contêm informação de controle, o cabeçalho e endereçamento. Os demais 48 bytes, chamados de *payload*, contêm os dados. O cabeçalho (*header*) do ATM é pequeno para maximizar a eficiência da rede ATM. Por outro lado, deveríamos ter o *payload* o maior possível para melhorar ainda mais o desempenho da rede. Todavia, as redes ATM foram projetadas para o transporte não-exclusivo de grandes quantidades de informação. Informações como voz e tráfego de vídeo são *payloads* endereçados pelo ATM. O ATM Forum, quando das discussões da concepção do padrão, não apenas se preocupou com a eficiência, mas também com o efeito do *retardo de empacotamento*. O retardo de empacotamento é o tempo gasto para o preenchimento de uma célula ATM com uma amostra de voz digitalizada de 64 kbps. O tamanho de 53 bytes da célula ATM foi um compromisso entre a eficiência de *payload* e o retardo de empacotamento. A Figura 7.7 nos mostra uma célula ATM, e nos ajuda a entender a habilidade de transferência eficiente de informação multimídia.

Célula ATM Genérica



GPC – Generic Flow Control (só para UNI)

VPI – Virtual Path Identifier

VCI – Virtual Channel Identifier

PTI – Payload Type

CLP – Cell Loss Priority

HEC – Header Error Control

PDU – Protocol Data Unit

Figura 7.7 Exemplo de uma célula ATM.

Apresentamos, a seguir, os campos de uma célula ATM:

- **GPC (Generic Flow Control):** estes 4 bits são usados para o controle local de fluxo para múltiplos usuários no lado do usuário de uma *switch*, compartilhando o acesso sob uma linha padrão, adotando-se uma *UNI (User Network Interface)* padronizada. Este campo geralmente não é usado e é setado para 0. No caso de uma rede privada para uma interface de rede P-NNI (*Private Network Network Interface*), estes bits são usados para informação de endereço.
- **VPI (Virtual Path Identifier):** os 8 bits provêm dos 255 possíveis caminhos para as células UNI e 4095 para P-NNI.

- VCI (*Virtual Channel Identifier*): cria a possibilidade de uso de mais 16 bits, ou seja, 65.536 possíveis conexões dentro de cada path de endereço. Alguns endereços são usados para funções reservadas como sinalização.
- PTI (*Payload Type Identifier*): este campo serve para a distinção entre células de usuários e células chamadas de OA&M (*Operation, Administration and Maintenance*), que são comandos e estatísticas na rede. No caso de um engarrafamento (*congestion*) na rede, o PTI é alterado à medida em que vai passando entre os *switches*. Assim, a rede pode diminuir o engarrafamento descartando células que estão em excesso para a garantia de uma determinada velocidade.

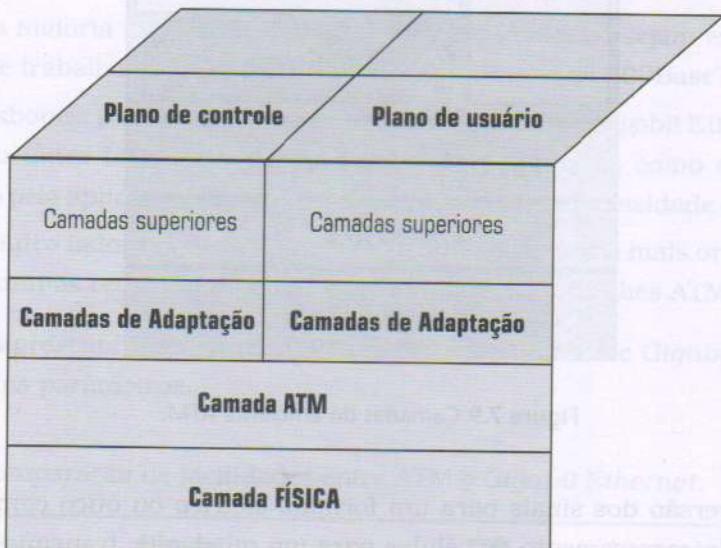


Figura 7.8 Modelo de referência de protocolo ATM.

- CLP (*Cell Loss Priority*): este bit é um indicador de dois estados de prioridade, informando à rede qual célula deve ser descartada no caso de engarrafamento da rede. O campo CLP é configurado inicialmente para 0 nas células. Quando as mesmas trafegam pela rede, e um determinado *switch* observa que existe um congestionamento, a célula terá seu CLP modificado para 1 pelo *switch*. Esta mudança sinaliza que não existe condição de serem atendidos os parâmetros negociados durante o início da conexão. As células com bit igual a 1 serão descartadas primeiramente. Caso o problema continue, aquelas com valor 0 começarão a ser descartadas.
- HEC (*Header Error Control*): tem a capacidade de corrigir erros simples de cabeçalho e detectar erros múltiplos para assegurar o endereçamento correto. No caso de header com múltiplos erros, estes serão descartados pelo nó, ou *switch*, que detectar o erro. O HEC não faz verificação de erros no payload, uma vez que os mesmos devem ser tratados pelos protocolos de transporte.

O modelo de referência do ATM é ilustrado na Figura 7.8. As três camadas do ATM têm as seguintes funções (Figura 7.9):

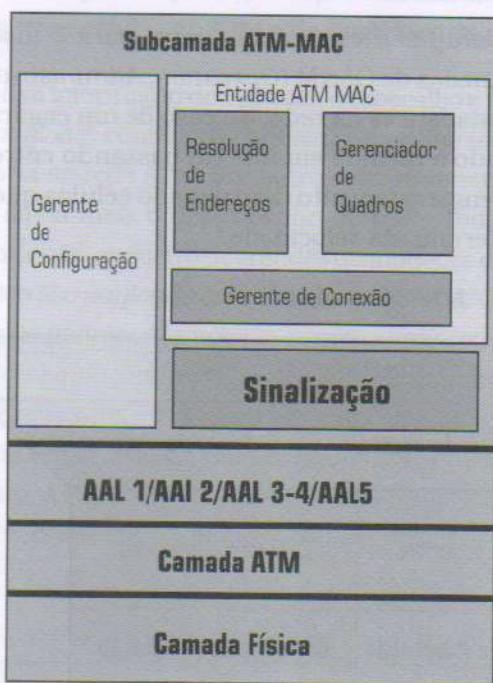


Figura 7.9 Camadas do ambiente ATM.

(1) Física: conversão dos sinais para um formato elétrico ou ótico compatível com o carregamento/descarregamento de células para um quadro de transmissão adequado. Alguns dos meios físicos suportados são:

- 155 Mbps – Sonet/STS-3c, fibra óptica Categoria 5 UTP
- 622 Mbps – Sonet/STS-12c, fibra óptica
- 25 Mbps – Categorias 3, 4 e 5

(2) ATM: prove a comutação e o roteamento dos pacotes ATM para seus respectivos VPIs e VCIs. Este nível é responsável por gerar os headers das células ATM e extraí-los quando as células chegam. De uma forma geral, a camada ATM é responsável por prover um conjunto comum de serviços para suporte aos protocolos de alto nível. Tais serviços podem ser traduzidos nos dados, voz, imagem e aplicações de vídeo.

(3) AAL (ATM Adaption Layer): esta camada garante a transferência de dados de uma determinada fonte para a aplicação destino sob uma rede ATM. A AAL empacota os dados da aplicação em células, antes do seu efetivo transporte, e os extrai no nó destinatário. O AAL é composto por diversos tipos, devido aos diferentes tipos de tráfego existente. Existem cinco AAL:

- AAL 1 – usado para aplicação de tempo real e aplicações de bit constante, tais como voz e vídeo.

- AAL 2 – usado para aplicação de tempo real e aplicações de bit variável, como por exemplo vídeo de MPEG.
- AAL 3/4 – estas camadas foram projetadas para prover suporte para aplicações que não necessitam de tempo real, originalmente idealizadas como suporte ao tráfego de LANs.
- AAL 5 – esta camada foi projetada para substituir a AAL 3/4 para propósitos de suporte às LANs, uma vez que apresenta baixo retardo por célula e um protocolo de encapsulamento simples.

É cada vez mais comum a comparação entre as tecnologias ATM e *Gigabit Ethernet*. Acreditamos que, em qualquer comparação entre o ATM e o *Gigabit Ethernet*, deve ser levado em conta o contexto, isto é, desktop, LAN, backbone e WAN. Assim, vale observar:

- Desktop: a maioria das placas de rede nos computadores, sejam estes pessoais ou estações de trabalho (workstations), emprega a tecnologia 100BaseT.
- LAN e Backbones: podem empregar indistintamente ATM e *Gigabit Ethernet*. A escolha de uma ou outra tecnologia é uma função de parâmetros como custo e serviços solicitados pela aplicação, tamanho da rede, topologia e necessidade de redundância.
- WAN: por outro lado, as redes WANs estão ficando a cada dia mais orientadas à ATM. Nos EUA, muitas redes frame relay estão empregando switches ATM.

A Tabela 7.2 apresenta um comparativo das tecnologias ATM e *Gigabit Ethernet* com relação a alguns parâmetros.

Tabela 7.2 Comparação de facilidades entre ATM e *Gigabit Ethernet*.

Facilidades	Ethernet	ATM
P/P/L *	Baixo custo	Custo moderado.
QoS	RSVP, IEEE802.1Q/p	Garantida com a gerência de tráfego.
Aplicações Usuários	Dados de alta velocidade voz/vídeo sobre IP	Dados, voz e vídeo.
Disponibilidade	Final de 1997	Começo de 1996.
Aplicações de Rede	Backbones, servidores Campus Backbones	WAN, backbones e servidores Campus Backbones.

* Preço/Performance/Largura de Banda

Os protocolos, que executam sobre o ATM, devem ser adaptados para executar em cima da camada de adaptação. Três clássicas soluções são:

- IP sobre ATM: é uma abordagem antiga com uma base instalada considerável. É um protocolo de nível 3, que faz o mapeamento dos endereços IP para endereços ATM. Assim, é permitido que dispositivos ATM enviem pacotes IP nas redes ATM. As desvantagens da abordagem são que: (1), o IP só aceita o protocolo IP; (2), o IP sobre

- ATM não tem suporte para tráfego multicast; (3), a falta de um protocolo de alocação dinâmica de endereços IP/ATM causa problema de escala.
- O protocolo LANE (*LAN Emulation*) foi desenvolvido para esconder dos usuários Ethernet a rede ATM. Assim, o LANE trabalha como uma ponte em cima do AAL5. O protocolo encapsula todos os pacotes no MAC Ethernet e, então, é enviado para a rede ATM. A Figura 7.10 ilustra um ambiente que utiliza o protocolo LANE.

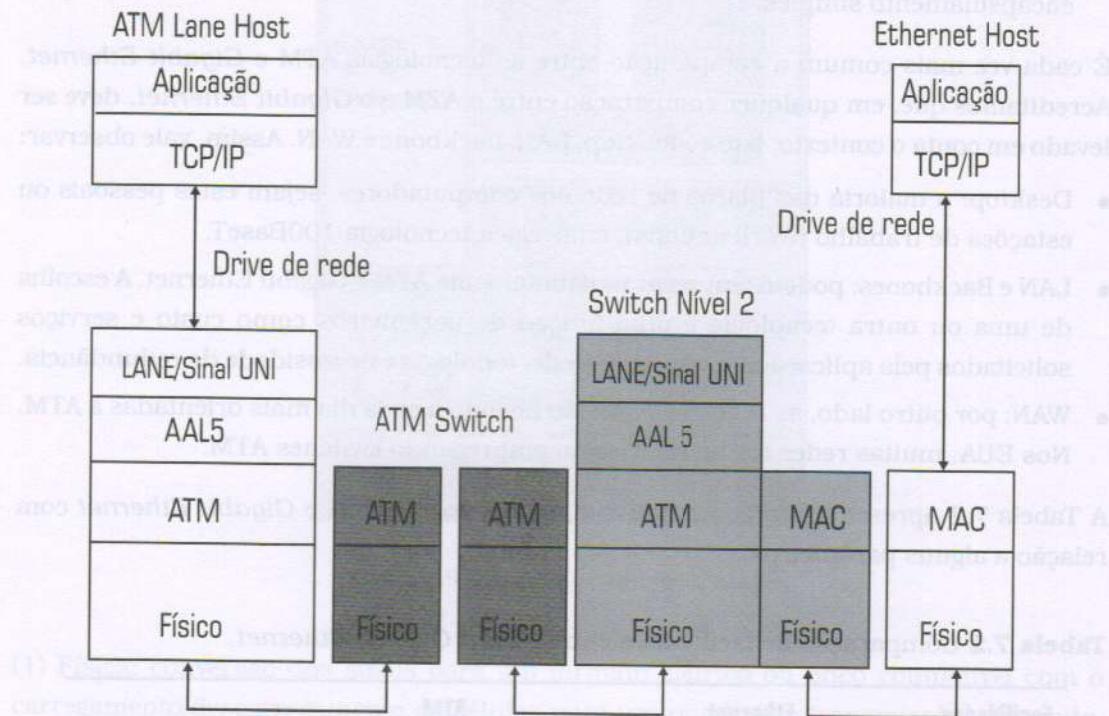


Figura 7.10 Ambiente utilizando o protocolo LANE.

- MPOA (*MultiProtocol Over ATM*) foi um protocolo desenvolvido pelo ATM Forum objetivando prover protocolo de roteamento para múltiplos protocolos. A idéia do MPOA é prover de forma limpa um ambiente de inter-rede nas redes ATMs consideradas antigos legados, como por exemplo o Ethernet. O MPOA provê os serviços do IP sobre ATM e LANE, fazendo a ponte e roteamento de pacotes.

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. Em adição, por causa da confusão criada pelas redes que estão implementadas em dispositivos do tipo caixa, vamos estudar também estes dispositivos nesta seção. Desta forma, abordaremos aos concentradores (hubs) e comutadores (switches), repetidores, pontes (bridges), roteadores e gateways.

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.

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 7.11 apresenta a situação de um repetidor considerando o modelo RM-OSI.

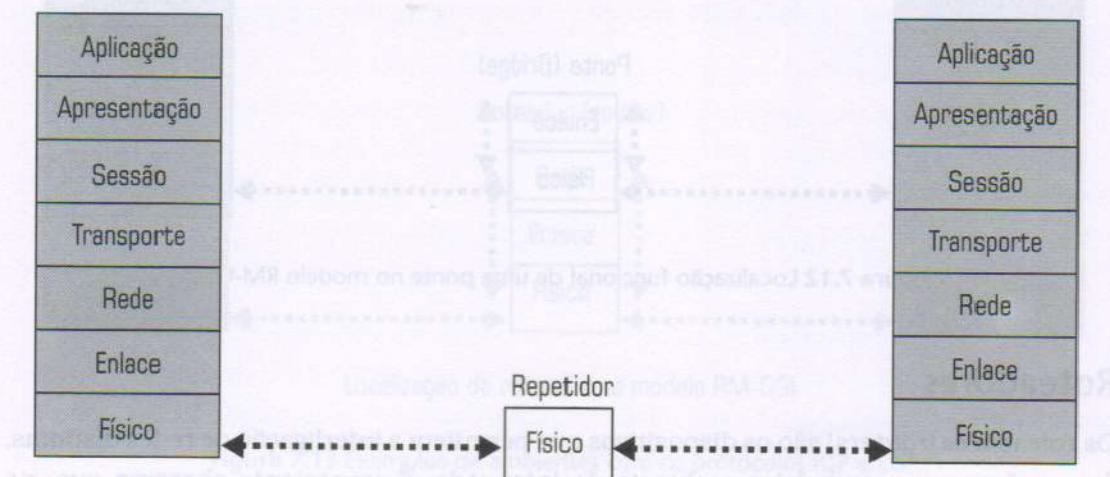


Figura 7.11 Localização funcional de um repetidor no modelo RM-OSI.

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.

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.

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). A Figura 7.12 apresenta a localização funcional de uma ponte segundo o modelo RM-OSI.

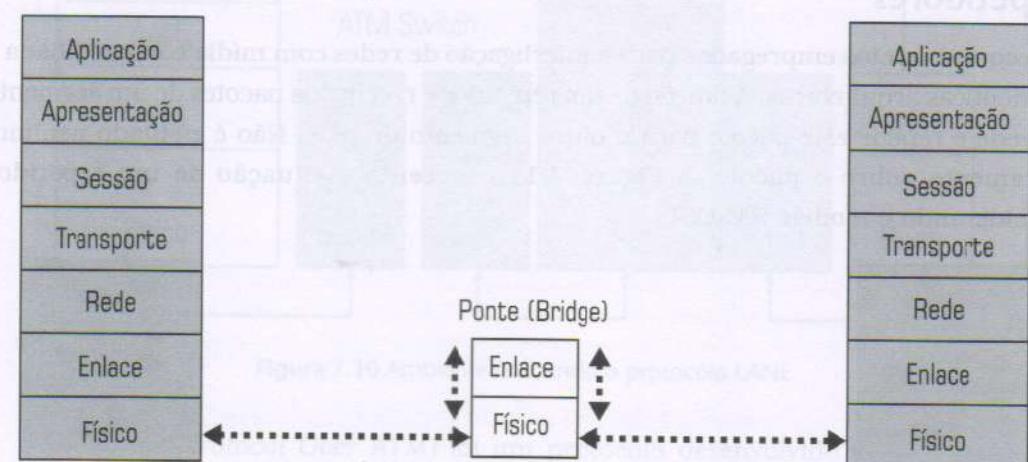


Figura 7.12 Localização funcional de uma ponte no modelo RM-OSI.

Roteadores

Os roteadores (*routers*) são os dispositivos que permitem a interligação de redes distintas, formando-se um verdadeiro ambiente de inter-rede. É importante observar que, na arquitetura TCP/IP, os roteadores são chamados de *gateways*. Esta definição, em nosso ponto de vista, não é adequada.

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.

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 sistema 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.

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 7.13 mostra dois sistemas autônomos e um exemplo de ligação dos ambientes.

NOTA

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*).

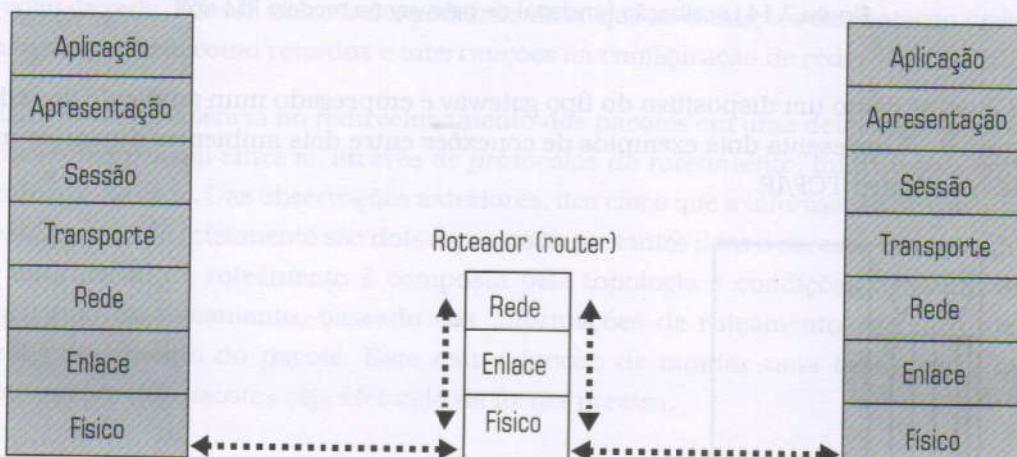


Figura 7.13 Exemplos de ambientes com os protocolos IGP e EGP.

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 arquitetura de redes existente 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 7.14 apresentamos a localização funcional de um *gateway* considerando o modelo RM-OSI.

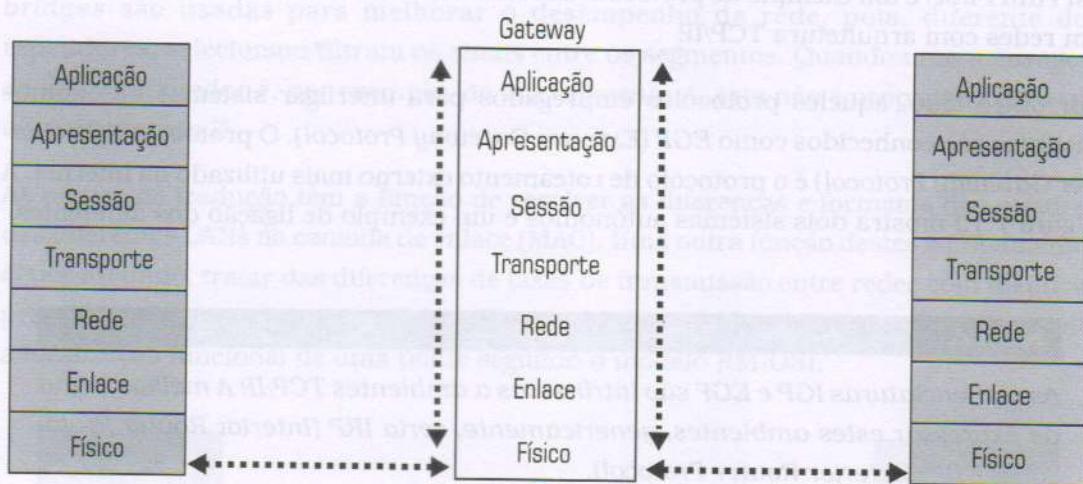


Figura 7.14 Localização funcional de gateway no modelo RM-OSI.

Para ilustrar como um dispositivo do tipo *gateway* é empregado num ambiente de rede, a Figura 7.15 apresenta dois exemplos de conexões entre dois ambientes distintos, um IBM/SNA e outro TCP/IP.

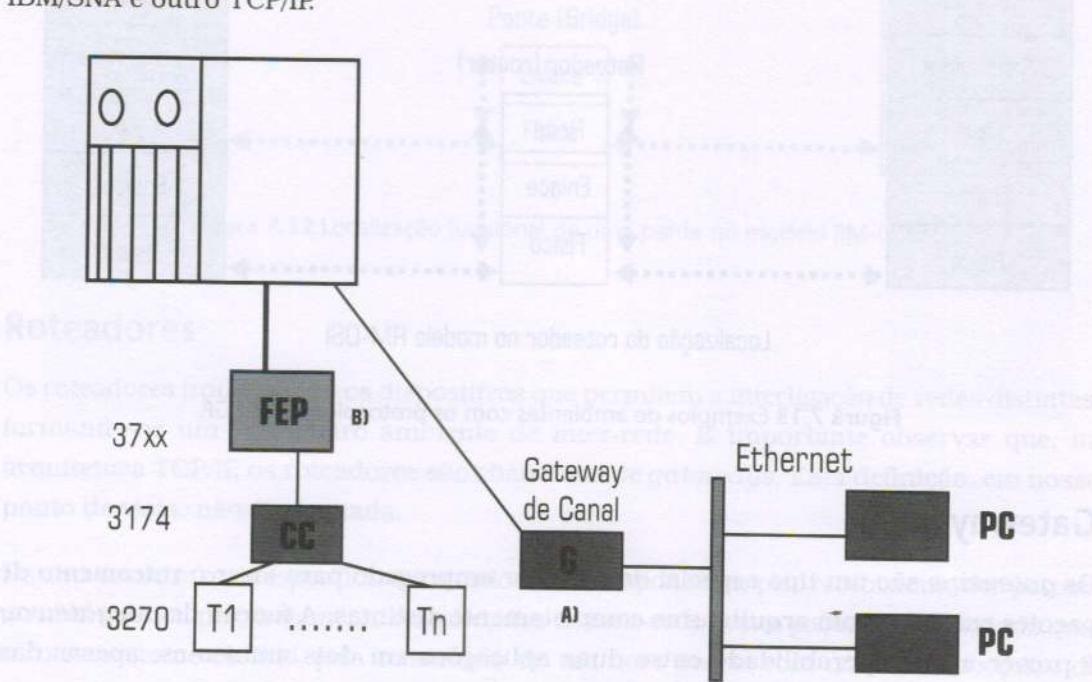


Figura 7.15 Uso de um gateway entre um ambiente IBM/SNA e um TCP/IP.

A Figura 7.15 (a) representa o uso de um dispositivo gateway de um fabricante não-IBM, provendo a interoperabilidade entre aplicações dos dois ambientes de rede. Na Figura 7.15 (b), o gateway é representado pelo dispositivo IBM FEP (Front-End Processor).

Protocolos de Roteamento

O roteador em uma rede geograficamente distribuída é um dos principais dispositivos do sucesso do ambiente. Esses equipamentos são responsáveis pelo recebimento e redirecionamento dos pacotes na rede. A decisão de redirecionamento é usualmente baseada na topologia e nas condições de contorno do ambiente.

Quanto ao aspecto de topologia, um fato que devemos observar é que diferentes ambientes de rede têm complexidade diferenciada. Em outras palavras, podemos imaginar, como exemplo, configurações de rede como um sistema autônomo com poucos computadores e apenas uma subrede, com milhares de computadores e inúmeras sub-redes (ou até centena de milhares de computadores e milhares de sub-redes) e ainda o próprio *backbone* da Internet.

Com relação às condições de contorno, vale lembrar que uma rede pode, em dado momento, ter um ou mais enlaces fora do ar ou apresentar um congestionamento em um determinado trecho da rede. Por um outro lado, podemos dizer que as condições de contorno provêm informações tais como retardos e interrupções na configuração de rede.

Visando uma eficiência no redirecionamento dos pacotes em uma determinada rede, os roteadores trocam entre si, através de *protocolos de roteamento*, informações sobre o ambiente de rede. Das observações anteriores, fica claro que a informação de roteamento e o algoritmo de roteamento são dois aspectos importantes para o sucesso dos roteadores. A informação de roteamento é composta pela topologia e condições de contorno. O algoritmo de roteamento, baseado nas informações de roteamento, efetua o melhor redirecionamento do pacote. Este tem a função de montar uma tabela para que o roteamento dos pacotes seja efetuado de forma precisa.

Os protocolos de roteamento são as rotinas de elaboração de mapas ou tabelas pelos quais os roteadores descobrem o formato da rede. Um ponto fundamental é sabermos como é efetuada a distribuição de informação de roteamento numa rede. Desta forma, a seguir, vamos estudar alguns protocolos de roteamento que adotam diferentes abordagens para roteamento.

De maneira geral, os protocolos de roteamento são classificados como não-adaptativos e adaptativos, onde os protocolos não-adaptativos não consideram em suas decisões medidas (ou estimativas) de tráfego e a topologia da rede. Por este motivo, são protocolos ditos estáticos. Em contraste, os protocolos adaptativos baseiam suas decisões como um reflexo da carga da rede e de uma possível troca da topologia da rede.

As tabelas de roteamento geralmente são classificadas em tabelas estáticas e dinâmicas. No tipo de abordagem conhecido como *rotas diretas e estáticas*, todas as informações da tabela de roteamento são inseridas de maneira direta, e não existe mudança de informação. Arquiteturas de protocolos, tais como SNA/IBM e X-25/ITU-T, são exemplos reais de ambientes onde podemos empregar a técnica de roteamento direto e estático. Todavia, vale lembrar que com o aumento das redes, em termos de conexões entre redes, as tabelas de roteamento tendem a crescer. O aumento das tabelas de roteamento torna o trabalho tedioso e mais propenso a erros.

Um tipo intermediário de abordagem que podemos adotar para a construção das tabelas de roteamento é conhecido como *roteamento default*. O objetivo desse paradigma é o estabelecimento de um determinado número mínimo de rotas de maneira direta e que os demais caminhos são atribuídos a um roteador default.

Em um ambiente de rede, é possível que as interligações entre roteadores sejam efetuadas de maneira contínua. Desta forma, é interessante que a tabela de roteamento seja montada e atualizada constantemente. Nessa abordagem, é necessário que, de forma dinâmica, os roteadores anunciem entre si suas ligações, através de protocolos de comunicação roteador-roteador. De forma geral, é desta maneira que um protocolo de roteamento tradicional opera. Protocolos que utilizam esta abordagem são chamados de protocolos de *roteamento dinâmico*. Na implementação dos protocolos que utilizam a abordagem de roteamento dinâmico, alguns parâmetros são essenciais para o estabelecimento do procedimento de roteamento:

- Conectividade: o protocolo deve saber se existe uma ligação direta entre os dois segmentos ou quantos pulos (*hops*) são necessários para o acesso à rede remota.
- Custo: qual é o menor custo entre os diversos caminhos (*paths*) existentes para interligar duas redes.

NOTA

Não se esqueça que nós podemos dispor de uma visão global de rede. Os roteadores, que não dispõem de uma visão, necessitam de alguns procedimentos para atingir maior conhecimento da configuração.

Exemplos de funcionamento de alguns dos protocolos de roteamento mais conhecidos são:

- *Shortest Path*: o conceito empregado neste tipo de algoritmo é a construção de um grafo da subrede. Cada ponto do grafo representa um roteador, e cada linha um meio de comunicação. Para achar uma rota entre dois roteadores quaisquer, o algoritmo acha a rota com menor distância (shortest path). Diversas métricas são empregadas neste tipo de protocolo, tais como o número de roteadores pulados na rede (*hops*) e a distância. Vale lembrar que protocolos baseados nesta abordagem são estáticos.

- *Flooding*: este tipo de protocolo estático é baseado na técnica de que cada pacote que chega será enviado para todas as interfaces do roteador, exceto aquela pela qual o pacote chegou. A conclusão mais obvia é que este tipo de abordagem provoca uma *inundação* de pacotes. Os protocolos baseados em *flooding*, embora não pareçam práticos, são utilizados onde uma solução robusta é necessária. Exemplos dessa utilização são: (1), o caso de redes militares, onde todos roteadores devem ser notificados para uma dada aplicação; (2), em banco de dados distribuídos, onde muitas vezes todas as bases devem ser atualizadas. Existem procedimentos chamados de represadores, que ajudam a melhorar o desempenho destes tipos de algoritmos. Dentre estas técnicas temos:
 1. Contadores de hops – fazem o decremento a cada pulo (hop).
 2. Reconhecimento de pacotes flooding – estes não serão reenviados.
 3. Flooding seletivo – só é feito um broadcast numa determinada direção.
- *Flow-Based* (baseado em fluxo): neste método estático, a carga de ligação entre dois pontos quaisquer e a topologia são levados em consideração. As métricas (carga e topologia) são conhecidas previamente para a consideração do roteamento nos protocolos baseados nesta abordagem.
- *Distance Vector* (vetor de distância): a maioria das redes modernas emprega algoritmos de roteamento dinâmico. O algoritmo conhecido por *distance vector* é um dos dois mais utilizados. A concepção deste protocolo é manter sua tabela (ou vetor) com as melhores distâncias para cada destino através de uma específica linha. O vetor é mantido atualizado através do processo dinâmico de troca de informação com seus roteadores vizinhos. Algumas informações do vetor são, por exemplo, o número de hops, o tempo de retardo em milisegundos e o número total de pacotes enfileirados ao longo do path (caminho).
- *Link State*: este protocolo com abordagem dinâmica é um dos dois mais populares algoritmos empregados em redes modernas. O link state substituiu o protocolo vector distance na rede ARPANET. Dentre as razões, a métrica de distância não leva em consideração a largura de banda das linhas, e o conceito de vetor demora muito na convergência. São cinco os pontos nos quais este protocolo se baseia:
 1. Descobrir seus vizinhos e seus endereços de rede.
 2. Calcular o retardo ou custo para cada um de seus vizinhos.
 3. Construir um pacote contanto tudo o que este aprendeu.
 4. Propagar o pacote conhecedor de todas as informações para todos os roteadores.
 5. Computar o menor caminho para todos os outros roteadores.

Os protocolos de roteamento podem efetuar a troca de informação entre os roteadores, empregando as seguintes abordagens:

- *Hierarchical Routing*: não é possível que, com o crescimento exponencial de uma rede, os protocolos até então apresentados possam atender plenamente a função de roteamento com sucesso. No roteamento conhecido por hierarchical, temos o roteamento em áreas chamadas de regiões. Cada roteador somente conhece sua região. Para grandes redes são necessárias algumas subdivisões para que os roteadores trabalhem com eficiência, tais como cluster de regiões, zonas de clusters, grupos de zonas e assim por diante.
- *Broadcast*: numa abordagem do tipo difusão, enviam-se pacotes para todos os roteadores simultaneamente. Aplicações como previsão do tempo e bolsa de valores são típicos exemplos onde devemos ter uma rede que possa absorver informações desta maneira. Vários protocolos podem implementar o broadcasting, exemplos de algoritmos são:
 1. algoritmo de broadcast simples
 2. algoritmo de flooding
 3. algoritmo de multidestinos
- *Multicast*: a idéia de enviar pacotes para um grupo seletivo de roteadores é chamado de multicasting, e os protocolos que implementam este tipo de roteamento são denominados de algoritmos multicast. Nesta abordagem, é necessário que a figura de gerência de grupo exista. Portanto, a necessidade de criação/destruição de grupos junto com a requisição de processos, que requerem sua junção/disjunção a um determinado grupo, são exemplos de tarefas a serem efetuadas pelo protocolo de multicast.

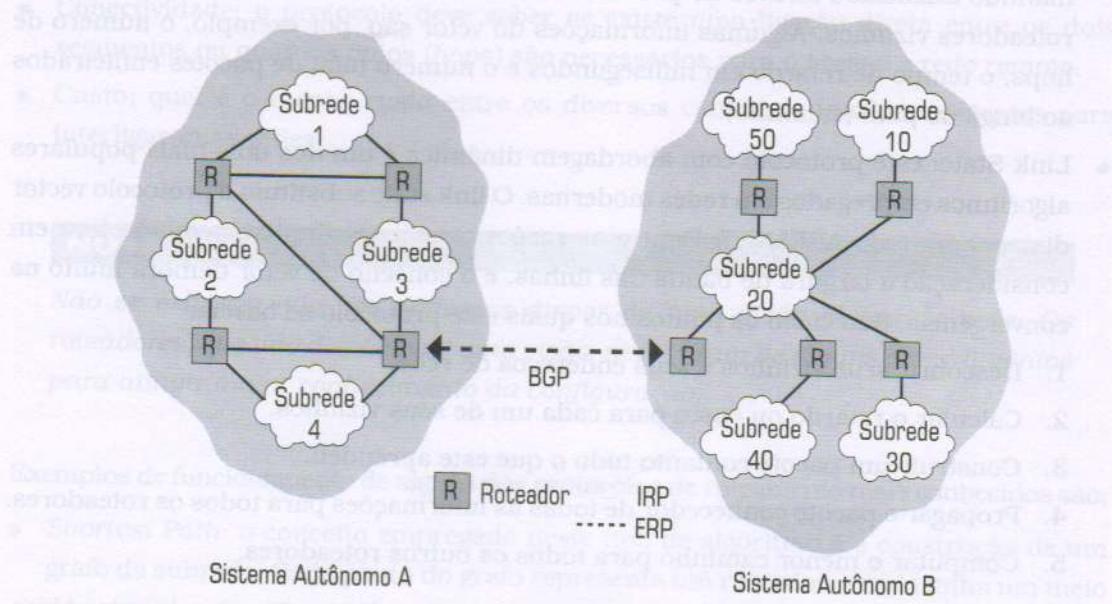


Figura 7.16 Sistema Autônomos, ERP e IRP.

Finalizando, na Figura 7.16, ilustramos o conceito de sistemas autônomos, ERP (Exterior Router Protocol) e IRP (Interior Router Protocol). Nessa figura, apresentamos dois sistemas autônomos cujo roteamento interno é efetuado pelo protocolo OSPF. A ligação entre os sistemas autônomos é realizada, por exemplo, pelo protocolo BGP.

Exercícios

- 1) Diferencie uma rede local e uma rede metropolitana.
- 2) Faça um esboço para apresentar um ambiente DQDB.
- 3) Faça um esboço e comente as diferenças entre um ambiente FDDI convencional e outro que apresentou um problema.
- 4) Explique as diferenças das estações do tipo SAS e do tipo DAS.
- 5) Qual a função de uma interface do tipo M numa configuração FDDI?
- 6) Comente o paradigma de self-healing de uma configuração FDDI.
- 7) Quais as principais características do ambiente Fibre Channel?
- 8) Quais as camadas do modelo de referência do Fibre Channel?
- 9) Explique o significado do HIPPI e do SCSI no modelo do Fibre Channel.
- 10) Diferencie uma rede metropolitana e uma rede geograficamente distribuída.
- 11) Enumere as principais característica do ATM.
- 12) Qual a diferença entre CoS e QoS?
- 13) Comente sobre as políticas de admissão e policiamento num ambiente que tem QoS.
- 14) Apresente o modelo de referência do ATM.
- 15) Descreva as AALs.
- 16) Faça um esboço de uma célula ATM descrevendo seus campos.
- 17) Qual a função de um repetidor numa rede com mídia compartilhada?
- 18) Descreva a função de uma ponte convencional e de uma ponte de tradução.
- 19) Qual a função de um roteador numa rede?
- 20) Defina com suas palavras um sistema autônomo.
- 21) Explique a diferença de abordagem de um protocolo IRP e outro ERP.

Referências

As referências Comer (2001), Freedman (1999), Halsall (1996), Soares (1995), Stalling (1997,1999) e Tanenbaum (1996) são recomendações clássicas de mais leitura sobre o assunto. Por outro lado, é interessante o leitor observar as referências ATM (2001), Enck (1995), Held (1998,1999) e Stalling (2000).

Bibliografia

- ATM Forum. <http://www.atmforum.org>, 2001.
- COMER, D. E. *Computer Networks and Internet*, 3rd ed. Prentice Hall, 2001.
- ENCK, J., BECKMAM, M., *LAN to WAN Interconnection*. McGraw-Hill, 1995.
- FREEDMAN, R., *Fundamentals of Telecommunications*. Wiley, 1999.
- HALSALL, F., *Data Communications, Computer Networks and Open Systems*, 4th ed. Addison Wesley, 1996.
- HELD, G., *Internetworking LANs and WANs*. John Wiley, 1998.
- _____, *Understanding Data Communications* – 6th ed. New Riders Publishing, 1999.
- SOARES, L.F. *Redes de Computadores – Das LANs, MANs e WANs às Redes ATM*. 2 ed. Campus, 1995.
- STALLING, W., *Local and Metropolitan Area Networks*, 6th ed. Prentice Hall, 1999.
- _____, *Business Data Communications*, 4th ed. Prentice Hall, 2000.
- _____, *Data and Computer Communications*, 5th ed. Prentice Hall, 1997.
- TANENBAUM, A.S. *Computer Networks*, 3rd ed. Prentice Hall, 1996.