Comunicação de Dados I
Introdução à Comunicação de Dados e Tecnologias de Comutação

Eleri Cardozo
Mauricio F. Magalhães

Departamento de Engenharia de Computação
e Automação Industrial
Faculdade de Engenharia Elétrica e de Computação
Universidade Estadual de Campinas

1998

Conteúdo

Capítulo 1

Introdução

Os últimos anos têm sido caracterizados por um desenvolvimento tecnológico importante em várias áreas do conhecimento. Duas destas áreas são a computação e as telecomunicações. Estas áreas eram separadas há alguns anos atrás mas a introdução na infra-estrura das redes de comunicações de dispositivos computacionais, e a tendência de digitalização das redes, têm impulsionado a convergência destas duas áreas. Esta tendência é tão forte que, na realidade, a rede está se tornando um grande computador abrindo perspectivas para novos serviços que irão afetar cada vez mais a forma de organização da sociedade. É possível afirmar que atualmente não existem diferenças fundamentais entre o processamento de dados e a comunicação de dados e a tendência é de que, no futuro, não existirão diferenças na comunicação de dados, voz e vídeo, da mesma forma que estão desaparecendo as barreiras entre as estruturas mono-processadas, multi-processadas, redes locais, redes metropolitanas e redes de longa distância.

Estas tendências têm como consequências práticas uma convergência das indústrias das comunicações e da computação, do desenvolvimento de uma infra-estrutura única capaz de transportar todo tipo de informação e, por último, mas talvez mais importante, a perspectiva de alterações fundamentais na forma de organização da sociedade e no acesso às informações. Neste primeiro módulo do Programa de Treinamento para a Ericsson do Brasil estaremos discutindo os aspectos básicos das redes de computadores. Os módulos seguintes abordarão as novas tecnologias nas áreas da Comunicação de Dados e da Engenharia de Software neste novo contexto representado pelas novas aplicações distribuídas executando em redes de alto desempenho.

1.1 Modelo de Comunicação

Podemos ilustrar uma rede de comunicação através do modelo apresentado na figura 1.1.

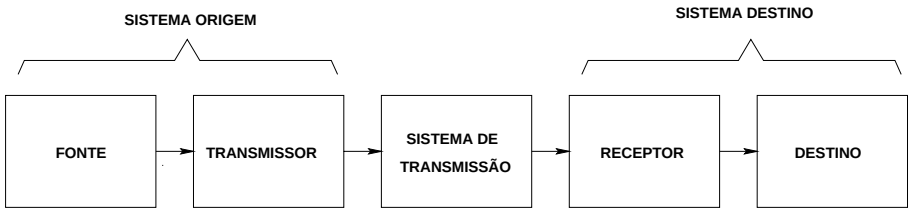


Figura 1.1: Modelo de Comunicação

Instâncias deste modelo podem ser ilustradas pelos sistemas da figura 1.2.

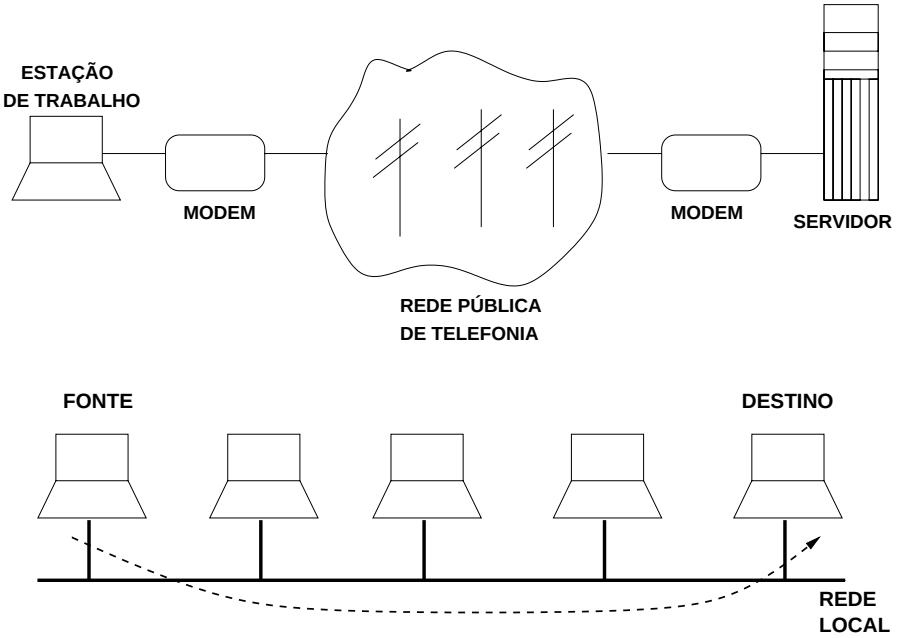


Figura 1.2: Instâncias do Modelo de Comunicação

No caso do modelo de comunicação, a fonte e o destino são representados pelos dispositivos que geram e consomem os dados transmitidos; o transmissor codifica a informação gerada pela fonte de modo que ela seja adequadamente propagada pelo sistema de transmissão utilizado. Este último pode ser caracterizado por uma infra-estrutura complexa formada por dispositivos de comutação e transmissão como no caso das redes públicas,

ou por uma estrutura simples como um comutador (switch) interconectando vários computadores em um ambiente local. Por último, o receptor transforma o sinal recebido do sistema de transmissão e converte-o de forma a ser adequadamente interpretado pelo destino.

Algumas das principais funções realizadas em um sistema aderente ao modelo de comunicação apresentado são: utilização eficiente do sistema de transmissão, interfaceamento dos dispositivos com o sistema de transmissão, geração do sinal, sincronização entre transmissor e receptor, gerenciamento dos serviços e da rede, deteção e correção de erro, controle de fluxo, endereçamento e roteamento, recuperação de falhas, formatação de mensagens, segurança, etc.

A forma mais simples associada ao modelo de comunicação discutido anteriormente seria representada pela conexão ponto a ponto dos dispositivos. Neste caso, o sistema de transmissão seria representado pelo enlace físico conectando a origem e o destino da informação. Entretanto, à medida que os dispositivos tornam-se cada vez mais remotos e que novos dispositivos (computadores) são introduzidos no sistema, torna-se inviável a utilização de enlaces físicos ponto a ponto interconectando todos os dispositivos. A forma de se contornar o problema é conectá-los à uma rede de comunicação. Dependendo da abrangência geográfica coberta pela rede é possível classificá-la em dois grandes grupos: redes de longa distância e redes locais. De um modo geral, as redes de longa distância são constituídas pela interconexão de nós de comutação e a informação transmitida pelo dispositivo fonte é roteada pela rede até alcançar o dispositivo destino especificado. O objetivo principal dos nós de comutação é fazer a informação (mensagem) alcançar o seu destino sem, no entanto, analisar o conteúdo da informação transportada. As tecnologias básicas utilizadas na implementação das redes de longa distância traduzem-se na comutação de circuitos e na comutação de pacotes. Na primeira, é estabelecido um caminho dedicado (circuito), através dos nós da rede, entre os nós origem e destino da informação. Este caminho é formado pela concatenação de vários enlaces físicos entre nós de comutação internos à rede. A informação transmitida pelo nó origem é enviada através do caminho dedicado sendo comutada de forma adequada pelos nós de comutação até alcançar o destino. A rede típica baseada na comutação de circuito é a rede telefônica. A outra forma de comutação utilizada nas redes de longa distância é a comutação de pacotes. Neste caso não existe, nas redes baseadas em datagramas, a alocação de um caminho dedicado para transmissão das informações entre a origem e o destino através da rede. A informação a ser transmitida é quebrada em unidades menores, denominadas de pacotes, e enviadas sequencialmente e de forma independente. Cada pacote é transmitido de nó em nó, ao longo do caminho, até alcançar o destino. Em cada nó da rede o pacote é recebido, armazenado e transmitido para o próximo nó. Este tipo de comutação é a tecnologia básica da comunicação computador-computador. A rede típica baseada no conceito de datagrama é a rede postal.

No caso das redes locais temos, da mesma forma que nas redes de longa distância, vários dispositivos interconectados para a troca de informação. Entretanto, diferentemente das redes WANs (*Wide Area Networks*), as LANs (*Local Area Networks*) cobrem distâncias pequenas, normalmente restritas a um prédio. As LANs tradicionais são baseadas em difusão (*broadcast*) onde os dispositivos conectados à rede compartilham o meio de comunicação levando à necessidade de mecanismos para viabilizar um acesso controlado à rede e evitar a degradação da informação caso mais de um dispositivo acesse a rede simultaneamente. Na realidade, as redes locais têm sofrido, nos últimos anos, uma mudança importante na sua estrutura através da introdução das redes locais comutadas. Neste caso, os meios de comunicação que antes eram compartilhados entre as várias estações ligadas à rede, estão sendo substituídos por comutadores de LANs permitindo alocar a uma única estação a capacidade que anteriormente era disputada por dezenas de estações conectadas ao meio.

1.2 Conceitos e Terminologia

Antes de iniciarmos o estudo das redes de comunicação, introduziremos alguns conceitos e terminologia associados aos sistemas abertos de comunicação.

1.2.1 Estruturação de Redes

É possível imaginar que a comunicação entre computadores envolve um contexto bem mais amplo do que aquele discutido até o momento e sintetizado no modelo de comunicações discutido nos itens anteriores. Além de um caminho de dados entre os computadores, seja diretamente ou através de uma rede para transporte da informação, uma série de outros requisitos são necessários: 1) o sistema origem da informação deve indicar à rede a identificação do destino e certificar-se que o destino está preparado, ou tem interesse, em receber os dados; 2) o formato da informação enviada pode ser incompatível com o formato da informação operada pelo destino levando à necessidade de uma translação de formato; 3) em geral, o envio da informação por parte da origem provoca uma reação do lado do destino, implicando em um relacionamento, ou diálogo, entre a origem e o destino. Este diálogo relaciona-se à semântica da aplicação, ou seja, um nível acima das questões associadas ao transporte dos dados pela rede e que se desenrola basicamente nos sistemas fins da informação, isto é, origem e destino. Estas questões envolvendo a cooperação entre os sistemas comunicantes e o transporte da informação pela rede são associadas a 2 questões básicas: protocolos e a arquitetura de protocolos. Podemos definir um protocolo de comunicação como um conjunto de regras que organizam o diálogo entre entidades em

sistemas diferentes. Podemos interpretar o conceito de entidade como sendo algo capaz de enviar e/ou receber informações. Uma entidade pode ser um componente de software (um processo, por exemplo) ou de hardware (uma interface de rede, por exemplo).

Entidades são organizadas em camadas dispostas verticalmente. As entidades na camada-(N) implementam serviços usados pela camada-$(N+1)$. Neste contexto, a camada-(N) é denominada *provedora de serviços* enquanto a camada-$(N+1)$ é dita *usuária de serviços*.

Serviços são disponíveis nos SAPs (Service Access Points). A camada-$(N+1)$ acessa os serviços oferecidos pela camada-(N) nos SAPs desta camada. Cada SAP possui um endereço que o identifica única e globalmente e oferece um conjunto de primitivas a partir das quais os serviços são requisitados.

A figura 1.3 ilustra os conceitos de protocolo, entidade, camada e SAP.

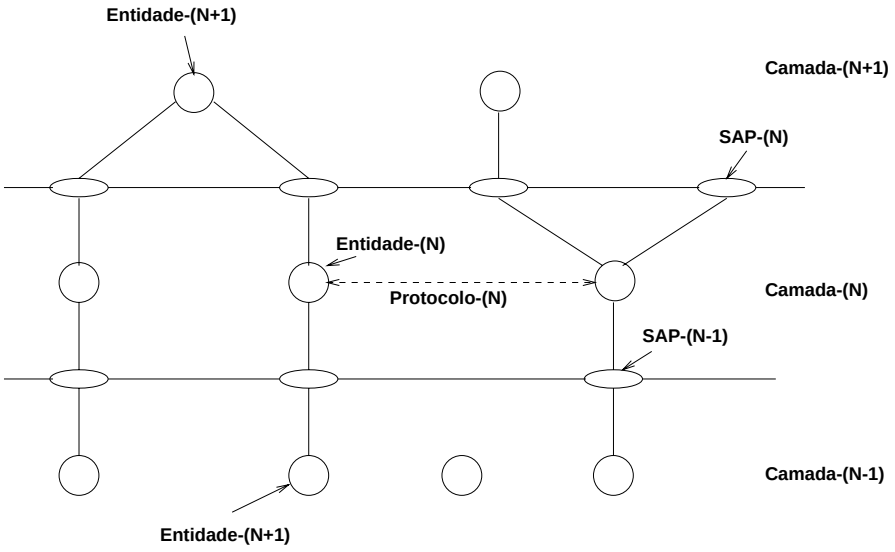


Figura 1.3: Relacionamento entre entidades, camadas, SAPs e protocolos.

Considere uma rede de cinco camadas como mostra a figura 1.4. Suponha que uma mensagem é gerada por um processo em um nó e direcionada para um segundo processo num outro nó. Vamos seguir esta mensagem pela rede da figura 1.4. Para processos do usuário, o ponto de entrada na rede é a camada 5. Nesta camada a mensagem é codificada num formato comum e encaminhada à camada 4. Nesta camada a informação é particionada em unidades menores, sendo a cada unidade adicionado um cabeçalho contendo informações de controle, tais como número de sequência e se a unidade é a última da sequência ou não. As unidades geradas na camada 4 são, uma a uma, conduzidas à

camada 3.

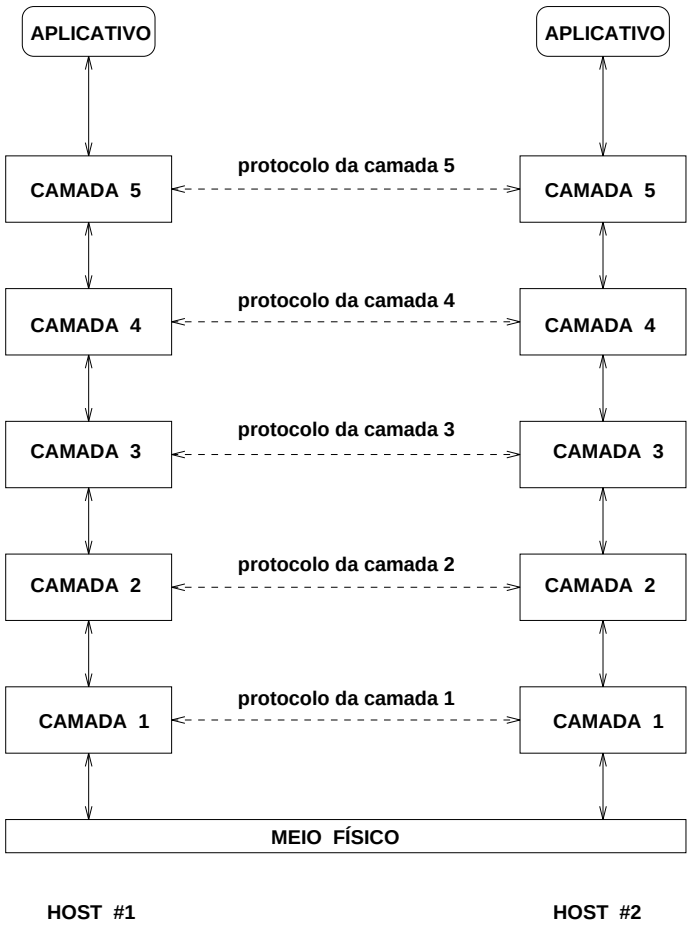


Figura 1.4: Camadas, protocolos e interfaces numa rede de computadores.

A camada 3 decide o caminho que as unidades irão percorrer (roteamento). Informações tais como identificação dos nó emissor e receptor são contidas num outro cabeçalho adicionado pela camada 3. Na camada 2 é computado um código para fins de detecção de erros (*checksum*). Esta camada adiciona tanto um novo cabeçalho quanto um rótulo demarcador de final nas unidades oriundas da camada 3. A camada 2 envia suas unidades para a camada 1, armazenando-as caso o protocolo desta camada exija confirmação de recepção. Na camada 1 serão gerados os sinais elétricos (ou óticos, ou eletromagnéticos, dependendo do meio físico de transmissão) que farão as unidades atingirem o nó receptor.

Ao receber (na camada 1) as unidades transmitidas, o nó receptor propaga-as para as camadas superiores, até atingir a camada 5, quando o processo receptor será notificado. No caminho inverso, as unidades são remontadas de acordo com as informações contidas

nos cabeçalhos: a mensagem atinge o processo receptor com o mesmo conteúdo semântico daquela gerada pelo processo emissor.

1.2.2 Serviços e Primitivas

Vimos anteriormente que SAPs disponibilizam serviços à camada superior. Estes serviços podem ser de natureza conectada ou sem conexão. Serviços conectados são análogos a um serviço telefônico. Estabelece-se uma conexão (discagem/atendimento), utiliza-se a conexão para troca de informações (conversação) e termina-se a conexão (volta ao gancho). Serviços conectados estabelecem um canal lógico (conexão) entre as entidades comunicantes. Neste canal, a ordem temporal no envio da informação é respeitada e duplicações são inexistentes. O canal é dito *lógico* ou *virtual* pelo fato de não dispor de uma conexão física exclusiva, ao contrário, múltiplos canais lógicos compartilham uma mesma conexão física. Serviços conectados se dividem em dois tipos: mensagens e cadeias de bytes (*streams*). Mensagens têm suas fronteiras delimitadas, o que não ocorre com as cadeias de bytes. Serviços típicos que demandam conexão são transferência de arquivos e *login* remoto.

Serviços sem conexão são análogos a serviços postais. Envia-se uma mensagem a um destinatário (carta ou telegrama) e faz-se votos que ele a receba. Serviços sem conexão são denominados *serviços de datagrama*, sendo mais rápidos que os serviços conectados, mas a garantia de entrega, ausência de duplicação e preservação da ordem de envio não são garantidas. Serviços típicos que podem ser baseados em datagrama são os do tipo requisição/resposta (acesso a banco de dados e sincronização de relógios, por exemplo).

A definição dos serviços suportados por uma determinada camada-(N) é caracterizada pelo conjunto de primitivas e os respectivos parâmetros que podem ser evocadas pelo usuário do serviço (entidade-$(N+1)$) e pelo provedor do serviço (entidade-(N)) através de um SAP-(N). A interação entre a entidade-$(N+1)$ e a entidade-(N) através das primitivas de serviço definidas involve a passagem de informações de controle ou de dados, ou ambos.

No modelo OSI (Open System Interconnection) da ISO (International Organization for Standardization), as primitivas para a requisição de serviços são divididas em quatro tipos (figura 1.5).

Vamos tomar o exemplo do estabelecimento de uma conexão entre duas entidades. A entidade que deseja se conectar executa a primitiva *CONNECT.request* (na notação OSI), passando como parâmetro o endereço da segunda entidade. A entidade endereçada

Primitiva	**Significado**
Requisição	Uma entidade requer a execução de um serviço
Indicação	Uma entidade é informada da ocorrência de um evento
Resposta	Uma entidade deseja responder a um evento
Confirmação	Uma entidade é informada sobre o resultado de sua requisição

Figura 1.5: Tipos de serviços no modelo OSI.

recebe um *CONNECT.indication* avisando que uma conexão está sendo requisitada. Como resposta, executa um *CONNECT.response* indicando se aceita ou rejeita a conexão. A entidade que requisitou está bloqueada num *CONNECT.confirm*, que volta exatamente o resultado do *CONNECT.response* emitido pela outra entidade.

Serviços envolvendo duas partes podem conter *negociação*. Por exemplo, uma conexão pode especificar certa taxa mínima de transferência de dados, máximo tamanho das mensagens, etc. Neste caso, a negociação deve fazer parte do protocolo que regulamenta o serviço.

Serviços podem ser *confirmados* ou *sem confirmação*. Serviços confirmados necessitam das quatro primitivas básicas (requisição, indicação, resposta e confirmação). Serviços sem confirmação necessitam apenas das primitivas do tipo requisição e indicação. Exemplo: serviço de desconexão. A figura 1.6 ilustra estes conceitos.

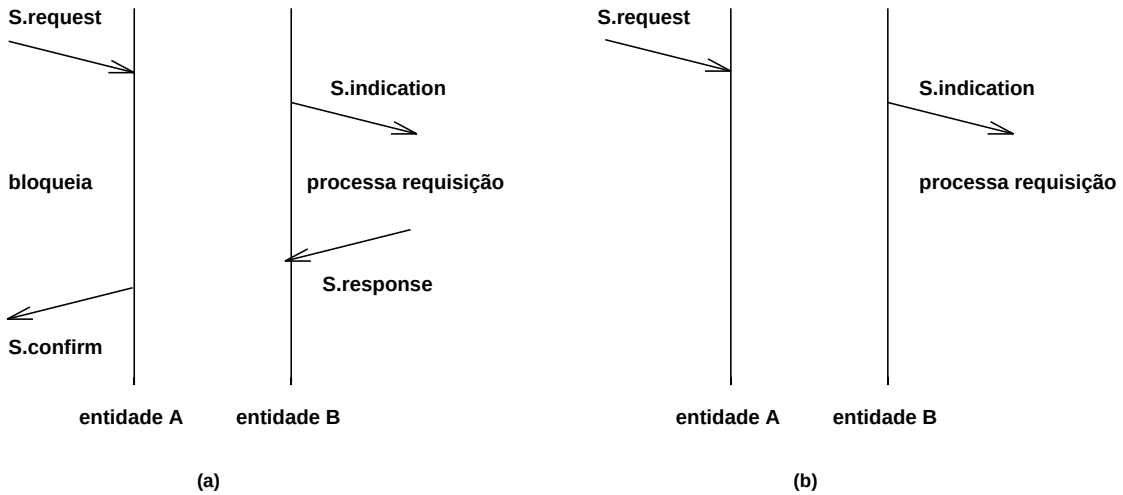


Figura 1.6: Serviços OSI confirmados (a) e sem confirmação (b).

1.2.3 Especificação de Protocolos

Um dos problemas fundamentais abordado na especificação de um sistema de comunicação aberto diz respeito ao protocolo envolvendo entidades pares. O conceito clássico de protocolo define a forma como entidades equivalentes interagem entre si para a realização de um objetivo comum para a prestação de serviços a entidades na camada superior. Desta forma, 2 entidades-$(N+1)$ que desejam se comunicar devem utilizar os serviços de comunicação suportadas pela camada-(N), com exceção da camada física para acesso ao meio físico diretamente.

Para suportarem os serviços de comunicação requisitados no SAP-(N) pelas entidades-$(N+1)$, as entidades-(N) devem se comunicar através de serviços da camada-$(N-1)$. Neste caso, a comunicação entre entidades pares é regida por um conjunto de regras e formatos que as entidades devem seguir para suportar os serviços. Este conjunto de regras e formatos representando por aspectos semânticos, sintáticos e temporais é denominado de protocolo da camada-(N).

A especificação de um protocolo relativamente a uma camada compreende:

- descrição dos tipos de mensagens permitidas pelo protocolo, denominadas *unidades de dado de protocolo*, ou PDUs (Protocol Data Units);
- descrição dos procedimentos do protocolo e os serviços evocados para transferência de cada tipo de PDU;
- definição formal da estrutura de cada tipo de PDU;
- definição formal da operação da entidade de protocolo.

PDUs são formadas por uma parte correspondente aos dados do usuário e outra parte contendo as informações de controle relativa ao protocolo (PCI: Protocol Control Information). Do ponto de vista de uma camada-(N), uma PDU gerada pela camada-$(N+1)$ é vista como uma unidade de dado à ser encapsulada por um protocolo da camada-(N). Esta unidade de dado é denominada *unidade de serviço de dado* (SDU: Service Data Unit). A figura 1.7 ilustra a relação entre PDU, PCI e SDU. Genericamente, uma camada recebe uma SDU da camada superior (contendo uma PDU desta camada) adiciona um PCI (cabeçalho) à esta SDU para formar uma PDU desta camada. Este processo é recursivo.

Como a PDU é uma informação que será trocada entre sistemas diferentes, é necessário que a PDU possua uma estrutura cujo significado seja comum às entidades de ambos os

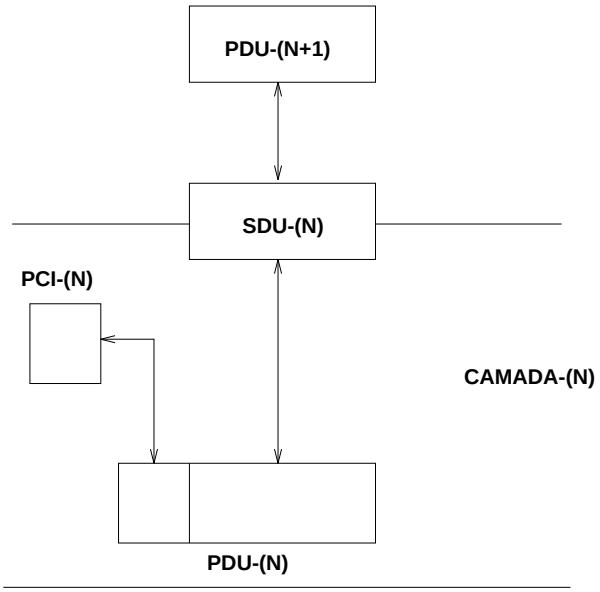


Figura 1.7: Relação entre PDU, PCI e SDU.

sistemas. Isto é obtido nos documentos de padronização através da utilização de cadeias de bits ou através de uma forma baseada em tipos abstratos de dados (*Abstract Syntax Notation Number One ou ASN.1*) acompanhada de regras de codificação.

A representação baseada em cadeia de bits é mais utilizada na especificação dos protocolos das camadas inferiores. A representação utilizando o ASN.1 é mais comum na especificação de PDUs dos protocolos de nível mais alto, isto é, dos protocolos orientados à aplicação. ASN.1 é baseada na tipificação dos dados como encontrado na maioria das linguagens de programação. Como ASN.1 é uma sintaxe abstrata, isto significa que nada é especificado com relação ao número e ordem dos bits correspondentes a cada tipo de dado encontrado na especificação. Neste caso, utiliza-se um conjunto de regras de codificação que irá gerar PDUs formadas de cadeias de bytes, cadeias estas que serão interpretadas da mesma forma em todos os sistemas.

Uma entidade de protocolo é modelada na forma de uma máquina de estados finitos (autômato). Isto significa que uma entidade de protocolo deve encontrar-se em um único estado de cada vez dentre um conjunto finito de estados possíveis.

A transição de um estado para outro acontece quando um evento válido ocorre na interface do autômato. Alguns exemplos de eventos são os seguintes:

- recepção de uma primitiva de serviço na interface com a camada superior;
- recepção de uma primitiva na interface com a camada inferior;
- ocorrência de eventos locais.

Em geral, associado à ocorrência de um evento válido, o autômato muda de estado e gera alguma ação interna específica como, por exemplo, o disparo de um relógio ou a evocação de uma primitiva.

1.3 Padronização

Um *padrão* é um conjunto de normas e procedimentos. O cumprimento destas normas e procedimentos pode ser obrigatório (normalmente quando relacionados à segurança do homem) ou recomendável (normalmente quando relacionados à qualidade de produtos e serviços). Padrões visam homogeneizar produtos e serviços num nível aceitável de qualidade e segurança, minimizar investimentos em estoques, compatibilizar equipamentos de diferentes procedências, etc.

Um padrão é dito *de facto* quando foi adotado sem nenhuma ação de entidade reguladora. Exemplo: IBM-PC. Por outro lado, padrões *de jure* são produzidos por entidades reguladoras, nacionais ou internacionais, governamentais ou não. Exemplo: ISO-9000.

Na área de redes de computadores as entidades de padronização estão centradas nos seguintes organismos:

- organismos internacionais (ITU-T, ISO);
- entidades de padronização nacionais/regionais (EIA/TIA, ETSI);
- entidades sem fins lucrativos (ANSI, IEEE, IETF);
- fórum de fabricantes (ATM Fórum, Frame Relay Fórum);
- laboratórios públicos e privados (Bellcore, US Bureau of Standards).

Os organismos internacionais mais importante são o ITU-T (International Telecommunications Union - Telecommunication Standardization), antiga CCITT (Comité Consultatif International de Télégraphique et Téléphonique), que congrega as companhias

de telecomunicações nacionais; e a ISO (International Organization for Standardization), que congrega as entidades de padronização nacionais.

Padrões ITU-T são voltados para serviços públicos de voz e dados e organizados em *séries*. Por exemplo a série I trata das Redes Digitais de Serviços Integrados (RDSI) em faixa estreita (RDSI-FE) e faixa larga (RDSI-FL); a série V de comunicação de dados sobre rede telefônica (padrões de modems, interfaces, etc.); a série X de comunicação de dados e a série M de padrões de gerência e manutenção de redes.

O padrão de rede mais notável é o modelo OSI (Open System Interconnection) da ISO[1]. Resultado de um grande esforço de padronização no início dos anos 80, o modelo OSI vem se mantendo atual, apesar do grande avanço nas tecnologias associadas às redes de computadores. A ISO tem aceito também padrões já estabelecidos por outras entidades (principalmente ANSI, IEEE e ITU-T) como padrões internacionais, simplesmente redigindo-os e catalogando-os de acordo com os seus critérios. Por exemplo, o padrão IEEE 802 para redes locais foi adotado integralmente pela ISO (ISO 8802).

As entidades locais e regionais de padronização, como o JIS (Japanese Industry Standards) e o ETSI (European Telecommunication Standard Institute), produzem ou adaptam padrões levando em contas as peculiariedades regionais.

As entidades de padronização sem fins lucrativos como o IEEE (Institite of Electrical and Electronic Engineers), a ANSI (American National Standard Institute) e o IETF (Internet Engineering Task Force) representam um peso considerável nos esforços de padronização. Por exemplo os padrões 802 do IEEE englobam as tecnologias de LANs e MANs mais utilizadas (Ethernet, Token Ring, DQDB, FDDI). O IETF é a entidade responsável pelos padrões da família TCP/IP, ou padrões Internet[2]. Uma entidade reguladora, a IANA (Internet Assigned Number Authority) é responsável pela atribuição de identificadores no âmbito dos padrões Internet (identificadores de nós de rede, protocolos, serviços, etc). IANA vinha sendo mantida pelo governo norte-americano, mas está em processo de tornar-se uma entidade sem fins lucrativos nos moldes do IEEE.

Na linha de fóruns de fabricantes, o ATM Fórum e o Frame Relay Forum, são organizações estabelecidas com o intuito específico de estabelecer padrões referentes à determinada tecnologia. Finalmente, laboratórios privados vêm assumindo um papel cada vez mais marcante no âmbito dos padrões para redes de computadores. O exemplo mais notório talvez seja o Bellcore, que patrocinou o desenvolvimento de tecnologias como o SONET (Synchronous Optical Network) e o ADSL (Assimetric Digital Subsdcriber Loop).

[1] Os padrões referentes ao modelo OSI fazem parte da série X da ITU-T.

[2] Abreviação de *interconnected networks*.

Capítulo 2

Comunicação de Dados

2.1 Transmissão de Dados

Os dados armazenados nos computadores e transmitidos na infra-estrutura de transmissão são sequências de 0's e 1's. Internamente ao computador os 0's e 1's são representados através da polaridade do sinal elétrico: sinal de nível alto corresponde a 1 e sinal de nível baixo corresponde a 0. A agregação de 0's e 1's permite a representação, segundo um determinado código, de números e caracteres.

A transmissão adequada dos dados depende de 2 aspectos principais: a qualidade do sinal transmitido e as características do meio de transmissão. Em qualquer situação a transmissão do sinal ocorre através de ondas eletromagnéticas em um meio classificado como guiado ou não-guiado. No primeiro caso as ondas são guiadas através de um caminho físico e, no segundo, a onda eletromagnética propaga-se em todas as direções.

2.1.1 Sinais

Como os sinais eletromagnéticos correspondem ao tipo de sinal que será utilizado para a transmissão dos dados é importante conhecer os conceitos básicos associados.

Um sinal eletromagnético pode ser representado em dois domínios: domínio do tempo e domínio da frequência. No domínio do tempo um sinal pode ser visto como contínuo ou discreto. No primeiro caso, a intensidade do sinal varia no tempo sem descontinui-

dades, ou seja, $lim_{t\to\infty} s(t) = s(a)$ para qualquer a. No caso discreto a intensidade do sinal mantem-se constante durante um intervalo de tempo e muda bruscamente para um outro nível constante que irá perdurar por um outro intervalo. A voz, por exemplo, é representada adequadamente por um sinal contínuo enquanto os 0's e 1's do computador são representados por um sinal discreto conforme ilustrado nas figuras 2.1a e 2.1b.

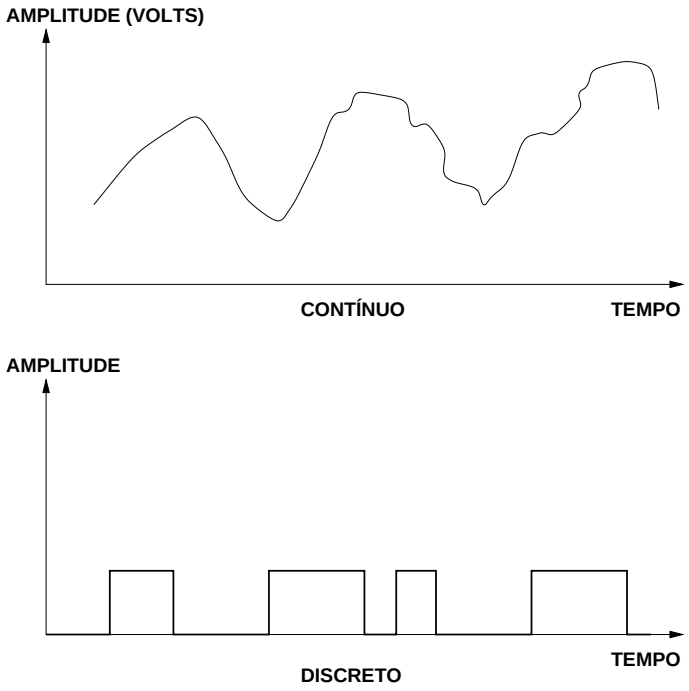


Figura 2.1: Exemplos de Sinais Contínuo e Discreto

Um conceito básico associado aos sinais contínuos e discretos no domínio do tempo é o do sinal periódico. Neste caso temos um padrão que se repete indefinidamente no tempo. Do ponto de vista matemático, um sinal periódico é definido como

$s(t + T) = s(t)$, $-\infty < t < \infty$ onde T corresponde ao período do sinal.

Uma forma de onda oscilante como aquela representada pela função seno pode ser vista como um sinal contínuo básico. Neste caso, o sinal é caracterizado por três parâmetros:

- amplitude(A): corresponde à intensidade do sinal nos instantes de tempo;
- frequência(f): corresponde à taxa de repetição do sinal em ciclos por segundo ou Hz. Associado ao conceito de frequência temos o do período (T) que corresponde ao intervalo de tempo de uma repetição do sinal, ou seja, $T = 1/f$;

- fase(ϕ): representa o ponto que o sinal avançou no seu ciclo.

Podemos representar matematicamente uma função seno no tempo através da expressão $s(t) = A\,sen(2\pi ft + \phi)$. A figura 2.2 ilustra os conceitos anteriores.

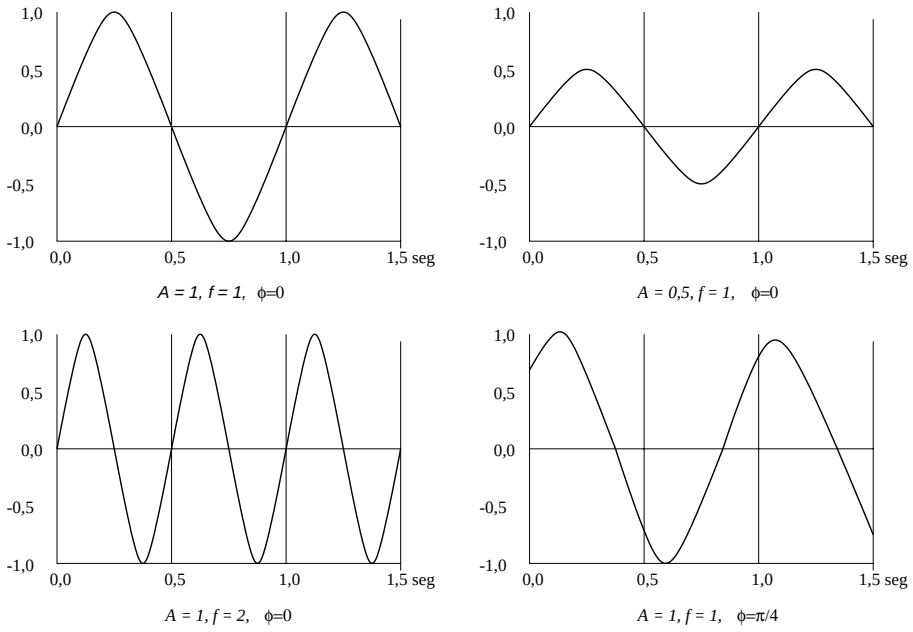


Figura 2.2: $s(t) = A\,sen(2\pi ft + \phi)$

Duas outras relações são ainda importantes do ponto de vista da função seno. O comprimento de onda λ de um sinal corresponde à distância ocupada pelo sinal em um ciclo, ou ainda, à distância entre dois pontos de mesma fase em ciclos consecutivos. A relação do comprimento de onda do sinal e o período através da velocidade v de propagação do sinal é dada por: $\lambda = vT$ ou $v = \lambda f$.

No caso do domínio da frequência, o sinal pode ser visto como constituído de várias frequências. Esta visão é fruto do trabalho do matemático Jean Fourier que provou que qualquer sinal periódico, representado como uma função do tempo $s(t)$, com período T_0, pode ser considerado como uma soma, provavelmente infinita, de senos e cossenos de diversas frequências denominada de série de Fourier.

$$g(t) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n sen(2\pi nft) + \sum_{n=1}^{\infty} b_n cos(2\pi nft)$$

A frequência $f = 1/To$, onde To corresponde ao período do sinal, é denominada de frequência fundamental. Podemos observar que as componentes do sinal são formadas por uma componente dc no caso de $f = 0$, das componentes na frequência fundamental e das componentes em frequências múltiplas da frequência fundamental denominadas de harmônicas. Consequentemente, da mesma forma que vimos que um sinal pode ser representado no tempo onde a função $s(t)$ é definida como uma função do tempo t, o sinal pode ser representado no domínio da frequência onde o sinal é definido em termos das suas componentes. Neste caso denominamos de espectro a apresentação, para cada frequência, das amplitudes an e bn correspondentes.

Na realidade, no caso dos sistemas de transmissão da informação, os sinais não são periódicos. Considerando que os sinais têm uma duração limitada, podemos imaginar que o sinal original corresponde a um ciclo de um sinal periódico criando, desta forma, um sinal periódico a partir do sinal de interesse. Através desta abordagem, e supondo que o período torne-se infinito, obtemos as fórmulas da Transformada de Fourier $S(f)$ de uma função $s(t)$. A Transformada de Fourier corresponde à representação do sinal não-periódico no domínio da frequência, da mesma forma que a Série de Fourier corresponde à representação do sinal periódico no mesmo domínio. A transformada $S(f)$ representa a energia do sinal em cada uma das suas componentes.

Durante a transmissão, sempre ocorre a perda de energia do sinal através da sua propagação no meio físico provocando uma redução na sua amplitude. Caso esta redução da energia do sinal ocorra de forma diferente para cada componente de frequência ela provoca, além da redução da amplitude do sinal, uma distorção do mesmo. A proporção da perda para cada frequência do espectro do sinal é uma característica do meio físico utilizado para a transmisão. Neste contexto, podemos definir a banda passante do meio físico como a faixa de frequência do sinal que é preservada pelo meio, ou seja, as perdas de energia do sinal ocorrem nas frequências que não se encontram nesta faixa.

2.1.2 Transmissão analógica e digital

Os termos analógico e digital podem ser associados a 3 contextos envolvidos na comunicação de dados:

- dado;
- sinalização;
- transmissão.

O dado é um elemento que possui uma semântica; o sinal corresponde à codificação elétrica ou eletromagnética do dado enquanto sinalização está associada à propagação do sinal através de um canal e, por último, a transmissão é a comunicação do dado através da propagação e processamento dos sinais.

Exemplos de dados analógicos são a voz e o vídeo que variam continuamente as suas intensidades. Exemplos de dados digitais são o texto e os inteiros. No caso dos sinais já vimos que um sinal analógico corresponde a uma onda eletromagnética que varia continuamente e, no caso dos sinais digitais, temos uma sequência de pulsos de voltagem que podem ser transmitidos em um fio. Geralmente, os dados analógicos são uma função do tempo e ocupam um espectro limitado de frequência. Estes dados podem ser representados por um sinal eletromagnético ocupando o mesmo espectro. Por outro lado, os dados digitais podem ser representados por sinais digitais onde cada um dos dígitos binários corresponde a um nível de voltagem. Outras possibilidades são ainda a representação do dado digital através de um sinal analógico como no caso do uso de um modem (*modulador/demodulador*), e a representação de um dado analógico, como por exemplo a voz, através de sinais digitais. O dispositivo que realiza esta última função é o codec (*codificador-decodificador*) através da aproximação do sinal de voz por um fluxo de bits. Na outra extremidade, o fluxo de bits é utilizado para reconstruir o dado analógico.

Ambos os sinais, analógico e digital, são transmitidos em meio físico adequado. O sistema de transmissão define a forma como os dados são tratados. No caso da transmissão analógica, o sinal é transmitido sem que o conteúdo seja observado, independentemente do sinal representar um dado analógico ou digital. Para permitir atingir grandes distâncias são utilizados amplificadores para aumentar a energia do sinal quando esta encontrar-se em níveis baixos. O problema dos amplificadores é que eles também amplificam o ruído provocando uma distorção no sinal que aumenta cada vez mais com a distância. A distorção no caso do dado digital é mais difícil de ser tolerada do que no analógico. Isto significa que o encadeamento de amplificadores na transmissão analógica de dados digitais irá introduzir erros. Por outro lado, a transmissão digital está relacionada ao conteúdo do sinal. Para permitir a transmissão do sinal digital a grandes distâncias utiliza-se repetidores. O papel do repetidor é receber os sinais digitais e recompor a sequência de bits 0's e 1's original permitindo contornar a atenuação e, consequentemente, oferecer uma qualidade bastante superior porque é possível recuperar exatamente o sinal original sem distorções. Esta técnica é a mesma utilizada no caso de um sinal analógico transmitindo dados digitais ao empregar-se repetidores no lugar de amplificadores. Neste caso o repetidor recupera o dado digital original a partir do sinal analógico e retransmite-o através de um novo sinal analógico sem ruído, não havendo portanto acúmulo do ruído.

Apesar da grande infra-estrutura de transmissão analógica implantada nas últimas décadas, existe uma migração para a transmissão digital que irá se consolidar nos próximos

anos em função dos seguintes benefícios:

- tecnologia digital compacta e a custos cada vez menores;
- integridade do dado em função da presença não acumulativa do ruído;
- utilização da capacidade do canal através de um esquema de multiplexação mais eficiente (multiplexação no tempo) do que no caso da transmissão analógica (multiplexação em frequência);
- segurança e privacidade através de técnicas de criptografia aplicáveis aos dados digitais e aos dados analógicos digitalizáveis;
- integração representada pelo tratamento digital dos dados analógicos e digitais através de uma infra-estrutura única de transmissão o que otimiza os custos e facilita o gerenciamento do sistema de comunicação.

2.1.3 Modos de Transmissão de Dados

A camada física é responsável pela transmissão através do meio físico dos quadros oriundos da camada de enlace. De acordo com o hardware empregado, a transmissão pode ocorrer em modo *full duplex* onde dois nós comunicantes transmitem simultaneamente, ou *half duplex* caso a informação tenha seu fluxo alternado no tempo (apenas um nó por vez pode transmitir). Em redes de computadores, a comunicação *half duplex* é a mais comum, dado que, na maioria das vezes, o meio físico é composto de duto único.

A transmissão de bits pelo meio físico pode se processar de forma *serial* ou *paralela*. Na transmissão serial um bit é transmitido a cada intervalo de tempo, enquanto na paralela os bits são transmitidos serialmente por N dutos independentes, resultando na transmissão de N bits por unidade de tempo. Como a transmissão paralela requer um meio físico composto de vários dutos, esta não é empregada em redes de computadores convencionais.

Uma transmissão de bits pode se dar de forma *síncrona* ou *assíncrona*. Na transmissão síncrona um bit é transmitido a cada intervalo de tempo bem definido, enquando na transmissão assíncrona um bit pode ser transmitido num instante de tempo arbitrário. A transmissão síncrona requer que tanto o nó transmissor quanto o nó receptor disponham de uma base de tempo comum, o que torna seu emprego muito restrito em redes de computadores. A transmissão assíncrona a nível de bits, por outro lado, é um processo ineficiente pois requer a introdução de um separador entre dois bits (caracter especial ou intervalo de tempo sem transmissão).

Na prática, utiliza-se um meio termo entre os modos síncrono e assíncrono, onde a transmissão assíncrona se dá a nível de bloco de bits (transmissão start-stop). Detectado a ocorrência de um bloco, os bits que o compõe são recebidos sincronamente. Cada bloco é iniciado com um delimitador de início (combinação de bits) e terminado com um delimitador de final de bloco. Ao detectar um delimitador de início, o receptor sincroniza seu relógio para receber, sincronamente, os bits que compõem o bloco. Mesmo que o nó transmissor e receptor apresentem um certo *drift* em seus relógios, a transmissão start-stop requer sincronismo apenas entre os delimitadores de início e final de bloco.

2.2 Meios de Transmissão

A transmissão de sinais através de meios de transmissão guiados utiliza dutos elétricos ou óticos para confinamento do sinal entre as extremidades emissora e receptora. Os meios de transmissão guiados mais empregados na atualidade são o par trançado metálico e a fibra ótica.

Por outro lado, a transmissão sem fio utiliza radiofrequência geradas pela fonte emissora de sinal e captada pelo receptor do sinal. A frequência de transmissão situa-se na faixa de microondas (propagação "outdoor") ou no espectro infravermelho (propagação "indoor").

2.2.1 Par Trançado Metálico

Um par trançado constitui-se de dois fios enrolados de forma helicoidal. Esta forma evita que os fios assumam características de uma antena, o que os tornaria susceptíveis a interferências eletromagnéticas, bem como minimizam a componente indutiva da impedância. A componente resistiva da impedância sofre o chamado *efeito pelicular*, segundo o qual a corrente elétrica tende a se concentrar nas bordas exteriores do condutor, aumentando sua resistência efetiva.

Pares trançados são utilizados tanto para transmissão de sinais analógicos (em redes telefônicas), quanto digitais (em redes de computadores). Este meio de transmissão tem como atrativo o baixo custo e a facilidade de instalação, aproveitando-se, em muitos casos, a própria fiação telefônica existente.

A freqüência máxima de transmissão depende do comprimento e da espessura do par de fios, o que em última instância dita a impedância elétrica do par. Para longas

distâncias (quilômetros) a taxa de transmissão não ultrapassa 20 Kbits/s, podendo atingir 155 Mbits/s em comprimentos de poucas dezenas de metros. É comum redes na faixa de 10 Mbits/s ter como meio de transmissão pares trançados para distâncias inferiores a 1 quilômetro.

2.2.2 Fibra Ótica

A fibra ótica é composta de um núcleo de sílica envolto por uma casca também de sílica, tudo protegido por uma capa plástica. O núcleo e a casca apresentam índices de refração distintos, apesar de construídos de materiais similares. A tecnologia mais comum é a chamada fibra *multimodo* onde a luz é mantida no núcleo por reflexão na casca (figura 2.3). Fibras multimodo possuem diâmetros entre 50 e 200 μm. Atenuações de 1 a 5 dB por quilômetro na potência do sinal ótico são típicas.

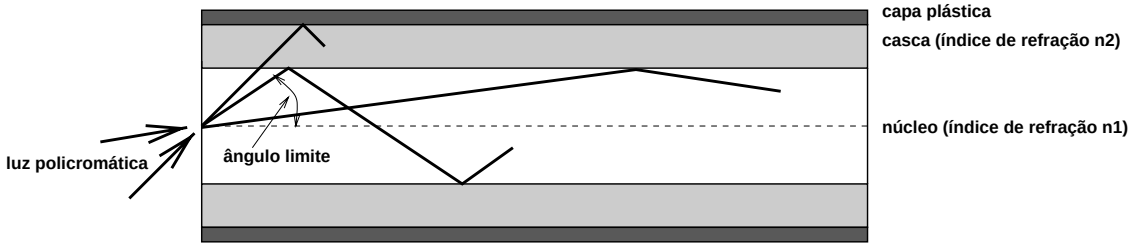


Figura 2.3: Fibra ótica multimodo.

O sinal ótico consite de luz policromática de comprimento de onda centrado em $0.8\mu m$. O sinal é produzido por diodos LED e captado por fotodetectores, sendo totalmente imune a interferências eletromagnéticas.

As fibras óticas são de difícil instalação, e utilizadas em redes com topologia em anel onde o tráfego da informação se dá num sentido único ou conexões ponto-a-ponto. A conexão de um nó numa rede de fibra ótica é um processo complicado. O sinal ótico é convertido num sinal elétrico correspondente, passado ao computador que, quando for o caso, o retransmite empregando o processo inverso. Essa regeneração do sinal coopera para o aumento da distância da rede

Redes baseadas em fibra ótica (FDDI, por exemplo) operam a taxas de 100 Mbits/s. Taxas de Gbits/s com percursos de longas distâncias necessitam fibras monomodo (diâmetros de 5 a 10 μm) e luz monocromática produzida por diodos laser.

2.2.3 Transmissão sem Fio

Redes locais sem fio (WLAN: Wireless Local Area Network) utilizam ondas eletromagnéticas não guiadas para a transmissão de dados. A frequência da emissão pode se situar na faixa do espectro infravermelho ou no espectro de radiofrequência.

Redes baseadas em infravermelho se restringem à utilização em ambientes totalmente abertos[1]. Devido ao baixo alcance, em torno de 10 m, o espectro infravermelho apresenta-se como vantajoso apenas em situações onde a implantação de fiação não é recomendada (em edifícios históricos, por exemplo). Transmissão por infravermelho utiliza modulação por posição de pulsos (PPM: Pulse Position Modulation).

Infravermelho no padrão IEEE 802.11 para WLANs define duas taxas de transmissão (1 e 2 Mbits/s), emissão de comprimento entre 850 e 950 nm, e modulação 4 ou 14-PPM.

Redes baseadas em radiofrequência utilizam faixas de frequência no espectro denominado ISM (Instrumentation, Science and Medical). Faixas ISM não requerem certificação para emissão e possuem valores entre 902 - 928 MHz, 2.4 - 2.483 GHz e 5.725 - 5.875 GHz. Como a emissão nestas faixas é livre, utiliza-se técnicas de *spread spectrum* para que a transmissão em uma rede se apresente como ruído para outras redes operando em sua mesma área. Técnicas de *spread spectrum* introduzem redundância na codificação de modo que o sinal transmitido pode ser recuperado na presença de ruído. Existem duas técnicas de *spread spectrum*: Frequency Hopping (salto em frequência) e Direct Sequence (sequência direta). O padrão IEEE 802.11 para WLANs utiliza tanto Frequency Hopping quanto Direct Sequence com técnicas de *spread spectrum*.

Frequency Hopping Spread Spectrum

Frequency Hopping (FH) subdivide determinada faixa de frequência ISM em sub-faixas centradas em frequências conhecidas. O emissor transmite numa dada frequência durante um curto período de tempo (slot) e comuta para outra. A escolha da próxima frequência seque uma sequência pseudo-aleatória conhecida apenas pelos membros da WLAN (figura 2.4). Uma técnica de modulação é empregada na codificação do sinal digital. Para outras WLANs uma emissão codificada em Frequency Hopping apresenta-se como ruído composto de pequenos impulsos que são filtrados pelo circuito receptor.

Frequency Hopping no padrão IEEE 802.11 subdivide uma faixa em 79 sub-faixas de

[1]Radiação infravermelho não atravessam obstáculos, podendo, no máximo, refletir num teto branco.

1 MHz cada. O emissor muda de frequência a cada 20 milisegundos segundo uma das 78 sequências definidas no padrão. A taxa de transmissão padrão é 1 ou 2 Mbits/s. A técnica de modulação é GFSK (Gaussian Frequency Shift Keying) de 2 ou 4 níveis, dependendo da taxa de transmissão.

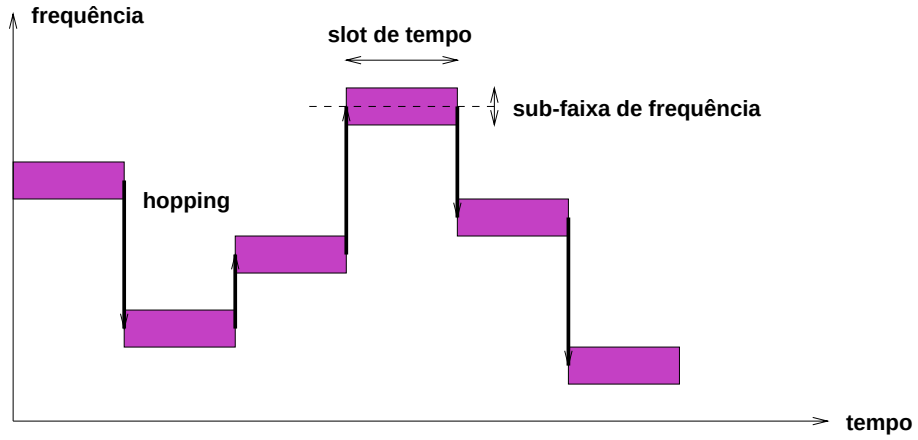


Figura 2.4: em Frequency Hopping Spread Spectrum.

Direct Sequence Spread Spectrum

Direct Sequence (DS) utiliza uma única frequência numa faixa ISM. DS "espalha" o espectro através de redundância na codificação do bit. Um códico, denominado sequência de *chipping* (chipping sequence) e composto de uma sequência binária, é utilizado na codificação do bit (figura 2.5). Este código (necessário para decodificar a informação) é conhecido apenas pelos membros da WLAN. Uma emissão DS se apresenta como ruído faixa larga de baixa potência para um receptor empregando outro código. A codificação do bit é processada efetuando-se uma operação de ou-exclusivo (XOR) de cada bit da sequência de chipping com o bit a ser transmitido (ver figura 2.5). Esta composição produz a sequência de bits a ser transmitida via modulação.

Quanto maior o comprimento do código[2] (ou fator de *spreading*), maior a quantidade de redundância e portanto maior a tolerância à interferência. Entretanto, o códigos de comprimento longo reduzem a capacidade do canal em termos de bits transmitidos por segundo.

Direct Sequence no padrão IEEE 802.11 define 11 ou 13 canais de 13 MHz. As fre-

[2]Para comunicação civil um comprimento de 128 bits é usual.

quências dos canais são centradas a cada 5 MHz (poranto, os canais se sobrepõem). Cada canal de 13 MHz transporta 1 ou 2 Mbits/s de informação. Para 1 Mbits/s, a modulação DBPSK (Differential Binary Phase Shift Keying) é empregada, enquanto para 2 Mbits/s utiliza-se a modulação DQPSK (Differential Quadrature Phase Shift Keying).

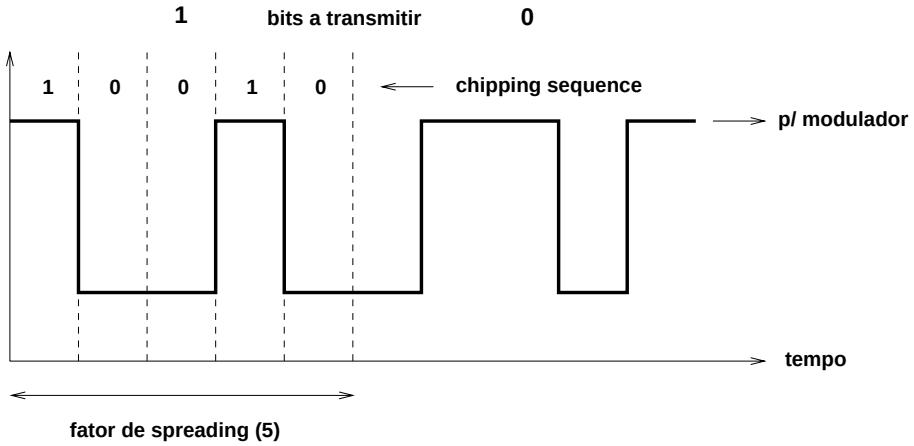


Figura 2.5: em Direct Sequence Spread Spectrum.

2.3 Características dos Meios de Transmissão Elétricos

Via de regra, os meios de transmissão elétricos são do tipo passa-baixas, isto é, permitem a propagação de freqüências baixas até determinado limiar (largura de banda B). Em geral, a largura de banda é definida como a freqüência em que o sinal injetado num extremo tem sua potência diminuida em 50% (-3 dB) na outra extremidade (figura 2.6-a).

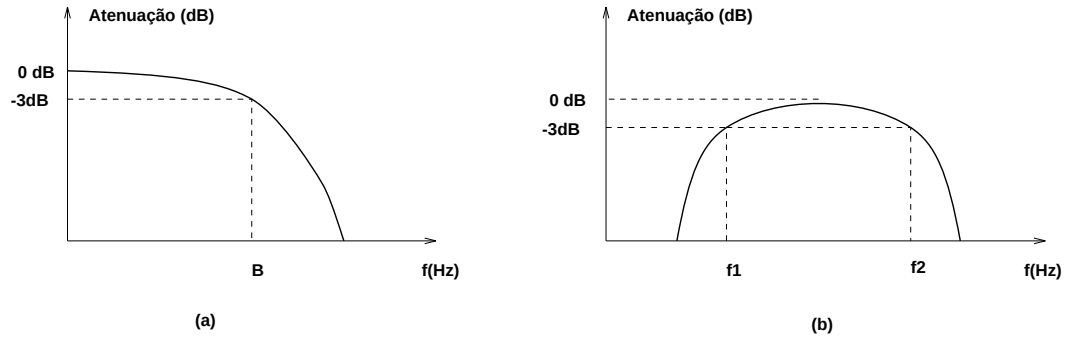


Figura 2.6: Um filtro passa-baixas (a) e passa-faixa (b).

Entretanto, se considerarmos os elementos elétricos diretamente conectados ao meio de transmissão, sua característica passa-baixas se altera para uma característica passa-faixa. Considere, por exemplo, que o circuto de transmissão e recepção esteja ligado ao meio através de um transformador de desacoplamento. Como transformadores exercem forte atenuação em baixas freqüências, o conjunto transformador-meio de transmissão passa a operar como um filtro passa-faixa (figura 2.6-b).

A característica passa-faixa de um meio de transmissão é a razão pela qual utiliza-se codificação de sinais diferentes de ON/OFF. Seja um sinal aleatório em codificação ON/OFF com amplitude unitária no caso de 1 e com igual probabilidade de ocorrência de 0s e 1s. Utilizando-se um filtro ideal que permite a passagem apenas de sinais na freqüência f, vamos aplicar o sinal ON/OFF ao filtro e computar a potência do sinal filtrado. Variando-se f de zero (nível DC) a infinito, obtem-se o gráfico (espectro de potência) da figura 2.7-a.

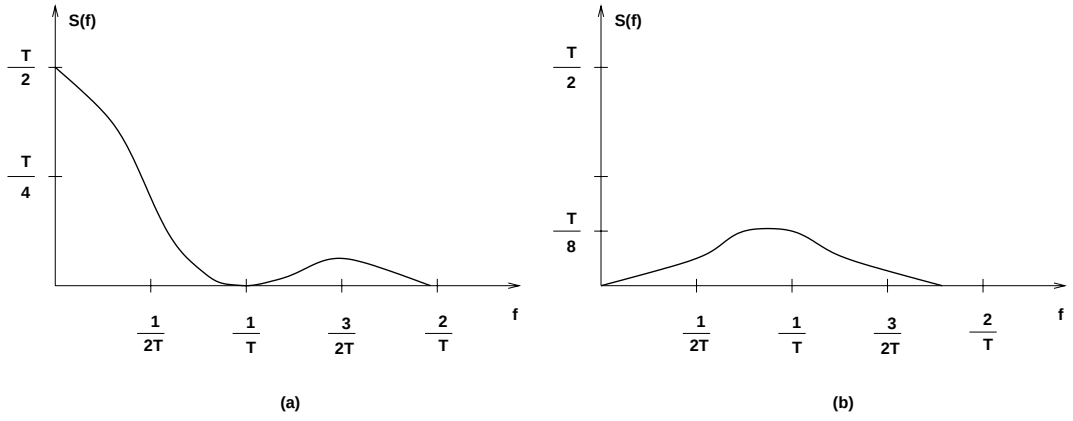


Figura 2.7: Espectro de potência de um sinal de amplitude unitária e período de ocorrência de bits igual a T: (a) codificação ON-OFF; (b) codificação Manchester.

Percebe-se agora que um meio de transmissão com características passa-faixa é inadequado para transmitir um sinal binário em codificação ON/OFF, pois este sinal demanda a propagação de potências consideráveis em baixas freqüências (de 0 até o inverso do período do bit-T). Impedindo-se a propagação de tais freqüências, tem-se um sinal altamente distorcido no receptor.

Passando agora o sinal ON/OFF por um codificador Manchester antes de aplicá-lo ao filtro, obtem-se o espectro de potência da figura 2.7-b. O código Manchester demanda a propagação de potências moderadas tanto de baixas quanto de altas freqüências, causando pouca distorção do sinal quando transmitido através de um meio passa-faixa.

2.3.1 Fontes de Distorção do Sinal

Característica Passa-faixa do Meio

A figura 2.8 mostra a distorção de um sinal periódico pela ausência (ou atenuação) de suas componentes de alta freqüência. A ausência de componentes de baixa freqüência dificulta ainda mais a identificação de 0s e 1s pelo receptor. Sinais periódicos necessitam apenas da propagação de submultiplos inteiros de sua freqüência (harmônicas da série de Fourier).

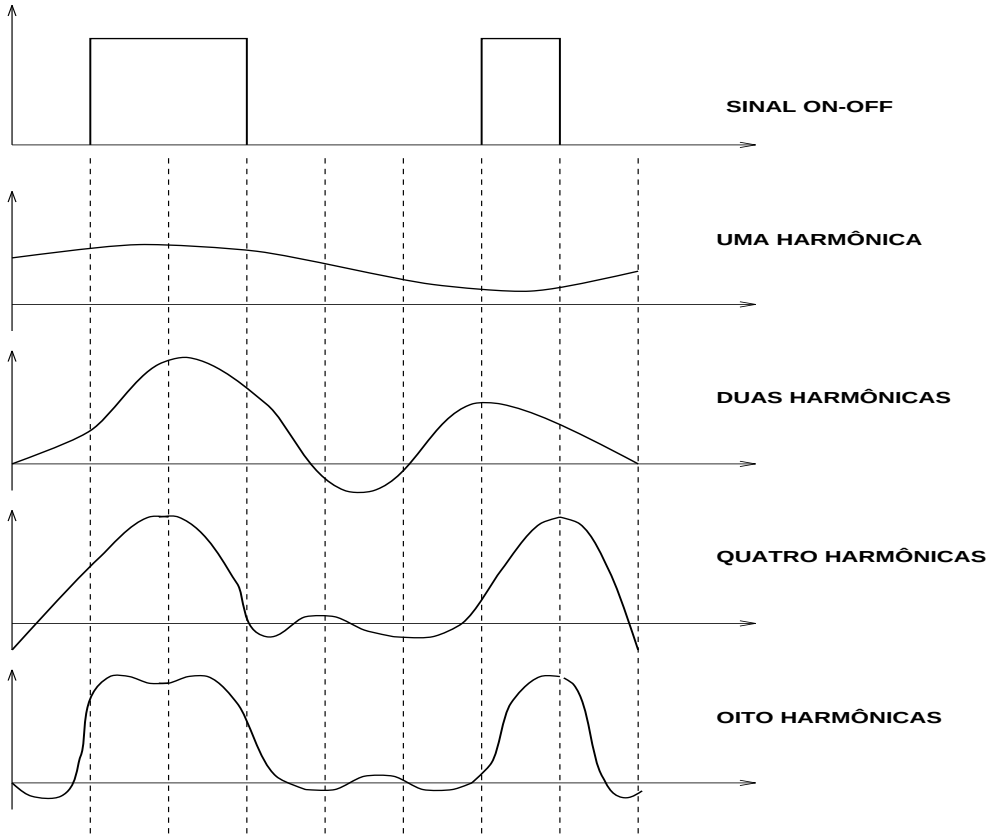


Figura 2.8: Um sinal periódico e suas harmônicas.

Interferência Entre Símbolos

Quando aplicamos uma onda retangular de tensão a um meio de transmissão elétrico, temos no receptor do sinal uma onda não retangular como mostra a figura 2.9. A subida

íngreme da tensão é impedida pelas capacitâncias inerentes do meio, que necessitam armazenar energia para ter sua tensão variada. Esta energia é devolvida quando a tensão decai, impondo igualmente um decréscimo suave da tensão no meio.

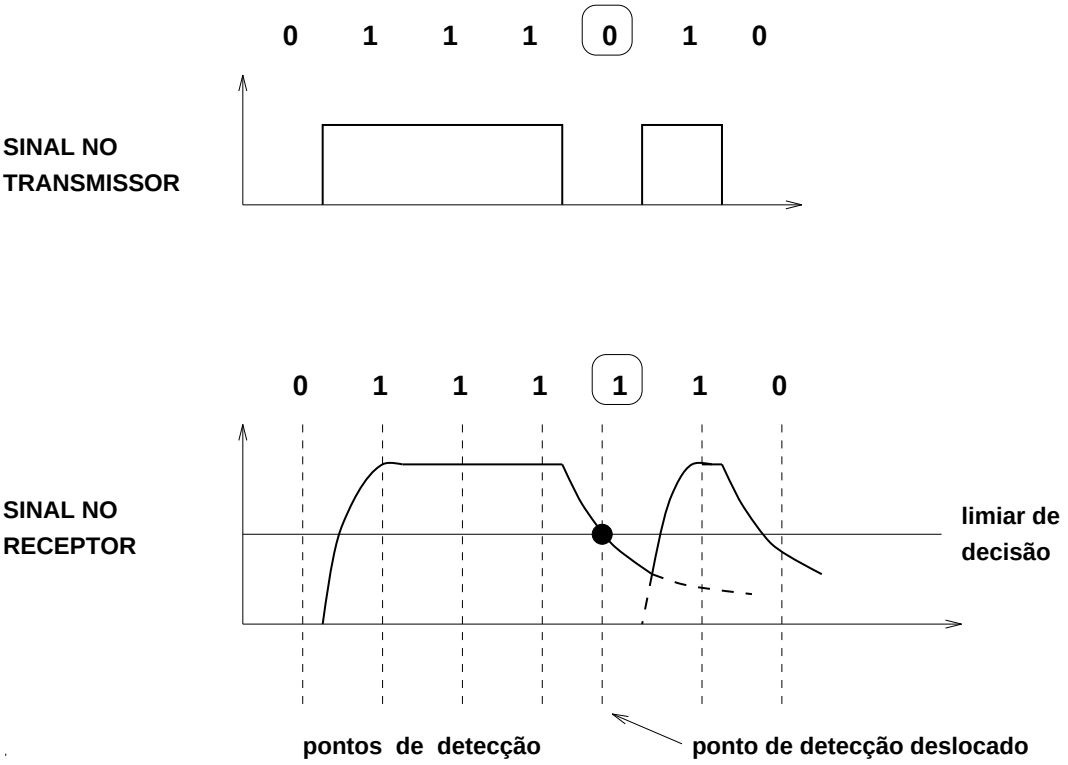


Figura 2.9: Interferência entre símbolos.

Suponha a ocorrência do bit 1 seguido do bit 0. O decaimento suave da tensão pode fazer com que o receptor detecte o bit 1 no lugar do bit 0, caso a amostragem se dê mais próxima do início do intervalo do bit. A este fenômeno denomina-se *interferência entre símbolos.*

Jitter de Fase

Jitter de fase é uma imprecisão na fase do sinal digital causada por alteração do ponto de operação normal dos circuitos eletrônicos devido a variações de temperatura, oscilações da tensão de alimentação, etc. O jitter de fase causa uma mudança no instante de passagem pelo limiar que distingue uma transição (figura 2.10). Como consequência, o período de ocorrência dos bits tem um valor não constante, podendo causar erros na recepção do sinal.

O jitter de fase é medido pela faixa de tempo em que a transição pode variar (em valor absoluto ou relativo ao período do bit).

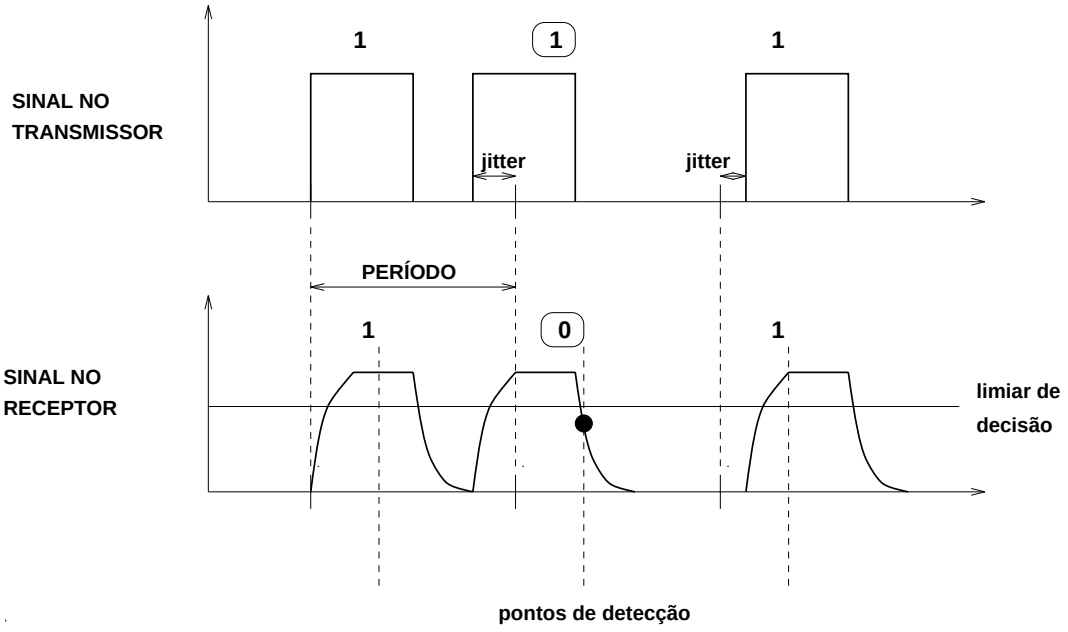


Figura 2.10: Erro de detecção devido ao jitter de fase.

Ruído Térmico

Ruído térmico é uma perturbação de natureza aleatória que distorce o sinal. Transitórios térmicos e eletromagnéticos são as causas mais comuns de ruído térmico. Transitórios mecânicos é outra fonte de ruído térmico, alterando as características elétricas dos contactos (resistência e capacitância de contacto).

A figura 2.11 ilustra a distorção causada pelo ruído térmico.

Distorção por Atraso de Propagação

Um sinal pode ser representado por um certo número de componentes harmônicas senoidais. Nos meios físicos usuais a velocidade de propagação de uma onda senoidal depende de sua freqüência. Caso esta dependência seja acentuada, uma harmônica de freqüência alta pode ter sua fase alterada em relação as harmônicas de freqüências baixas. A figura 2.12 mostra este efeito.

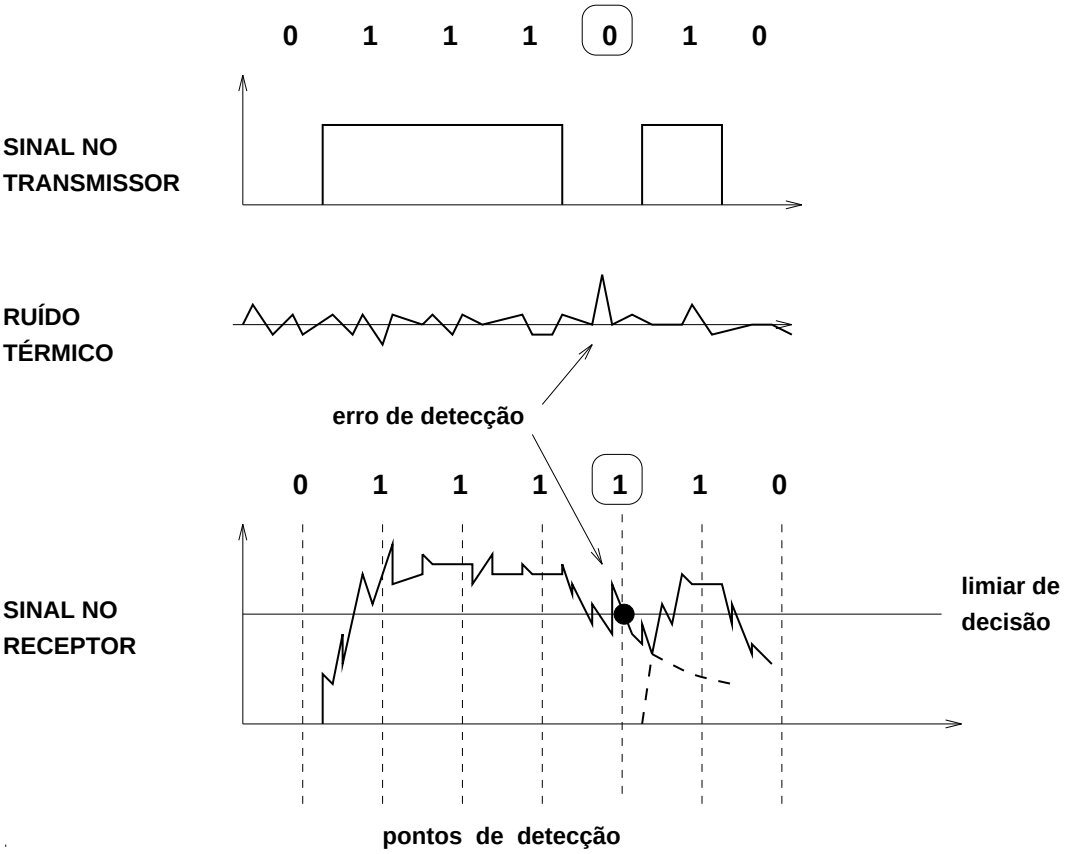


Figura 2.11: Erro de detecção devido ao ruído térmico.

2.3.2 Capacidade de Transmissão de um Canal

A freqüência com que um sinal pode se propagar no meio de transmissão é denominada *baud*. Um canal de 10 Mbaud permite 10^6 variações do sinal por segundo. A relação entre baud e bits por segundo (bits/baud) depende da forma de codificação do sinal. Um canal com capacidade de N bauds pode transportar N bits/s no caso de sinal digital com codificação ON/OFF ou NRZ. No caso de codificação Manchester, teremos N/2 bits/s em média.

Um canal de N bauds pode transportar um número maior que N de bits/s. É o caso de, por exemplo, utilizar-se um sinal digital com codificação ON/OFF e 4 níveis de tensão representando as ocorrências dos bits 00, 01, 10 e 11. Neste caso temos 2N bits/s. A codificação de múltiplos bits numa única variação do sinal é rara em redes locais devido a alta taxa de falhas na decodificação do sinal. Quando utilizada (principalmente em troncos

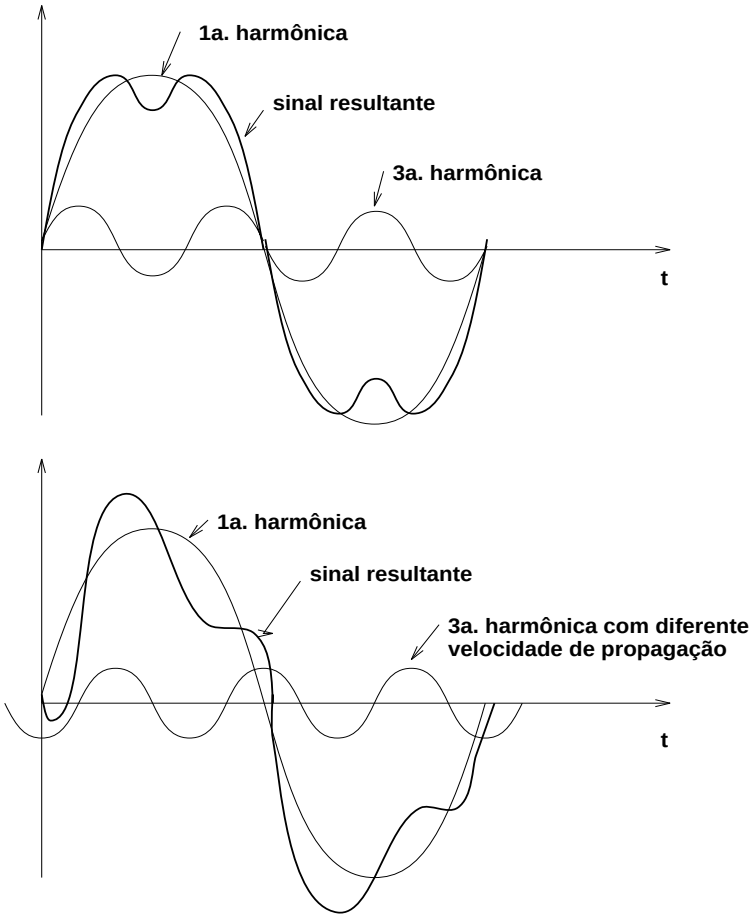


Figura 2.12: Distorção devido a variação da velocidade de propagação das harmônicas com a freqüência.

telefônicos), emprega-se transmissão analógica com modulação PSK e ASK combinadas. (figura 2.13).

A capacidade de transmissão de um canal passa-baixas é limitada pelo teorema de Nyquist: Um canal livre de ruído com largura de banda B transmitindo um sinal com V diferentes amplitudes possui uma taxa de transmissão T (em bits/s) dada por

$$T \leq 2B \log_2 V$$

Por exemplo, um canal com largura de banda 3 KHz apresenta uma capacidade máxima de 6 Kbits/s caso sejam empregadas duas amplitudades (modulação ASK) para codificar os níveis 0 e 1.

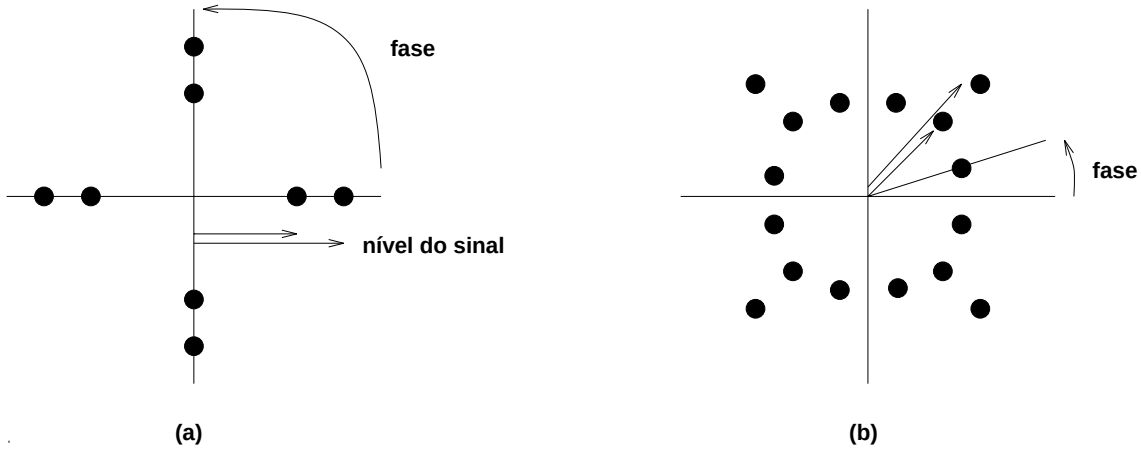


Figura 2.13: Modulações PSK e ASK combinadas para 3 bits/baud (a) e 4 bits/baud (b).

Intuitivamente, o limite de Nyquist se deve a filtragem de freqüências altas pelo canal tornando inútil amostragens com taxa maior que 2B.

Devido a presença das fontes de distorção descritas acima, o limite teórico de Nyquist nunca é atingido na prática. A interferência entre símbolos causadas pelas indutâncias e capacitâncias ao longo do meio é um fator preponderante na limitação da taxa de transmissão de um canal elétrico.

Em redes de computadores baseadas em canais elétricos, taxas da ordem de 10 a 155 Mbits/s são típicas. Em redes baseadas em fibra ótica, 100 a 622 Mbits/s são taxas típica. Redes operando na faixa de Gbits/s como as baseadas em tecnologias ATM (Asynchronous Transfer Mode) e Gibabit Ethernet já estão disponíveis comerciamente.

2.4 Codificação de Dados

Dados (sequência de bits) podem ser codificados através de sinais analógicos ou digitais. Sinais analógicos são formas de ondas senoidais onde a informação (valor do bit) é codificada na frequência, amplitude ou fase do sinal, num processo denominado *modulação*.

Sinais digitais são codificados através de pulsos onde a informação é codificada na amplitude do pulso (ON/OFF) ou transição (subida/descida). A forma mais imediata de codificação digital é a codificação ON/OFF onde um valor alto de amplitude representa o código 1 enquanto um valor baixo representa o código 0 (ou vice-versa). Esta forma de

codificação produz ondas quadradas de formato altamente irregular o que dificulta sua transmissão através do meio físico (justificativa adiante). Outras formas de se codificar um sinal digital ON/OFF para sua posterior transmissão são (figura 2.14):

- Código Polar NRZ (Non Return to Zero): idêntico ao sinal ON/OFF, exceto que duas polaridades são empregadas (positiva e negativa). Raramente empregado em redes locais de computadores;
- Código Unipolar RZ (Return to Zero): o bit 1 coincide com um pulso de relógio, enquanto o bit 0 é representado pela ausência do pulso. Raramente empregado em redes locais de computadores;
- Código Manchester: uma transição sempre ocorre no meio do intervalo de um bit. Se positiva (subida), a transição representa o bit 1, se negativa (descida) o bit 0. Transições são do tipo RZ;
- Código Bifase: idêntico ao Manchester, mas empregando transições NRZ;
- Código Manchester Diferencial: uma transição sempre ocorre no meio do intervalo de um bit. Uma transição adicional no início do intervalo representa o bit 0, enquanto a ausência desta representa o bit 1. Transições são do tipo RZ;
- Código Bifase Diferencial: idêntico ao Manchester Diferencial, mas empregando transições NRZ;
- Código CMI (Code Mark Inversion): o bit 0 é representado por uma transição positiva (subida) no meio do intervalo do bit, e o bit 1 pela ausência de transição positiva. Uma transição no final do intervalo ocorre quando bits 1s se repetem. Transições são do tipo NRZ.

O padrão IEEE 802.3 (CSMA/CD) utiliza transmissão digital com codificação Manchester injetando no cabo pulsos de tensão com amplitude variando entre 0 e -2.05 Volts.

2.4.1 Modulação de Sinais Digitais

O processo de modulação consiste em variar a amplitude, a freqüência ou a fase de um sinal senoidal para representar determinado nível de um sinal digital.

A *Modulação por Chaveamento de Amplitude* (ASK) emprega uma onda senoidal de freqüência fixa e dois níveis de amplitude que representam os níveis do sinal digital (figura 2.15).

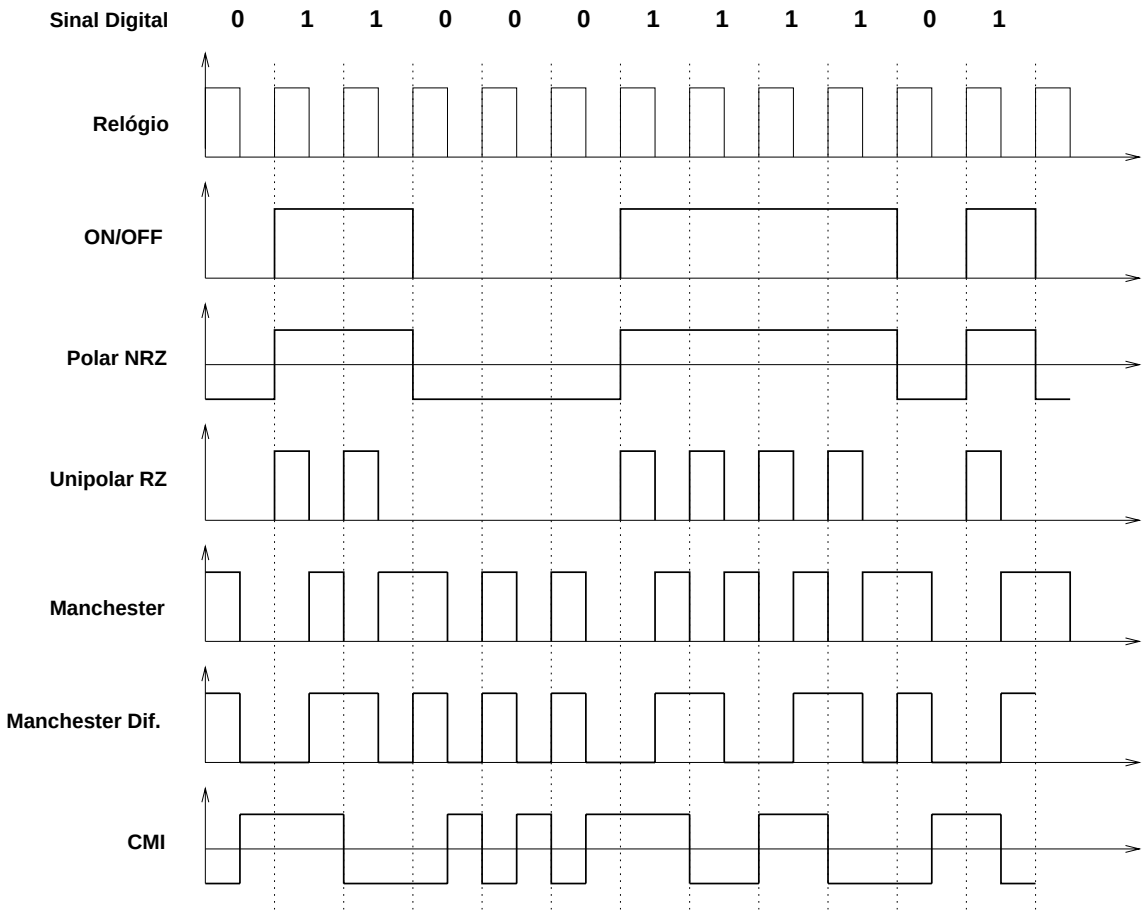


Figura 2.14: Formas de se codificar um sinal digital.

A *Modulação por Chaveamento de Freqüência* (FSK) emprega duas freqüências para codificar os níveis do sinal digital (figura 2.15). A passagem da freqüência alta para a baixa pode se dar de forma contínua ou de forma discreta. Na passagem contínua (modulação FSK-contínua), existe um tempo máximo para ocorrer a transição entre as duas freqüências e uma variação máxima nas amplitudes correspondentes às freqüências alta e baixa. Na passagem discreta (FSK-coerente), normalmente se empregam N ciclos de freqüência baixa para representar determinado nível binário, e $2N$ ciclos de freqüência alta (o dobro da baixa) para o outro nível.

O padrão IEEE 802.4 (Token Bus) prevê ambas as formas de modulação FSK (não coexistentes na mesma rede, obviamente). Na moduação FSK-contínua, as freqüências são 3.75 e 6.25 MHz com uma tolerância de $\pm$ 80 KHz. O período de transição não pode ultrapassar 100 nanosegundos e as amplitudes nas freqüências alta e baixa não devem ter

uma variação superior a 10%. Na modulação FSK-coerente, são empregadas freqüências de 5 e 10 (ou 10 e 20) MHz e um ciclo de freqüência baixa para representar o bit 1 ($N = 1$).

Finalmente, a *Modulação por Chaveamento de Fase* (PSK) representa os níveis binários por um avanço ou atraso de fase no sinal senoidal. Por exemplo, uma transição negativa (de 1 para 0) é representada por um avanço de 90^o na fase do sinal senoidal, enquanto uma transição positiva (de 0 para 1) é representada por um atraso equivalente (figura 2.15).

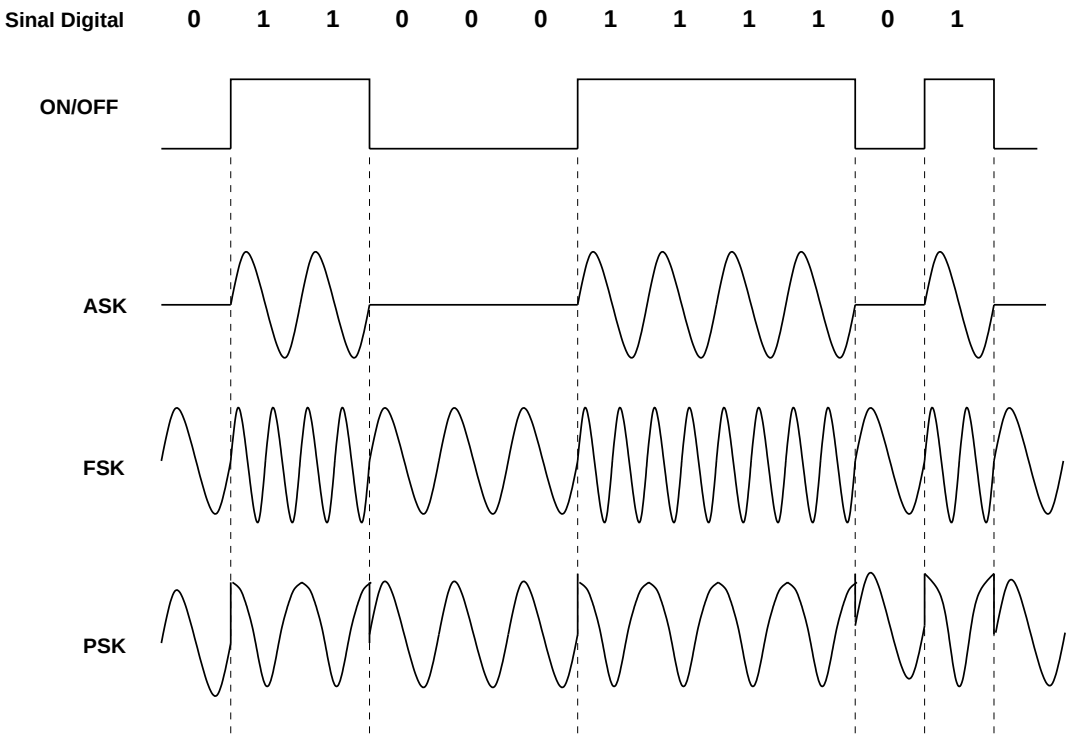


Figura 2.15: Modulação de sinais digitais.

Capítulo 3

Técnicas de Multiplexação e Comutação

3.1 Multiplexação

A situação comum nos sistemas de comunicação é que a banda passante disponível no meio físico é muito superior à banda passante efetiva do sinal a ser transmitido. Como forma de viabilizar economicamente os sistemas de transmissão, a estratégia utilizada corresponde no compartilhamento da banda passante do meio entre vários usuários, ou seja, na multiplexação do meio. As técnicas básicas de multiplexação são a temporal e a frequencial. A demultiplexação, por outro lado, corresponde ao processo de separação dos fluxos de informação no destino.

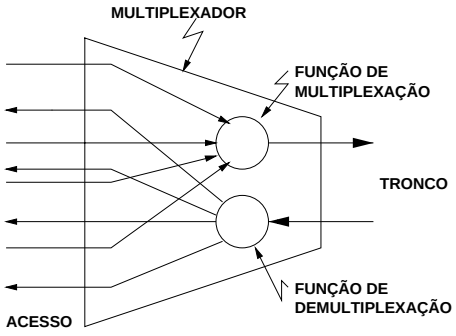


Figura 3.1: Exemplo de Multiplexador

3.2 Multiplexação por Divisão de Frequência (FDM)

FDM (Frequency Division Multiplex) corresponde à multiplexação, em um mesmo meio, de vários sinais através do deslocamento da faixa de frequência dos sinais (banda básica) para faixas de frequência distintas de modo que eles não interfiram entre si. A FDM baseia-se em eletrônica analógica possuindo problemas associados a ruído, distorção e, eventualmente, interferência entre canais. Estes problemas dificultam a comunicação de dados tornando os custos bastante elevados.

O uso da FDM foi bastante empregado para a agregação de canais de voz e o respectivo transporte em enlaces de alta capacidade (*trunks*). Um esquema básico de multiplexação FDM consiste na agregação de 12 canais de voz de 4 KHz cada, em um grupo de 48 KHz de banda passante através da translação da frequência de cada sinal. Estes grupos de 12 canais são multiplexados, num total de 24 grupos, em um grupo maior denominado grupo mestre. Múltiplos grupos mestres são transmitidos através de sistemas de microondas. Outros exemplos de FDM são as transmissões de rádio e TV (por difusão e por cabo).

A figura 3.2 Ilustra o esquema básico da multiplexação por divisão de frequência.

Na figura, vários sinais analógicos e digitais são multiplexados no mesmo meio de transmissão. Cada sinal $m_i(t)$ é modulado através de uma portadora $f_{sc}i$, na realidade, sub-portadora, porque são utilizadas várias portadoras, uma para cada sinal, que desloca o espectro de frequência do sinal para uma nova faixa de frequências centrada em $f_{sc}i$. Os valores de cada $f_{sc}i$ devem ser escolhidos de modo a não permitir o intercalamento das frequências dos sinais modulados por sub-portadoras vizinhas. O sinal resultante desta multiplexação pode ainda ser modulado por uma portadora de outra frequência de modo a deslocar o sinal completo para uma nova faixa de frequências. No destino, o sinal passa por vários filtros, cada um centrado em $f_{sc}i$ e com uma banda compatível com a dos canais modulados na transmissão. Desta maneira, o sinal é separado nos seus componentes básicos e cada componente é demodulado para permitir a recuperação do sinal original.

3.3 Multiplexação por Divisão do Tempo (TDM)

TDM (Time Division Multiplex) baseia-se no fato de que a capacidade de bits por segundo do meio de transmissão é superior à taxa média de geração de bits pelos dispositivos conectados ao multiplexador. Este último divide a capacidade do canal entre os usuários através da alocação de *slots* de tempo. Cada usuário possui um *slot* de tempo para

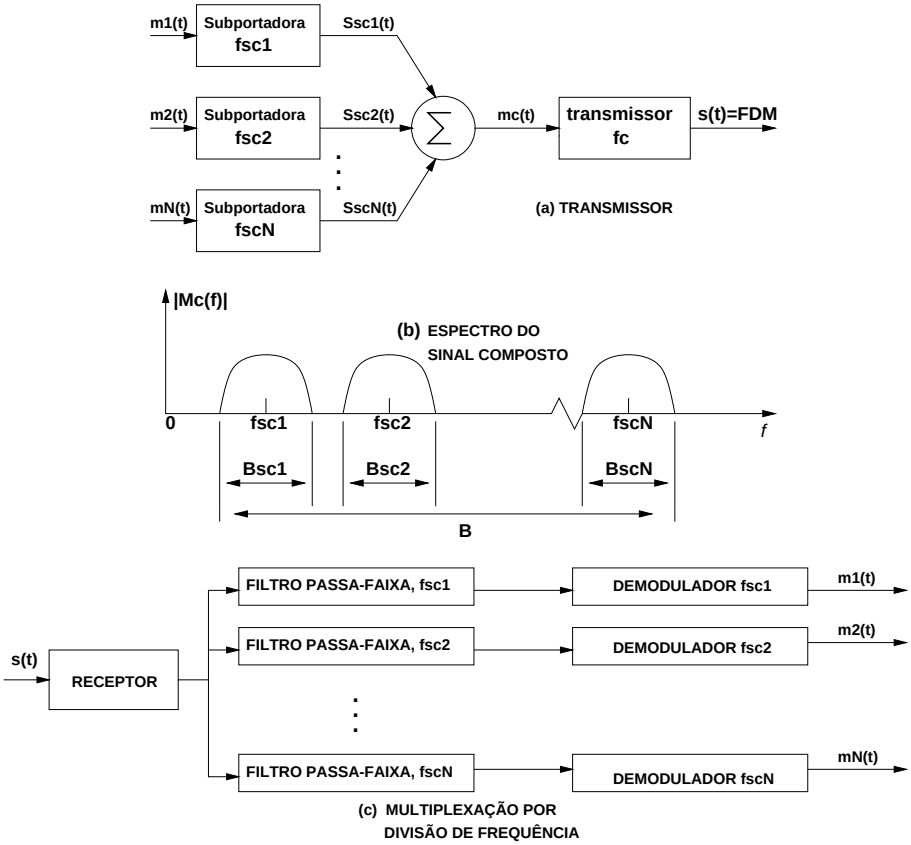


Figura 3.2: Esquema Básico de Multiplexação por Divisão de Frequência

transmitir o seu sinal e este direito é roteado entre os dispositivos dos usuários traduzindo a operação do multiplexador em uma varredura cíclica dos sinais de entrada. As informações dos usuários podem ser intercaladas nos níveis de bit, bytes ou blocos de dados em uma interface de saída do multiplexador de alta velocidade.

O Multiplexador TDM envia sinais de pulsos para os dispositivos conectados nas suas entradas com o objetivo de manter os fluxos de dados sincronizados. Estes pulsos são gerados por um relógio mestre situado no multiplexador. Muitos dispositivos conectados na entrada do multiplexador têm tempos de transmissão diferentes e tempos de propagação também diferentes. Neste caso, o TDM isócrono não envia o pulso de sincronização, mas sim, provê *buffers* internos para armazenamento dos dados que são enviados com um intervalo independente do tempo. Estes dados armazenados nos respectivos *buffers* são, posteriormente, multiplexados na interface de saída do multiplexador.

A multiplexação no tempo pode ser classificada como síncrona ou estatística.

3.3.1 TDM Síncrono (STDM)

O STDM divide o tempo em intervalos de tamanho constante denominados de quadros (*frames*). Os quadros são divididos ainda em pedaços menores denominados de *slots*. Todos os *slots* correspondentes a uma mesma posição fixa do quadro definem o que se denomina de canal. Por exemplo, o canal 2 é constituído de todos os segundos *slots* de cada quadro (fig. 3.3). Os *slots* não necessitam ter o mesmo tamanho e, neste caso, supondo que o slot ocupa $1/a$ do quadro e que a capacidade de transmissão do meio é de C bps, a taxa de transmissão efetiva do canal será C/a bps.

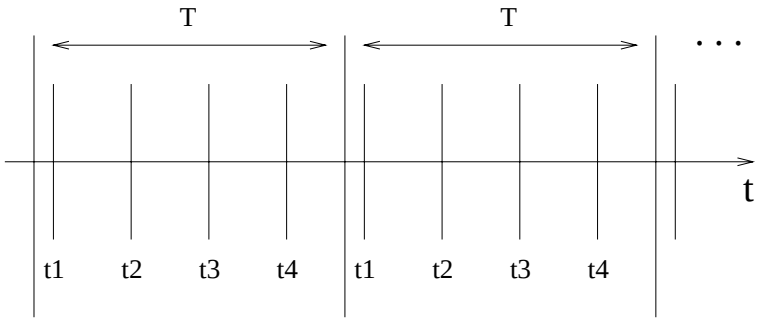


Figura 3.3: TDM Síncrono

As estações que desejarem transmitir solicitam um canal e devem aguardar a sua vez de utilizar o meio, ou seja, o seu canal. Neste instante, a estação transmite na taxa máxima do meio até terminar o intervalo associado ao seu canal. A alocação fixa de um canal durante todo o tempo corresponde ao conceito de canal dedicado. Quando a alocação do canal é dinâmica, ou seja, uma estação que deseja transmitir solicita um canal e após terminar a transmissão libera o canal, temos o caso de uma alocação dinâmica denominada de canal chaveado ou chaveamento de circuitos. Quando uma estação solicita a alocação de um canal e não transmite informação quando do seu *slot* teremos um desperdício de capacidade do meio físico pois o canal não poderá ser utilizado por uma outra estação até que a estação que solicitou o canal libere-o. Na recepção os dados intercalados são demultiplexados e encaminhados para o buffer apropriado.

A denominação síncrono no STDM não está associada à transmissão síncrona dos dados, mas sim, ao fato dos *slots* de tempo serem pré-atribuidos e dedicados às fontes específicas. Uma questão importante relativamente ao STDM diz respeito à questão do enquadramento. Com o objetivo de manter o sincronismo entre o emissor e o receptor, introduz-se um bit em cada quadro. À medida que os quadros são enviados o sistema deve detectar um padrão do tipo 1010101... correspondente ao bit reservado para este controle em cada quadro. Caso este padrão não seja observado é indicação que houve

uma perda de sincronismo. Neste caso, posições sucessivas de bits são testadas até que o padrão anterior seja encontrado (*framing search mode*).

Outro aspecto técnico importante no STDM é relacionado à sincronização das várias fontes de dados. Como cada fonte possui um relógio local e existem variações entre estes relógios, pode ocorrer uma perda de sincronismo entre o emissor e o receptor. A maneira de se contornar este problema corresponde à introdução de bits (*pulse stuffing*) em posições específicas do quadro. Como a taxa de saída do multiplexador é superior à soma das taxas de dados dos sinais de entrada, este excesso é utilizado para introdução de bits extras em cada sinal de entrada até que a taxa do sinal do relógio gerado no local seja alcançada. Como estes bits são introduzidos em posições fixas, os mesmos podem ser identificados e retirados no demultiplexador.

Hierarquia Digital Síncrona

Como no STDM a divisão do tempo depende da capacidade de transmissão do canal e, também, com o objetivo de tornar a tecnologia STDM independente dos avanços tecnológicos na direção de taxas de transmissão cada vez mais elevadas, desenvolveu-se uma hierarquia TDM. A estratégia consiste na definição de um sinal básico com taxa de C bps a partir do qual toda a hierarquia é estruturada. A base desta hierarquia, no caso dos Estados Unidos e do Japão, é o formato de transmissão DS-1 que corresponde à multiplexação de 24 canais. Cada quadro (*frame*) possui 8 bits por canal e um bit de controle correspondendo a um total de 193 bits por quadro. Esta estrutura é voltada para a transmissão da voz digitalizada onde cada canal contém uma amostra de 8 bits obtida através da digitalização baseada em PCM (*Pulse Code Modulation*) a uma taxa de 8000 amostras por segundo, correspondendo a uma largura de banda de 4 KHz o que é suficiente para a voz já que a maior parte das frequências situam-se entre 300 Hz e 3300 KHz. Desta maneira, cada canal e, consequentemente cada quadro, deverá ter uma frequência correspondente a 8000 quadros por segundo, o que implicará em uma taxa de dado de 8000 x 193 = 1,544 Mbps. A cada 5 quadros utiliza-se as amostras de 8 bits do PCM e no próximo quadro cada canal contém palavras de 7 bits mais um bit usado para controle (sinalização). Estes bits de sinalização formam um fluxo de bits de controle para cada canal contendo informações relacionadas, por exemplo, ao estabelecimento de conexão ou terminação de uma chamada e de informações de rota. A mesma estrutura de formato do quadro DS-1 pode se empregada para suportar dados digitais. Neste caso são oferecido 23 canais de dados, sendo o vigésimo quarto utilizado para sincronização de modo a permitir um recuperação de sincronismo ou de erro de enquadramento de forma mais rápida e confiável, condições importantes no caso do tráfego de dados.

No caso da utilização do DS-1 para transmissão de dados é possível oferecer várias taxas de acesso. Cada canal do DS-1 possui 7 bits sendo o oitavo utilizado para indicar se o canal possui informação de dados do usuário ou de controle o que corresponde a uma taxa de 7 x 8000 = 56 kbps para cada canal. Taxas menores são possíveis retirando-se mais um bit do canal para indicar qual sub-taxa de multiplexação está sendo utilizada. Desta maneira teremos uma taxa de 6 x 8000 = 48 kbps que pode ser sub-dividida em 5 canais de 9,6 kbps, 10 canais de 4,8 kbps ou 20 canais de 2,4 kbps. O DS-1 pode ainda ser utilizado contendo canais de voz e dados.

Acima desta taxa básica de 1,544 Mbps define-se um nível hierárquiso superior através do intercalamento de bits provenientes de entradas DS-1. No caso do DS-2 temos a combinação de 4 DS-1 correspondendo a uma taxa de dados de 6,312 Mbps. Podemos observar que 1,544 x 4 = 6,176 Mbps é inferior aos 6,312 Mbps do DS-2. Neste caso os bits em excesso são utilizados para funções de controle. Outros sinais podem ser derivados conforme mostrado na figura 3.4.

SINAL DIGITAL	NÚMERO DE CANAIS DE VOZ	TAXA DE TRANSMISSÃO
DS-1	24	1,544 Mbps
DS-1c	48	3,152 Mbps
DS-2	96	6,312 Mbps
DS-3	672	44,736 Mbps
DS-4	4032	274,176 Mbps

Figura 3.4: Hierarquia DS-1

A Europa definiu uma hierarquia com as mesmas características, denominada E1, com a diferença de que o quadro é formado por 30 canais de voz e 2 canais de controle em um sinal básico E-1 correspondendo a uma taxa de 2,048 Mbps. O quadro correspondendo a esta hierarquia, que é a mesma adotada no Brasil, encontra-se na figura 3.5.

NÍVEL	EUA	EUROPA	JAPÃO
1	1,544 Mbps (DS-1)	2,048 Mbps (E-1)	1,544 Mbps
2	6,372 Mbps (DS-2)	8,848 Mbps (E-2)	6,372 Mbps
3	44,736 Mbps (DS-3)	34,304 Mbps (E-3)	32,064 Mbps
4	274,176 Mbps (DS-4)	139,264 Mbps (E-4)	97,728 Mbps

Figura 3.5: Hierarquia E-1

As hierarquias DS-1 e E-1 são denominadas de PDH (Hierarquia Digital Plesiócrana

- do grego: "quase síncrono"). Isto porque os relógios das várias fontes não são totalmente síncronos levando o multiplexador a utilizar a técnica de *pulse stuffing* mencionada anteriormente.

Ainda neste contexto de hierarquias digitais síncronas é importante mencionar a hierarquia SONET (proposta nos Estados Unidos) / SDH (proposta na Europa) desenvolvida para aproveitar as altas taxas de transmissão da fibra ótica.

No caso do SONET o sinal básico é o STS-1 (Synchronous Transport Signal) ou OC-1 (Optical Carrier Level 1) correspondendo a uma taxa de dados de 51,84 Mbps. Esta taxa pode ser utilizada para transportar sinais DS-1, DS-2, E-1, etc., ou seja, sinais correspondendo à hierarquia plesiócrana. Sinais múltiplos de STS-1 podem ser combinados para formar sinais STS-N através do intercalamento de N sinais STS-1 sincronizados mutuamente. No caso Europeu especificou-se a hierarquia SDH cujo sinal básico, denominado de STM-1, tem taxa de 155,52 Mbps e corresponde ao STS-3 do SONET. As duas propostas têm pequenas diferenças que podem ser compatibilizadas sem grandes esforços.

A figura 3.10 ilustra o formato do sinal básico do SONET (STS-1). O quadro é formado de 810 bytes e repete-se a uma taxa de 8000 vezes por segundo o que equivale à taxa de 51,84 Mbps.

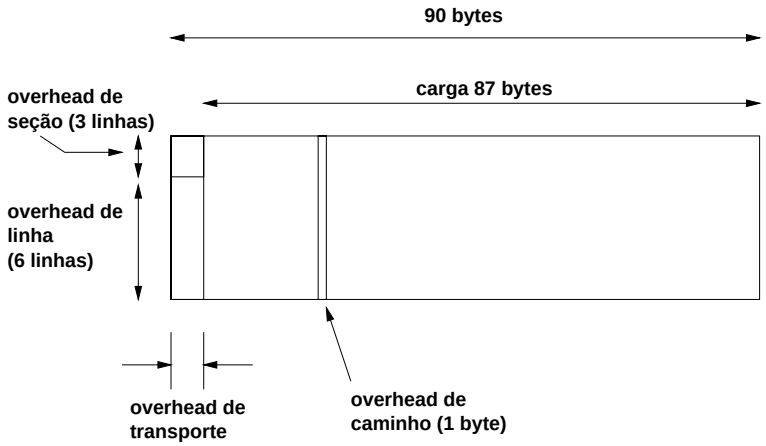


Figura 3.6: Estrutura do Quadro SONET

O quadro pode ser interpretado como uma matriz contendo 9 x 90 e transmitida uma linha de cada vez, da esquerda para a direita e de cima para baixo. As três primeiras colunas, correspondendo a um total de 27 bytes (3 x 9), são utilizadas para controle. O restante do quadro representa a carga transportada. A figura 3.7 apresenta a estrutura geral do formato do quadro STM-N do SDH.

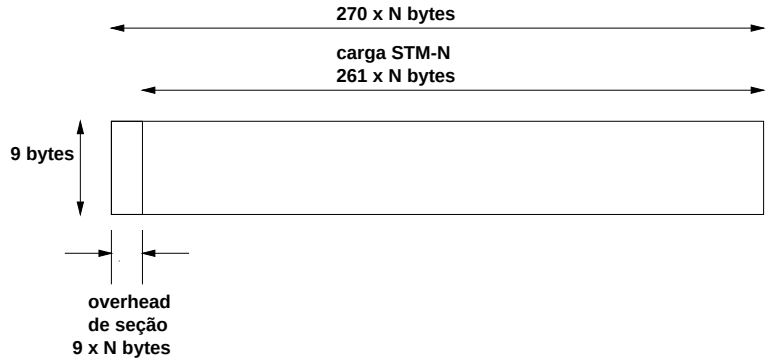


Figura 3.7: Estrutura do Quadro SDH

3.3.2 TDM Estatístico

O STDM apresenta a desvantagem de que se um canal alocado a um usuário não for utilizado esta capacidade não pode ser transferida a outra usuário causando um desperdício do recurso. Uma solução para este problema é o TDM estatístico, também denominado por vários autores de TDM assíncrono (ATDM). O multiplexador estatístico procura explorar o caráter de transmissão em rajada (*burstiness*) do tráfego entre computadores alocando os *slots* de tempo sob demanda. A arquitetura do multiplexador estatístico corresponde a N interfaces de entrada mas somente K *slots* de tempo disponíveis em cada quadro sendo $K < N$, ou seja, caso os N usuários decidam transmitir simultaneamente, não haverá *slots* suficientes, havendo necessidade do armazenamento temporário de informações até que hajam *slots* disponíveis para transmissão da informação armazenada. O multiplexador explora o caráter estatístico do tráfego de dados levando em conta o fato de que os dispositivos conectados no multiplexador não transmitem todos, em média, ao mesmo tempo. Isto permite que a interface de saída do multiplexador possua uma taxa menor do que a soma das taxas das interfaces de entrada. Neste sentido o multiplexador estatístico pode utilizar uma interface de saída com taxa menor do que a interface de saída do multiplexador síncrono caso eles suportem o mesmo número de interfaces de entrada, ou então, suportar um número maior de usuários caso ambos os multiplexadores tenham interfaces de saída de mesma taxa de dados.

Como, diferentemente do STDM, o multiplexador estatístico não pode mais basear-se na posição do *slot* para identificar o canal correspondente, será necessário uma identificação, isto é, um cabeçalho, associado à informação transmitida em cada canal para permitir ao multiplexador estatístico o encaminhamento adequado da informação até ao seu destino. A figura 3.8 ilustra estes conceitos.

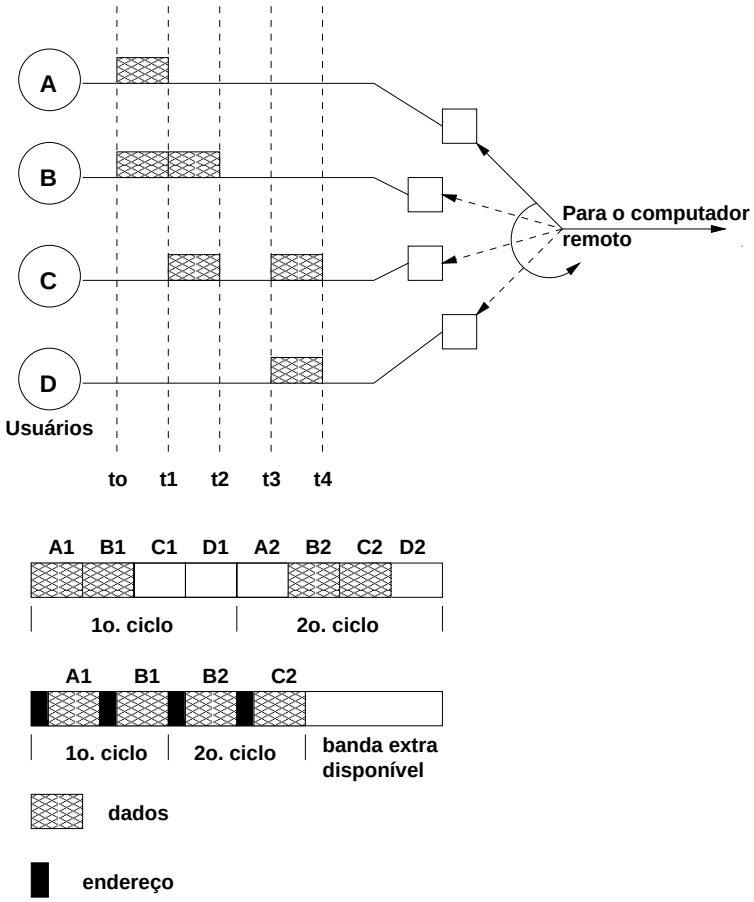


Figura 3.8: TDM síncrono X TDM assíncrono

Caso pretenda-se aumentar a eficiência é possível introduzir mais uma informação no cabeçalho correspondendo ao tamanho do campo de dado. Nesta situação não temos mais o quadro dividido em *slots* fixos com os consequentes cabeçalhos associados. Com o campo de tamanho pode-se utilizar um único cabeçalho para especificar o tamanho do *slot* a ser utilizado pelo usuário naquele instante.

3.4 Técnicas de Comutação

As redes atuais cobrem grandes distâncias e possuem um número elevado de dispositivos computacionais conectados à rede. Como o interesse é que cada dispositivo possa comunicar-se com qualquer outro dispositivo, e não é razoável interconectá-los to-

dos através de uma malha completa de conexões ponto a ponto, uma solução é colocar comutadores (chaveadores) no meio dos caminhos de transmissão. Os dispositivos não encontram-se ligados diretamente mas utilizam o(s) comutador(es) para fazer com que a informação seja propagada nos meios de transmissão e encaminhada, de forma adequada nos elementos de comutação, até que a informação seja recebida pelo computador de destino. A figura 3.9 ilustra uma estrutura comutada.

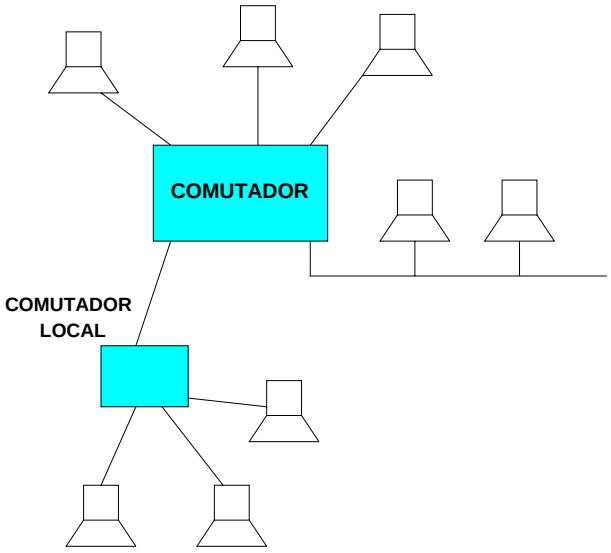


Figura 3.9: Rede Comutada

A comutação corresponde a um rearranjo dos fluxos de informação entre as interfaces de entrada e as interfaces de saída do comutador. Estas entradas e saída acessam meios de transmissão nos quais os sinais propagam-se, provavelmente, de forma multiplexada. A figura 3.10 apresenta uma estrutura genérica de uma rede simples comutada.

A estrutura mostrada na figura 3.10 é típica de redes de longa distância podendo ser utilizada, entretanto, para redes locais e metropolitanas. Na figura temos 2 tipos de componentes: 1) os componentes de borda que são respresentados por estações nas quais são executados as aplicações, ou seja, estão preocupadas com a semântica da informação e da qualidade da informação trocada com outras estações remotas. Cada estação conecta-se a um nó da rede permitindo o seu acesso à rede de comunicação; 2) os nós de comunicação da rede situados no interior da nuvem que representa a infra-estrutura de transmissão. O papel básico destes nós de comunicação é o transporte da informação da origem ao destino. Algumas observações adicionais podem ser feitas ao modelo da figura 3.10:

- alguns nós da rede conectam-se somente a outros nós da rede, por exemplo, os nós

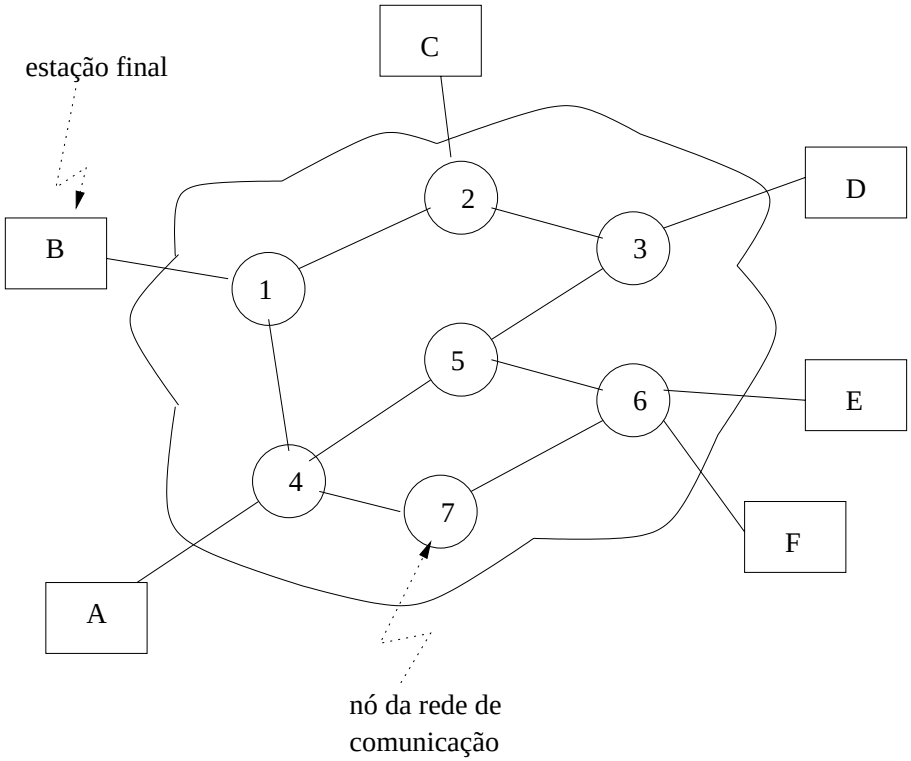


Figura 3.10: Interconexão Através de Comutadores

5 e 7. O único objetivo destes nós é comutar as informações de modo que elas sejam encaminhadas aos seus destinos. Alguns nós da rede, além de estarem conectados a outros nós, também suportam o acesso à rede por parte dos usuários para envio e recebimento de dados;

- enlaces nó para nó: são normalmente multiplexados na forma FDM ou TDM;
- nós não-completamente conectados, ou seja, não existe um enlace direto entre todos os possíveis pares de nós. Por outro lado, é sempre possível ter mais de um caminho através da rede entre pares de estações aumentando a confiabilidade da rede.

Duas tecnologias diferentes são utilizadas nas redes de longa distância comutadas: comutação por circuito e comutação por pacotes. Estas duas tecnologias diferem basicamente na forma como comutam a informação, entre um enlace de entrada e um enlace de saída, na rota interconectando a origem e o destino da informação.

3.5 Redes Comutadas por Circuito

As redes baseadas na comunicação por circuitos são caracterizadas pela alocação de um caminho dedicado para comunicação entre duas estações. Este caminho é composto pela concatenação de canais multiplexados nos vários enlaces entre os nós da rede de comunicação. A comutação de circuitos possui 3 fases bem definidas na sua utilização:

- estabelecimento do circuito: antes da troca de informações é necessário o estabelecimento de um circuito fim a fim entre as estações participantes da comunicação. Este estabelecimento do circuito é realizado pelos procedimentos de sinalização de forma semelhante, por exemplo, quando iniciamos uma ligação telefônica. Suponhamos, por exemplo, que a estação B solicite à rede o estabelecimento de um circuito com a estação F. Para tal, ela deve especificar o endereço de F para que a rede tenha condições de encaminhar o pedido de sinalização e, eventualmente, especificar algum requisito de qualidade para o circuito a ser estabelecido. Como o enlace entre a estação B e o nó 1 é um enlace dedicado esta parte da conexão já existe. O nó 1, baseado no endereço da estação F, analisa o pedido e considerando as informações de roteamento, de qualidade e, eventualmente, custos decide por encaminhar o pedido do estabelecimento do circuito na direção do nó de rede 6. Este procedimento se desenrola da mesma forma até alcançar o nó de rede 6 que envia a sinalização para a estação C para que esta decida se aceita ou não o pedido de estabelecimento de um circuito solicitado por B. Este ponto corresponde ao instante em que o telefone do número chamado soa a sua campanhia e a pessoa naquele local atende o telefone;

- após o recebimento da confirmação, por parte da estação B, indicando que a estação F aceitou o pedido de estabelecimento de circuito, inicia-se a fase de troca de informações. Em geral a conexão estabelecida é full-duplex;

- após um período de transferência de dados uma das duas estações decide encerrar a conexão. Isto é feito também por um procedimento de sinalização que percorre os elementos de rede que fazem parte do circuito indicando que os recursos associados à conexão podem ser liberados devido ao seu encerramento.

A comutação por circuito tem o potencial de tornar-se ineficiente caso nenhum dado seja transferido no canal alocado à conexão. Do ponto de vista do desempenho, existe um atraso devido aos procedimentos de sinalização quando do estabelecimento do circuito mas, por outro lado, após o circuito estabelecido a informação é transmitida em uma taxa constante e os atrasos devem-se somente aos de propagação nos enlaces dado que os atrasos que ocorrem no interior dos nós de comutação são desprezíveis.

O exemplo mais típico da comutação de circuitos é representado pela rede pública de telefonia rede esta concebida para transporte do sinal de voz. Deve ser destacado que a comutação por circuitos é a solução adequada no transporte de tráfego como a voz, em função da componente temporal associado ao dado. Na medida em que a comutação por circuito aloca recursos dedicados ao canal não há risco de que a informação de voz se degrade em função, por exemplo, de atrasos ou variações do atraso (jitter) imprevisíveis. O grande atrativo da comutação por circuitos é o fato que, após o seu estabelecimento,tem-se uma ligação direta entre as estações.

3.6 Técnicas de Comutação de Pacotes

Existem duas técnicas básicas de comutação de pacotes: datagrama e circuito virtual. No caso de datagramas, cada pacote é tratado independentemente sem qualquer relação com os pacotes que anteriormente passaram pelo comutador. A característica básica da comutação baseada no conceito de datagramas é que pacotes endereçados por uma estação a uma mesma estação destino podem percorrer caminhos (rotas) diferentes dentro da rede até alcançarem o destino comum. Como consequência deste fato é possível que os pacotes cheguem no destino em uma ordem diferente daquela em que foram enviados pela origem, ou seja, os pacotes 1 e 2 enviados nesta ordem pela estação A para a estação B, podem ser recebidos por esta última na ordem inversa pois em função do estado da rede podem ter percorrido rotas diferentes o que faz o pacote 1 atrasar-se com relação ao pacote 2. Neste tipo de técnica os pacotes tratados de forma independente são denominados de datagrama.

Na abordagem baseada em circuito virtual há o estabelecimento inicial de uma rota antes do envio de pacotes. No caso do exemplo anterior a estação, antes de enviar os pacotes 1 e 2 para a estação B, irá solicitar à rede, através dos procedimentos de sinalização, o estabelecimento de uma conexão com a estação B. Uma mensagem do tipo Call-Request irá percorrer a rede através de uma determinada rota até alcançar a estação B que irá reponder indicando se aceita ou não o estabelecimento da conexão solicitada. Em caso positivo, B irá enviar uma mensagem do tipo Call-Accept que percorrerá, no sentido contrário, a mesma rota percorrida pela mensagem de sinalização Call-Request. Ao fazer este caminho de volta até alcançar A a mensagem de sinalização Call-Accept consolida a conexão e ao ser recebida pela estação A a conexão está apta a ser utilizada para a troca de informações. A partir deste momento as estações A e B irão trocar informações naquela conexão e os pacotes irão percorrer a mesma rota definida quando do estabelecimento da conexão. Como a rota é fixa durante a duração da conexão ela é similar ao conceito de circuito nas redes comutadas por circuito que discutimos anteriormente. Devido a este

fato a conexão é referida como circuito virtual isto porque, diferentemente da comutação de circuito, não existe o estabelecimento de um circuito físico entre as estações. Cada nó situado na rota estabelecida conhece como encaminhar os pacotes não havendo mais a necessidade de tomar decisões de roteamento. Nota-se aqui a difereça da técnica baseada em datagramas onde, para cada pacote enviado de A para B, uma decisão de roteamento dever ser tomada.

Por decisão de uma das estações envolvidas na conexão, uma mensagem de sinalização do tipo *Clear-Request* é enviada à rede encerrando a conexão. Deve ser observado que uma estação pode possuir, em qualquer instante, mais de uma conexão virtual com outra estação, bem como possuir circuitos virtuais com mais de uma estação.

Podemos sintetizar esta discussão afirmando que a maior característica da técnica baseada em circuito virtual é o fato de que uma rota é estabelecida entre as estações antes da transferência de informações.

Ao compararmos as duas técnicas temos, do lado da comutação baseada em circuito virtual, as vantagens de uma maior eficiência na fase de troca de informação porque não há necessidade de tomar decisões de roteamento, e a garantia de que os pacotes serão entregues corretamente e na ordem em que foram enviados, condições estas básicas para que os circuitos virtuais emulem adequadamente circuitos reais. A desvantagem relaciona-se à necessidade da sinalização para o estabelecimento da conexão e ao desperdício de recursos caso o circuito tenha baixa taxa de utilização. Desta forma a técnica de circuitos virtuais é interessante para o caso de duas estações que irão trocar dados continuamente durante um período de tempo relativamente longo.

Na mesma linha de argumentação, uma vantagem do mecanismo de datagrama é o fato de não ser necessária a fase de estabelecimento de conexão o que agiliza o envio dos pacotes já que não sofrem o atraso da sinalização. Um aspecto importante do datagrama é que, em se tratando de uma tecnologia mais primitiva do que a de circuito virtual, ela é mais flexível. Uma ilustração típica desta flexibilidade é quando a rede tem problemas de congestionamento. Neste caso, o mecanismo de datagrama permite que os pacotes sejam roteados para outras partes da rede que não estejam sofrendo do problema o que não é possível no caso do circuito virtual onde a rota não se altera.

3.7 Arquitetura dos Comutadores

A arquitetura geral de um comutador é mostrada na figura 3.11.

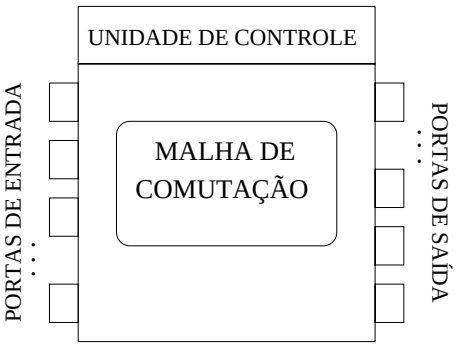


Figura 3.11: Estrutura Típica de um Comutador

A unidade de controle tem como função estabelecer, manter e encerrar a conexão. A malha de comutação é responsável pelo encaminhamento da informação internamente ao comutador. O projeto da malha de comutação é fundamental e pode apresentar 2 dois tipos básicos de arquitetura: comutação por divisão do espaço ou comutação por divisão do tempo. Inicialmente a comutação de circuito era projetada como uma conexão elétrica direta entre dois componentes

3.7.1 Comutação por Divisão Espacial

Esta arquitetura de comutador foi desenvolvida originalmente para o ambiente analógico. No caso, os caminhos dos sinais são fisicamente separados uns dos outros. Para cada conexão é necessário o estabelecimento de um caminho dedicado para transferência entre os dois pontos. A estrutura clássica deste tipo de comutador é representada por uma matriz completamente interconectada entre as portas de entrada e de saída. Os pontos de interconexão entre as portas de entrada e saída podem ser habilitadas ou desabilitadas pela unidade de controle criando, desta forma, um caminho entre uma porta de entrada e uma porta de saída. A figura 3.12 ilustra uma matriz com 10 entradas e 10 saídas e 100 pontos de interconexão. As maiores restrições desta arquitetura são o número de pontos de cruzamento que cresce com o produto do número de interfaces de entrada e de saída o que torna inviável o custo de comutadores de grande porte, a perda de qualquer possibilidade de estabelecimento de circuito entre dois pontos caso ocorra a quebra de um ponto de cruzamento e, por último, a utilização ineficiente do comutador pois mesmo quando todos os dispositivos estão ativos somente uma parcela de pontos de cruzamento estão engajados no estabelecimento dos circuitos.

Uma forma de contornar as restrições anteriores consiste na utilização de múltiplos

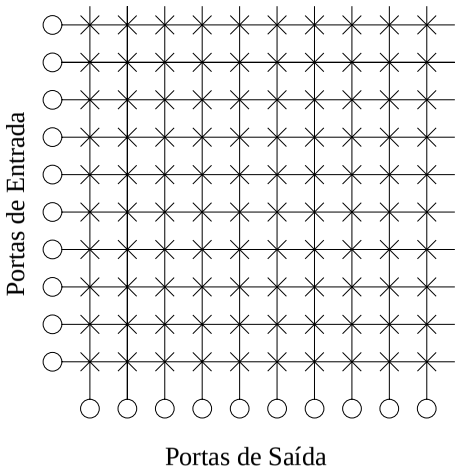


Figura 3.12: Estrutura da Matriz *Crossbar*

estágios de comutação conforme mostrado na figura 3.13 onde são utilizados 3 estágios.

As grandes vantagens da utilização de múltiplos estágios consistem na redução do número de pontos de cruzamento necessários. No caso da figura, para as mesmas 10 entradas e 10 saídas são utilizados 48 pontos de cruzamento, e a disponibilidade de mais de um caminho entre dois pontos o que aumenta a confiabilidade do dispositivo. O aspecto negativo consiste na maior complexidade da unidade de controle em função que, no caso de múltiplos estágios, é necessário determinar um caminho livre, habilitando-se as portas nos respectivos pontos de cruzamento. Uma análise do comutador de um único estágio mostra que se trata de uma estrutura não bloqueante para o encaminhamento interno da informação porque sempre existe um caminho livre para interligar uma porta de entrada a uma porta de saída. Por outro lado, a arquitetura com vários estágios é bloqueante, ou seja, um caminho estabelecido internamente pode impedir que novos caminhos se formem até o seu encerramento.

3.7.2 Comutação por Divisão do Tempo

O projeto dos comutadores sofreu alterações profundas no projeto e tecnologia devido às técnicas mais recentes de multiplexação por divisão do tempo dos sinais digitais, tanto de dados analógicos como de dados digitais. No lugar das arquiteturas anteriores baseadas na comutação espacial, novos sistemas de comutação surgiram baseados em um controle mais sofisticado da divisão espacial e temporal. Os comutadores de circuito atuais utilizam técnicas de divisão do tempo para o estabelecimento e manutenção de circuitos. Os *slots*

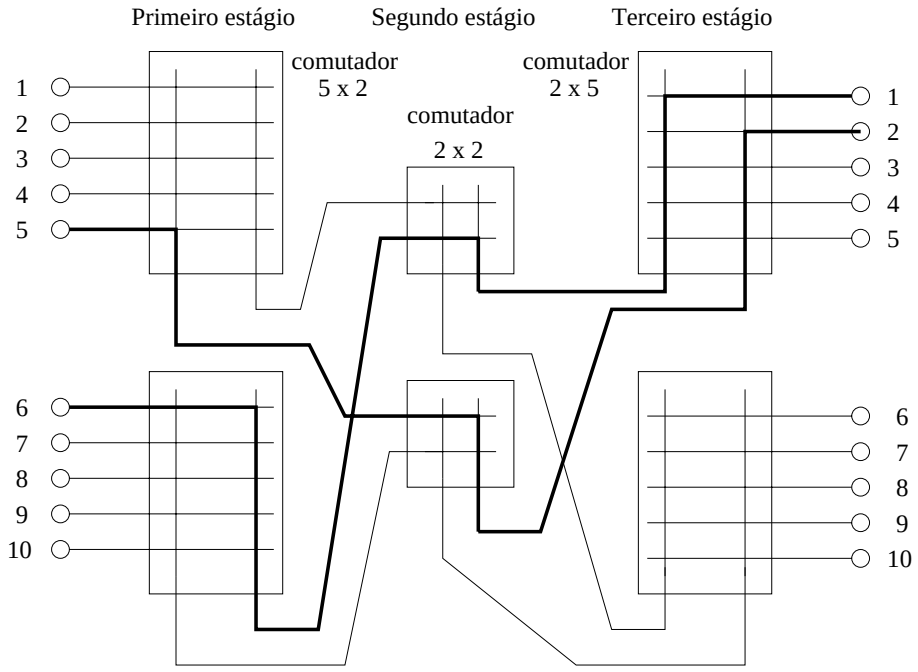


Figura 3.13: Arquitetura de Comutador Multiestágio

são alocados pela unidade de controle no roteamento dos dados da entrada para a saída correspondente. Esta abordagem possui uma série ampla de variações. Dentre as mais simples encontra-se a arquitetura baseada em barramento.

3.8 Comutação por Pacotes

O conceito de comutação de mensagens e posteriormente o de comutação por pacotes surgiram para atender especificamente o tráfego de dados. Neste caso as estações envolvidas na comunicação não possuem uma conexão física direta como aquela estabelecida na comutação de circuitos. As mensagens são transmitidas ao comutador onde ela é armazenado em uma fila para ser posteriormente encaminhada. A expressão *store-and-forward* é associada a esta forma de operação baseada na comutação de mensagens. Ao receber a mensagem o comutador examina o seu cabeçalho, decodifica o endereço de destino e roteia a mensagem na interface de saída apropriada no sentido de avançar na direção onde encontra-se a estação destino. Deve ser observado que é possível que o próximo enlace no qual a mensagem vai ser enviada pode encontrar-se ocupado pela transmissão de uma outra mensagem, ou ainda, outras mensagens já podem estar esperando para serem

transmitidas no mesmo caminho.

Algumas considerações importantes podem ser feitas relativamente à comutação de mensagens: 1) possibilidade de acomodar múltiplas velocidades de linha. Duas estações com taxas de dados diferentes podem trocar pacotes porque cada uma delas conecta-se ao seu nó de rede na sua própria taxa de dados; 2) possibilidade de difusão (*broadcast*) da mensagem para todos as estações ou um subconjunto dos estações; 3) possibilidade de atribuição de prioridades às mensagens permitindo um tratamento diferenciado para tráfegos diferenciados; 4) mecanismos para deteção e recuperação de erros; 5) melhor aproveitamento dos enlaces físicos entre os nós da rede pois os canais podem ser compartilhados por várias mensagens já que não existe uma alocação fixa de canais para mensagens específicas, ou seja, as mensagens são transmitidas em função da demanda; 6) as mensagens são sempre aceitas mesmo que não existam recursos disponíveis no momento como, por exemplo, capacidade de transmissão suficiente. O que acontece neste caso é que as mensagens ficarão mais tempo armazenadas nos comutadores aumentando os tempos de transferência; 7) as mensagens possuem tamanho variável. Esta característica tem o inconveniente de que uma mensagem muito longa possa monopolizar os enlaces por muito tempo.

Uma diferença fundamental entre a comutação de circuitos e a comutação de mensagens é que no, caso da primeira, o endereço é importante quando do estabelecimento do circuito mas, após o circuito ter-se estabelecido, as informações são trocadas sem a necessidade de examinar endereços pois o caminho já está montado. No caso das mensagens elas são, em geral, tratadas individualmente e as decisões de encaminhamento da mensagem são tomadas de forma independente em cada nó da rede à medida que a mensagem avança.

A comutação de pacotes é muito semelhante à comutação de mensagens com a diferença inicial que os pacotes tem um tamanho máximo. Caso uma mensagem tenha tamanho superior a este tamanho máximo, a mensagem deve ser segmentada em unidades menores denominadas de pacotes. A comutação de pacotes significa comutadores com menor capacidade de armazenamento e os procedimentos para recuperação de erros são mais eficientes do que no caso da comutação de mensagens.

Capítulo 4

Controle do Enlace de Dados

O controle do enlace de dados é responsável pela detecção e recuperação de erros ocorridos na transmissão de dados, obtendo-se com isto uma comunicação de dados mais confiável. Denomina-se enlace uma conexão virtual por onde fluem segmentos de dados denominados quadros de enlace. Esta conexão implementa protocolos simples de detecção e recuperação de erros, por exemplo detecção através de *checksum* e recuperação por retransmissão. Protocolos de enlace segmentam os dados que transmitem em *quadros* e, via de regra, implementam as seguintes funcionalidades:

- detecção de quadros corrompidos por erros de transmissão;
- recuperação de quadros corrompidos;
- estabelecimento e gerenciamento de conexões virtuais;
- controle do fluxo de quadros.

4.1 Montagem de Quadros

Na montagem de quadros, a delimitação dos mesmos merece alguns comentários. Caso os quadros sejam compostos exclusivamente de caracteres (o que é raro na atualidade) pode-se definir caracteres especiais para a delimitação de quadros. Por exemplo, o código ASCII reserva alguns códigos especiais para delimitação de blocos de dados como o *Data Link Escape* (DLE), o *Start of Text* (STX) e o *End of Text* (ETX). Assim, um quadro pode ser delimitado por:

```
DLE STX ... <texto em ASCII> ... DLE ETX
```

Os caracteres DLE, STX e ETX não ocorrem no interior do texto, pois são caracteres de controle.

Atualmente, os dados que compõem o quadro são sequências arbitrárias de bits (números, segmentos de memória, etc) que não podem ser representados como sequência de caracteres (texto). Nestes casos, duas técnicas são bastante empregadas: enchimento de bits (*bit stuffing*) e violação de códigos da camada física.

Na técnica baseada em enchimento de bits escolhe-se um delimitador de ínicio de quadro (por exemplo 01111110) e previne-se de sua ocorrência nos dados com uma regra simples como: *A cada ocorrência de cinco 1s adiciona-se um 0.* O receptor do quadro executa procedimento inverso na recepção. A figura 4.1 ilustra este procedimento.

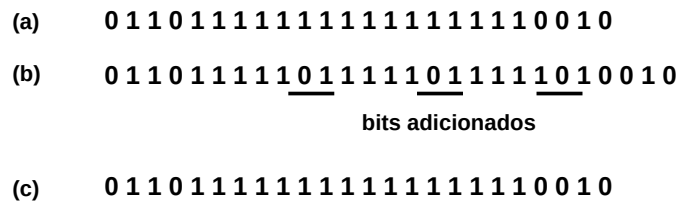


Figura 4.1: Enchimento de bits: (a) dados originais, (b) dados no quadro, (c) dados decodificados pelo receptor.

Na técnica baseada em violação de códigos da camada física delimita-se o quadro com códigos inválidos empregados pela camada física [1]. Dado que tais códigos jamais ocorrem na codificação de 0s e 1s, sua detecção indica o início ou o final de quadros. No código Manchester Diferencial (empregado pelo 802.5) utiliza-se transições positivas (H) seguidas de negativas (L): HHLLHHLL. Na modulação FSK-coerente (empregada no 802.4), pode-se misturar frequências altas e baixas num mesmo período do bit, gerando assim um código inválido (figura 4.2).

[1] A rigor, quem gera os quadros inválidos é a camada física.

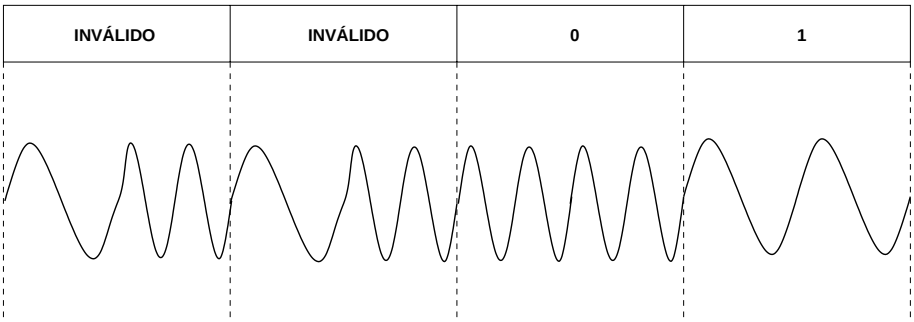


Figura 4.2: Exemplo de modulação FSK-coerente com códigos inválidos.

4.2 Detecção de Erros

A técnica mais usual para detecção de erros[2] durante a transmissão de quadros é a *Redundância Cíclica* (CRC). Esta técnica não utiliza bits de redundância o suficiente para correção do erro. Via de regra, detectado que um quadro chegou com erro, o receptor solicita ao emissor sua retransmissão. Em redes de computadores, a retransmissão é a técnica mais usual de correção (recuperação) de erros.

A técnica CRC é similar aos *dígitos de controle* presentes no CPF, contas bancárias, etc. O dígito de controle é computado por uma sequência de operações bem definida na origem e transmitido ao destino que o recomputa. Em havendo diferença entre os valores transmitido e computado, conclui-se sobre a invalidade do dado transmitido.

Na técnica CRC pode-se imaginar que os bits do quadro formam um (gigantesco !) número inteiro. Se o quadro é composto por k bits (numerados de 0 a k-1), este número é dado pelo polinômio:

$$P(x) = b(k-1).x^{k-1} + b(k-2).x^{k-2} + ...b(1).x + b(0)$$

onde b(j) é o valor do bit na posição j (0 ou 1) e x é a base da representação (2). Por exemplo, a sequência de 10 bits 1101011011 é representada pelo polinômio $x^9 + x^8 + x^6 + x^4 + x^3 + x + 1$.

A técnica CRC reserva um número arbitrário de bits (n) para detecção de erros *(checksum)*. Assim, são transmitidos n+k bits, sendo k de informação seguidos de n bits de *checksum*. Os n bits de *checksum* são computados de forma que os n+k bits do quadro sejam representados por um polinômio $F(x).P(x)$, sendo $F(x)$ de ordem n.

[2]Erro neste contexto é a inversão do valor de um ou mais bits. Inversões de N bits em sequência é denominada *erro de rajada de comprimento N*.

Seja um polinômio de referência, $G(x)$ de ordem n (denominado *polinômio gerador*). Podemos escrever a seguinte igualdade:

$$F(x).P(x) = Q(x).G(x) + R(x)$$

onde Q(x) é de ordem k-1 e R(x) de ordem n-1.

Na técnica CRC escolhe-se $F(x) = x^n$ e computa-se $R(x)$ dividindo-se os inteiros (não os polinômios !) $F(x).P(x)$ por $Q(x)$. Neste caso, $R(x)$ formará os bits de *checksum*.

As operações são feitas em aritmética módulo 2 (sem o "vai 1"):

Adição	Subtração	Multiplic.	Divisão
0 + 0 = 0	0 - 0 = 0	0 x 0 = 0	0 ÷ 1 = 0
0 + 1 = 1	0 - 1 = 1	0 x 1 = 0	1 ÷ 1 = 1
1 + 0 = 1	1 - 0 = 1	1 x 0 = 0	
1 + 1 = 0	1 - 1 = 0	1 x 1 = 1	

Em aritmética módulo 2, pode-se escrever

$$F(x).P(x) = Q(x).G(x) + R(x)$$

como

$$F(x).P(x) + R(x) = Q(x).G(x)$$

Como $F(x) = x^n$ o lado esquerdo da igualdade acima representa os bits originais acrescidos dos bits referentes a R(x) a direita.

No exemplo da sequência 1101011011, considerando-se $n = 4$ (4 bits de *checksum*) e tomando-se o polinômio gerador: $G(x) = x^4 + x + 1$ temos

$$Q(x) = x^9 + x^8 + x^3 + x$$

$$R(x) = x^3 + x^2 + x$$

A figura 4.3 ilustra as operações, que nas implementações práticas são efetuadas por hardware.

Asssim os bits 1101011011 são transmitidos com quatro bits adicionais: 1101011011-1110

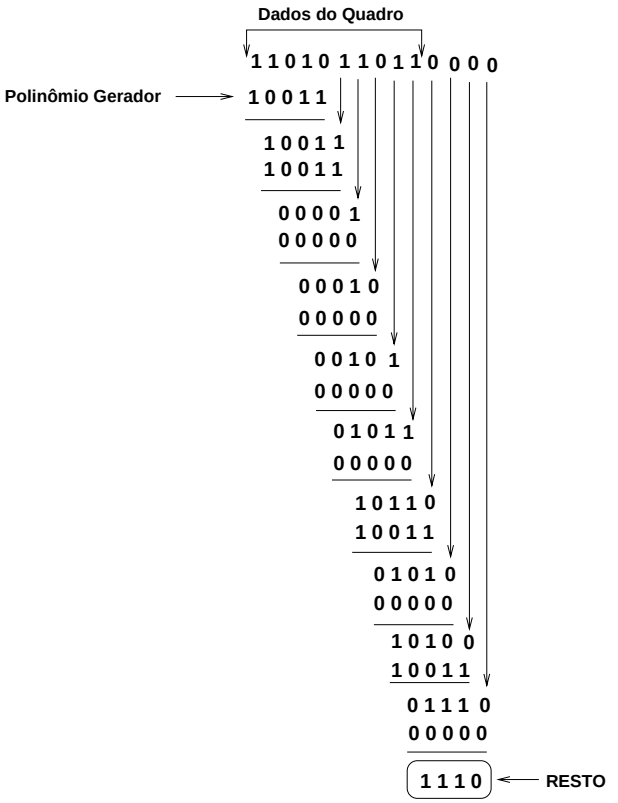


Figura 4.3: Exemplo do cômputo do *checksum*.

Tanto a ITU-T como o IEEE padronizaram polinômios geradores para o cômputo de *checksum*.

$CCR-16 : x^{16} + x^{15} + x^2 + 1$

$CCR-CCITT : x^{16} + x^{12} + x^5 + 1$

$IEEE-802.2 : x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

Os polinomios CCR-16 e CCR-CCITT, para 16 bits de *checksum* são capazes de detectar:

- inversões de 1 ou 2 bits;
- inversões de um número ímpar de bits;
- rajadas de comprimento menor ou igual a 16;

- 99,997% das rajadas de comprimento 17;
- 99,998% das rajadas de comprimento 18.

4.3 Técnicas de Recuperação de Erros por Retransmissão

As técnicas mais usuais de recuperação de erros por retransmissão são baseadas em reconhecimento.

Reconhecimento Positivo

Neste método, ao transmitir um quadro, o emissor aguarda outro de reconhecimento por parte do receptor, caso o primeiro tenha sido recebido livre de erros. Recebido um quadro de reconhecimento, o emissor envia o próximo quadro e assim sucessivamente. Caso o receptor tenha detectado um erro (por exemplo, diferença entre o *checksum* computado e enviado), este simplesmente suprime o envio do reconhecimento. Expirado o tempo de espera pelo reconhecimento, o emissor retransmite o quadro.

Reconhecimento Negativo

Neste método o receptor sempre transmite um quadro de reconhecimento imediatamente após a recepção de um quadro: reconhecimento positivo, caso nenhum erro tenha sido detectado, ou negativo, caso contrário. A recepção de um reconhecimento negativo faz o emissor retransmitir prontamente o quadro, sem a necessidade de espera como no método anterior.

Reconhecimento Contínuo

Os métodos de reconhecimento positivo e negativo apresentam dois inconvenientes:

1. duplicação de quadros: o receptor recebe quadros duplicados em duas situações:

quando o reconhecimento chegar após ter-se expirado seu tempo de espera; ou quando o reconhecimento é descartado na sua recepção devido a erros;

2. baixa eficiência: para cada quadro transmitido, circula outro de controle (reconhecimento) no sentido inverso.

O método de reconhecimento contínuo permite o emissor transmitir até N (largura da janela) quadros sem a necessidade de espera por reconhecimento. Cada quadro carrega dois contadores, N(S) e N(R), cujos valores dependem do tipo do quadro (de informação ou reconhecimento).

A figura 4.4 compara o reconhecimento contínuo com o reconhecimento negativo.

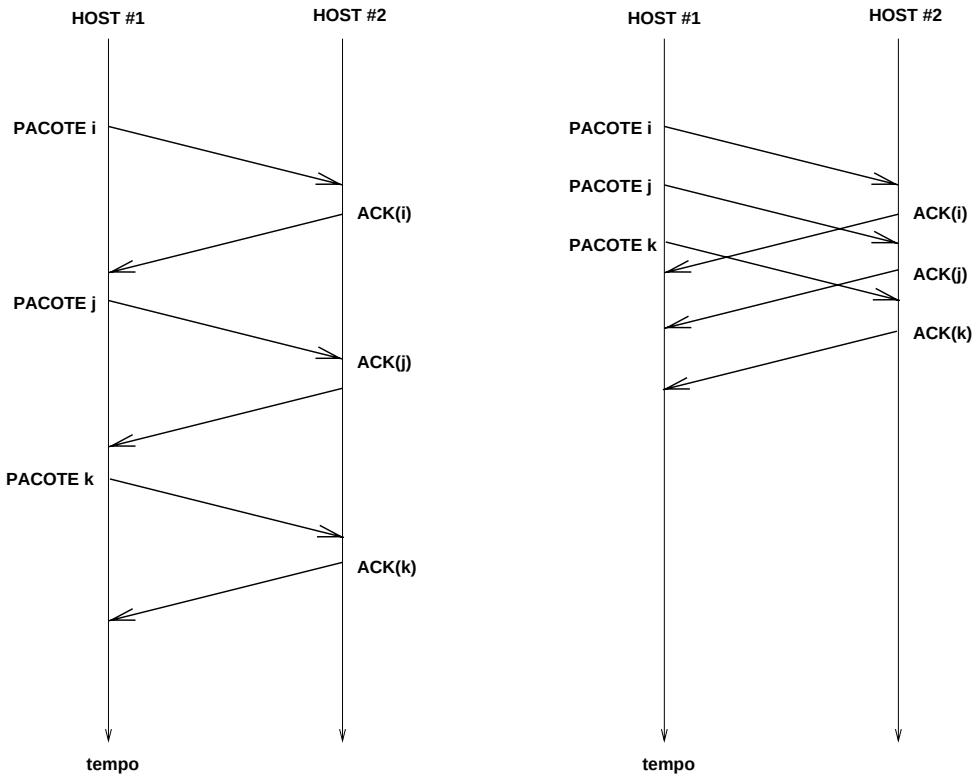


Figura 4.4: Reconhecimento negativo (esquerda) comparado com reconhecimento contínuo com janela de tamanho 3.

Nos quadros de informação (que fluem no sentido emissor-receptor), N(S) indica o número do quadro sendo transmitido e N(R) o número do próximo quadro esperado pelo emissor.

Nos quadros de reconhecimento, N(R) indica o próximo quadro sendo esperado (implicitamente os quadros numerados até N(R)-1 foram recebidos livres de erros). N(S) e N(R) ocupam poucos bits, tipicamente 3, sendo neste caso um contador em módulo 8. Isto justifica a introdução da janela em curso, permitindo maior segurança na identificação dos quadros.

O reconhecimento contínuo permite duas formas de operação quanto ao reconhecimento:

1. um quadro de reconhecimento para toda a janela;
2. quadros individuais de reconhecimeto.

No primeiro caso o emissor verifica se N(R) indica que a janela em curso se completou com sucesso. Neste caso, uma nova janela é iniciada com a transmissão dos próximos N quadros. Caso contrário, o emissor retransmite os quadros a partir de N(R) até o último quadro da janela, aguardando novo reconhecimento. Esta técnica reduz considravelmente os quadros de reconhecimento, aumentando a eficiência do enlace.

No segundo caso (figura 4.4) o transmissor *desliza* (avança) a janela a cada quadro de reconhecimento recebido. Como para cada quadro de dado existe um de reconhecimento, a janela desliza continuamente, o que não ocorre no primeiro caso. Esta técnica minimiza as retransmissões, sendo atrativa para enlaces sujeitos a altas taxas de erro.

Quadros duplicados podem ainda ocorrer (por exemplo, quando um quadro de reconhecimento é corrompido), mas sua detecção é simples, posto que os quadros são identificados um a um.

4.4 Formas de Estabelecimento do Enlace

O enlace (conexão virtual) pode se dar entre duas estações ou emanando de uma estação para várias outras. No primeiro caso o enlace é dito *ponto-a-ponto*, enquanto no segundo tem-se um enlace *multiponto*. Um enlace ponto-a-ponto ocorre, por exemplo, quando duas estações se conectam para efetuar a transferência de um arquivo. Exemplo de enlace multiponto é um computador central controlando vários terminais dispersos geograficamente.

Podemos identificar três tipos de estações quanto suas responsabilidades pelo enlace:

1. estações primárias: controlam totalmente o enlace;
2. estações secundárias: recebem comandos da primária, podendo transmitir pelo enlace somente quando autorizadas por esta;
3. estações combinadas: atuam de forma dual, ora como primária ora como secundária, dependendo do contexto.

Enlaces ponto-a-ponto são constituídos tipicamente por duas estações combinadas, enquanto enlaces multiponto são formados por uma primária e várias secundárias.

Um enlace pode ser estabelecido para operar em um dos três modos abaixo:

1. modo de resposta normal: a estação primária envia um quadro de consulta para as suas secundárias inquirindo sobre a existência de quadros para transmitir; em caso positivo, a secundária transmite imediatamente após ter recebido o quadro de consulta;
2. modo de resposta assíncrono: as estações secundárias transmitem independentemente da consulta por parte da primária; este modo é geralmente empregado quando as estações secundárias se conectam à primária por canais exclusivos (por exemplo, linhas seriais); este modo não é empregado em redes de computadores;
3. modo de resposta assíncrono balanceado: utilizado em enlaces ponto-a-ponto envolvendo apenas estações combinadas; as estações gerenciam o enlace de acordo com um protocolo definido pelas camadas de enlace das estações comunicantes.

Finalmente, um enlace é governado por um protocolo composto de quatro fases:

1. estabelecimento do enlace, onde uma estação toma a iniciativa do estabelecimento de uma conexão virtual com uma ou mais estações;
2. transferência de dados, onde as estações que compõem a conexão trocam quadros de informação através desta;
3. encerramento do enlace, onde uma da estações toma a iniciativa de propor o encerramento da conexão;
4. reiniciação do enlace, onde uma estação toma a iniciativa de reinicializar o protocolo de transferência de quadros pelo enlace pela ocorrência de um erro irrecuperável.

4.5 Controle do Fluxo de Quadros

O controle de fluxo é necessário quando um receptor de quadros vê-se na impossibilidade momentânea de continuar a recepção. Várias são as razões para isso ocorrer: exaustão de buffers, ocorrência de erros internos de hardware ou software, atendimento de atividades de comunicação mais prioritárias, etc.

Em protocolos baseados no reconhecimento positivo ou negativo, o controle do fluxo é desnecessário, pois o emissor só envia o próximo quadro após o recebimento do reconhecimento do receptor. Caso o receptor deseje a suspensão temporária do envio de quadros, este simplesmente deixa de enviar os quadros de reconhecimento.

Em protocolos que empregam o reconhecimento contínuo, dois quadros de controle são empregados para o controle de fluxo:

- quadros RR (Receiver Ready): informa o emissor que o receptor está pronto para iniciar ou continuar a recepção de quadros;
- quadros RNR (Receiver Not Ready): informa o emissor que o receptor está impossibilitado temporariamente de receber quadros.

Os quadros RR e RNR visam aumentar a eficiência do canal compartilhado evitando a circulação de quadros de dados que com certeza serão descartados pelo receptor.

4.6 O Protocolo de Enlace HDLC

O protocolo HDLC (High-level Data Link Control) é padronizado pela ISO, servindo de base para o X.25/camada 2 que emprega um subconjunto denominado LAPB (Link Access Procedure, Balanced)[3].

No HDLC, os quadros têm o formato apresentado na figura 4.5. O quadro possui um delimitador de início e final composto dos bits 01111110. Um procedimento de codificação de bits é empregado para evitar a ocorrência desta sequência no quadro. O campo de endereço é utilizado em conexões multiponto para identificar as estações secundárias da

[3]O LAPB restringe o HDLC por permitir apenas enlace no modo de resposta assíncrono balanceado - ver subseção 4.4.

conexão. Em conexões ponto-a-ponto este campo é utilizado para distinguir quadros de comandos dos de resposta.

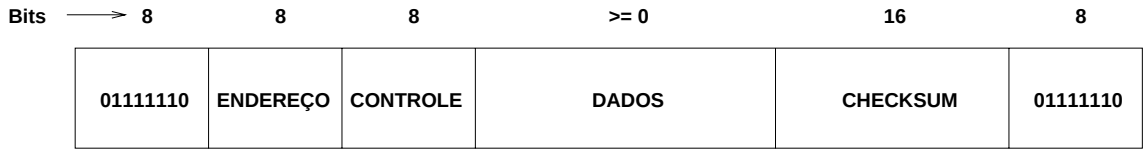


Figura 4.5: Formato do quadro no protocolo HDLC.

O campo de dados possui tamanho arbitrário, mas normalmente limitado por restrições impostas pela camada física.

O campo de *checksum* é computado pelo polinômio gerador $x^{16} + x^{12} + x^5 + 1$.

O campo de controle define três tipos de quadros: de informação (I), de supervisão (S) e não numerados (N), sendo os dois últimos quadros de controle (figura 4.6).

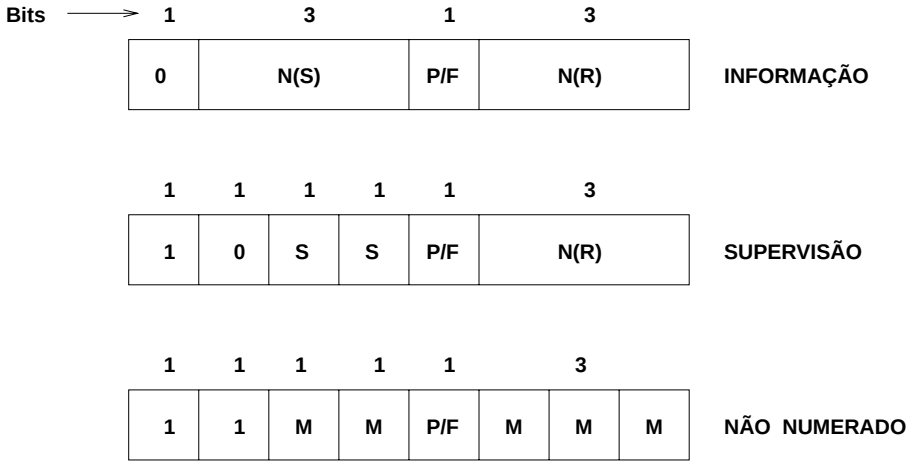


Figura 4.6: Formatos do campo de controle no protocolo HDLC.

Os quadros de informação carregam os contadores N(S) e N(R) para reconhecimento contínuo do fluxo de quadros.

Os quadros de supervisão são empregados no controle de fluxo e como reconhecimento da recepção de quadros. Três tipos instruções podem estar contidas no campo SS:

1. RR (Receiver Ready): informa que o receptor está pronto para continuar a recepção de quadros a partir de N(R), inclusive.

2. RNR (Receiver Not Ready): informa que o receptor reconhece o recebimento de todos os quadros até N(R)-1, e solicita a suspensão temporária do envio de novos quadros.

3. REJ (Reject): informa que o receptor detectou um erro na recepção do quadro N(R) e solicita o envio a partir deste.

Os quadros não numerados são utilizados para estabelecimento e término de conexões. Seis tipos de intruções são definidas:

1. SNRM (Set Normal Response Mode): estabelece uma conexão entre estação primária e secundária.

2. SABM (Set Asynchronous Balanced Mode): estabelece uma conexão entre estações combinadas.

3. DISC (Disconnect): informa o outro extremo da conexão que esta estação deseja terminar o enlace.

4. DM (Disconnect Mode): Informa que uma conexão solicitada não pode ser estabelecida (por exemplo, por falta de espaço para armazenar os parâmetros de controle da conexão).

5. UA (Unnumbered Acknowledgement): reconhece positivamente comandos de estabelecimento, término e reinicialização de conexão.

6. FRMR (Frame Reject): um quadro foi recebido com erro através da conexão e seu conteúdo não pôde ser identificado.

O bit P/F (Pool/Final) é ativado por uma estação primária quando em consulta a uma secundária. Caso tenha quadros para transmitir, a estação secundária o faz com o bit P/F ativado, até o último quadro onde o bit P/F é desativado, indicando o final da transmissão.

Capítulo 5

Redes de Computadores

5.1 Conceitos Básicos

Definiremos **Rede de Computadores** como um conjunto de computadores *autônomos* e *interconectados*. O termo *autônomo* exclui arranjos de processadores que apresentam relação mestre/escravo ou disponham de um controle centralizado como os multiprocessadores, as máquinas *data flow* e os *array processors*. Numa rede, nenhum computador obedece a comandos de outro, possuindo inclusive autonomia para se desconectar da rede.

Os meios de interconexão são muitos: cabos de cobre, fibras óticas, rotas de microondas, radiodifusão, etc. Atualmente, os cabos de cobre (coaxiais e pares trançados) são os mais empregados, devendo a fibra ótica assumir este papel num futuro próximo. Os meios de interconexão limitam tanto a taxa de transmissão de informação quanto a extensão geográfica da rede. Quanto a sua extensão geográfica, as redes se classificam em:

1. Redes Locais (LAN: Local Area Network): interconectam computadores localizados numa mesma sala ou edifício (10 m - 1 Km). Tipicamente, um único meio de transmissão é empregado.
2. Redes de Campus (CAN: Campus Area Network): interconectam computadores a nível de campus (fábrica, universidade, etc.) em extensões não superiores a 10 Km. Tipicamente são compostas de várias LANs interligadas por uma rede de alto desempenho (backbone).
3. Redes Metropolitanas (MAN: Metropolitan Area Network): interconectam computadores e LANs a nível regional (5 - 100 Km), usualmente empregando uma ou mais

redes de alto desempenho interconectadas.

4. Redes de Longa Distância (WAN: Wide Area Network): interconectam computadores e LANs a nível nacional ou continental (100 - 5000 Km). Via de regra são operadas por *holdings* nacionais de telecomunicações.

Uma rede é dita *homogênea* se todos os computadores por ela interconectados são idênticos. Caso contrário, temos uma rede *heterogênea*. Obviamente, redes heterogêneas demandam padronização tanto no nível de hardware (tensões, frequências, etc.) quanto no nível de software (por exemplo, representação de dados e formatação de mensagens).

O objetivo central de uma rede de computadores é o compartilhamento de informação e recursos. Outros benefícios importantes são:

- o crescimento gradual da capacidade de processamento da informação;
- a diversidade de equipamentos e a liberdade de escolha;
- o aumento da confiabilidade (via redundância);
- o processamento da informação *in loco*;
- um meio alternativo de comunicação social.

5.2 Topologias de Redes

Um computador conectado à rede é denominado *Host* ou *End System* (ES). Hosts são conectados por uma *subrede de comunicação*. Subredes carregam *mensagens* de um host para outro. Tipicamente, em redes locais, a subrede de comunicação se reduz a um duto elétrico ou ótico. Em redes de longa distância, a subrede de comunicação é composta de *linhas de transmissão* (ou *canais*) e *dispositivos de chaveamento* denominados roteadores ou ISs (Intermediate Systems). Roteadores são computadores especializados que conectam duas ou mais linhas de transmissão e/ou subredes de comunicação (figura 5.1).

Subredes de comunicação se dividem em dois grupos: ponto-a-ponto e de difusão (broadcast). Em subredes ponto-a-ponto os roteadores são conectados por linhas de transmissão, de sorte que apenas roteadores diretamente conectados se comunicam. Se uma mensagem necessita ser transmitida entre dois roteadores não conectados, a mesma deve

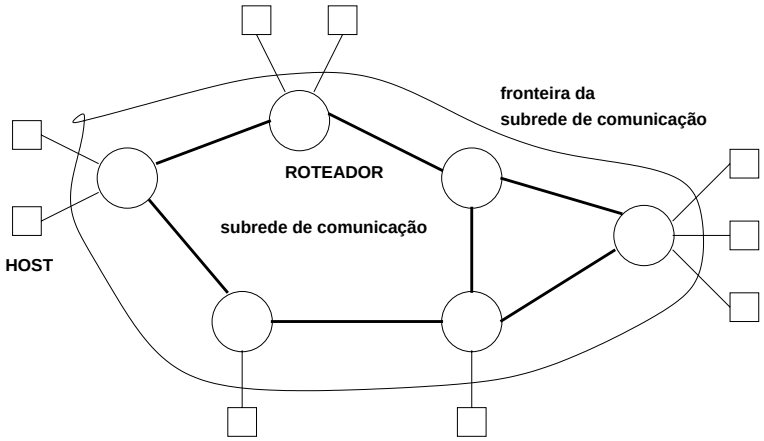


Figura 5.1: Hosts e roteadores numa subrede de comunicacão.

ser roteada através de outros roteadores. A figura 5.2 mostra as topologias típicas de subredes ponto-a-ponto.

Em subredes de difusão todos os hosts compartilham uma mesma linha de transmissão. Mensagens enviadas por um host são recebidas por todos os demais. Se o endereço de destino contido na mensagem for diferente do endereço do host que a recebeu, a mensagem é simplesmente descartada. A figura 5.3 mostra as topologias típicas de subredes de difusão.

5.3 O modelo OSI

O modelo OSI é composto das 7 camadas apresentadas na figura 5.4. O modelo OSI não é uma arquitetura, posto que não especifica os protocolos empregado pelas camadas. Entretanto, a ISO tem produzido protocolos para as 7 camadas, publicados como padrões internacionais.

A Camada Física

A camada física é a responsável pela geração dos sinais elétricos, óticos ou eletromagnéticos que serão propagados pelo meio físico. Protocolos nesta camada especificam qual a duração e intensidade do sinal, técnica de multiplexação, pinagem, etc. Obviamente esta

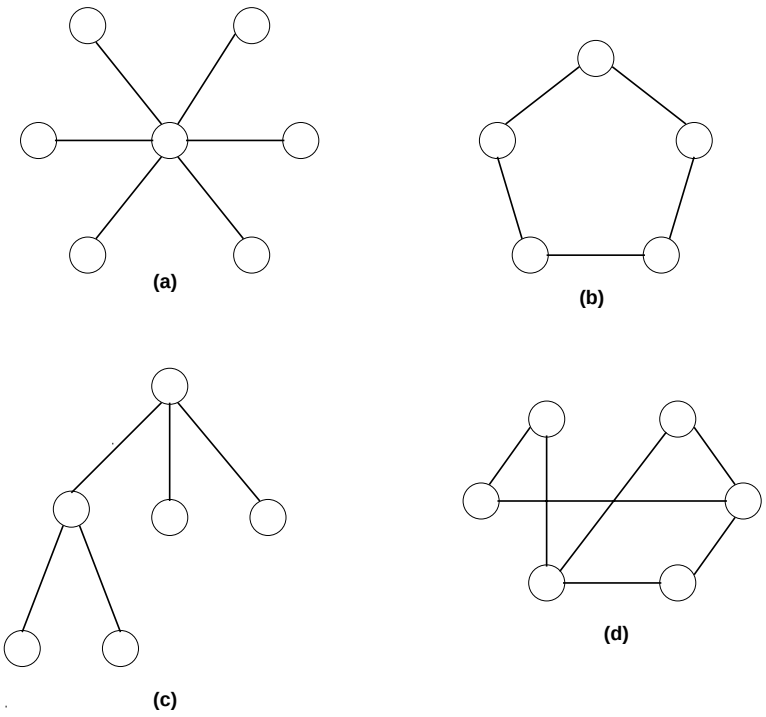


Figura 5.2: Topologias típicas em subredes ponto-a-ponto: (a) Estrela (b) Anel, (c) Árvore, (d) Genérica.

camada está intimamente relacionada ao meio físico empregado.

A Camada de Enlace

A camada de enlace é responsável pelo enlace de dados, conforme descrito no capítulo 4. Esta camada utiliza a camada física para a transmissão de quadros de enlace. A camada de enlace também controla o fluxo de quadros, evitando que um host envie quadros numa taxa superior a que o receptor é capaz de processar.

A Camada de Rede

A camada de rede controla a operação da subrede de comunicação. Uma de suas funções é o roteamento de *pacotes*[1] do host de origem ao host de destino. O roteamento pode

[1] A taxa de utilização de uma subrede é medida pelo fluxo de pacotes por unidade de tempo.

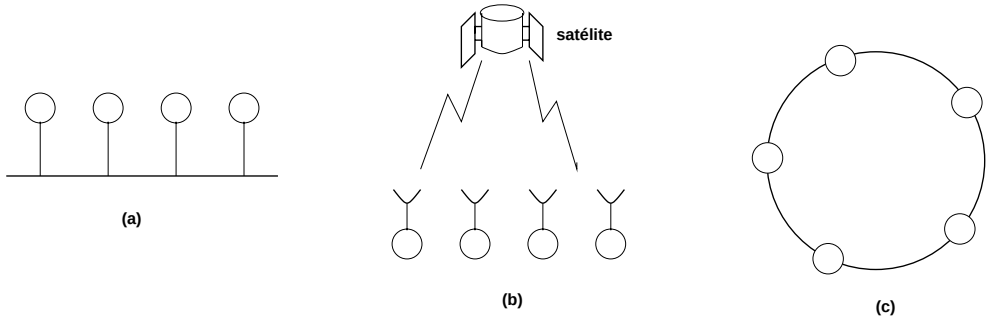


Figura 5.3: Topologias típicas em subredes de difusão: (a) Barramento (b) Radiodifusão, (c) Anel.

apresentar características dinâmicas, evitando gargalos em certos roteadores, ou estáticas, empregando-se sempre a mesma rota entre dois hosts.

Outra função desta camada é a fragmentação e remontagem de pacotes para atender a limites impostos por determinados segmentos da subrede de comunicação. Em subredes de difusão e redes locais esta camada é extremamente simples, dado que sua principal atribuição (roteamento) é inexistente nestas subredes.

A Camada de Transporte

A função principal da camada de transporte é receber dados da camada de sessão, particionar estes dados em unidades menores e, em certos casos, garantir que estas unidades cheguem a seu destino sem duplicação e na ordem correta.

Esta camada possui tipicamente dois tipos de serviços: um serviço rápido onde mensagens são limitadas em tamanho e não existe garantia de entrega, ordem ou ausência de duplicação; e um serviço mais lento, porém altamente confiável e sem limites de tamanho nas mensagens. Um terceiro serviço, difusão de mensagens para todos os hosts da subrede, pode estar disponível nesta camada.

No caso de serviço com entrega confiável, a camada de transporte é responsável pela remontagem dos quadros oriundos da camada de rede, respeitando a ordem em que foram enviados e descartando duplicações.

É função também desta camada o controle do fluxo de dados entre dois processos comunicantes (a camada de rede controla o fluxo apenas entre roteadores).

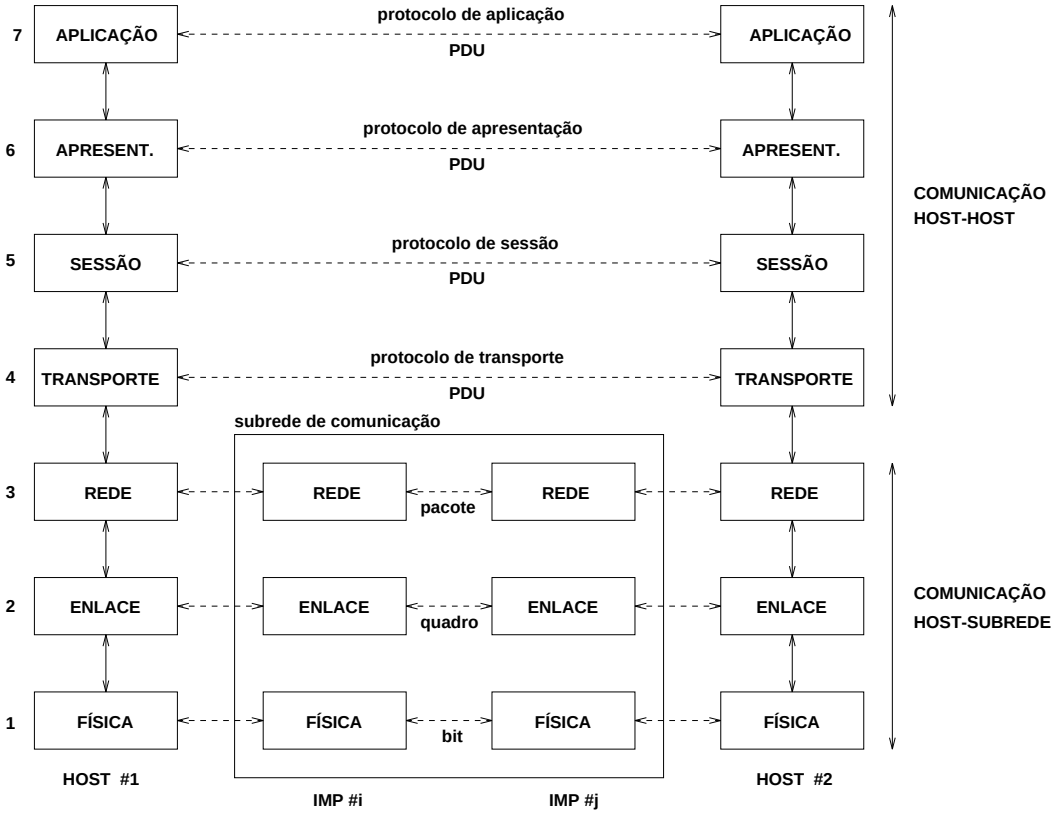


Figura 5.4: As sete camadas do modelo OSI.

As camadas anteriores (física, de enlace e de rede) são empregadas na comunicação roteador-roteador. A camada de transporte é a primeira a promover comunicação host-host (ver figura 5.4).

A Camada de Sessão

Esta camada permite dois processos de aplicação (APs: Application Processes) estabelecerem sessões entre si a fim de organizar e sincronizar a troca de informação. Para tal, uma *conexão de sessão* é estabelecida, definindo-se as regras de diálogo entre os dois APs. Existem três variantes de diálogo quanto ao sentido do fluxo de dados: TWS (Two Way Simultaneous): bidirecional simultaneamente, TWA (Two Way Alternate): bidirecional alternadamente (um por vez), e OW (One Way): unidirecional.

A Camada de Apresentação

Esta camada fornece serviços de representação canônica de dados, compressão de dados e criptografia. Uma representação canônica dos dados se faz necessária quando hosts de arquiteturas diferentes devem se comunicar. Por exemplo, a representação de números em ponto flutuante varia de arquitetura para arquitetura. Quando um *float* é transmitido, o mesmo é convertido para uma representação padronizada, enviado via rede, e reconvertido na representação adotada pelo host de destino. A camada de apresentação dispõe de um protocolo para tal (EDR: External Data Representation).

Compressão de dados é útil para o envio de grandes massas de dados como imagens e textos. Criptografia é utilizada quando os dados a serem transmitidos são confidenciais e visa evitar sua interceptação em trânsito por pessoas não autorizadas. Protocolos para compressão e criptografia de dados também são definidos nesta camada.

A Camada de Aplicação

Esta camada dispõe de serviços comumente utilizados por usuários de redes. Correio eletrônico, transferência de arquivos, *login* remoto, serviços de diretório e submissão de *jobs* remotos são exemplos destes serviços.

Esta camada também se constitui no ponto de acesso à rede por processos de aplicação (APs). Estão em vias de padronização as chamadas APIs (Application Program Interfaces), que são bibliotecas de funções para envio/recepção de mensagens, estabelecimento de conexões, etc.

A figura 5.5 ilustra uma pilha de protocolos OSI implementados na rede DECnet Fase V ou DECnet/OSI da Digital Equipment Corporation (DEC).

O nível físico implementa as interfaces RS-232-C, RS-422, RS-423, V.35 e redes Ethernet, Token Ring e FDDI.

O nível de enlace implementa os protocolos HDLC/LAPB utilizados no X.25 e 802.2 (LLC) utilizados nas LANs Ethernet, Token Ring e FDDI.

O nível de rede implementa os protocolos de rede X.25 PLP, CONS (Connection Oriented Network Service)[2] e CLNS (Connectionless Mode Network Service); além do

[2]Implementado sobre o X.25.

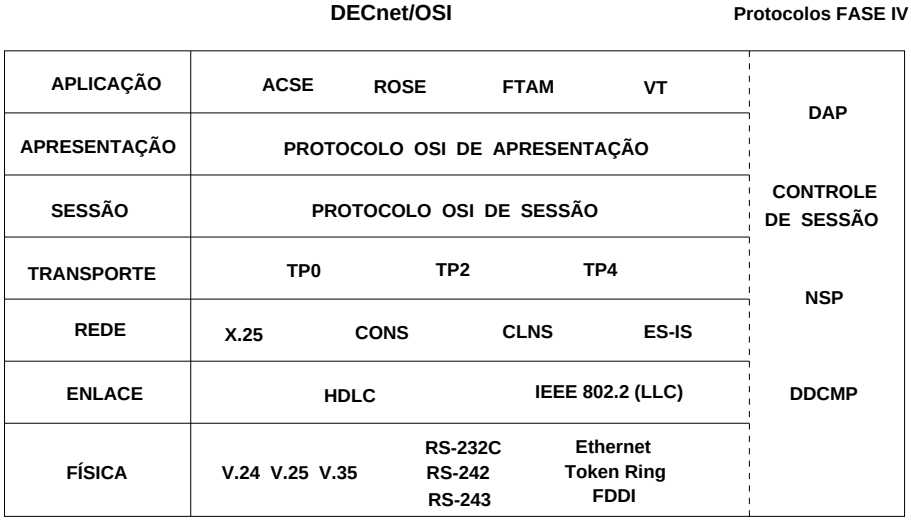


Figura 5.5: Arquitetura DECnet/OSI.

protocolo IS-IS de roteamento.

O nível de transporte implementa os protocolos OSI orientados à conexão de classe 0, 2 e 4; além do protocolo NSP presente na DECnet Fase IV.

O nível de sessão implementa o protocolo ISO de sessão orientado à conexão; além do protocolo DNA da Fase IV.

O nível de apresentação implementa o protocolo de OSI apresentação (orientado a conexão) que oferece basicamente os mesmos serviços de sessão.

Finalmente o nível de aplicação implementa os elementos ACSE (Association Control Service Element) e ROSE (Remote Operations Service Element), bem como os serviços FTAM (File Transfer Access and Management) e VT (Virtual Terminal).

5.4 A Arquitetura TCP/IP

5.4.1 Comparação Entre OSI e TCP/IP

A arquitetura TCP/IP é composta de apenas quatro camadas: interface de rede, inter-redes, transporte e aplicação. A figura 5.6 relaciona as camadas da arquitetura TCP/IP com as correspondentes do modelo OSI. TCP/IP é uma arquitetura porque especifica protocolos para cada uma de suas camadas (o que não ocorre com o modelo OSI).

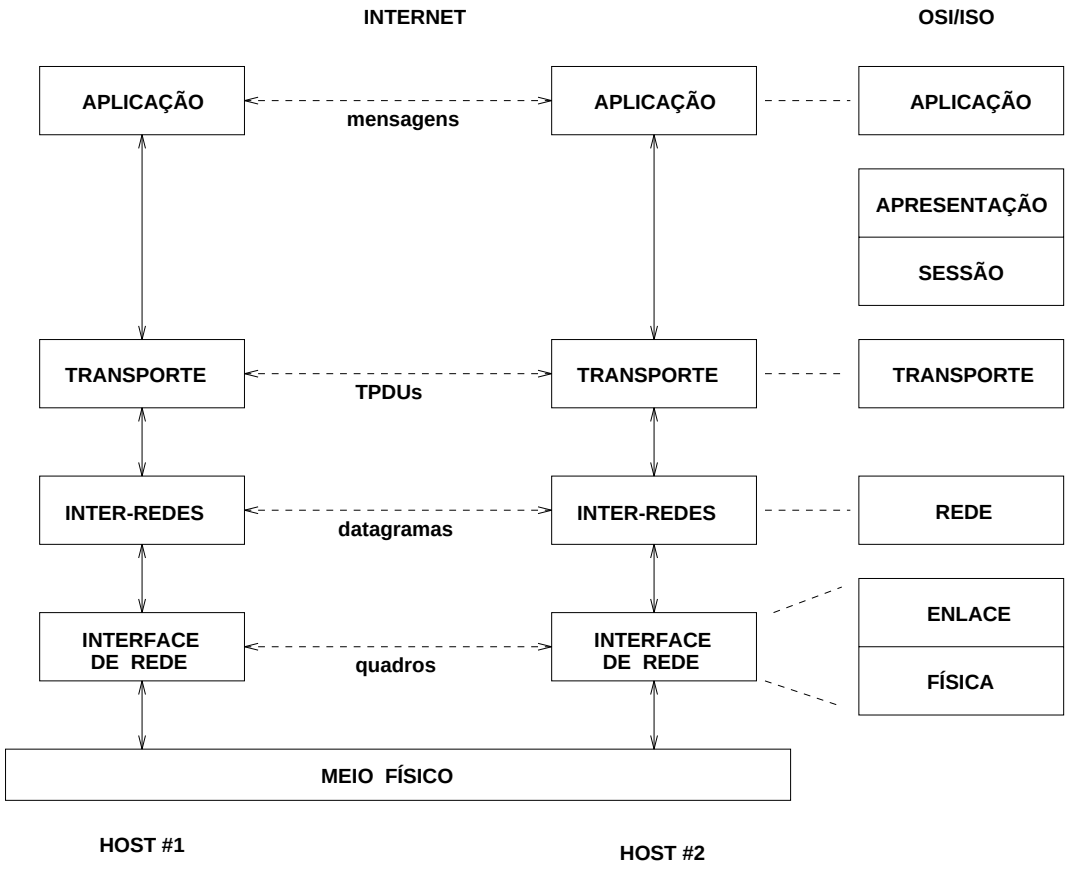


Figura 5.6: A arquitetura TCP/IP e sua comparação com o modelo OSI/ISO.

A camada interface de rede e enlace são agrupadas numa única camada na arquitetura TCP/IP. Apesar disto, as funcionalidades da camada interface de rede correspondem às previstas nas duas primeiras camadas do modelo OSI.

A camada inter-redes da arquitetura TCP/IP é prevista para operar sem conexão.

No modelo OSI, os padrões ISO para a camada 3 enfatizam mais o serviço com conexão (exemplo: X.25/camada 3).

A maior similaridade está na camada de transporte. A ISO possui protocolos de transporte com e sem conexão muito similares ao TCP/IP e UDP.

A arquitetura TCP/IP não prevê protocolos de apresentação e sessão. Entretanto, muitos autores considerarem os padrões XDR (eXternal Data Representation) e RPC (Remote Procedure Call) introduzidos pela SUN Microsystems como padrões de apresentação e sessão, respectivamente, para a arquitetura TCP/IP. A inexistência de padrões de apresentação dificulta a elaboração de padrões de aplicação. De fato, na arquitetura TCP/IP os padrões de aplicação ou são baseados em caracteres ASCII (como o SMTP) ou definem sua própria apresentação de dados (como o NVT[3] empregado no aplicativo TELNET).

5.4.2 A Camada Interface de Rede

Esta camada corresponde às camadas física e de enlace do modelo OSI. A interface de rede pode operar sobre uma rede local ou uma rede de longa distância (rede pública). No primeiro caso, a interface de rede é uma placa que implementa um protocolo de enlace e de acesso ao meio. No segundo caso, a interface de rede é um subsistema mais complexo que implementa um protocolo de conexão física do host à subrede de comunicação e de enlace entre os roteadores da subrede de comunicação. Padrões neste nível foram discutidos nos capítulos anteriores.

Endereçamento

Toda comunicação via rede supõe a existência de um emissor e um destinatário identificados por *endereços*. Diferentes camadas do modelo de redes tratam endereços de forma distinta. Para a camada de aplicação, endereços devem assumir uma forma próxima a comunicação humana: estações, usuários, domínios e serviços são identificados por nomes simbólicos. Endereços neste nível identificam processos de aplicação em comunicação.

Para a camada inter-redes, o endereço deve identificar um host e a subrede no qual o host está conectado. Neste nível o endereço é composto por números que identificam univocamente o par (subrede, host). Endereços neste nível identificam hosts comunicantes.

[3]Network Virtual Terminal.

Para a camada interface de rede, o endereço deve identificar um dispositivo físico ligado ao meio. Neste nível, o endereço é composto por uma cadeia de bits (atribuido pelo fabricante do dispositivo).

5.4.3 Endereço IP

Endereços IP são utilizados pelo protocolo IP (Internet Protocol) para o transporte de datagramas entre dois hosts (se referem portanto a camada inter-redes). Endereços IP ocupam 32 bits e são divididos em 5 classes conforme mostrado na figura 5.7.

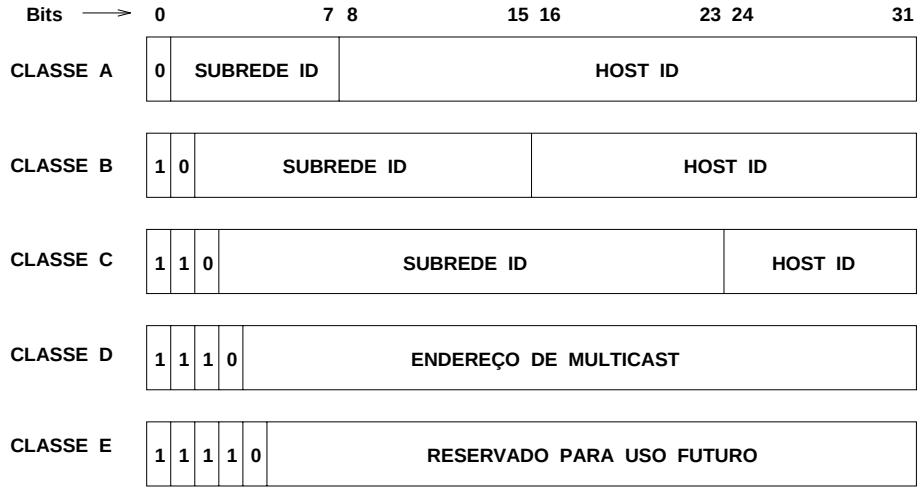


Figura 5.7: Classes de endereços IP.

A classe A é utilizada para subredes que comportam muitos hosts. Como apenas 7 bits são utilizados para identificar a subrede, podem existir apenas $2^7 = 128$ subredes da classe A (cada uma com no máximo $2^{24} = 16M$ hosts). A classe C é o oposto: embora o número de hosts na subrede é limitado (256), pode-se dispor de $2^{21} = 2M$ subredes desta classe.

Endereços da classe D são utilizados para *multicast* (comunicação envolvendo múltiplos destinatários). Nesta classe de endereços não há separação entre hosts e subrede.

Finalmente, a classe E é reservada para uso futuro, por exemplo para redes especiais.

Notação Decimal

É comum representar o endereço IP numa notação decimal. Para tal, divide-se o endereço em 4 grupos de 8 bits, converte-se os 8 bits para notação decimal, separando-os um ponto. Exemplo:

```
10000000000001010000001000011110
10000000 00001010 00000010 00011110
            128.10.2.30
```

A notação decimal é utilizada por administradores de sistema para, por exemplo, atribuir endereço IP a um novo host, configurar roteadores, identificar servidores, etc.

Relativamente ao valor do primeiro byte (x) do endereço IP podemos observar que:

- $x < 128$: endereçamento classe A;
- $128 \leq x < 192$: endereço classe B;
- $192 \leq x < 224$: endereço classe C;
- $x \geq 224$: multicast e reservado.

Endereços Especiais

A figura 5.8 mostra endereços especiais e os correspondentes significados. Trata-se apenas de convenção seguida pelos protocolos da camada inter-redes.

Duas observações importantes. A primeira refere-se a *broadcast*, onde um datagrama é endereçado a todos os hosts de uma subrede. Via de regra, *broadcast* tende a deteriorar o desempenho da rede, pois interrompe todos os hosts daquela subrede. Por esta razão, requisições de *broadcast* são comumente limitadas à subrede do host que o emitiu.

A segunda observação refere-se a endereços *loopback* da forma 127.0.0.0. Tais endereços são utilizados para "curto-circuitar" a rede em situações onde a comunicação deve ser circunscrita ao host. Ao reconhecer um endereço *loopback* a camada inter-redes não aciona a camada física para propagar a mensagem pois trata-se de uma comunicação local.

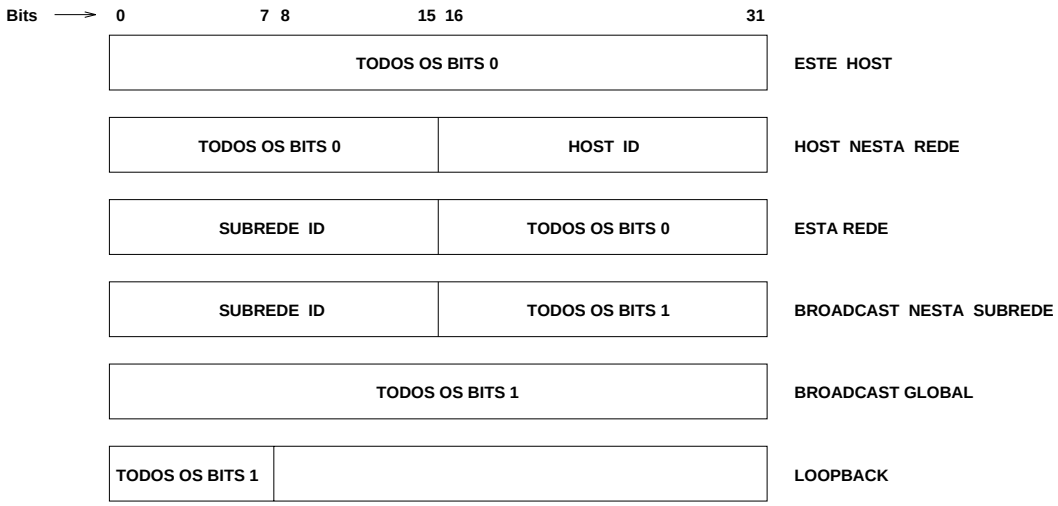


Figura 5.8: Formatos especiais de endereços IP.

Subredes

Para ilustrar o conceito de subredes, considere a figura 5.9. A figura apresenta uma empresa fictícia que utiliza 4 subredes. Considere ainda que a empresa detém um endereço classe C (215.194.97). Isto significa que a empresa em tese pode alocar até 256 (ie, 2^8) hosts.

Entretanto, para qualquer classe de endereço IP os limites inferior (0) e superior (FF..FF) do endereço de estação são reservados. Um endereço IP com todos os bits do endereço de estação iguais a 0 identifica a própria subrede. No caso, 215.194.97.0 (endereço classe C) refere-se à subrede 215.196.97. Este tipo de endereço é utilizado nas tabelas de roteamento para referenciar uma subrede na Internet. Um endereço IP com todos os bits do endereço da estação iguais a 1 representa o endereço de *broadcast*, permitindo endereçar simultaneamente todas as estações da subrede. Por exemplo, um datagrama com endereço 215.194.97.255 é recebido por todas as estações presentes na subrede 215.194.97.

Deve ser destacado que o endereço IP refere-se a uma interface de rede e não ao host propriamente dito. No caso da figura 5.9, os hosts GW, Rio, Zeus e Sol possuem 2 endereços IP, um para cada rede na qual o host encontra-se conectado. O protocolo IP utiliza o endereço de subrede do endereço IP para roteamento do datagrama entre subredes. O endereço completo, incluindo o endereço do host é utilizado para entregar o datagrama quando o mesmo alcança a subrede de destino.

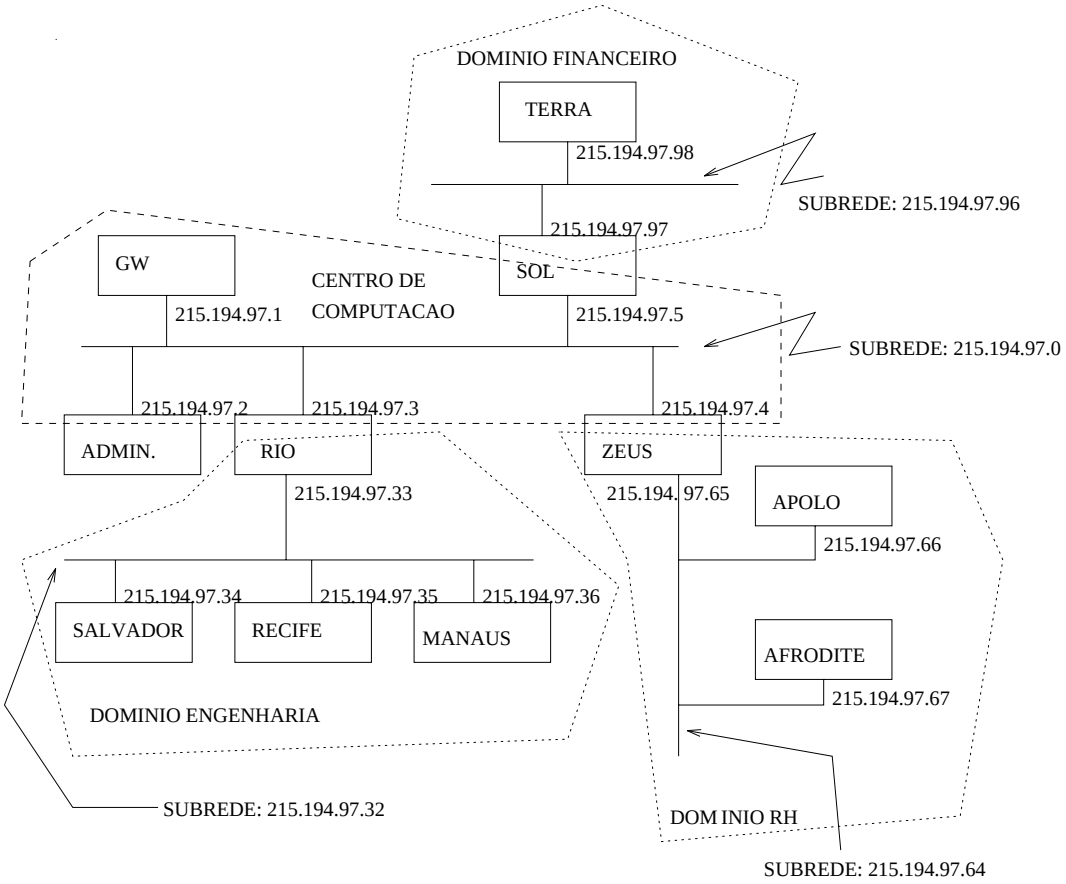


Figura 5.9: Uma empresa hipotética dividida em 4 subredes.

Estabelecimento de Subredes

A estrutura padrão do endereço IP pode ser modificado internamente ao domínio através da utlização de alguns bits do endereço do host como bits adicionais do endereço de subrede. Desta forma, a linha divisória entre os endereços do host e subrede (ver figura 5.7) é deslocada criando subredes adicionais e reduzindo o número máximo de hosts que podem participar de uma subrede. Os novos bits definem uma nova subrede dentro de uma subrede maior. A decisão de se criar subredes é normalmente associada a decisões topológicas ou administrativas. A criação de subredes permite uma descentralização no gerenciamento de endereços das estações. No caso do esquema de endereçamento tradicional um único administrador é responsável pelo gerenciamento dos endereços de todas os hosts conectados à subrede. Com a criação de subredes esta tarefa é descentralizada. No caso da figura 5.9, caso o administrador não tenha interesse em gerenciar as informações do Departamento de Engenharia da empresa, uma subrede pode ser designada para o

Departamento e o seu gerenciamento ser realizado internamente ao Departamento.

Uma subrede é definida através da aplicação de uma máscara ao endereço IP. Os bits 1 da máscara definem que os bits equivalentes no endereço IP devem ser interpretados como bits do endereço de rede. Consequentemente, os bits 0 da máscara definem a parte do endereço IP que deve ser interpretada como endereço de host. A subrede é conhecida somente do ponto de vista local. Do ponto de vista externo, o endereço é interpretado como um endereço IP padrão. No caso, por exemplo, de um endereço classe B padrão, a máscara associada é 255.255.0.0. Uma possibilidade frequentemente utilizada estende em um byte a parte do endereçamento de rede da classe B. Neste caso a máscara de subrede é 255.255.255.0. Os dois primeiros bytes definem um endereço de rede classe B; o terceiro byte define o endereço de subrede e o quarto byte define o host naquela subrede.

Muitos administradores de rede preferem utilizar uma máscara orientada a byte porque é mais fácil de ser lida e compreendida. Entretanto, a máscara pode ser orientada ao bit e utilizada em qualquer classe de endereço. No caso do exemplo da figura 5.9 o endereço classe C foi subdivido em 8 subredes, sendo que na figura aparecem somente 4 subredes ficando os outros 4 endereços reservados para subredes futuras. Ao endereço IP 215.194.97.0 foi associada a máscara 255.255.255.224[4]. A aplicação desta máscara a um endereço classe C define os três bits de ordem mais alta no quarto byte como a parte que especifica a subrede. Os itens a seguir ilustram o efeito provocado pela adoção da máscara 255.255.255.224:

Assim sendo, temos para as 8 subredes os endereços de subrede e *broadcast* dados pela tabela 5.1.

subrede	broadcast
214.194.97.0	214.194.97.31
214.194.97.32	214.194.97.63
214.194.97.64	214.194.97.95
214.194.97.128	214.194.97.159
214.194.97.96	214.194.97.127
214.194.97.160	214.194.97.191
214.194.97.192	214.194.97.223
214.194.97.224	214.194.97.251

Tabela 5.1: Endereços de subrede e broadcast para a rede 214.194.97.0 e máscara 255.255.255.224.

Exemplos:

[4]224 equivale à máscara binária 11100000.

- endereço IP: 215.194.97.1 interpretação: máquina 1 na subrede 215.194.97.0;
- endereço IP: 215.194.97.35 interpretação: máquina 3 na subrede 215.194.97.32;
- endereço IP: 215.194.97.67 interpretação: máquina 3 na subrede 215.194.97.64;
- endereço IP: 215.194.97.97 interpretação: máquina 1 na subrede 215.194.97.96;

CIDR - *Classless Inter-Domain Routing*

O crescimento explosivo da Internet nos últimos anos colocou a questão para o IETF de que ações realizar para suportar, do ponto de vista do roteamento, este crescimento. As questões principais que precisavam ser respondidas eram relativas a:

- perspectiva do término de espaço de endereços Classe B;
- crescimento vertiginoso do tamanho das tabelas de roteamento na Internet;
- perpectiva de término do espaço de endereço de 32 bits do IPv4.

Os dois primeiros pontos, caso nada fosse feito há tempo, teria consequências imediatas por volta dos anos 1994/1995. Neste sentido, a resposta a estes itens traduziu-se na proposta do CIDR e, no caso do terceiro item, a solução está associada ao projeto *IP Next Generation* traduzido na proposta de um novo protocolo em substituição ao IPv4 denominado de IPv6.

As principais características do CIDR são:

- eliminação dos conceitos de classes A, B e C no caso do endereço IPv4. Esta decisão é fundamental para permitir uma alocação eficiente do espaço de endereços do IPv4;
- viabilização da agregação de rotas, ou seja, permite que através de uma única entrada na tabela de roteamento seja possível representar o espaço de endereços de milhares de rotas.

Dados da literatura referenciam que se não tivesse ocorrido à rápida adesão às idéias do CIDR, como efetivamente ocorreu, as tabelas de roteamento atuais teriam da ordem de 70.000 entradas além das 30.000 atuais e que, provavalmente, a Internet não estaria funcionando.

CIDR - Alocação do espaço de endereços do IPv4

O conceito de classes do endereçamento tradicional do IPv4 é substituído pelo conceito de *prefixo de rede*. Os roteadores baseiam-se no prefixo de rede, ao invés dos 3 primeiros bits do endereço IP, para distinguir a fronteira entre o endereço de rede e o endereço do host naquela rede. Consequentemente o CIDR suporta, no lugar das redes com 8, 16 ou 24 bits do endereçamento tradicional, qualquer tamanho de rede. O CIDR especifica estas informações através de uma máscara de bits que define o comprimento do prefixo utilizado e que é difundida para os roteadores. No caso, por exemplo, de uma rede com um número de rede de 20 bits e 12 bits para número de host, o seu endereço deverá ser difundido com um prefixo de comprimento 20 (/20), independentemente do endereço que está sendo difundido ser um endereço tradicional Classe A, B ou C. Desta forma, os roteadores que suportam o CIDR não fazem qualquer hipótese sobre os 3 primeiros bits do endereço e sim na informação de prefixo fornecida para a rota. Os exemplos a seguir ilustram um prefixo /20 abribuído a endereços tradicionais Classe A, Classe B e Classe C.

- Endereço tradicional Classe A: 10.23.64.0
  Endereço CIDR: 10.23.64.0/20 00001010.00010111.0100**0000.00000000**;
- Endereço tradicional Classe B: 130.5.0.0
  Endereço CIDR: 130.5.0.0/20 10000010.00000101.0000**0000.00000000**;
- Endereço tradicional Classe C: 200.7.128.0
  Endereço CIDR: 200.7.128.0/20 110001000.00000111.1000**0000.00000000**.

Deve ser observado nos exemplos acima que todos os endereços CIDR possuem o mesmo número de hosts, ou seja, 4096 hosts (2^12).

Alocação Eficiente de Endereços

No esquema tradicional de atribuição de endereços na Internet, somente endereços /8, /16 e /24 podem ser atribuídos. No contexto CIDR os endereços são atribuídos na forma de um bloco que atenda as necessidades do usuário, mais um espaço adicional para futuras expansões, mas não existe um desperdício de recursos, ou seja, de endereços IP que nunca serão utilizados como acontecia anteriormente.

Podemos imaginar um Provedor de Acesso Internet que possua o seguinte bloco de endereço: 206.0.64.0/18. Este bloco corresponde a 16.384 (2^{14}) endereços IP que podem

ser interpretados como 64 endereços /24. Suponhamos agora que um cliente necessite de 800 endereços de host. No lugar de alocar um endereço Classe B e desperdiçar, no caso, aproximadamente 64.700 endereços, ou ainda, alocar 4 endereços Classe C e com isto introduzir 4 novas entradas nas tabelas de roteamento na Internet, o Provedor atribui ao cliente o bloco 206.0.68.0/22 (1.024 endereços = 2^{10}) que corresponde a 4 blocos /24. O diagrama a seguir ilustra a eficiência desta alocação de endereços.

- Bloco de endereços do Provedor: 206.0.64.0/18 11001110.00000000.01000000.00000000;
- Bloco do Cliente: 206.0.68.0/22
  11001110.00000000.01000100.0000000;
- Bloco 1 do Cliente: 206.0.68.0/24
  11001110.00000000.01000100.0000000;
- Bloco 2 do Cliente: 206.0.69.0/24
  11001110.00000000.01000101.0000000;
- Bloco 3 do Cliente: 206.0.70.0/24
  11001110.00000000.01000110.0000000;
- Bloco 4 do Cliente: 206.0.71.0/24
  11001110.00000000.01000111.0000000;

Controle do Crescimento das Tabelas de Roteamento na Internet

Um consequência fundamental do CIDR é o papel que ele representa relativamente ao crescimento das tabelas de roteamento. A redução da informação de roteamento passa pela divisão da Internet em domínios de endereçamento. Desta forma, externamente a um domínio de roteamento, somente o prefixo de rede comum precisa ser propagado. Como consequência, uma única entrada na tabela de roteamento especifica uma rota para muitos endereços de redes individuais internamente aquele domínio.

Na figura 5.10 podemos observar que a Organização A agrega 8 blocos /24 através de uma única informação (200.25.16.0/21), a Organização B agrega 4 blocos /24 através da propagação de 200.25.24.0/22, a Organização C agrega 2 blocos /24 e envia um única anúncio correspondendo a 200.25.28.00/23 e a Organização D agrega 2 blocos /24 em um único anúncio 200.25.30.0/23. Por último, o Provedor Internet agrega os 256 blocos de prefixo /24 em um único anúncio para a Internet através de 200.25.0.0/16.

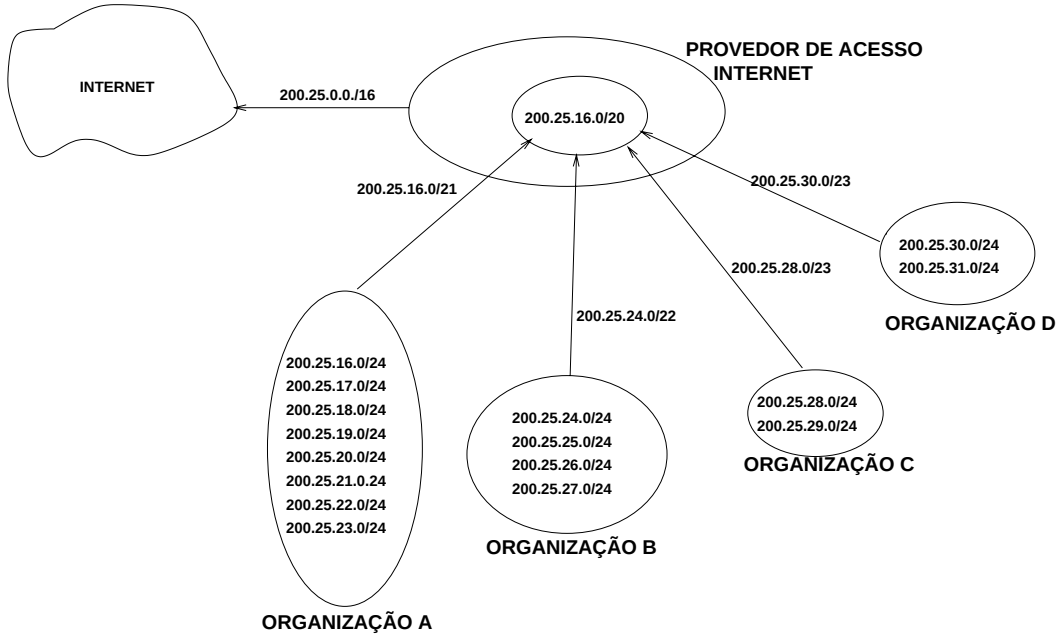


Figura 5.10: Propagação de Endereços CIDR.

Endereços Físicos

A camada interface de rede utiliza endereços físicos para localizar a interface que gerou o quadro e a interface destinatária. No caso do padrão IEEE 802.3 (Ethernet) o endereço físico é composto de 6 bytes (48 bits) atribuídos de forma única pelo fabricante da interface[5]. Este endereço é comumente fornecido como 6 números hexadecimais separados por ponto, sendo que cada número corresponde a um byte do endereço. Por exemplo, o endereço 67.F3.AF.3E.12.FF identifica a interface

```
011001110111100110101111001111100001001011111111
```

Ao receber um quadro, a interface de rede compara o campo do quadro que carrega o endereço destino com o seu endereço. Se coincidir, o quadro é processado pela interface de rede, caso contrário é descartado. Por convenção, um endereço IEEE 802.x do tipo FF.FF.FF.FF.FF.FF (todos os bits 1) significa um quadro de *broadcast* e, apesar de diferir do endereço local da interface, o quadro é processado pela interface.

[5]No caso de endereços IEEE 802.x, o IEEE é a entidade que supre os fabricantes com endereços evitando assim a possibilidade de existirem duas interfaces com o mesmo endereço.

Mapeamento Endereço IP - Endereço Físico: Protocolo ARP

Para enviar um quadro para um host destino, a camada interface de rede necessita do endereço físico do host. Este endereço deve ficar circunscrito à camada interface de rede, permitindo que as camadas superiores utilizem formas de endereçamento mais abstratas. Surge então o problema: dado um endereço IP de determinado host, como descobrir seu endereço físico?

A solução ideal seria as interfaces de rede armazenarem endereços IP ao invés de endereços físicos. Como tal não ocorre com a maioria das tecnologias de rede (inclusive Ethernet, a tecnologia mais utilizada) uma forma de mapeamento entre endereços IP e físico é imprescindível.

Uma solução simples é manter uma tabela relacionando endereço IP com o correspondente endereço físico. Tal solução é impraticável dadas as dimensões das redes atuais. Uma outra alternativa é difundir um quadro em *broadcast* com a seguinte requisição: quem possuir tal endereço IP, mande o seu correspondente endereço físico. O protocolo ARP (Address Resolution Protocol) adota exatamente esta idéia.

O protocolo mantém uma memória cache que armazena os últimos mapeamentos obtidos. Isto evita que antes de cada transmissão de quadro um *broadcast* para resolução de endereços seja efetuado.

Mapeamento Endereço Físico - Endereço IP: Protocolo RARP

O endereço IP de um host é mantido em disco e acessado pelo sistema operacional durante o processo de *boot*. Esta informação é fundamental para a instalação dos processos que compõem o software de rede. O que ocorre no caso de um host *diskless* (sem disco)? Estações *diskless* acessam uma imagem do sistema operacional de um host servidora. Esta imagem não possui nenhuma referência a endereços IP pois é comumente utilizada por várias estações *diskless*. Neste caso, o host dispõe de seu endereço físico e necessita descobrir seu próprio endereço IP. Este processo é exatamente o inverso do que estabelece o protocolo ARP.

O mapeamento endereço físico - endereço IP é estabelecido também através de *broadcast* pelo protocolo RARP (Reverse ARP). No caso do protocolo ARP, um único host responde ao *broadcast*: aquele que possui o endereço físico procurado. Entretanto, para o protocolo RARP deve haver um host especial na rede que conheça os endereços físicos dos demais. Este host especial é denominado *servidor de RARP* e possui uma tabela em

disco contendo o mapeamento entre endereços físico e IP de um subconjunto de máquinas da rede (tipicamente aquelas *diskless*). É importante notar que um host utiliza o protocolo RARP uma única vez durante o *boot*: após obtido o seu endereço IP, este dado é armazenado permanentemente em memória.

5.4.4 A Camada Inter-Redes

É equivalente à camada de rede do modelo OSI. Esta camada define protocolos para:

1. Transporte não confiável de mensagens: o protocolo IP (Internet Protocol).
2. Controle da comunicação e informe de erros: o protocolo ICMP (Internet Control Message Protocol).
3. Roteamento de mensagens: protocolos EGP (Exterior Gateway Protocol), RIP (Routing Information Protocol), etc.

Examinaremos aqui apenas o protocolo IP.

O protocolo IP (Internet Protocol) é a base da arquitetura TCP/IP. A interconexão de redes na arquitetura TCP/IP supõe que todas as subredes são capazes de manipular datagramas (pacotes) padronizados. O protocolo IP fornece exatamente um padrão para a construção e manipulação de datagramas que irão circular pelas subredes de comunicação.

Um datagrama possui um cabeçalho e um campo de dados contendo a informação que o datagrama transporta. Exceto para datagramas especiais, o conteúdo semântico dos dados é completamente ignorado pelo protocolo IP, sendo de interesse apenas das camadas superiores.

Um datagrama IP tem seu tamanho limitado em 65.535 bytes, incluindo o cabeçalho. Os campos e seus respectivos tamanhos que compõem o cabeçalho de um datagrama é apresentado na figura 5.11.

O campo VERSÃO contém a versão do protocolo, sendo utilizado como garantia que os hosts comunicantes dispõem da mesma versão do protocolo IP.

O campo TAM-CAB supre o tamanho do cabeçalho, medido em múltiplos de 32 bits.

O campo TIPO DE SERVIÇO (comumente ignorado) possui 4 sub-campos:

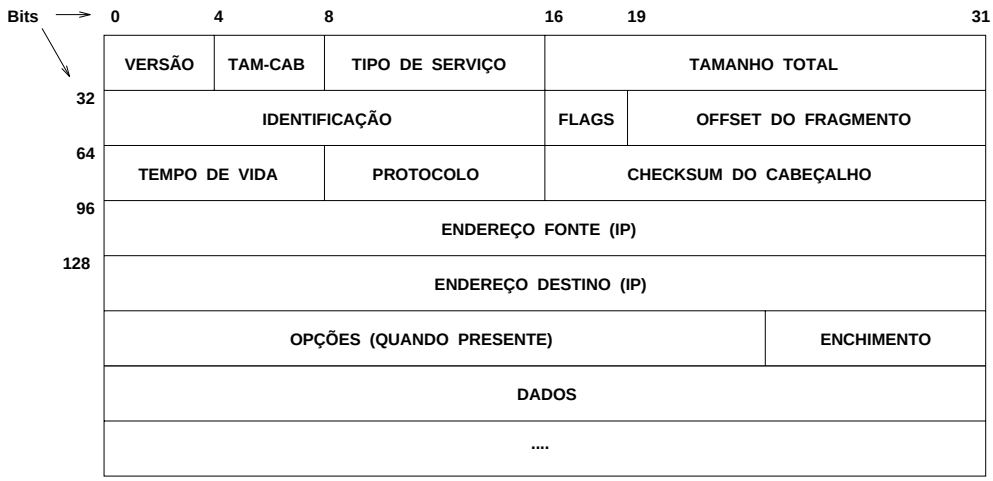


Figura 5.11: Cabeçalho do protocolo IP.

1. Os três primeiros bits do campo identificam o tipo de datagrama, e pode servir de indicativo de sua prioridade. O valor 0 identifica um datagrama de dados. O valor 7 identifica um datagrama de controle (merecendo portanto alta prioridade no tratamento).

2. O quarto bit (bit D: *delay*) se ativo (1) solicita um roteamento com baixo atraso.

3. O quinto bit (bit T: *throughput*) se ativo solicita um roteamento por vias de alta vazão.

4. o sexto bit (bit R: *reliability*) se ativo solicita um roteamento por vias de alta confiabilidade.

Os bits D, T e R quando utilizados fornecem informações adicionais para o roteamento. Comumente são ignorados.

O campo TAMANHO TOTAL indica o tamanho total do datagrama medido em bytes (8 bits). Por dispor de 16 bits, o tamanho do datagrama fica limitado a $2^{16} = 65.536$ bytes.

Os campos IDENTIFICAçÃO, FLAGS e OFFSET DO FRAGMENTO dizem respeito a fragmentação[6] e remontagem de datagramas. O campo IDENTIFICAçÃO carrega um número gerado pelo emissor e comum a todos o fragmentos. O primeiro bit do campo

[6] A fragmentação ocorre quando o tamanho do datagrama supera o tamanho máximo para dados num quadro de enlace.

FLAGS (bit DF: *disable fragmentation*) quando ativado informa que o datagrama não deve ser fragmentado. O segundo bit indica se o datagrama carrega o último fragmento do datagrama original, ou um fragmento que não o último. O campo OFFSET DO FRAGMENTO especifica em múltiplos de 8 bytes (64 bits) a posição que o fragmento ocupa no datagrama original. Com estes campos é possível remontar um datagrama fragmentado, mesmo que seus fragmentos chegarem duplicados ou fora de ordem. A perda de um fragmento impossibilita a remontagem, causando o descarte de todos os demais fragmentos (e portanto do datagrama original).

O campo TEMPO-DE-VIDA (TTL: *time-to-live*) especifica o tempo máximo que o datagrama pode permanecer na *internet* (segundos). Em cada roteador[7] que o datagrama passa, seu tempo de vida é decrementado. O roteador pode computar o decremento de uma forma simplificada (subtraindo uma unidade do campo), ou mais elaborada (subtraindo o tempo de permanência do datagrama no roteador). Em ambos os casos o tempo de trânsito entre roteadores não é levado em conta. Quando o tempo de vida de um datagrama atinge o valor zero, o mesmo é descartado.

O campo PROTOCOLO indica o tipo de dados que o datagrama carrega. Usualmente especifica um protocolo de transporte como o TCP/IP ou o UDP.

O campo CHECKSUM DO CABEÇALHO contém o valor do checksum computado apenas para o cabeçalho. O receptor do datagrama computa novamente o checksum do cabeçalho, comparando-o com o valor armazenado no campo. Em havendo diferença o datagrama é descartado. O protocolo IP não computa checksum para os dados transportados em datagramas, deixando esta tarefa para a camada de transporte.

Os campos ENDEREÇO FONTE e ENDEREÇO DESTINO contêm, respectivamente, os endereços IP do host emissor e do host destinatário. Note que nenhuma informação de rota está presente no cabeçalho.

O campo OPÇÕES não está presente em datagramas comuns que carregam dados oriundos da camada de transporte. Quando presente[8], o campo é composto de 1 byte dividido em 3 sub-campos:

1. O primeiro bit, quando ativo (1) informa que o campo deve ser copiado em todos os fragmentos, caso o datagrama necessite ser fragmentado em seu trajeto. Quando inativo (0), o campo é copiado apenas no primeiro fragmento.

2. Os dois bits seguintes estabelecem a classe da opção, podendo assumir 4 valores:

[7] Comporta (gateway) no jargão TCP/IP.

[8] A presença é indicada quando o tamanho do cabeçalho excede a 5 unidades de 32 bits.

- valor 0: controle da subrede;
- valor 1: reservado para uso futuro;
- valor 2: depuração e medição;
- valor 3: reservado para uso futuro.

3. Os 5 bits seguintes especificam a opção propriamente dita. Exemplo de opções:

   - registro de rota, para teste do roteamento;
   - rota específica, para enviar um datagrama por uma rota estipulada;
   - manipulação restrita do datagrama, para datagramas carregando dados confidenciais;
   - registro de tempo, para medida do tempo gasto na rota.

Os dados referentes à opção seguem o cabeçalho. Por exemplo, na opção de registro de rota, cada roteador adiciona ao campo de dados do datagrama um novo segmento de rota.

Finalmente, ENCHIMENTO não é um campo mas uma simples adição de bits (sem nenhum significado) para que o tamanho do cabeçalho do datagrama seja múltiplo de 32 bits.

5.4.5 A Camada de Transporte

É equivalente à camada 4 do modelo OSI. Esta camada define dois protocolos: TCP/IP (Transfer Control Protocol/Internet Protocol) que provê um transporte confiável de dados, e UDP (User Datagram Protocol) que deixa a confiabilidade do transporte a cargo das camadas inferiores. O protocolo TCP/IP garante um transporte confiável mesmo operando em subredes de baixa confiabilidade onde as mensagens estão sujeitas a perda, duplicação e alteração do conteúdo.

O protocolo TCP/IP opera sob uma camada de rede orientada a datagrama. As principais características do protocolo são:

- utilização de conexões full-duplex (permitindo comunicação nos dois sentidos da conexão);
- transferência "bufferizada" de dados sem delimitação de fronteiras;
- controle de fluxo por janela deslizante.

O Conceito de Port

Para as camadas interface de rede e inter-redes, o destinatário é identificado univocamente por um endereço de host apenas. A camada de transporte atende a múltiplas aplicações e portanto deve ser capaz de diferenciar os quadros endereçados a estas aplicações. Obviamente, um componente adicional ao host deve estar presente no endereçamento empregado pela camada de transporte. Este componente é denominado *port* e se presta a identicar uma aplicação usuária da camada de transporte num dado host. O port é único num host, sendo o par (host, port) suficiente para endereçar uma aplicação.

Ports identificam também recursos utilizados para o envio e recepção de mensagens. Estes recursos constituem-se de buffers onde mensagens em trânsito são armazenadas temporariamente. Em sendo recurso de máquina, ports são alocados pelo sistema operacional via chamada de sistema. No protocolo TCP/IP ports são identificados por inteiros sem sinal ocupando 16 bits.

A figura 5.12 ilustra múltiplas aplicações compartilhando um única instância de protocolo de transporte.

O protocolo TCP/IP identifica duas aplicações comunicantes atráves da conexão estabelecida entre elas. Uma conexão é referenciada por duas duplas (host, port). Por exemplo o par

```
(143.106.11.188, 1234)  (143.106.1.10, 21)
```

indica que a aplicação que possui o port 1234 no host 143.106.11.188 está conectada à que possui o port 21 no host 143.106.1.10.

Um port é dito *ativo* se através deste uma aplicação toma a iniciativa, via chamada de sistema, para o estabelecimento de uma conexão. Um dos parâmetros da chamada é o par (host, port) que constituirá o outro extremo da conexão. Este segundo port é dito *passivo*, sendo que a aplicação que o detém executa uma chamada de sistema "aceitando" o estabelecimento da conexão.

Cabeçalho do Protocolo TCP/IP

Mensagens trocadas via protocolo TCP/IP são transportadas no campo de dados de datagramas e possuem o cabeçalho dado pela figura 5.13.

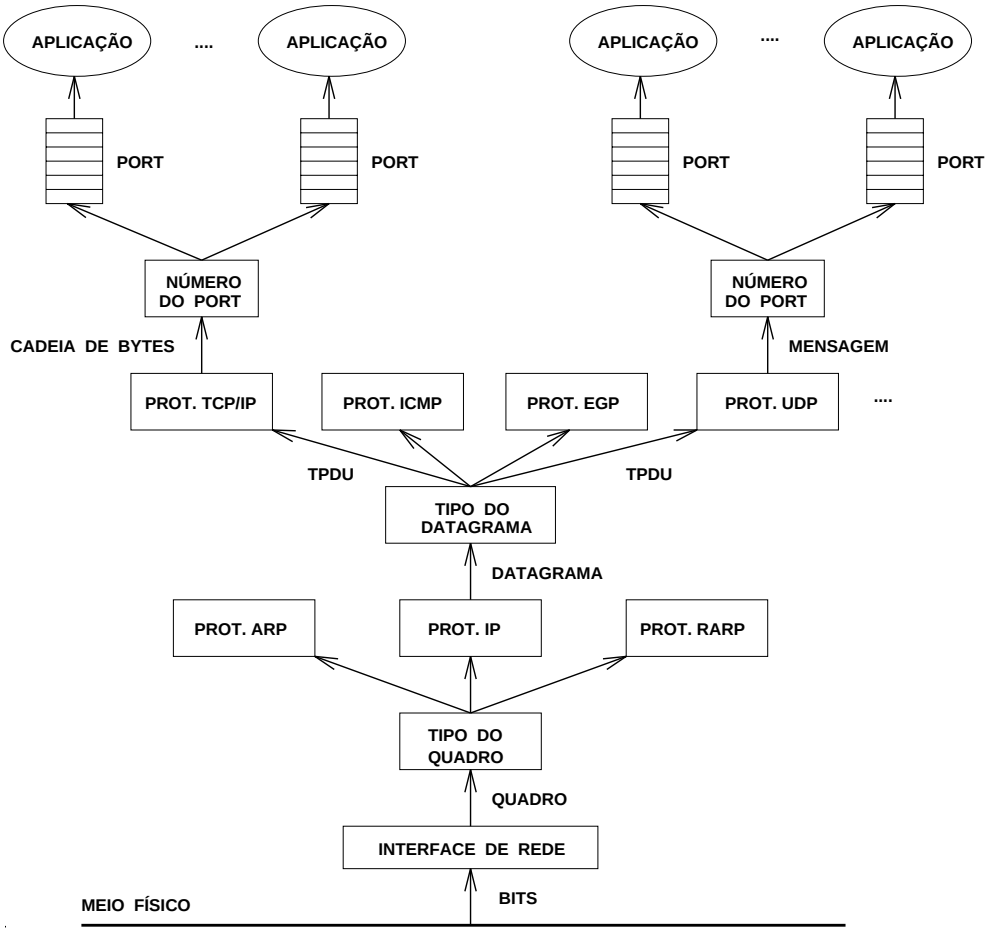


Figura 5.12: Ports permitem uma única instância de protocolo de transporte atender múltiplas aplicações.

Os campos PORT DE ORIGEM e PORT DE DESTINO identificam os ports da conexão de transporte. Note que o hosts não são estipulados no cabeçalho pois os mesmos estão presentes no cabeçalho do protocolo IP (veja figura 5.11).

O campo NÚMERO DE SEQUÊNCIA estabelece a posição dos dados que o pacote carrega com relação à cadeia de bytes transferida desde o estabelecimento da conexão.

O campo RECONHECIMENTO identifica a posição na cadeia de bytes que o emissor espera receber no próximo pacote a ele endereçado. Este campo provê reconhecimento expontâneo *(piggybacking)*.

O campo TAM-CAB contém o tamanho do cabeçalho em múltiplos de 32 bits. Este

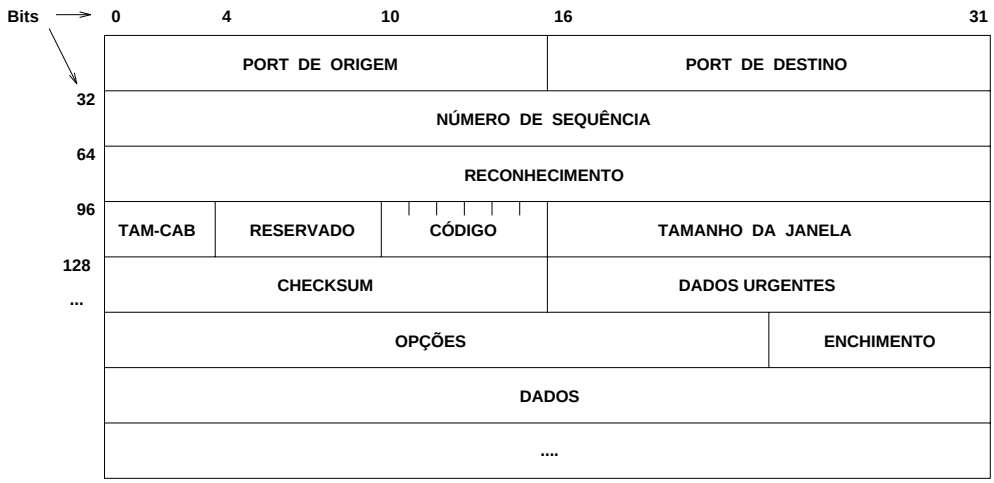


Figura 5.13: Cabeçalho do protocolo TCP/IP

campo se faz necessário dado que o campo OPÇÕES possui tamanho variável.

O campo CÓDIGO possui seis bits assim distribuídos:

1. bit URG: o pacote carrega dados urgentes;
2. bit ACK: o pacote carrega um TPDU de reconhecimento;
3. bit PSH: solicita à camada de transporte um *push*, isto é, um envio sem "bufferização";
4. bit RST: solicita ao destinatário um *reset* da conexão;
5. bit SYN: solicita ao destinatário o estabelecimento de conexão;
6. bit FIN: solicita ao destinatário o encerramento da conexão.

O campo TAMANHO DA JANELA informa a quantidade de bytes o emissor deseja receber sem a necessidade de reconhecimento. Note que o tamanho da janela é dinâmico e não necessariamente idêntico nos dois sentidos da conexão.

O campo CHECKSUM contém o cômputo do checksum para o cabeçalho mais os dados.

O campo DADOS URGENTES especifica a posição na cadeia em que os dados urgentes terminam[9]. Este campo é válido apenas se o bit URG estiver ativo. Quando dados urgentes são enviados, o receptor é notificado assincronamente de sua chegada[10].

Finalmente, o campo OPÇÕES é utilizado para troca de informação entre as camadas de transporte que mantêm a conexão. Uma informação importante é o tamanho máximo do segmento (MSS), que dita o tamanho máximo dos dados num pacote que o emissor está apto a processar. Usualmente, MSS possui um valor *default* de 4288 bytes[11], mas pequenos microcomputadores ou determinadas subredes podem impor um tamanho menor para os pacotes.

O Protocolo UDP

O protocolo UDP (User Datagram Protocol) é orientado a datagrama, não suportando portanto conexões de transporte. O protocolo UDP deixa a cargo da camada de rede toda a confiabilidade do transporte. Como o protocolo IP não provê nenhum mecanismo de confiabilidade, o protocolo UDP é mais empregado quando as aplicações que dele fazem uso executam em hosts de uma mesma rede local.

Como no TCP/IP, o protocolo UDP também se utiliza do serviço de entrega de datagramas da camada IP. Dado que o protocolo UDP não emprega nenhum mecanismo de reconhecimento, retransmissão e controle de fluxo, o mesmo possui um cabeçalho muito simples (figura 5.14).

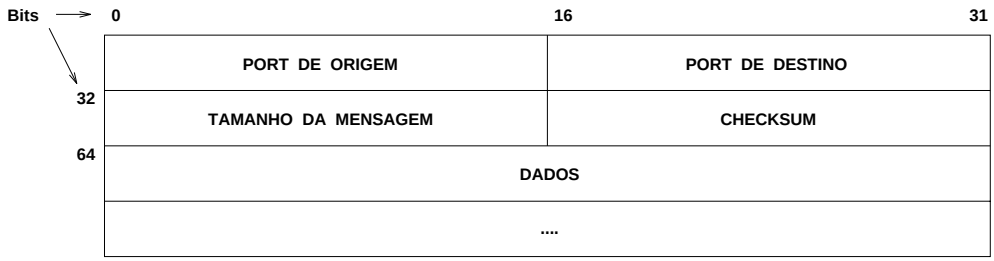


Figura 5.14: Cabeçalho do protocolo UDP

Os campos PORT DE ORIGEM e PORT DE DESTINO especificam o port emissor e

[9]Dados urgentes iniciam sempre no primeiro byte do campo de dados.

[10]UNIX, o processo recebe o sinal SIGURG e extrai a posição dos dados urgentes na cadeia de bytes através da chamada de sistema *ioctl*.

[11]Por razões de ordem prática, nunca o limite de 64 Kbytes que um datagrama pode transportar é empregado.

o port destinatário. No protocolo TCP/IP estes campos são empregados para identificar a conexão de transporte (juntamente com os respectivos hosts) e garantir portanto a existência do receptor. Tal não ocorre no protocolo UDP: o destinatário é identificado apenas pelo seu port (e respectivo host). Caso este port inexista no host destino, o host simplesmente descarta a mensagem sem que a aplicação que emitiu a mensagem seja notificada.

O campo TAMANHO DA MENSAGEM determina o tamanho em bytes da mensagem (cabeçalho mais dados). O campo CHECKSUM é utilizado para garantir a integridade do cabeçalho mais dados. Quando este campo for zero significa que o checksum não deve ser levado em conta. Não existe campo de opções no protocolo UDP.

5.4.6 A Camada de Aplicação

A camada de aplicação define um conjunto de serviços manipulados diretamente pelo usuário ou pelo administrador de sistema. Tais serviços são acessados através de protocolos e disponíveis em aplicativos diversos. Muitos destes aplicativos fazem parte do sistema, enquanto outros mais sofisticados são produtos comercializados por terceiros.

Na arquitetura TCP/IP os serviços da camada de aplicação utilizam a filosofia cliente-servidor. Os aplicativos são clientes de serviços definidos pelas implementações TCP/IP. Clientes e servidores se comunicam através de protocolos de aplicação que regem a interação cliente-servidor. Protocolos de aplicação se utilizam dos protocolos TCP/IP e UDP para o envio/recepção de suas mensagens.

Servidores provêem ports de comunicação para fins de acesso aos serviços. Tais ports são reservados e possuem número fixo independente da implementação (os chamados *ports notáveis*). A maioria das implementações TCP/IP definem um arquivo no diretório */etc* denominado *services*. Algumas linhas deste arquivo são apresentadas abaixo:

```
# @(#)services 1.16 90/01/03 SMI
#
# Network services, Internet style
#
tcpmux 1/tcp # rfc-1078
systat 11/tcp users
netstat 15/tcp
ftp-data 20/tcp
```

```
ftp 21/tcp
telnet 23/tcp
smtp 25/tcp mail
time 37/tcp timserver
time 37/udp timserver
name 42/udp nameserver
whois 43/tcp nicname # usually to sri-nic
sunrpc 111/udp
sunrpc 111/tcp
```

Por exemplo, o serviço de terminal virtual, denominado TELNET é provido no port 23 através do protocolo TCP/IP. Note que um mesmo serviço pode estar disponível através de diferentes protocolos de transporte com o mesmo número de port.

Serviços interativos de longa duração como *login* remoto e transferência de arquivos devem possuir um modo de operação de forma a evitar a indisponibilidade do serviço quando um cliente dele faz uso. Neste caso, o servidor quando recebe uma conexão de um cliente cria uma instância de si próprio[12] para interagir com o cliente, retomando seu estado de espera de conexão. Com isto, múltiplos clientes podem fazer uso do mesmo serviço simultaneamente.

[12]No UNIX, tal se dá pela chamada de sistema *fork*.

Capítulo 6

Redes Locais e Metropolitanas

6.1 Introdução

Em redes locais, o meio físico é compartilhado por todas as estações. A transmissão de um quadro em redes locais requer antes um procedimento de acesso ao meio. Este procedimento é denominado MAC (Medium Access Control) e varia em complexidade em função da topologia e demais características da rede. Dada a importância do controle de acesso ao meio em redes locais, é comum reservar uma subcamada no modelo de rede exclusiva para tal. A *subcamada de acesso ao meio* é parte da camada de enlace e situa-se na interface desta com a camada física. O restante da camada de enlace denomina-se Controle de Enlace Lógico (LLC: Logical Link Control) e podemos considerá-la como uma segunda subcamada, acima da subcamada de acesso ao meio. Para a maioria das redes locais a subcamada LLC é inexistente ou resume-se num protocolo elementar[1].

6.2 A Subcamada de Acesso ao Meio (MAC)

A subcamada de acesso ao meio implementa uma disciplina (seguida à risca por todos as estações) de acesso ao meio físico. As mais difundidas técnicas de controle de acesso ao meio são as baseadas em *acesso aleatório (ou de contenção)* e *passagem de permissão*.

[1] Constituído por um cabeçalho fixo de 3 bytes no caso do protocolo IEEE 802.2.

6.2.1 Técnicas de Acesso Aleatório

As técnicas de acesso aleatório são utilizadas em redes com topologia de barramento. Dois métodos de acesso aleatório serão descritos: métodos ALOHA (pioneiros) e sua evolução para os métodos de acesso múltiplo com detecção de portadora (CSMA: Carrier Sense Multiple Access).

Método ALOHA Puro

Este médodo foi concebido na Universidade do Hawaii para uma rede conectando unidades em quatro ilhas via rádio. A técnica necessita de reconhecimento por parte do receptor e segue o algoritmo abaixo:

1. transmita o quadro;
2. aguarde o reconhecimento da recepção por T unidades de tempo; se recebido, fim;
3. gere um número aleatório (r) entre 0 e R;
4. vá para 1 após r unidades de tempo.

A técnica ALOHA pura é basteante simples. Sempre que necessitar transmitir um quadro, a estação simplesmente o faz. Caso ocorra colisão (interferência entre duas transmissões), o quadro será propagado com erro, causando o seu descarte pelo destinatário. O emissor detecta colisão pelo não recebimento do reconhecimento. Neste caso, a próxima retransmissão se dará após um intervalo de tempo aleatório. É importante tentar nova transmissão após um intervalo de tempo aleatório, pois, caso contrário, uma nova colisão certamente ocorrerá se ambos as estações colidentes tentarem a retransmissão ao mesmo tempo.

A técnica ALOHA pura apresenta baixa eficiência na utilização do canal pois uma transmissão em curso está sempre sujeita a interferência de outra que se inicia. A variante a seguir impede interferências numa transmissão em curso.

Método ALOHA Particionado

Esta variante do ALOHA puro permite que transmissões se iniciem em intervalos de tempo bem definidos (partições). Se o período das partições for superior ao tempo de

transmissão de um quadro, uma transmissão que se iniciou sem colisão será concluída sem colisão. Como desvantagem, a estação deve esperar o início do próxima partição para transmitir, mesmo que o meio esteja livre. O algoritmo é dado abaixo:

1. aguarde o *beep* de início de partição (fornecido por uma estação mestre);
2. transmita o quadro;
3. aguarde o reconhecimento da recepção por T unidades de tempo; se recebido, fim.
4. gere um número aleatório (r) entre 0 e R;
5. vá para 1 após r unidades de tempo.

Método CSMA Não Persistente

Os métodos da família CSMA têm em comum a capacidade de *escutar* o meio físico para a detecção de uma transmissão em curso. Uma estação somente inicia a transmissão se detectar o meio em repouso (sem transições, no caso de transmissão digital). Colisões ainda podem ocorrer, se duas estações detectarem o meio em repouso e iniciarem a transmissão ao mesmo tempo. Neste caso, a confirmação por parte do receptor, como nos métodos ALOHA, também é imprescindível.

O método CSMA Não Persistente opera segundo o algoritmo:

1. escute o meio;
2. se o meio estiver em repouso:
   (a) transmita o quadro;
   (b) aguarde o reconhecimento da recepção por T unidades de tempo; se recebido, fim;
   (c) vá para 1.
3. caso contrário (transmissão em curso):
   (a) gere um número aleatório (r) entre 0 e R;
   (b) vá para 1 após r unidades de tempo.

Quando detectada uma transmissão em curso, o método aguarda um intervalo aleatório antes de reiniciar a escuta do meio a fim de aguardar a sua liberação. Se a transmissão terminar logo após o início do intervalo aleatório, uma sub-utilização do meio é acarretada.

Método CSMA 1-Persistente

Este método é idêntico ao anterior, apenas fazendo o intervalo aleatório igual zero (escuta permanente do meio até cessar a transmissão em curso). Este método evita as esperas com o meio em repouso do anterior (aumentando portanto a utilização do canal) sob pena de um aumento da possibilidade de colisões quando duas estações estiverem sensoriando o meio ocupado por uma terceira.

Método CSMA p-Persistente

É um meio termo entre o método Não Persistente e o 1-Persistente. O método detecta o meio permanentemente até a transmissão em curso se encerrar. Neste ponto, o método pode transmitir ou suspender a transmissão por um intervalo de tempo aleatório. Os passos do algoritmo CSMA p-Persistente são os seguintes:

1. escute o meio até ser detectada a condição de repouso;
2. gere um número aleatório (s) entre 0 e 1;
3. Se s $\geq$ p:
   (a) transmita o quadro;
   (b) aguarde o reconhecimento da recepção por T unidades de tempo; se recebido, fim;
   (c) vá para 1.
4. Caso contrário (s $<$ p):
   (a) gere um número aleatório (r) entre 0 e R;
   (b) aguarde r unidades de tempo;
   (c) escute o meio; se em repouso vá para 2;
   (d) caso contrário (transmissão em curso):
      i. gere um número aleatório (u) entre 0 e U;

ii. vá para 1 após u unidades de tempo.

O método CSMA p-Persistente apresenta uma boa taxa de utilização do meio com baixa probabilidade da de ocorrência de colisões caso p seja ajustado às características do tráfego.

Método CSMA-CD

O método CSMA-CD (Collision Detection) adiciona aos métodos CSMA a detecção de colisões *sem a necessidade de aguardar reconhecimento por parte do receptor*. Detectada uma colisão, a estação interrompe imediatamente a transmissão, entrando em seguida num processo de retransmissão. O processo de detecção de colisão é simples: durante uma transmissão a estação escuta o meio, comparando o sinal no meio com aquele sendo transmitido. Ocorrida uma diferença, a estação conclui que uma segunda transmissão está se sobrepondo à sua.

Detectada uma colisão, a estação reforça a colisão com a injeção de sinais espúrios no meio *(jamming)* a fim de que as demais estações transmitindo detectem imediatamente a colisão e suspendam igualmente a transmissão. O algoritmo é composto dos seguintes passos:

1. escute o meio até ser detectada a condição de repouso;
2. inicie a transmissão do quadro, escutando o meio para se certificar que apenas esta transmissão está em curso; encerrada a transmissão do quadro sem colisão, fim;
3. reforce a colisão (jamming);
4. caso o número de colisões (c) na transmissão deste quadro exceder um limite, sinalize um erro à camada superior e termine;
5. gere um número aleatório (r) entre 0 e R(c);
6. vá para 1 após r unidades de tempo.

Como o método CSMA-CD detecta colisões independente do reconhecimento por parte do receptor, esta técnica pode suportar serviços de datagrama sem confirmação.

A rede Ethernet foi pioneira na introdução do método CSMA-CD, sendo, inclusive, comum empregar-se o termo *Ethernet* para este método de acesso ao meio.

6.2.2 Métodos Baseados em Passagem de Permissão

Os métodos baseados em passagem de permissão foram desenvolvidas para redes com topologia em anel. A idéia básica é ter-se uma ficha *(token)* circulando pelo anel, de estação para estação. A estação que detiver o *token* está autorizada a transmitir. Transmitido um quadro, este circula pelo anel até atingir a estação destino. Recebido sem erros no destino, a estação ativa no próprio quadro um bit de reconhecimento e transmite ao seu sucessor até atingir a estação que o emitiu (note que um quadro sempre dá uma volta completa pelo anel). O emissor pode então se certificar que o quadro foi corretamente recebido ou ignorado (devido a erros ocorridos na camada física ou inexistência do destinatário), drenando-o do anel.

Nenhuma estação pode manter a posse do *token* por um intervalo de tempo superior a um limite pré-estabelecido. Efetuadas as transmissões ou expirado o tempo máximo de posse do *token*, a estação o passa para sua sucessora. Redes com topologia em anel que empregam passagem de permissão como método de acesso ao meio são denominadas redes *token ring*. Métodos baseados em passagem de permissão apresentam duas características básicas: inexistência de colisões e tempo máximo de espera para acessar o meio (este tempo, em teoria, é infinito para os métodos de acesso aleatório). O anel pode conter uma *estação mestre* que tem como função verificar se o *token* não se perdeu, reiniciar o anel em caso de falhas, remover quadros corrompidos, etc. Em caso de falha desta estação, outra é eleita como mestre (automaticamente ou com a intervenção do operador).

Apesar da simplicidade do conceito, métodos de acesso ao meio baseados na passagem de permissão são bem mais complexos que os métodos de acesso aleatório. A seguintes situações devem ser tratadas:

- iniciação do anel quando o primeira estação é ligada;
- inserção de novas estações no anel;
- reconfiguração do anel ante a falha ou o desligamento programado de estações.

Apesar de associados à topologia em anel, métodos baseados em passagem de permissão também se aplicam a topologia de barramento. Neste caso, forma-se um anel lógico ordenando as estações de acordo com algum critério, por exemplo, seus endereços. O *token* circula neste anel lógico, dando permissão à estação que o detém de difundir quadros no meio físico. Redes com topologia de barramento que empregam passagem de permissão como método de acesso ao meio são denominadas redes *token bus* (figura 6.1).

Nestas redes a estação emissora não dispõe de confirmação por parte da receptora como nas redes *token ring* visto que o quadro é simplesmente difundido no barramento.

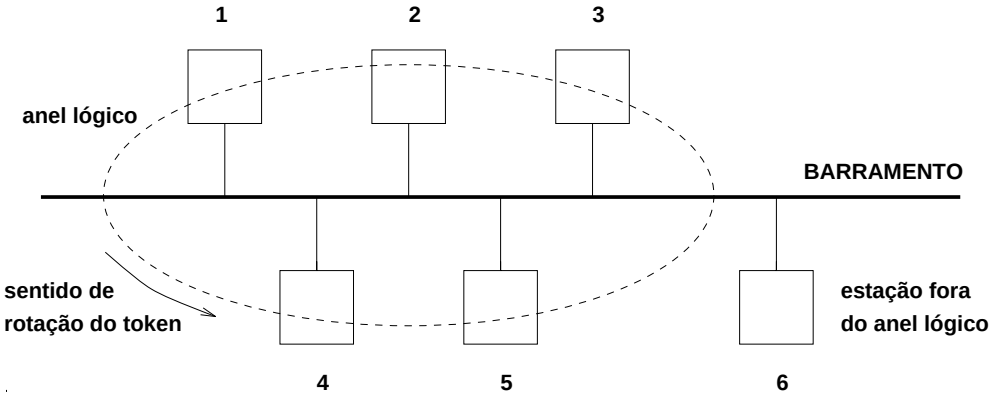


Figura 6.1: Passagem de permissão em redes com topologia de barramento.

Redes *token bus* apresentam um atrativo adicional em relação a redes *token ring*: uma estação pode receber mensagens sem estar participando do anel lógico (estação 6 na figura 6.1), posto que todas as mensagem são transmitidas em difusão pelo meio físico. Tais estações são incapazes de transmitir, pois jamais estarão de posse do *token* (no máximo podem responder a uma mensagem a elas direcionada). Esta característica das redes *token bus* viabiliza a inclusão de processadores extremamente simples na rede (microcontroladores, por exemplo), sem dotá-los da capacidade plena de acesso ao meio.

6.3 CSMA-CD no Padrão IEEE 802.3

O padrão IEEE 802.3 (Ethernet) estabelece o formato de quadros apresentado na figura 6.2.

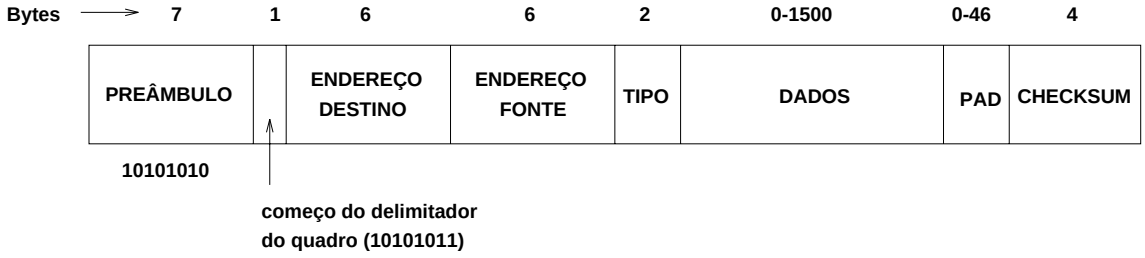


Figura 6.2: Formato dos quadros no IEEE 802.3.

O quadro inicia com um preâmbulo de 7 bytes composto dos bits 10101010. A seguir vem um byte de início de quadro composto dos bits 10101011. Duas seqüências de 6 bytes estabelecem os endereços do destinatário e do emissor, respectivamente. Seguem 2 bytes contendo o tipo da informação contida no quadro e os bytes correspondentes (1500 máximo). Caso o número de bytes da informação contida no quadro seja insuficiente para atingir o tamanho mínimo de quadro (64 bytes a partir do byte de início), um *pad* de 0 a 46 bytes completa as informações do quadro. Finalmente, 4 bytes são reservados para *checksum*.

A imposição de um tamanho mínimo de quadro se dá por duas razões:

1. quadros muitos curtos emitidos nos extremos da rede podem entrar em colisão sem que os respectivos emissores a detectem (isto é, quando um quadro atinge o extremo oposto a tansmissão do quadro neste extremo já foi concluída);
2. reforçar o *checksum*, diminuindo a probabilidade de diferentes arranjos de bits gerarem o mesmo *checksum*.

6.4 Passagem de Permissão no Padrão IEEE 802.5

O padrão IEEE 802.5 (Token Ring) é bem mais complexo que o CSMA-CD do 802.3. Duas características não presentes no 802.3 são definidas no 802.5: prioridade de acesso ao meio e reserva do meio.

O *token* é composto de 3 bytes: DI (delimitador de início) CA (controle de acesso) e TIPO. O primeito byte, DI, identifica o início do *token* e é formado por transições inválidas do código Manchester Diferencial (transições que jamais ocorrem em cadeias de 0s e 1s tais como duas transições positivas ou negativas seguidas). O segundo byte, CA, é utilizado para controle de acesso ao meio, sendo composto de agrupamentos de bits em 4 categorias:

1. status (1 bit): se o *token* está livre ou não;
2. monitor (1 bit): se o *token* passou pela estação mestre ou não. A estação mestre ativa este campo sempre que um *token* passar por ela;
3. prioridade (3 bits): estipula a prioridade mínima dos quadros que podem ser transmitidos com a captura do *token*. Se o valor deste campo for N, uma estação detentora do *token* pode transmitir quadros de prioridade maior ou igual a N;

4. reserva (3 bits): determina a prioridade do próximo *token* livre. Ao gerar um novo *token*, caso o valor da reserva seja maior que o valor da prioridade do token capturado, a estação atribui o valor da reserva como prioridade do *token*. Se uma estação desejar reservar o *token*, esta atribui ao campo de reserva a prioridade dos quadros que tem para transmitir, caso esta prioridade seja maior que a prioridade de reserva corrente. Para evitar que a prioridade do *token* cresça indefinidamente, toda a estação que aumentar a prioridade da reserva e capturar o *token* se compromete a liberá-lo com prioridade menor.

O byte de TIPO estipula o tipo da informação que o quadro carrega: dados oriundos das camadas superiores ou controle (este último utilizado para a manutenção do anel).

É frequente na literatura a afirmação que redes *token ring* são determinísticas, isto é, apresentam um tempo de acesso ao meio limitado (aproximadamente o tempo máximo de retenção do *token* multiplicado pelo número de estações no anel). Tal propriedade ocorre somente se o esquema de prioridade e reserva não seja utilizado.

A figura 6.3 mostra o formato de um quadro no padrão IEEE 802.5.

Figura 6.3: Formato dos quadros no IEEE 802.5.

Capturado o *token*, o quadro é injetado no anel logo a seguir. Os campos de endereço e *checksum* são idênticos ao IEEE 802.3. A quantidade de dados é ilimitada (a rigor, limitada pelo tempo máximo que uma estação pode reter o *token*). O campo DF (delimitador de final) também é composto por transições Manchester Diferencial inválidas. Um campo após o DF, ST (status) contém dois bits: A e C. O bit A é ativado pela estação de destino, informando a estação emissora que tomou conhecimento do quadro a ela endereçado. O bit C é ativado se a estação de destino aceitou o quadro (pode tê-lo rejeitado por falta de área para armazenamento, por exemplo).

Duas observações importantes:

1. um quadro no IEEE 802.5 não define campo de tamanho do quadro; o campo de dados começa 14 bytes após o campo DI do *token* e termina 4 bytes antes do campo DF do quadro;

2. o campo DF deve obrigatoriamente preceder o campo ST; o destinatário está em condições de aceitar um quadro (bit C do campo ST) somente após computar o *checksum* e, como não existe quadro de tamanho de dados, o campo de *checksum* só é definido após o recebimento do campo DF.

6.4.1 Manutenção do Anel

Uma das estações do anel é rotulada como estação mestre (EM). Via de regra, é a primeira estação a completar o procedimento de *boot*. Caso esta estação falhe, uma nova EM é eleita. Periodicamente, a EM circula um *token* com o campo TIPO contendo a informação ACTIVE_MONITOR_PRESENT. Se este *token* ficar sem circular por determinado período, inicia-se um procedimento de escolha de uma nova EM.

Assim que uma estação termina o procedimento de *boot*, ela aguarda a passagem do *token* ou um quadro de ACTIVE_MONITOR_PRESENT. Expirado este tempo de espera, a estação gera um quadro de controle com a informação CLAIM_TOKEN. Se este quadro circular sem alteração, a estação que o emitiu se torna a estação mestre. Se já existir uma EM, a mesma altera o quadro de CLAIM_TOKEN, informando ao emissor do quadro a sua existência.

São atribuições da estação mestre:

- drenar quadros corrompidos do anel;
- drenar quadros órfãos do anel (quadros não drenados pelo emissor por falhas de hardware ou software);
- verificar se o *token* não se perdeu (a etsação detentora do *token* falha em injetar um novo *token* no anel). Neste caso, a estação mestre gera um novo *token* no anel.

O dreno de quadros pela estação mestre é feito caso o bit de monitor do quadro CA estiver ativado quando o quadro passar pela EM (indicando que se trata de uma segunda passagem).

Finalmente, quando uma estação suspeitar da ruptura do anel (tempo longo sem a passagem de *tokens*), esta injeta um *token* de controle com a informação BEACON no campo TIPO. Se o quadro voltar à estação emissora, esta supõe que o problema foi sanado. Caso contrário, a estação entra num estado de *standby* aguardando o reestabelecimento do anel.

6.5 Passagem de Permissão no Padrão IEEE 802.4

O padrão IEEE 802.4 (Token Bus) emprega topologia de barramento, sendo o meio controlado por passagem de permissão. O anel lógico (figura 6.4) é estabelecido ordenando-se as estações de acordo com os respectivos endereços (número formado pelos 48 bits que compõem o endereço). O *token* circula no sentido do endereço mais alto para o mais baixo.

O padrão define quatro prioridades para os quadros: 0, 2, 4 e 6 (a mais alta). Logicamente, é como se cada estação tivesse quatro filas de quadros para serem transmitidos. De posse do *token*, a estação transmite os quadros de prioridade 6. Esgotados estes, os de prioridade 4 são transmitidos e assim por diante até que todos os quadros pendentes se esgotem ou o tempo máximo de posse do *token* for atingido.

Os quadros do padrão IEEE 802.4 têm o formato dado pela figura 6.4.

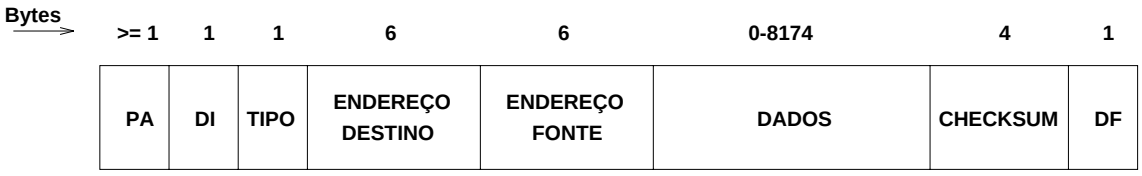


Figura 6.4: Formato dos quadros no IEEE 802.4.

O preâmbulo (PA) tem duracão superior ou igual a um período de um byte. Sua função básica é permitir que as estações se preparem para receber o quadro, sincronizando seus relógios com o da estação emissora. A seguir, o campo DI (delimitador de início) contém codificações inválidas como no IEEE 802.5. O campo TIPO contém os seguintes dados:

1. tipo do quadro (2 bits): se quadro de controle, de dados ou de gerenciamento do anel.
2. prioridade (3 bits): prioridade mínima dos quadros que podem ser transmitidos com a captura do token.

O padrão IEEE 802.4 não provê mecanismo de reserva como no IEEE 802.5. O campo de dados pode conter no máximo 8174 bytes. O campo de *checksum* e o delimitador de final (DF) são similares ao 802.5.

6.5.1 Manutenção do Anel Lógico

Cada estação mantém o endereço de sua antecessora e de sua sucessora no anel. Não existe estação mestre. O anel é iniciado quando a primeira estação termina o procedimento de *boot*. A estação monitora o meio por determinado período de tempo. Caso nenhuma atividade seja detectada, a estação emite um quadro de controle to tipo CLAIM_TOKEN. Se não houver contestação, a estação se torna detentora do *token* (e neste caso, sozinha no anel).

De posse do *token* e terminadas as transmissões, caso o período de posse do *token* não tenha se expirado, a estação cria uma *janela de inclusão*, dando chance a outras estações de ingressarem no anel lógico. A estação detentora do *token* propaga um quadro do tipo SOLICIT_SUCESSOR com o seu endereço no campo de endereço fonte e o de sua atual sucessora no campo de endereço destino do quadro. Caso alguma estação esteja esperando para ingressar no anel (isto é, sua tentativa de iniciar o anel falhou) e seu endereço esteja situado entre estas estações, a mesma responde informando seu endereço. A estação emissora armazena o novo endereço de sua sucessora, e informa a sua antiga sucessora que sua antecessora mudou. A estação ingressante tem os endereços de sua antecessora e sucessora no quadro que iniciou o procedimento. Caso mais de uma estação responda à proposta de inclusão, um procedimento de contenção seleciona apenas uma (ficando as demais aguardando as próximas janelas de inclusão).

A saída de uma estação no anel é um procedimento mais simples que o ingresso. De posse do *token*, a estação propaga um *token* do tipo SET_SUCESSOR dirigida a sua antecessora com o endereço de sua sucessora no quadro. A estação antecessora armazena sua nova sucessora, eliminando assim a estação que iniciou o processo do anel lógico.

A passagem do *token* é um processo delicado. A estação cria um quadro de controle do tipo TOKEN com o campo de endereço destino igual ao de sua sucessora. Recebido pela sucessora, esta se considera de posse do *token*. A estação que passou o *token* certifica-se de seu recebimento através da escuta do meio. A estação que recebeu o *token* acessa o meio logo a seguir seja para transmitir seus quadros, seja para passar o *token* adiante. Caso o meio fique inativo, a estação que passou o *token* propaga um quadro do tipo WHO_FOLLOWS fornecendo o endereço de sua sucessora no campo de endereço destino do quadro. A estação que tiver como antecessora este endereço responde, tornando-se a nova sucessora a receber o *token* (a estação que falhou em receber o *token* é eliminada do anel lógico, podendo ingressar mais tarde via janela de inclusão). Caso o procedimento de WHO_FOLLOWS falhe, um quadro do tipo SOLICIT_SUCESSOR2 é propagado solicitando que todas as estações que seguem a emissora no anel lógico respondam. Neste procedimento, mais de uma estação é eliminada do anel lógico.

Duas situações devem ainda ser gerenciadas:

- *tokens* duplicados: se uma estação detentora do *token* "ouvir" uma transmissão, esta o descarta (eventualmente todos os *tokens* duplicados são descartados, vide abaixo);
- perda do *token*: se uma estação não receber o *token* por um período longo, esta inicia um procedimento de CLAIM_TOKEN. Caso mais de uma estação o faça, um algoritmo de contenção indica a estação vencedora (que terá a posse do *token*).

6.6 O Padrão ANSI X3T9.5 (FDDI)

O padrão ANSI X3T9.5 (FDDI: Fiber Distributed Data Interface) normatiza uma rede com duplo anel em fibra óptica operando a 100 Mbits/s. O comprimento do anel pode chegar a 100 Km, o que dá à rede características de rede metropolitana. Foi adicionado posteriormente ao padrão como meios de transmissão alternativos o par metálico trançado e a fibra óptica monomodo. O padrão define duas classes de estações:

1. classe A: conectadas no duplo anel;
2. classe B: conectadas via *hub* (este ligado no duplo anel).

A Figura 6.5 ilustra a topologia de uma rede FDDI.

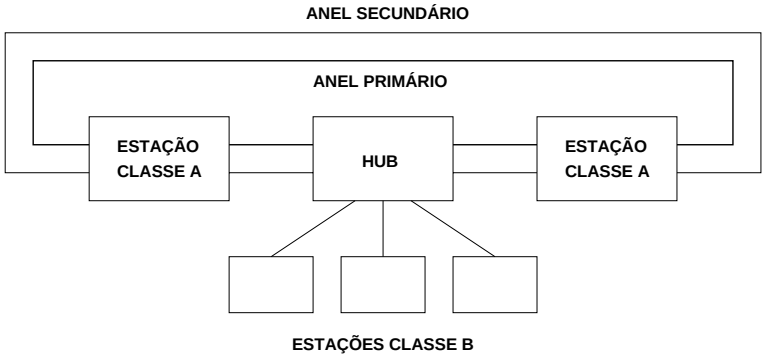


Figura 6.5: Topologia de uma rede FDDI.

A rede utiliza apenas um anel (dito primário) para o tráfego de dados, deixando o segundo anel (secundário) para reconfiguração. Os dois anéis se fundem quando uma interrupção é detectada no anel primário.

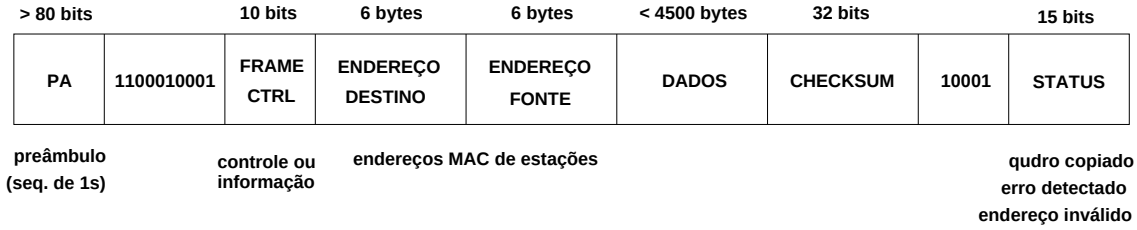


Figura 6.6: Quadro FDDI. Campos com tamanhos em bits contém símbolos TAXI.

O padrão FDDI prevê dois tipos de tráfego:

1. síncrono, com garantia de banda e atraso máximo, mas não isócrono;
2. assíncrono, sem qualquer garantia de qualidade de serviço.

No modo assíncrono o FDDI se comporta como uma rede Token Ring de alta taxa de transmissão. O acesso ao meio se dá por passagem de permissão.

O quadro de informação é exposto na Figura 6.6. O padrão admite um campo de dados de tamanho máximo de 4500 bytes. Quadros de permissão (token) possuem os dois primeiros campos idênticos ao quadros de dados, um tipo de quadro que identifica uma permissão e um delimitador de final de quadro.

O padrão FDDI define um protocolo de gerenciamento denominado SMT (Station Management) com funções que permitem gerenciar a configuração física do anel, gerenciar o estabelecimento de conexões (alocação de banda) e gerenciar a operação da rede. Através de SMT é possível estabelecer parâmetros como o tempo máximo que uma estação pode permanecer sem a posse do token, o tempo máximo de posse do token e o tempo máximo para a transmissão de tráfego síncrono.

As estações começam sua operação no modo assíncrono. Quando uma estação desejar utilizar o serviço síncrono, ao capturar a permissão a mesma transmite quadros da classe de serviço síncrono por um período negociado pelo SMT. Isto dá a cada estação a possibilidade de utilizar um percentual de sua banda máxima para tráfego síncrono e o restante para tráfego assíncrono. O padrão garante um tempo máximo de espera pelo token o que propicia uma banda mínima (de pior caso) para o tráfego síncrono. O padrão ainda prevê oito tipos de prioridade para o tráfego assíncrono. Um percentual do tempo de posse do token é reservado para cada nível de prioridade.

O tráfego síncrono é um meio termo entre o tráfego isócrono e o tráfego assíncrono para o transporte de áudio e vídeo. O tráfego síncrono torna o FDDI adequado para o transporte de áudio e vídeo pois pode-se compensar o jitter com uma pequena bufferização no destino. Infelizmente, interfaces de rede e *hubs* FDDI não implementam tráfego síncrono, tornando o FDDI simplesmente uma Token Ring mais rápida.

6.7 O Padrão IEEE 802.6 (DQDB)

O padrão IEEE 802.6 (DQDB: Distributed Queue Dual Bus) emprega uma topologia com dois barramentos unidirecionais (Figura 6.7). As estações em cada extremidade são responsáveis pela geração de slots de tamanho fixo (53 bytes).

Os padrões físicos DQDB suportam transmissão nas taxas de 44,736 Mbits/s (padrão ANSI DS3 para cabo coaxial e fibra óptica); 155,52 Mbits/s (padrão SONET para fibra óptica) e 34,368/139,264 Mbits/s (padrão ITU-T G.703).

DQDB suporta dois modos de enlace: assíncrono e isócrono. No modo assíncrono o DQDB comporta-se como uma LAN convencional (803.5 por exemplo). No modo isócrono, quadros são gerados a uma taxa constante e reservados às conexões dedicadas a este tipo de tráfego.

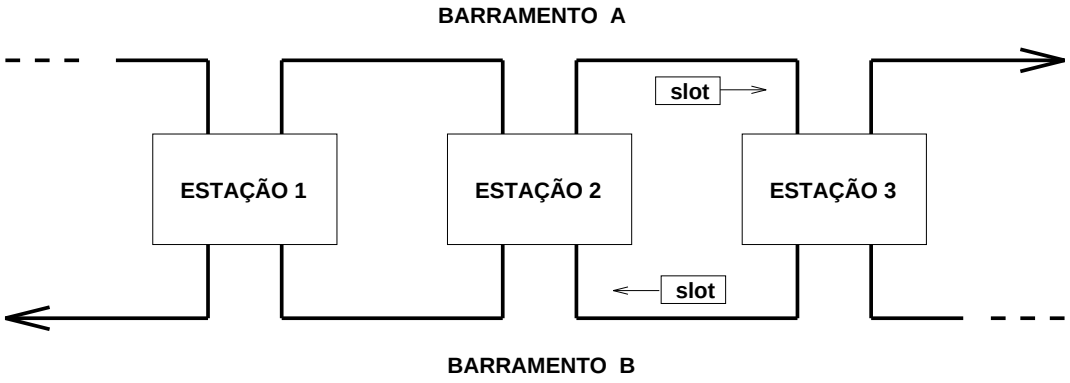


Figura 6.7: Topologia de redes DQDB.

A configuração de um slot é dada na Figura 6.8. O primeiro bit (L/O) do slot indica se este está livre ou ocupado (carregando dados). O segundo bit do slot (TS) indica o tipo do slot: fila arbitrada (QA) ou pré-arbitrado (PA) conforme exposto a seguir. Os três próximos bits são reservados para uso futuro. Os últimos três bits (RESERVA) são usados para reservar slots com determinada prioridade, onde cada bit indica um nível de

prioridade. Estes oito primeiros bits formam o campo de controle de acesso (ACF) do slot. Seguindo o ACF do slot vem um cabeçalho de quatro bytes composto de quatro campos:

- VCI: indica o número do canal virtual (20 bits);
- TD: tipo dos dados (2 bits) — 00 indica dados gerados pela camada superior;
- PRIO: prioridade do segmento (2 bits) — reservado para a interconexão de redes DQDB;
- CRC: detecção de erros por redundância cíclica (8 bits).

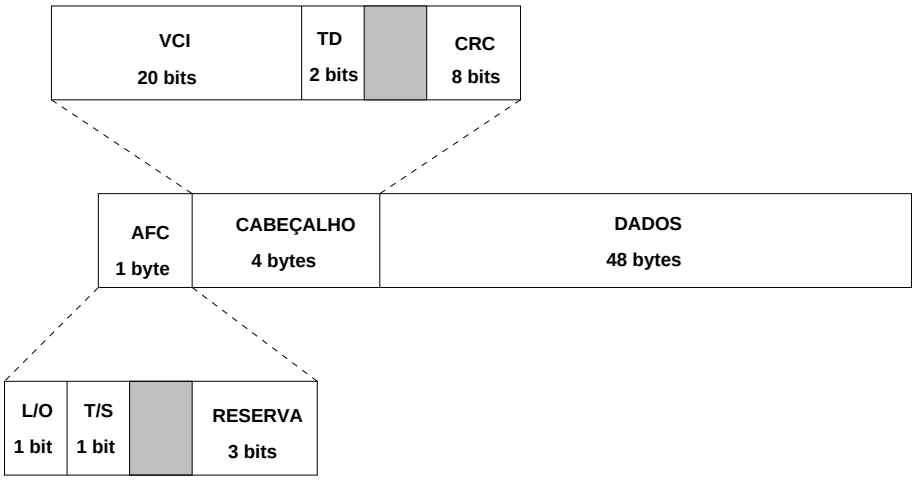


Figura 6.8: Formato de um slot DQDB.

Seguindo o cabeçalho, um campo de 48 bytes contém dados oriundos das camadas superiores.

DQDB oferece dois modos de enlace: isócrono e assíncrono. O modo isócrono emprega um controle de acesso ao meio denominado pré-arbitrado (PA). Durante o estabelecimento de uma conexão para tráfego isócrono a unidade de gerenciamento da estação geradora de slots é instruida a gerar slots numa taxa média com determinada variação máxima. A estação receptora irá compensar esta variação na taxa de geração de slots com o uso de buffers. Os slots para este serviço são gerados com o número da conexão, tornando-os portanto de uso exclusivo das estações que fazem parte da conexão.

Serviços assíncronos empregam um mecanismo de reserva de slots conhecido como fila distribuída. Seja a Figura 6.7 onde a estação E2 deseja transmitir um slot à estação E3.

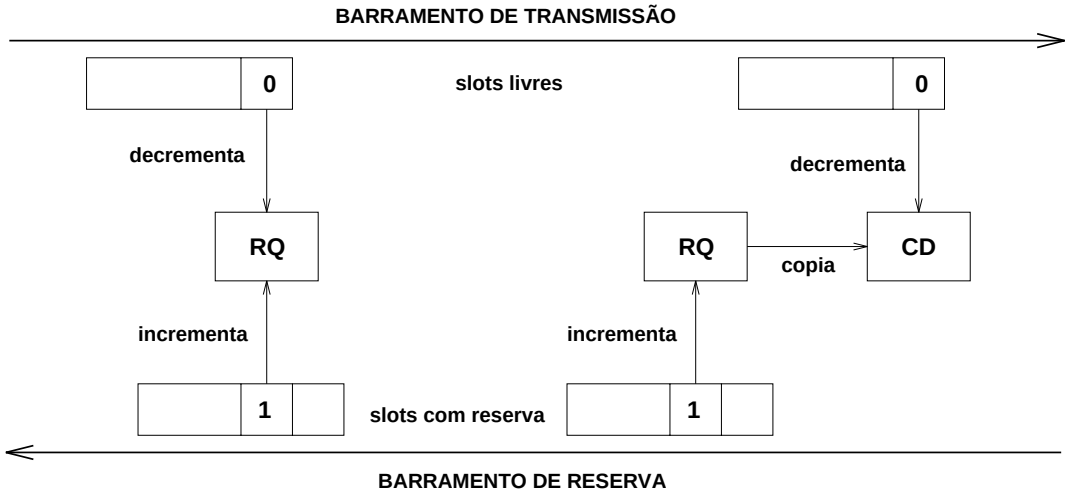


Figura 6.9: Algoritmo da fila distribuída. Situações em que a estação não tem slots para transmitir (A) e imediatamente após reservar um slot (B).

Neste caso, em relação à estação E2, o barramento A é dito de transmissão e o barramento B de reserva. A estação E2 aguarda um slot livre (bit L/O zerado) e ativa um bit no campo de reserva (veja Figura 6.8). Por simplicidade vamos considerar que todas as estações se utilizam de apenas um nível de prioridade. Com esta ação, a estação E2 indica a todas suas antecessoras na barra de transmissão seu desejo de transmitir um slot. Cada estação possui um contador de reservas (RQ) que armazena o número de reservas solicitadas por estações à sua frente em cada um dos barramentos. Este contador é atualizado todas as vezes que um slot contendo uma requisição passa pelo barramento oposto (de reserva).

Quando uma estação não possui slots para transmitir e detecta um slot vazio no barramento de transmissão, o contador RQ é decrementado pois o slot irá atender uma requisição para uma estação sucessora neste barramento. Caso a estação tenha gerado uma reserva no barramento de reserva (e portanto deseja transmitir um slot) o valor do contador RQ é copiado para outro (CD), que também é decrementado na passagem de um slot vazio no barramento de transmissão. O contador CD indica a posição relativa da estação em relação às outras que efetuaram reservas à sua frente. Quando o contador CD estiver zerado e passar um slot livre, a estação transmite neste slot (isto indica que todas as estações sucessoras que reservaram slots primeiro já foram atendidas). A Figura 6.9 ilustra a operação do algoritmo da fila distribuída.

Consideramos apenas um nível de prioridade para expor o algoritmo da fila distribuída. Para o caso dos três níveis de prioridade, utiliza-se três contadores RQ e CD (um para cada nível). Neste caso o contador CD relativo ao nível de prioridade j além de ser

decrementado na passagem de um slot vazio (barramento de transmissão), deve ser incrementado na passagem de uma reserva de prioridade superior a j (barramento de reserva). Uma estação somente transmite um quadro de prioridade j quando o contador relativo a este nível estiver zerado.

O padrão IEEE 802.6 é adequado para aplicações multimídia distribuídas. Sua taxa de transmissão elevada combinada com sua capacidade de prover tráfego isócrono torna a tecnologia DQDB muito superior às tecnologias CSMA/CD e Token Ring. Múltiplas redes DQDB interconectadas formam uma rede metropolitana.

6.8 Serviço SMDS

SMDS (Switched Multimegabit Data Service) é um serviço comutado sem conexão oferecido por provedores públicos tipicamente numa região metropolitana. SMDS não é uma tecnologia de rede, mas um serviço comutado acessado via rede DQDB (seção 6.7). O acesso DQDB ao serviço SMDS se dá à taxas de 4, 10, 16, 25 ou 34 Mbits/s. Estas taxas são suficientemente altas para qualificar o SMDS como um serviço de interconexão de LANs de alta velocidade. SMDS pode ser oferecido também à taxas entre 64 Kbits/s e 1.544 Mbits/s (T1). Nesta forma de acesso a rede DQDB é substituida por um acesso síncrono tipo ISDN.

Os componentes do serviço SMDS são ilustrados na figura 6.10. CPEs (Customer Premisses Equipments) são equipamentos de comunicação de dados (DTEs) que conectam computadores e redes do assinante à malha de comutação SMDS através de rede DQDB (ou linha síncrona no caso de acesso de baixa velocidade). O protocolo SIP (SMDS Interface Protocol) disciplina o acesso do CPE à malha de comutação. SIP é um protocolo com 3 níveis:

- Nível 3: corresponde à unidade de serviço (SDU) do padrão IEEE 802.6;
- Nível 2: corresponte ao nível de segmentação e remontagem do padrão 802.6;
- Nível 1: corresponde à camada física (DS3 ou SONET STS-3).

O nível 3 do protocolo SIP permite o encapsulamento de até 9188 bytes. A PDU deste nível consiste de 24 bytes de cabeçalho e 4 bytes de fecho. Endereçamento no SMDS utiliza o padrão ITU-T E.164. A figura 6.11 ilustra um PDU de nível 3 do protocolo SIP. O campo BEtag (Begin-End tag) consiste de um contador incrementado a cada PDU

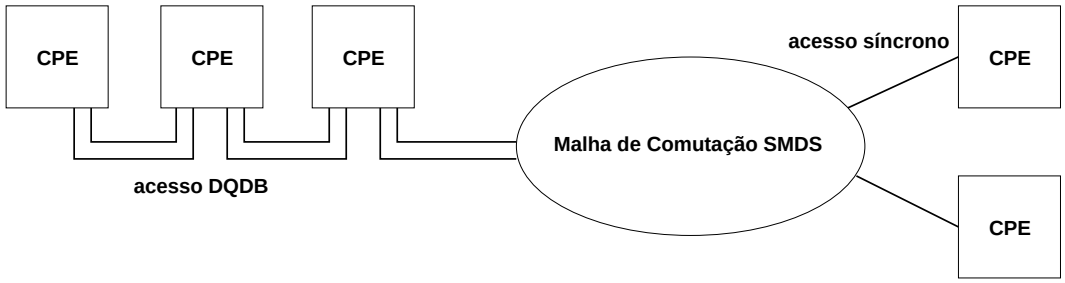


Figura 6.10: Componentes do serviço SMDS.

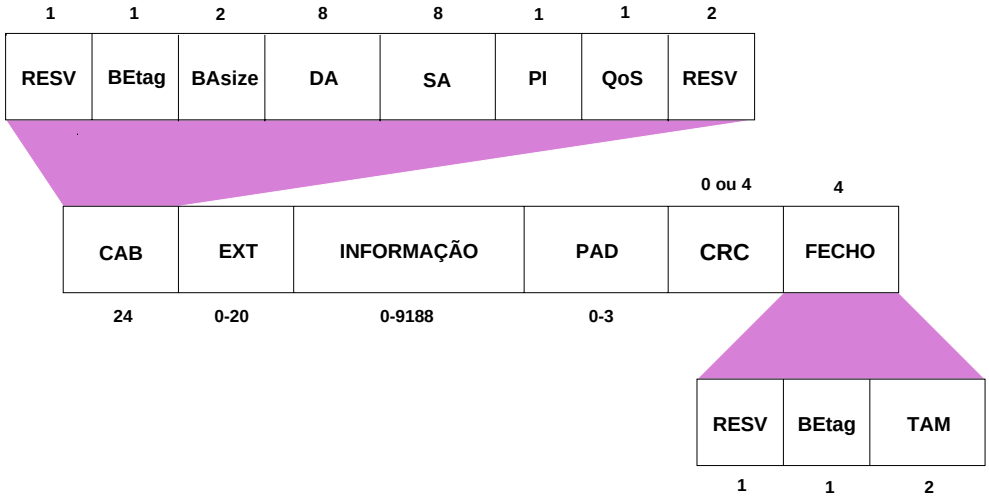


Figura 6.11: PDU de nível 3 do protocolo SIP (tamanho dos campos em bytes).

emitido e se presta a delimitar um PDU para fins de remontagem no destino. O campo BAsize (Buffer Allocation size) informa o receptor a quantidade de buffers necessária à sua recepção (via de regra, o tamanho da PDU). Os campos DA (Destination Addres) e SA (Source Address) contém os endereços destino e fonte. O campo PI (Protocol Identifier) identifica o protocolo de camada superior sendo transportado. O campo QoS (Quality of Service) estipula a qualidade de serviço associada ao PDU (atraso e taxa de perda), além de sinalizar a presença ou não do campo CRC. O campo PAD torna o tamanho do PDU múltiplo de 4 bytes, restrição esta imposta pelo procedimento de segmentação e remontagem do nível 2. O campo CRC, quando presente, contém o código de redundância cíclica computado sobre todos os bytes do PDU e visa garantir que a PDU recebida não foi alterada em curso. Finalmente, o campo TAM (tamanho) carrega o tamanho exato do PDU.

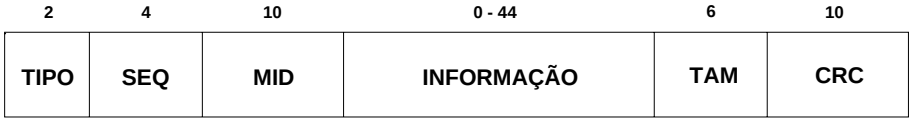


Figura 6.12: PDU de nível 2 do protocolo SIP (tamanho dos campos em bits).

No nível 2, o PDU de nível 3 é segmentado em unidades de 48 bytes (o tamanho da carga na célula DQDB). Destes 48 bytes, 2 são utilizados como cabeçalho e 2 como fecho (figura 6.12). O campo TIPO informa o tipo de segmento: início de mensagem, continuação de mensagem, término de mensagem e mensagem de único segmento. O campo SEQ é um número de sequência para fins de remontagem. O campo MID (Message IDentifier) permite multiplexar o tráfego de PDUs de nível 3 sobre uma única conexão DQDB. O campo TAM informa o tamanho dos dados transportados pelo segmento. O campo CRC possui a mesma função de seu correspondente de nível 3.

6.9 O Padrão IEEE 802.11 (Wireless)

O padrao IEEE 802.11 define elementos da camada física e de acesso ao meio para redes locais sem fio. A camada física utiliza radiofrequência ou infravermelho e opera com taxas de 1 ou 2 Mbits/s conforme descrito na seção 2.2.3. Nesta seção descreveremos a subcamada MAC para redes sem fio em geral e redes 802.11 em particular.

Redes sem fio 802.11 podem operar numa configuração *ad-hoc* (peer-to-peer) ou com ponto de acesso (AP: Access Point). A figura 6.13 ilustra estas duas formas de organização. Em configurações *ad-hoc* cada estação se comunica diretamente com qualquer outra estação da rede (analogamente às topologias de barramento). Por outro lado, configurações com ponto de acesso demanda a intervenção do AP para que duais estações se comuniquem. A motivação para configurações com APs é uma cobertura maior da rede com a utilização de múltiplos APs e a interconexão com redes tradicionais.

A técnica de acesso ao meio do padrão IEEE 802.11 denomina-se CSMA/CA (Carrier Sensing Multiple Access/Colision Avoidance). Diferentemente do padrão CSMA/CD utilizado em redes 802.3 (Ethernet), colisões no CSMA/CA devem ser evitadas, não apenas detectadas. Outra diferença importante é o que o CSMA/CA utiliza reconhecimento no nível de subcamada MAC, enquanto o CSMA/CD não utiliza.

O procedimento CSMA/CA opera da seguinte forma. Uma estação que deseja trans-

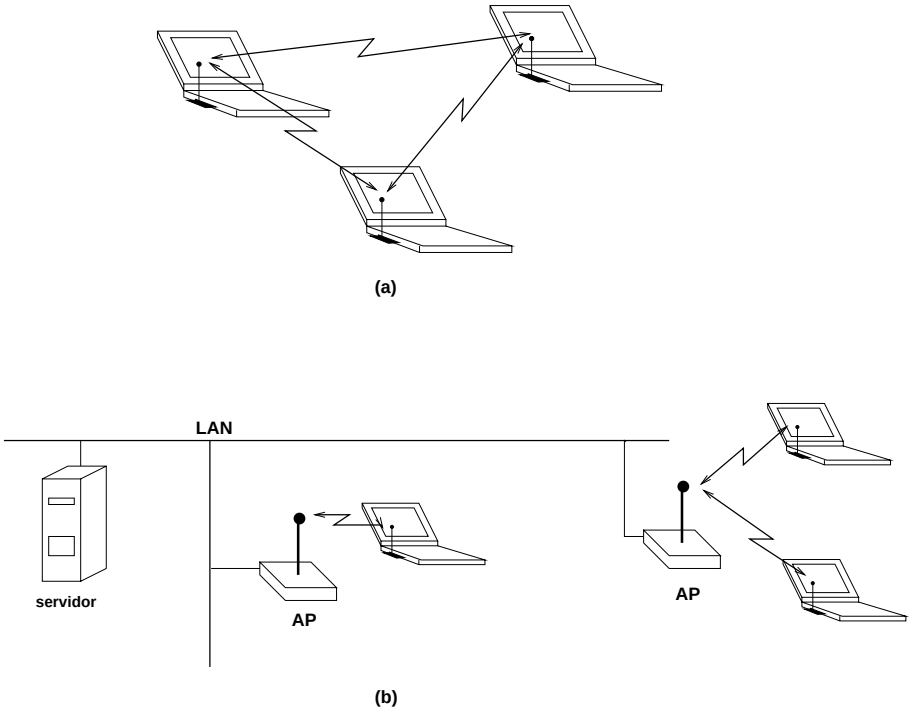


Figura 6.13: Organização de uma WLAN: (a) ad-hoc; (b) baseada em APs.

mitir primeiro detecta se existe uma emissão em curso. Em existindo, a estação suspende o processo por um período de tempo (backoff), voltando a detectar o meio após este período. Cada vez que a estação detecta o meio em atividade, a mesma diminui o backoff, aumentando a probabilidade de detecção do meio livre. Caso nenhuma emissão esteja em curso, a estação inicia a transmissão do quadro. A estação receptora deve emitir um breve reconhecimento (ACK) após 10 microsegundos, caso o código de redundância cíclica (CRC) do quadro recebido esteja correto. Dado que o protocolo exige um espaçamento entre quadros de 50 microsegundos, a estação receptora não necessita executar o procedimento de acesso ao meio para transmitir o ACK.

A rigor, nesta forma de operação o protocolo CSMA/CA não é livre de colisões. Seja a figura 6.14 onde as estações A e B estão na região de cobertura do AP, mas em distância tal que a emissão de uma não seja captada pela outra. Assim sendo, se A está transmitindo para o AP, B pode detectar o meio livre e iniciar uma transmissão provocando colisão no AP. Este problema é conhecido como "estação escondida".

Opcionalmente o protocolo CSMA/CA pode operar de forma mais restritiva onde uma estação para transmitir necessita solicitar permissão ao AP (figura 6.15) através de um quadro RTS (Request To Send). Quando o meio ficar disponível o AP difunde um

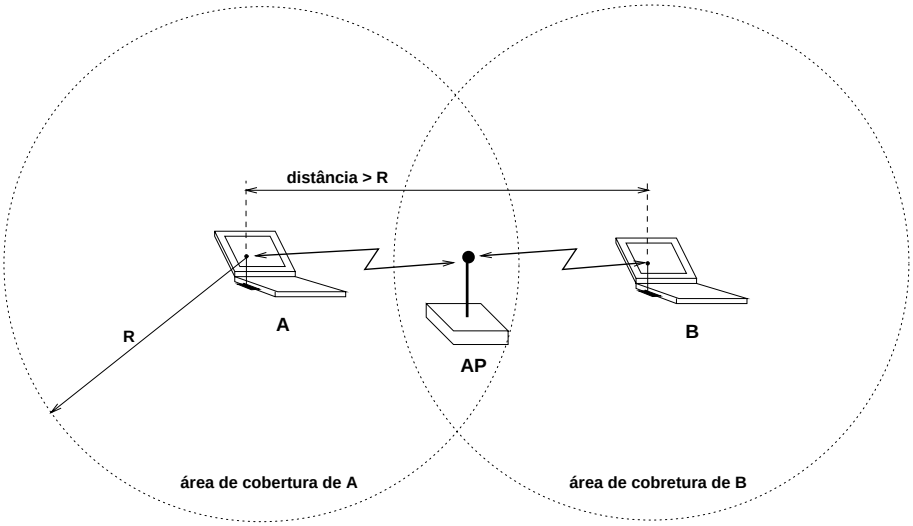


Figura 6.14: O problema da "estação escondida".

quadro CTS (Clear To Send). Este quadro é captado por todas as estações concedendo permissão para transmitir à estação que solicitou tal permissão. Este procedimento pode ser desabilitado caso o problema da estação escondida não exista (isto é, todas as estações encontram-se numa área de cobertura comum).

Adicionalmente, o protocolo MAC 802.11 permite ainda:

- fragmentação de mensagens: aumenta o desempenho da rede em ambientes de alta interferência;
- *roaming*: permite a WLAN operar numa estrutura celular (cada AP gerencia uma célula e estações podem se desassociar de um AP e associar-se a outro AP);
- gerenciamento de potência: permite estações baixarem o nível de potência do receptor face à inatividade do meio;
- privacidade: permite criptografia para a carga dos quadros.

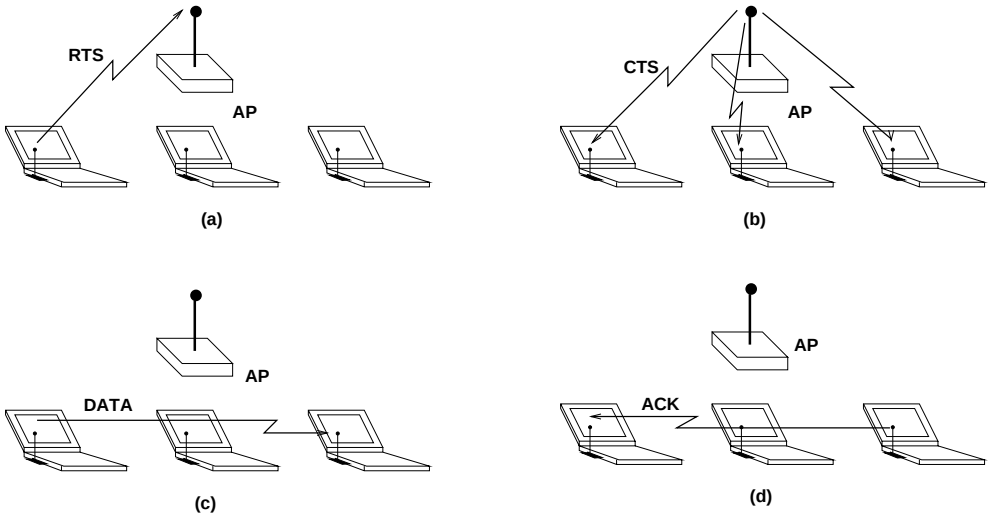


Figura 6.15: Protocolo CSMA/CA com quadros RTS e CTS.

Capítulo 7

Interconexão de Redes de Computadores

O objetivo das técnicas envolvidas na interconexão de redes de computadores visa permitir que se crie uma rede única global que será constituida na realidade da interconexão de sub-redes. A idéia de uma rede global procura emular, por exemplo, a funcionalidade oferecida atualmente pela rede telefônica através da qual é possível acessar sem dificuldades qualquer outro telefone em qualquer parte do planeta. Esta mesma possibilidade é desejável no caso das redes de computadores de modo que um computador possa interagir com outro independentemente das suas localizações. Este objetivo seria mais facilmente alcançável se fosse utilizada uma única tecnologia de rede para criar a infra-estrutura necessária à interconexão dos computadores. Entretanto, a utilização de uma única tecnologia não representa em geral a melhor solução já que dificilmente existirá uma tecnologia que possa atender satisfatoriamente os requisitos dos diversos usuários e das várias aplicações. Desta maneira, a interconexão de computadores passa pela interconexão de subredes, onde subrede neste contexto representa uma estrutura de comunicação envolvendo uma única tecnologia. Por exemplo, uma rede local Ethernet, rede local Token Ring, Rede Pública baseada em X.25, etc.

No contexto da discussão envolvendo a interconexão de redes de computadores, um aspecto essencial consiste na localização dos sistemas computacionais que se deseja acessar. Esta localização depende do uso de esquemas de endereçamento adequados os quais dependem do protocolo utilizado. Do ponto de vista da questão do endereçamento, dois tipos de endereços devem ser destacados: endereço da camada de enlace e endereço da camada de rede[1]. Em geral o endereço de enlace (endereço físico) no caso da maioria das

[1]Estes endereços foram ilustrados no apresentação da arquitetura TCP/IP (capítulo 6).

redes locais tem o seu valor fixado a uma interface de rede. Este endereço costuma ser único, ou seja, ele não deve se repetir em qualquer outra interface que venha a ser fabricada, sendo o controle dos endereços realizado pela organização responsável pela definição do padrão da interface. Como em geral a maior parte dos computadores possui uma única conexão física de rede, eles somente possuem um único endereço para a camada de enlace. No caso dos roteadores, por outro lado, estes possuem mais de um endereço de enlace. Os endereços de enlace possuem uma estrutura plana (flat), isto é, a sua estrutura não possui qualquer referência hierárquica na constituição do respectivo endereço.

Os endereços correspondentes à camada de rede, também denominados de endereços lógicos ou virtuais, costumam ser organizados em uma forma hierárquica. Eles podem ser ilustrados, por exemplo, através do endereçamento postal, onde o endereço do destinatário é formado pelo seu nome, a rua onde mora e o número da sua casa, a cidade, o estado e o país. Este tipo de estrutura permite, por exemplo, que um remetente em Paris de uma correspondência para alguém em Campinas, SP., ao estruturar o endereço do destinatário segundo esta hierarquia, permitirá à central dos correios na França que encaminhe a correspondência para a central dos correios no Brasil baseando-se somente no país destino da correspondência. Ao chegar em São Paulo a distribuição poderá encaminhar a correspondência para os Correios em Campinas, etc. Desta forma, podemos perceber que a estrutura hierárquica de endereços facilita o encaminhamento da mensagem através da consulta de parte do endereço.

Resolvida a questão do endereçamento, a informação poderá ser trocada entre o remetente e destinatário. Dependendo da camada do Modelo OSI na qual a informação é trocada ela será denominada de quadro (frame) quando a interação situar-se no nível da camada de enlace (camada 2 do Modelo OSI), pacote quando a interação ocorrer no nível da camada de rede (camada 3 do Modelo OSI) e mensagem quando a interação for relativa a entidades de camadas do Modelo OSI superiores à camada de rede.

7.1 Dispositivos de Interconexão

Os dispositivos de interconexão de redes de computadores podem ser classificados em cinco dispositivos principais:

- repetidores (repeters);
- pontes (bridges);
- chaves (switches);

- roteadores (routers);
- comportas (gateways).

A distinção entre estes dispositivos pode ser feita levando-se em conta a camada do Modelo de Referência OSI/ISO na qual a funcionalidade do dispositivo está relacionada. A figura 7.1 fornece uma idéia inicial da utilização destes dispositivos.

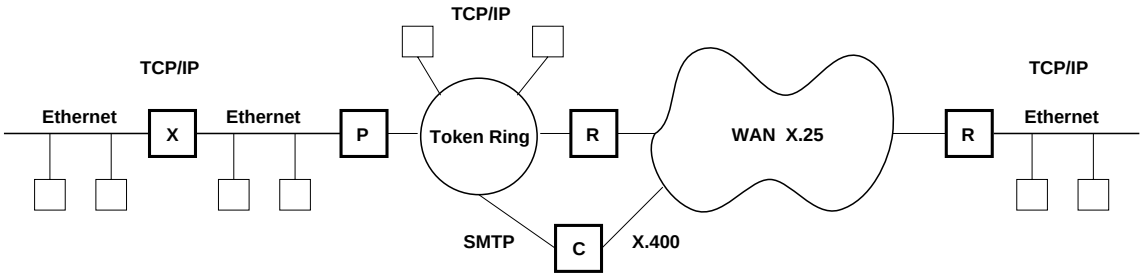


Figura 7.1: Exemplo de interconexão de redes. Retângulos com a letra X são repetidores; com a letra P pontes; com a letra R roteadores; e com letra C comportas. Demais retângulos representam hosts.

7.1.1 Repetidores

O repetidor é o dispositivo mais básico dentre aqueles utilizados na interconexão de redes. O seu objetivo é a interconexão física entre LANs do mesmo tipo sendo que a única diferença permitida diz respeito ao canal utilizado em cada LAN.

As principais funções de um repetidor são:

- restauração do sinal - significa restaurar o sinal à sua forma original o que inclui não somente uma reamplificação do sinal mas também alguma interpretação do sinal recebido;
- isolamento de falha no cabo - significa que uma falha em um dos segmentos interconectados não deve repercutir no sistema como um todo causando a falha completa. Os repetidores monitoram continuamente os segmentos interconectados com o objetivo de detetar e isolar segmentos com falha;

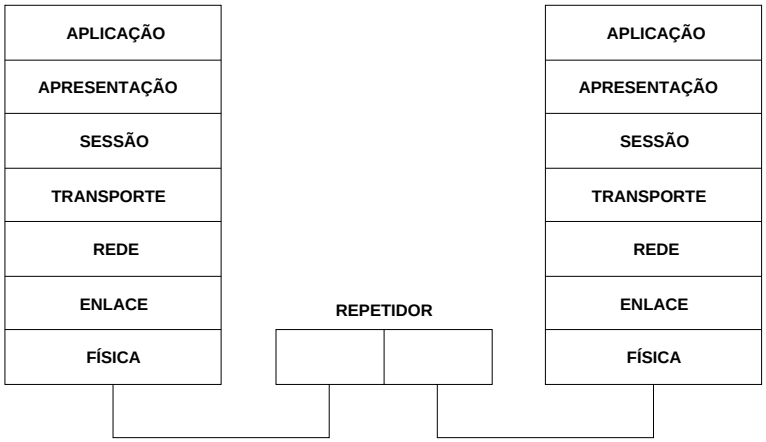


Figura 7.2: Posicionamento de um repetidor no modelo OSI/ISO.

- conexão de meios físicos diferentes - os vários padrões de LANs podem suportam vários meios de transmissão diferentes. Por exemplo, a interconexão de segmentos de rede Ethernet, onde um segmento utiliza cabo coaxial e o outro segmento utiliza fibra ótica;
- interface de gerenciamento - o gerenciamento de redes integradas requer que os repetidores sejam dispositivos gerenciáveis.

Os repetidores são dispositivos cuja unidade básica de operação diz respeito ao bit, isto é, operam independentemente da estrutura do quadro. Alguns equipamentos atuais são capazes de interpretar os endereços dos quadros e desta forma suportar serviços relacionados à privacidade de dados.

7.1.2 Pontes (Bridges)

Incialmente as pontes foram concebidas para permitir o tráfego de pacotes entre segmentos de rede homogêneos. Atualmente, encontram-se disponíveis pontes que permitem interconectar redes heterogêneas. Diferentes tipos de pontes podem ser relacionados:

- pontes transparentes - geralmente utilizadas para interconexão de redes Ethernet;
- pontes SRB (Source-Route Bridging) - encontradas em geral nos ambientes Token Ring;

- pontes de conversão (translational bridging) - suporta a conversão entre formatos e aspectos de tráfego entre tipos de meios diferentes (em geral entre Ethernet e Token Ring);
- pontes transparentes SRB: combinam os algoritmos das pontes transparentes e das pontes SRB.

A utilização dos dispositivos do tipo ponte se dá na camada de enlace do Modelo OSI/ISO, camada esta responsável por funções como deteção e recuperação de erros, controle de fluxo, endereçamento físico (em oposição ao endereçamento lógico da camada de rede) e gerenciamento do acesso ao meio físico.

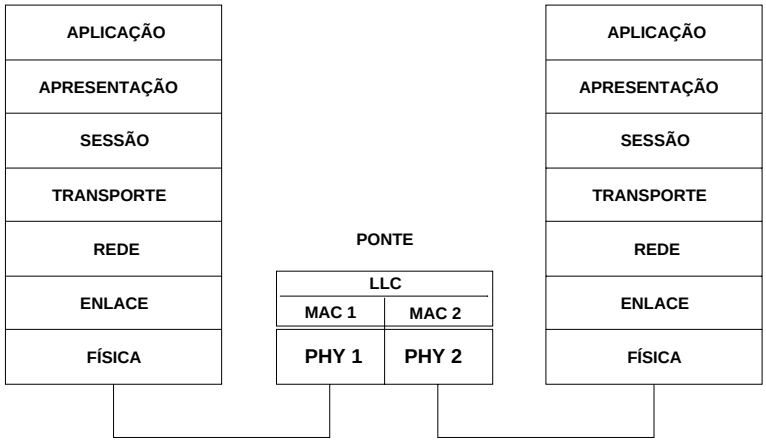


Figura 7.3: Posicionamento de uma ponte no modelo OSI/ISO.

As pontes são dispositivos em geral não muito complexos e que trabalham analisando os quadros recebidos para tomada de decisão baseadas no conteúdo de campos do quadro como, por exemplo, o encaminhamento do quadro na direção do destino. Em alguns casos, o quadro é recebido na ponte já contendo o caminho a ser percorrido para que o quadro alcance o destino (pontes SRB). No caso das pontes transparentes, os quadros são encaminhados um passo (uma ponte) de cada vez, na direção do seu destino. Outro aspecto importante no caso das pontes é a transparência relativamente aos protocolos de nível mais alto. Isto porque ao limitarem-se ao nível de enlace as pontes não necessitam acessar as informações da camada de rede. Outra função importante diz respeito à função de filtragem. Por exemplo, a ponte pode ser programada para não propagar para outros segmentos interconectados quadros recebidos de um segmento específico. Ainda neste contexto, como os quadros dos protocolos da camada de enlace costumam trabalhar com um campo de tipo que permite referenciar os protocolos da camada superior, a ponte também pode filtrar quadros relativamente a um determinado protocolo. Outro aspecto

consiste na filtragem de pacotes de broadcast e multicast desnecessários. Estas funções de filtragem significam que somente uma porcentagem do tráfego gerado em um segmento é encaminhado para outros segmentos da subrede. Isto permite uma melhor distribuição através do isolamento do tráfego que diga respeito somente a um segmento. Desta forma, um número maior de estações pode ser suportado comparativamente ao número que seria suportado caso fosse utilizada uma única LAN. As pontes permitem que a LAN seja estendida a grandes distâncias.

As pontes podem ser classificadas em locais ou remotas. O primeiro tipo permite uma conexão direta entre múltiplos segmentos de LANs em uma mesma área (figura 7.4). Pontes remotas conectam múltiplos segmentos de LANs em áreas diferentes normalmente através do uso de uma infraestrutura de comunicação suportada por provedores públicos ou privados de serviços de telecomunicações (figura 7.5).

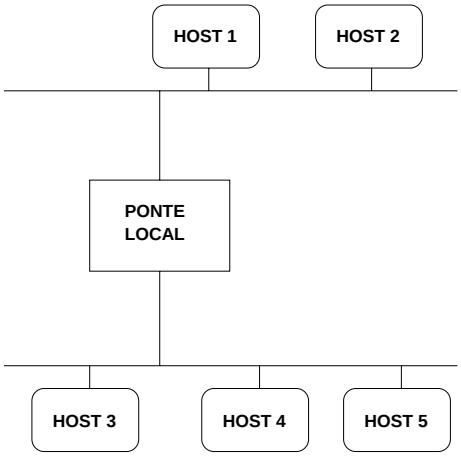


Figura 7.4: Ponte local.

Um dos aspectos críticos relacionados às pontes remotas diz respeito às diferenças de velocidade entre as LANs e as WANs, isto porque as primeiras apresentam velocidades com diferença de uma ordem de grandeza relativamente às segundas. Isto tende a ser alterado em função do suporte de novos serviços de comunicação de alta velocidade oferecidos pelos provedores públicos e privados. Esta diferença de velocidades impede muitas vezes que aplicações que executam em redes locais e que são sensíveis ao atraso executem através de uma interconexão utilizandos redes WANs. Apesar de não ser capaz de melhorar as velocidades das WANs, as pontes podem amortecer as diferenças de velocidades entre os dois tipos de rede através do armazenamento temporário dos quadros a serem transmitidos da LAN para a WAN. Este armazenamento deve durar um intervalo curto de tempo para não comprometer a capacidade de armazenamento da ponte.

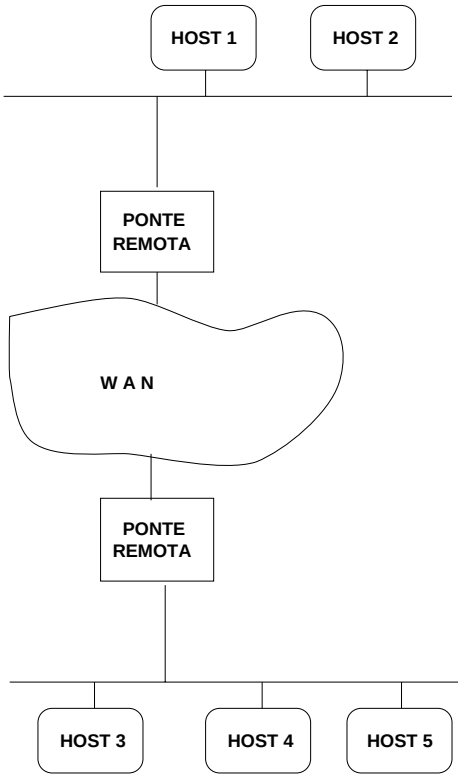


Figura 7.5: Ponte remota.

Outra função importante das pontes diz respeito (com exceção da ponte SRB) ao aprendizado da topologia da rede através dos segmentos interconectados. Em geral as pontes do tipo pontes transparentes possuem uma tabela que indica em quais segmentos da rede os hosts estão conectados. Desta maneira uma ponte aprende sobre um determinado host quando um quadro é recebido pela ponte e esta não possui o endereço daquele host na tabela. Neste caso, a ponte atualiza automaticamente a tabela através do armazenamento do endereço de origem do quadro recebido, juntamente com o número da porta ao qual encontra-se conectado o segmento onde o quadro foi recebido, ou seja, a ponte aprendeu que aquele host situa-se naquele segmento da rede. Outro aspecto que deve ser destacado relativamente à interconexão de redes via pontes é o fato de que os vários segmentos de rede interconectados constituem uma única subrede. Desta forma os hosts conectados a segmentos diferentes de LANs que são conectados através de pontes podem interagir diretamente entre si.

7.1.3 Pontes SRB (Source-route based)

Este tipo de ponte foi inicialmente introduzido pela IBM nos ambientes de rede Token Ring e tem como característica o fato de que o caminho a ser percorrido pelo quadro para alcançar o destino é determinado antes de deixar o ponto de origem. A figura 7.6 ilustra uma rede baseada no algoritmo SRB (Source-route based).

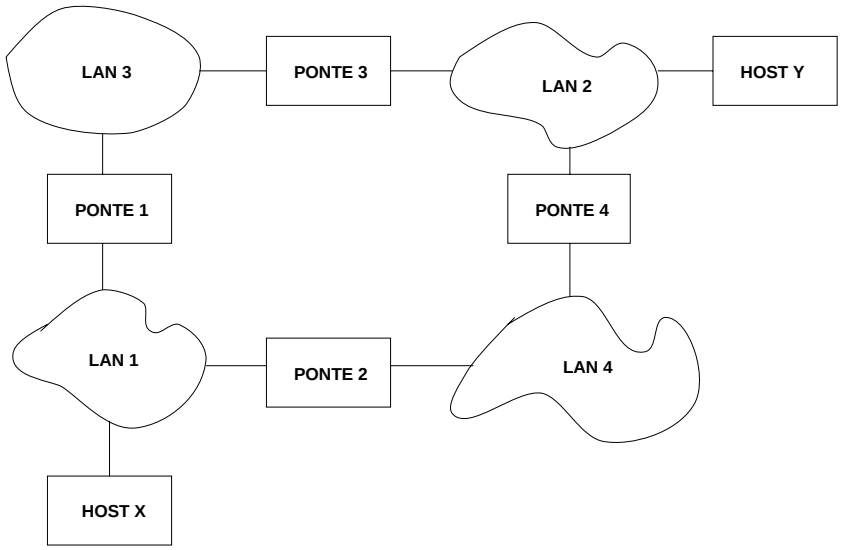
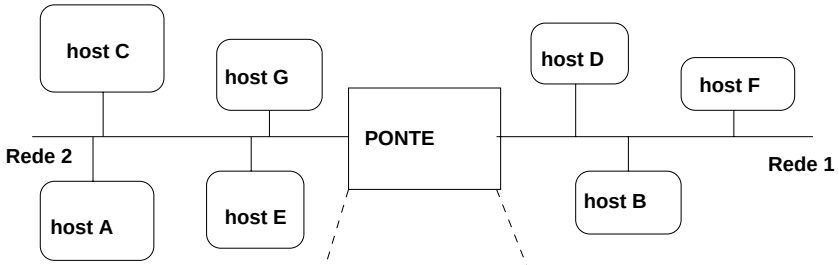


Figura 7.6: Ponte SRB.

Suponha que o host X deseja enviar um quadro para o host Y. O host X desconhece se o host Y reside na mesma LAN ou em LAN diferente. Neste caso o host X envia um quadro de teste. Caso não seja recebida uma resposta indicando que o host Y encontra-se no mesmo segmento, o host X conclui que o host Y encontra-se em um segmento remoto. Caso a mensagem de teste tenha uma resposta positiva, o host X envia um quadro de exploração na tentativa de determinar a localização exata do host Y. Cada ponte ao receber o quadro de exploração (pontes 1 e 2 na figura 7.6) copia o quadro em todas as portas de saída. A informação do caminho percorrido é acrescentada ao quadro à medida que ele trafega pelas pontes. Quando os quadros de exploração alcançam o host Y este responde a cada um dos quadros recebidos enviando uma resposta ao host X com informações sobre o caminho percorrido. Após o recebimento de todas as respostas, o host X escolhe um caminho segundo algum critério. Alguns dos critérios que podem ser utilizados são: adotar o caminho obtido no primeiro quadro recebido, ou o caminho com o menor número de pontos intermediários (hops). Após a seleção de um caminho, este é inserido nos quadros enviados ao host Y em um campo destinado à informação da rota.

7.1.4 Pontes Transparentes

Estas pontes têm a sua presença e a forma como operam totalmente transparentes aos hosts da rede. Quando ligada, a ponte aprende a topologia da rede através da análise do endereço de origem do quadro conforme comentado anteriormente. A figura 7.7 mostra a tabela construida no caso da rede apresentada. A tabela é utilizada como base para encaminhamento do tráfego através da ponte. Quando da recepção de um quadro em uma das portas, a ponte procura o endereço de destino na tabela. Caso exista uma associação do endereço com uma porta diferente daquela onde o quadro foi recebido, o mesmo é encaminhado para esta porta. Caso não exista qualquer associação do endereço na tabela, o quadro é enviado a todas as portas exceto à porta na qual foi recebido. As pontes transparentes isolam o tráfego em cada segmento individualmente melhorando o tempo de resposta da rede.



endereço host	Rede
A	2
B	1
C	2
D	1
E	2
F	1
G	2

Figura 7.7: Ponte transparente.

As pontes transparentes necessitam de um algoritmo que impeça a criação de loops quando existem vários caminhos entre duas LANs interconectadas. A figura 7.8 ilustra uma estrutura contendo loop. No caso da figura, suponhamos que o host A envie um quadro ao host B. Ambas as pontes recebem o quadro e concluem que o host A está na rede 2. Após o host B receber 2 cópias do quadro enviado pelo host A, ambas as pontes também receberão o quadro nas suas interfaces conectadas à rede 1. Neste caso as pontes podem atualizar as suas tabelas indicando que o host A está na rede 1. Desta maneira, quando o host B responde a um quadro do host A, as pontes irão descartar o

quadro porque as suas tabelas indicarão que o host A, destino do quadro, encontra-se na mesma subrede que o host origem. Outra questão relativamente às pontes transparentes diz respeito quando do envio de quadro com endereço de broadcast. Neste caso as pontes irão transmitir o quadro indefinidamente nos segmentos interconectados. Desta forma, uma rede contendo uma topologia com loops pode ser útil no caso de tolerância a falhas através de uma maior flexibilidade na topologia, mas também pode ser destastroso em função das situações comentadas anteriormente. Com o objetivo de preservar os benefícios dos loops no caso das pontes e ao mesmo tempo eliminar os seus problemas o IEEE 802 publicou a especificação IEEE 802.1d que propõe o algoritmo Spanning-Tree Algorithm (STA).

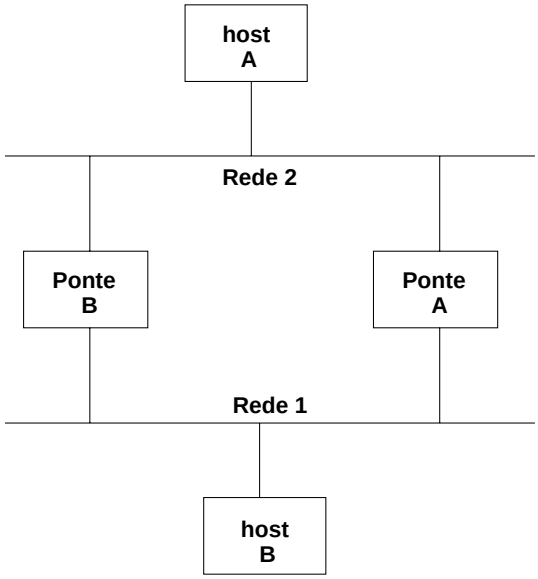


Figura 7.8: Rede com loops.

Spanning-Tree Algorithm (STA)

O objetivo do algoritmo STA consiste na determinação de uma parte da topologia da rede isenta de loop. Isto é obtido através da colocação em situação de bloqueio (standby) portas das diversas pontes que, se na condição ativa, criariam loops. As portas colocadas na condição de bloqueio poderão ser reativadas no caso de falha em algum dos segmentos primários criando novos caminhos na estrutura de interconexão. O algoritmo baseia-se em uma afirmação da teoria de grafo para a determinação de um subconjunto de uma topologia de rede isento de loop. Esta afirmação diz que para qualquer grafo formado de nós e arcos conectando pares de nós, existe uma árvore que mantém a conectividade do

grafo e não contém loops. A figura 7.9 mostra como o algoritmo STA elimina os loops. Cada uma das pontes recebe um idenficador único. Cada porta de uma ponte recebe também um identificador único naquela ponte. Por último, a cada porta de uma ponte é associado um custo para o caminho. Este custo corresponde ao custo de transmissão de um quadro na LAN através da porta.

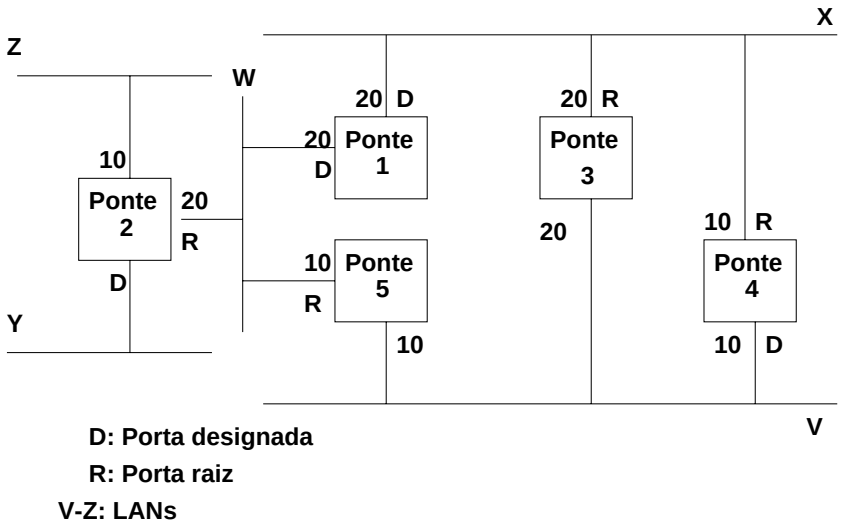


Figura 7.9: Rede com Pontes Transparentes antes de executar o STA.

O algoritmo escolhe inicialmente a ponte que fará o papel de raiz selecionando aquela que possui o menor identificador. No caso da figura 7.9 trata-se da ponte 1. A seguir determina-se nas outras pontes a porta que permite acessar a ponte raiz com o menor custo agregado (Porta Raiz). Este custo denomina-se Custo do Caminho para a Raiz. Por último, determina-se a ponte em cada LAN que fornece o menor Custo do Caminho para a Raiz. Esta ponte é a única autorizada a encaminhar/receber quadros para/da raiz. Caso duas pontes tenham o mesmo Custo do Caminho para a Raiz (pontes 4 e 5 com relação à ponte 1 no caso da figura 7.9) escolhe-se aquela com menor identificador. A figura 7.10 mostra o resultado após a aplicação do algoritmo STA para a figura 7.9.

7.2 Chaves (Switches)

Chaves operam no mesmo nível que pontes (enlace). As diferenças básicas entre pontes e chaves são:

- chaves tipicamente interconectam um maior número de LANs;

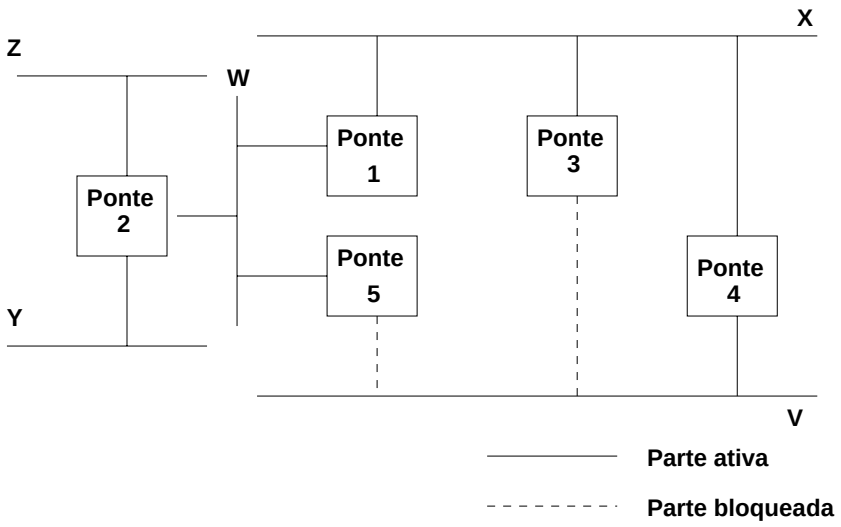


Figura 7.10: Rede com Ponte Transparente após executar o STA.

- chaves são muito mais rápidas que pontes;
- chaves modernas além de prover isolamento de tráfego entre múltiplas LANs permitem a implantação de *LANs Virtuais*.

7.2.1 LANs Virtuais

Numa LAN Virtual (VLAN) os recursos de rede são agrupados segundo critérios de utilização, não de proximidade física. Seja a figura 7.11 onde três chaves são conectadas por uma quarta através de portas de alta velocidade (ATM, Fast Ethernet, etc.). Nesta configuração são definidas três LANs virtuais (VLAN 10, 20 e 30), além de uma LAN convencional.

No caso da figura 7.11 as seguintes funções são implementadas pela VLAN:

- isolamento de tráfego: por exemplo, um quadro dirigido do host A para o host B fica circunscrito ao segmento conectado à porta P11;
- minimização da contenção: por exemplo, um quadro dirigido do host A para o host F é propagado, via chave #4, na porta 31 (os hosts D e E não são afetados pela transmissão).

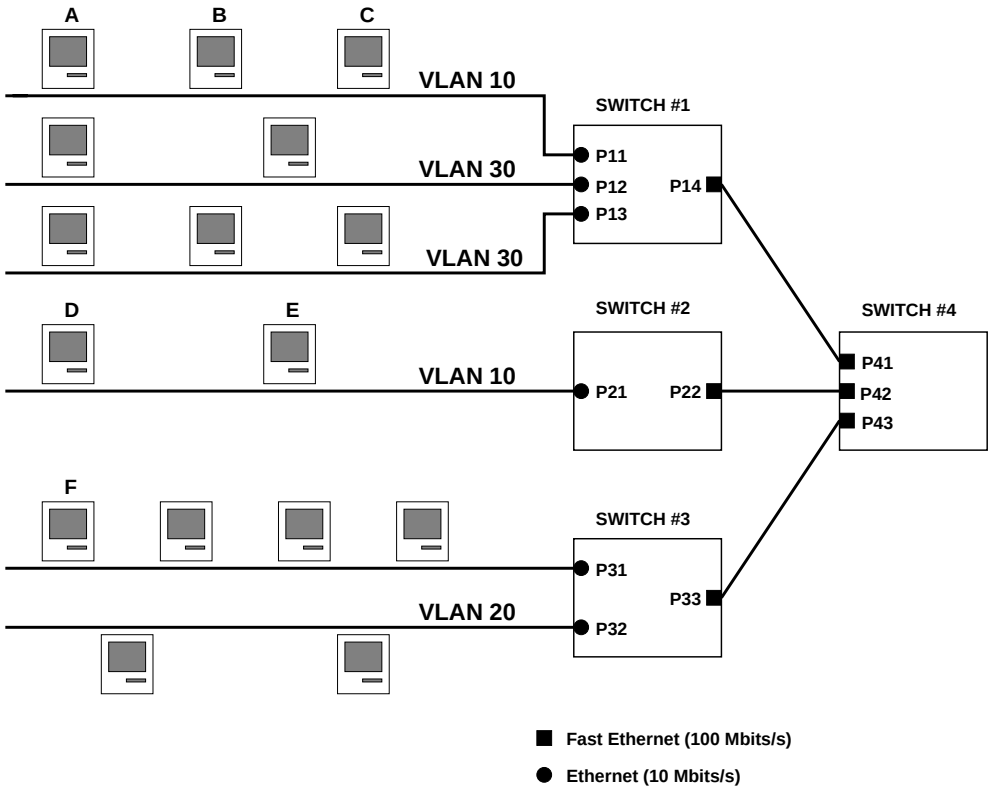


Figura 7.11: LANs Virtuais.

- delimitação de *broadcast*: por exemplo, um quadro difundido (broadcast) pelo host A atinge apenas os hosts pertencentes à VLAN 10.

VLANs oferecem ainda duas importantes propriedades:

1. escalabilidade;
2. mobilidade.

No primeiro caso suponha que o host C seja um servidor muito requisitado. Pode-se dedicar uma porta exclusiva para a interconexão do host C, permitindo uma banda dedicada de 10 Mbits/s para o mesmo. No segundo caso suponha que o host D deva se deslocar para para uma área servida pela chave #3. Pode-se implantar um segmento de LAN numa porta desta chave e associar o segmento à VLAN 10. A figura 7.12 ilustra estas duas situações.

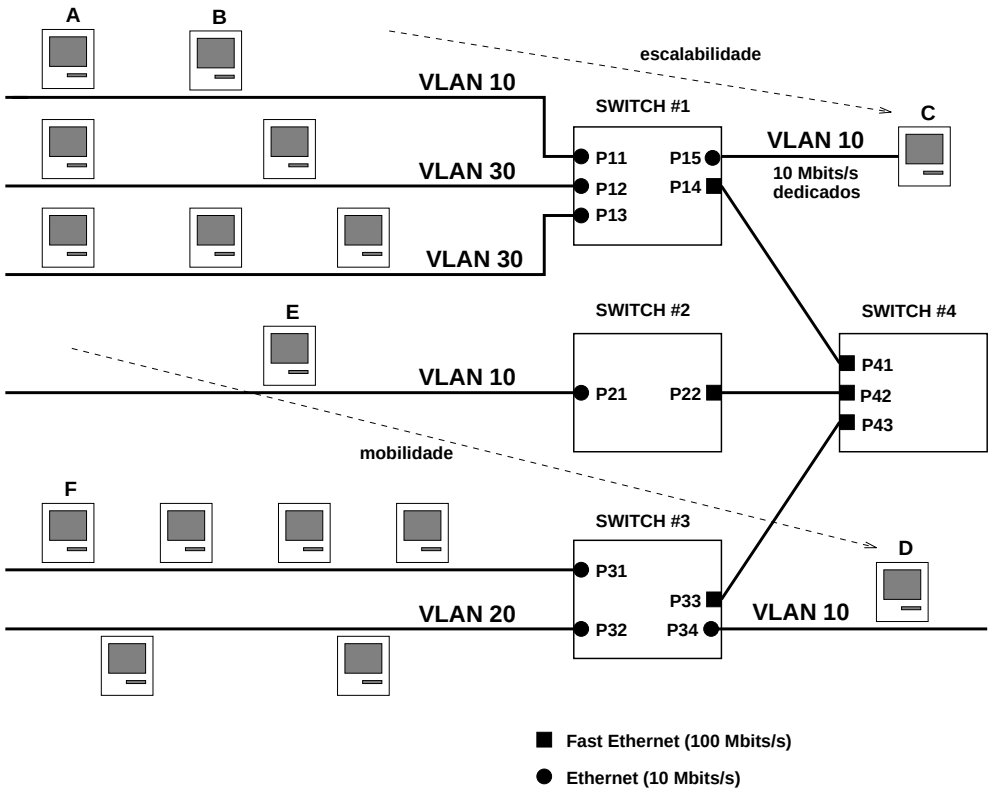


Figura 7.12: Escalabilidade e mobilidade em LANs virtuais.

7.2.2 Roteadores

Roteadores atuam nas três primeiras camadas do modelo OSI conforme ilustra a figura 7.13.

Os roteadores possuem duas funções básicas: determinação das rotas ótimas e o transporte da informação (pacote) através da internet. Para determinação de rotas ótimas os algoritmos de roteamento utilizam métricas como, por exemplo, o comprimento do caminho. Para auxiliar neste processo emprega-se informações de roteamento armazenadas em tabelas de roteamento. As informações variam dependendo do algoritmo de roteamento empregado. As tabelas são normalmente organizadas através da associação do destino com o próximo roteador no caminho para alcançar o destino do pacote. Ao receber um pacote em uma das suas entradas, o roteador analisa o endereço de destino contido no pacote e tenta associar este endereço com o próximo roteador. A figura 7.14 ilustra um exemplo de uma tabela de roteamento.

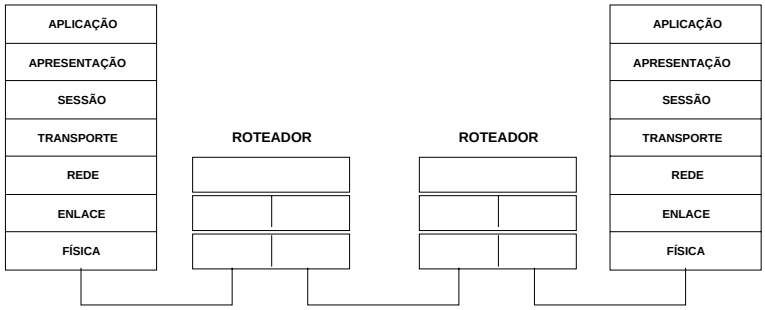


Figura 7.13: Posicionamento de um roteador no modelo OSI.

SUBREDE DESTINO	ENVIAR PARA O NÓ
18	A
45	B
76	A
17	C
14	B
DEFAULT	B

Figura 7.14: Exemplo de tabela de roteamento.

O encaminhamento dos pacotes por parte dos roteadores é relativamente simples. Na maior parte das vezes um host determina que ele tem que enviar um pacote a outro host. Após adquirir o endereço do roteador, o host de origem envia um pacote endereçado especificamente ao endereço físico do roteador. Após examinar o endereço do destino do pacote o roteador determina se ele conhece ou não onde encaminhar o pacote. Caso ele não conheça ele deve descartar o pacote ou enviá-lo em uma rota default. Caso ele conheça como encaminhar o pacote, o roteador altera o endereço físico do destino[2] para encaminhar o pacote ao próximo roteador e envia o pacote. O próximo roteador pode ou não ser o responsável pela entrega ao host destino caso este último esteja conectado em uma subrede conectada ao roteador. Caso contrário, o processo se repete com o envio do pacote a um outro roteador. Do ponto de vista do Modelo OSI/ISO foi definida uma teminologia para descrever os processos anteriores. Segundo esta terminologia, dispositivos de rede sem capacidade de encaminhar pacotes entre subredes são denominados de

[2]Deve-se observar que o endereço da rede de destino não é alterado pelos roteadores.

Sistemas Finais (End Systems), enquanto que os dispositivos de rede com estas capacidades são ditos de Sistemas Intermediários (IS). Estes últimos são divididos entre aqueles que podem se comunicar dentro de domínios de roteamento (Sistemas Intermediários Intradomínio) e aqueles que podem se comunicar tanto dentro como entre domínios de roteamento (Sistemas Intermediários Interdomínios). Um domínio de roteamento é normalmente classificado como uma porção da inerconexão sob o controle de uma autoridade administrativa comum. Domínios de roteamento são também conhecidos como Sistemas Autônomos.

7.3 Roteamento

Roteamento é um *processo de decisão* do qual roteadores se valem para encaminhar tráfego para outros roteadores. Os objetivos básicos do roteamento são:

- determinar a topologia atual da rede;
- determinar a melhor rota (segundo algum critério) para um dado destino.

Em sendo um processo de decisão, roteamento é uma tarefa computacionalmente intensiva, além de consumir determinada banda da rede de comunicação na troca de informações de roteamento entre roteadores.

Conforme mencionado anteriormente, roteadores utilizam *tabelas de roteamento* para conduzir o processo de tomada de decisão. Tipicamente, uma tabela de roteamento possui três colunas: subrede de destino, interface do roteador e custo. A subrede de destino é o endereço de destino do pacote a ser roteado. A interface do roteador é o ponto de saída do pacote sendo uma via de conexão para para um roteador mais próximo da subrede de destino ou a própria subrede de destino. O custo é uma métrica associada à decisão de rotear o pacote via determinada interface.

Roteadores se utilizam de protocolos de roteamento que normatizam a troca de informações de roteamento entre os roteadores, bem como a estratégia de cômputo de rotas. Estes protocolos podem ser abertos ou proprietários. Protocolos abertos são padronizados pela ISO, IETF (Internet Engineering Task Force) e por outros organismos de padronização.

Roteamento possui várias classificações:

- centralizado ou distribuído;
- interior ou exterior;
- estático ou dinâmico;
- plano ou hierárquico;
- baseado em estado das linhas *(link state)* ou em vetor de distâncias.

Roteamento centralizado é conduzido por um agente único que propaga as decisões de roteamento para os roteadores. É utilizado apenas em *backbones*. Roteamento distribuído é conduzido pelos próprios roteadores via troca de informações através de um protocolo de roteamento.

Roteamento interior é circunscrito a um domínio de roteamento enquanto roteamento exterior se processa entre domínios diferentes. Via de regra roteamento interior e exterior são conduzidos por protocolos distintos. A figura 7.15 ilustra estes conceitos.

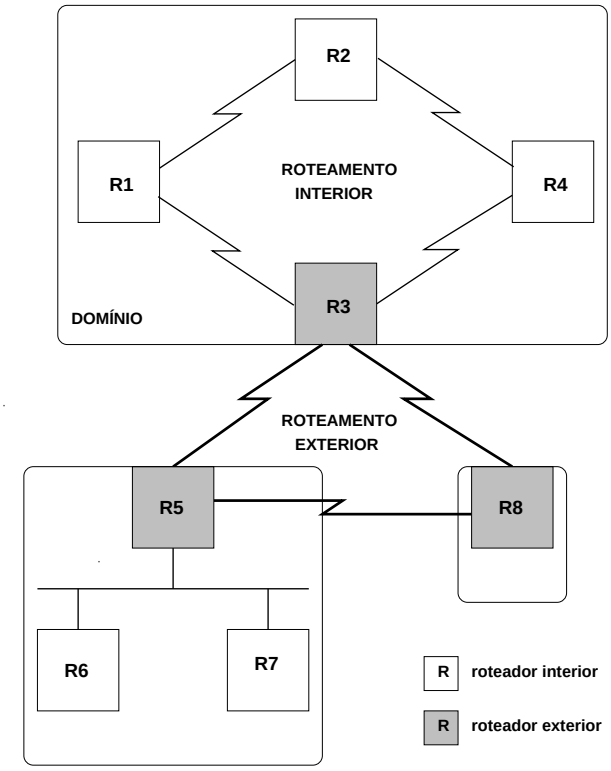


Figura 7.15: Domínios, roteamento e roteadores.

No roteamento estático as tabelas de roteamento são incorporadas ao roteador pelo administrador de rede e permanecem imutáveis até uma nova intervenção do administrador. No roteamento dinâmico o próprio roteador atualiza (novamente, via protocolo de roteamento) suas tabelas de roteamento.

No roteamento plano um roteador se comunica com qualquer outro, independente das fronteiras dos domínios. No roteamento hierárquico apenas um pequeno número de roteadores de um domínio (os *roteadores exteriores* da figura 7.15) podem trocar tabelas de roteamento com roteadores em outro domínio. Os demais roteadores trocam tabelas de roteamento apenas com roteadores pertencentes ao seu domínio. Roteadores exteriores que trocam tabelas de roteamento são denominados *roteadores vizinhos* (roteadores R3, R5 e R8 da figura 7.15).

No roteamento baseado em estado das linhas *(link state)* os roteadores propagam para todos os demais a porção de sua tabela de roteamento que contém as rotas diretamente conectadas às suas interfaces. No roteamento baseado em vetor de distâncias os roteadores enviam sua tabela de roteamento completa, mas a um conjunto restrito de roteadores (via de regra seus vizinhos).

As métricas utilizadas no processo de decisão se referem a uma rota. Uma rota é um caminho constituido de linhas e roteadores de uma origem até um destino. Métricas comumente empregadas são:

- comprimento;
- banda (vazão);
- atraso;
- taxação (custo);
- taxa de utilização (carga);
- taxa de falhas (confiabilidade).

Comprimento é a métrica mais comum e determina o número de roteadores (*hops*) na rota ou qualquer métrica arbitrária atribuida pelo administrador de rede.

Banda é uma métrica de capacidade da rota (bits/s), limitada pela linha de menor capacidade na rota.

Atraso mede o tempo médio de propagação na rota (segundos), sendo influenciado por vários outros parâmetros tais como carga e capacidade dos equipamentos na rota.

Taxação determina o custo incorrido ($/bit) pela utilização da rota.

A taxa de utilização mede o uso de recursos (linhas e roteadores) na rota em termos do percentual de utilização em relação à capacidade máxima do recurso.

A taxa de falhas é uma métrica de confiabilidade dos equipamentos na rota (linhas e roteadores). Usualmente os administradores de rede atribuem índices de confiabilidade às rotas de forma comparativa e com base na ocorrência passada de falhas.

7.4 Protocolos de Roteamento

7.4.1 Roteamento Interior TCP/IP: Protocolo RIP

O protocolo de roteamento RIP (Routing Information Protocol) é empregado para que roteadores interiores ao domínio cooperem nas atividades de roteamento. É o protocolo de roteamento interior introduzido nos sistemas UNIX BSD e utilizado com pequenas variantes nas redes Novell e AppleTalk. RIP é um protocolo baseado em vetor de distâncias.

A métrica de custo no protocolo RIP é o número de *hops* na rota. Este número varia de 1 a 15, sendo 16 utilizado para distância infinita (inexistência de caminho).

O protocolo se RIP utiliza um protocolo de transporte (UDP) para a condução de suas mensagens. No protocolo RIP roteadores difundem periodicamente informações de roteamento. Hosts apenas se utilizam destas informações.

As mensagens possuem formato dado pela figura 7.16.

O campo COMANDO pode assumir o valor 1 para requisição ou 2 para resposta. Informações de roteamento se constituem de pares (subrede, distância). O roteador pode enviar toda a sua tabela de roteamento nestes pares. O campo FAMÍLIA DA SUBREDE usualmente assume valor 2 para subredes operando com o protocolo IP.

Roteadores e hosts “aprendem” novas rotas recebendo mensagens RIP ou solicitando que roteadores enviem sua tabela de roteamento. Por exemplo, seja o sistema autônomo da figura 7.17.

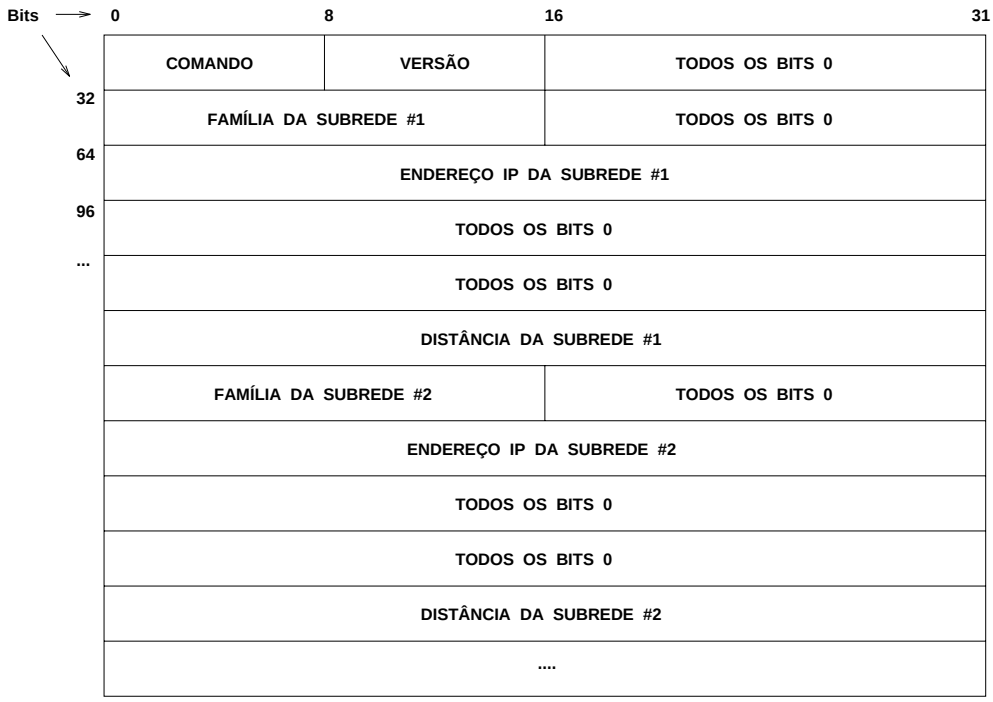


Figura 7.16: Formato de mensagens do protocolo RIP.

O roteador R_1 propaga na subrede 2 uma mensagem (1, 1) informando que pode atingir a subrede 1 a um custo 1. Os roteadors R_2 e R_3 recebem esta mensagem e atualizam em suas tabelas a informação que a subrede 1 pode ser atingida a partir de R_1 a um custo 2. Mais tarde, roteadors R_2 e R_3 propagam mensagens para as subredes abaixo informando que podem atingir a subrede 1 a partir de um custo 3 (1, 3) e a subrede 2 a partir de um custo 2 (2, 2). Sucessivamente, todos os hosts e roteadors terão a partir de que roteador cada subrede do sistema autônomo pode ser atingida e a que custo.

Tipicamente um roteador propaga sua tabela de roteamento a cada 30 segundos. Caso uma rota não seja atualizada após 60 segundos, a mesma é removida após 30 segundos.

Sempre que um host ou roteador é informado de uma rota já existente em sua tabela de roteamento, o mesmo a substitui caso o custo da nova rota seja inferior.

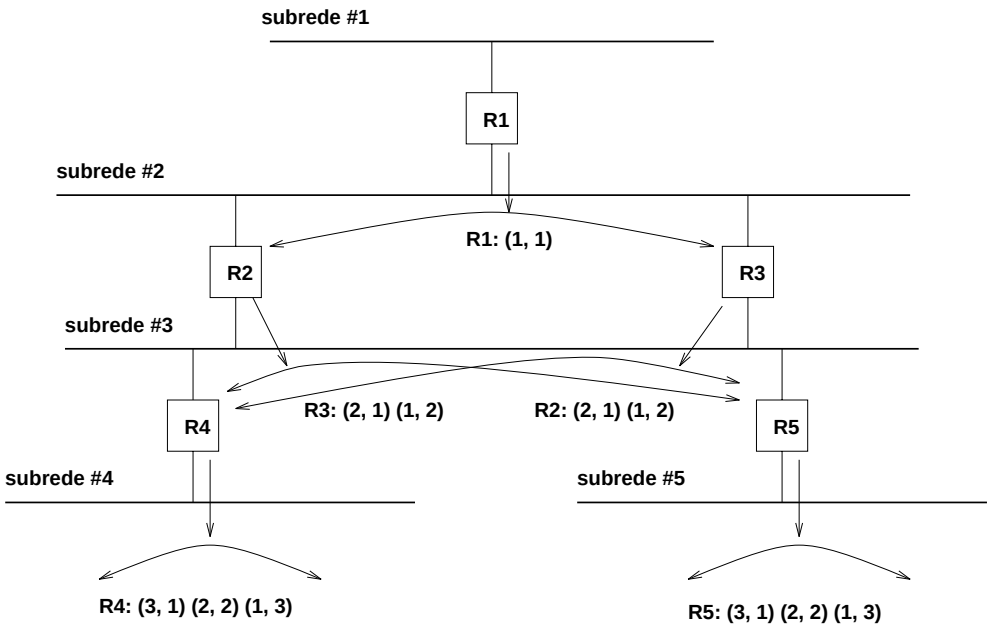


Figura 7.17: Sistema autônomo empregando o protocolo de roteamento interior RIP.

7.4.2 Roteamento Interior TCP/IP: Protocolo OSPF

O protocolo OSPF (Open Shortest Path First) é uma alternativa ao protocolo RIP para roteamento interior em domínios de grandes dimensões. OSPF é um protocolo do tipo *link state* que propaga *Link State Advertisements* (LSA) para todos os roteadores. De posse das informações contidas nos LSA, roteadores executam o algoritmo SPF (Shortest Path First) para cômputo de rotas ótimas.

Opcionalmente, para efeito de roteamento, o protocolo OSPF divide o domínio em *áreas* conectadas por uma área especial: o *backbone*. Cada roteador mantém informações de topologia referente à(s) área(s) em que está conectado. Informações de topologia interna à uma área é invisível às demais áreas. Isto minimiza o tráfego de informação de roteamento pois quando a topologia de uma área muda apenas os roteadores pertencentes à esta área atualizam suas tabelas de roteamento.

O OSPF utiliza o conceito de roteadores vizinhos. No contexto do OSPF roteadores são classificados como vizinhos quando estão conectados a uma mesma subrede. Roteadores descobrem vizinhos via mensagens de *Hello*. Estabelecidas as relações de vizinhança, roteadores enviam para toda a área um LSA a cada intervalo de tempo ou quando uma variação de topologia é detectada. LSA contém informações sobre as linhas conectando o

emissor à seus vizinhos.

O protocolo OSPF opera com uma ou mais métricas arbitrárias ou com a combinação das três métricas presentes no datagrama IP: atraso, vazão e confiabilidade.

A figura 7.18 ilustra o cabeçalho do protocolo OSPF.

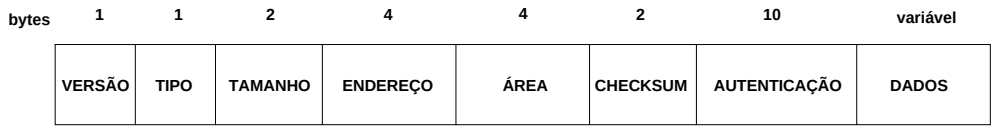


Figura 7.18: Cabeçalho do protocolo OSPF.

O campo VERSÃO identifica a versão do protocolo. O campo TIPO lista o tipo da mensagem:

1. *Hello*: para estabelecer e manter relações de vizinhança;
2. *Database Description*: para propagar informações de topologia quanto uma relação de vizinhança é estabelecida;
3. *Link State Request*: requisita a um roteador vizinho informações de topologia;
4. *Link State Update*: responde à requisição acima;
5. *Link State Acknowledgement*: reconhece uma mensagem do tipo acima.

O campo TAMANHO especifica o tamanho total da mensagem. O campo ENDEREÇO contém o endereço do roteador que emitiu a mensagem. O campo ÁREA identifica a área do emissor. O campo CHECKSUM contém o código de redundância cíclica computado para a mensagem inteira. O campo AUTENTICAÇÃO permite ao receptor autenticar a mensagem como proveniente de um roteador de seu domínio.

Para ilustrar o cômputo de rotas no OSPF considere um domínio composto de uma única área dado pela figura 7.19.

Após trocas de LSA na área o roteador R1 possui, por exemplo, a tabela de roteamento dada pela tabela 7.1

O algoritmo SPF executa uma busca do tipo *Best-First*. Seja o exemplo de computar a melhor rota para uma subrede conectada ao roteador R5. A figura 7.20 ilustra a sequência

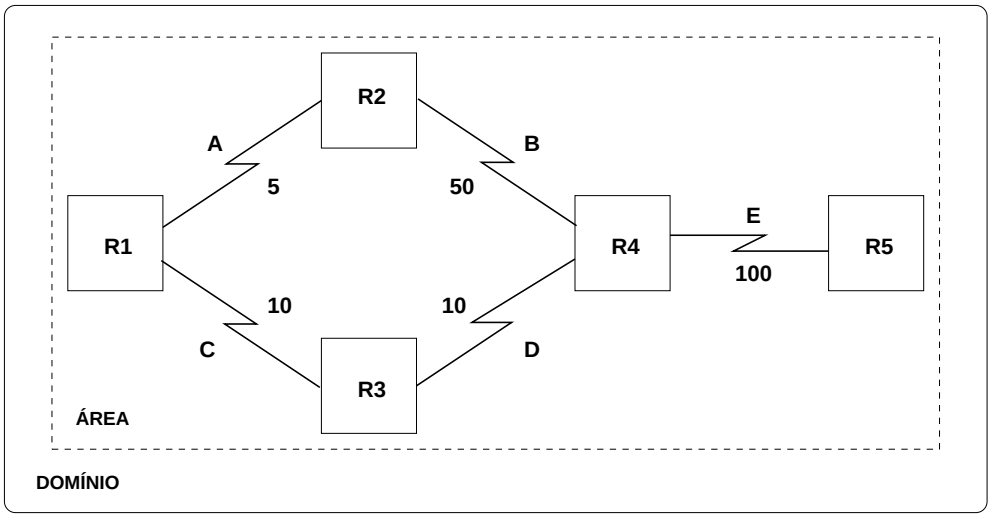


Figura 7.19: Exemplo de domínio.

da busca. Note que o nó marcado com X não necessita ser explorado quando um caminho melhor para R4 for descoberto. Esta propriedade diminui consideravelmente o tempo de busca em domínios de grandes dimensões.

7.5 Encapsulamento (Tunelamento)

Encapsulamento é uma técnica de interconexão de redes empregada tipicamente em interconexão LAN-WAN-LAN e enlaces ponto-a-ponto. Nesta técnica o tráfego entre as LANs interconectadas (quadros MAC ou pacotes de rede) flui como dados em pacotes da WAN. Encapsulamento de quadros MAC (Ethernet, Token Ring, etc.) é conduzido tipicamente por pontes remotas, enquanto o encapsulamento de pacotes de rede (IP, IPX, etc.) é conduzido por roteadores. A figura 7.21 ilustra LANs TCP/IP interconectadas por uma WAN.

O encapsulamento pode se dar de várias formas:

- encapsulamento implícito: associa-se determinada interface do roteador ou ponte a um protocolo de rede ou quadro MAC;
- encapsulamento negociado: durante a abertura de conexão de rede negocia-se que protocolo de rede ou quadro MAC será encapsulado na conexão;

De	Para	Link	Custo
R1	R2	A	5
R1	R3	C	10
R2	R1	A	5
R2	R4	B	50
R3	R1	C	10
R3	R4	D	10
R4	R2	B	50
R4	R3	D	10
R4	R5	E	100
R5	R4	E	100

Tabela 7.1: Exemplo de tabela de roteamento mantida pelo roteador R1 da figura acima.

- encapsulamento nulo: cada pacote na rede de interconexão identifica o protocolo de rede ou quadro MAC encapsulado (multiplexação de múltiplos protocolos sobre uma única conexão).

A figura 7.22 ilustra estas possibilidades.

A identificação dos protocolos de rede ou quadros MAC seguem duas normas. A primeira identificação consiste de 1 byte cujo conteúdo é estabelecido pela recomendação ISO/IEC TR 9577. Este conteúdo é denominado NLPID (Network Layer Protocol IDentifier) e possui valor 204 (hexadecimal CC) para o protocolo IP, 129 para o protocolo CLNP, e assim por diante. O valor 0 identifica encapsulamento nulo (figura 7.22-c). NLPID define valores apenas para protocolos de rede.

A segunda identificação denomina-se SNAP (Subnetwork Access Protocol) sendo padronizada pelo IEEE. Um identificador SNAP normalmente segue um NLPID de valor 128 (hexadecimal 80). Um identificador SNAP é composto de 5 bytes: três para identificar a organização que atribui identificadores de protocolos (OUI: Organizationally Unique Identifier) e dois para identicicar o protocolo encapsulado (PID: Protocol IDentifier). Em geral cada um destes 5 bytes são identificados por dois números em hexadecimal cada qual representando 4 bits. Ao contrário do NLPID, SNAP identifica tanto protocolos de rede quanto quadros MAC. Por exemplo, a organização identificada por 0x00-80-C2 representa o projeto IEEE 802. Os dois bytes restantes possuem valor de 0x00-01 para quadros IEEE 802.3 (Ethernet), 0x00-03 para quadros IEEE 802.5 (Token Ring), e assim por diante. Protocolos de rede possuem organização EtherType (0x00-00-00), isto é, possuem a mesma identificação presente nos quadros Ethernet: 0x08-00 para o protocolo IP, 0x80-9B para o protocolo AppleTalk, e assim por diante.

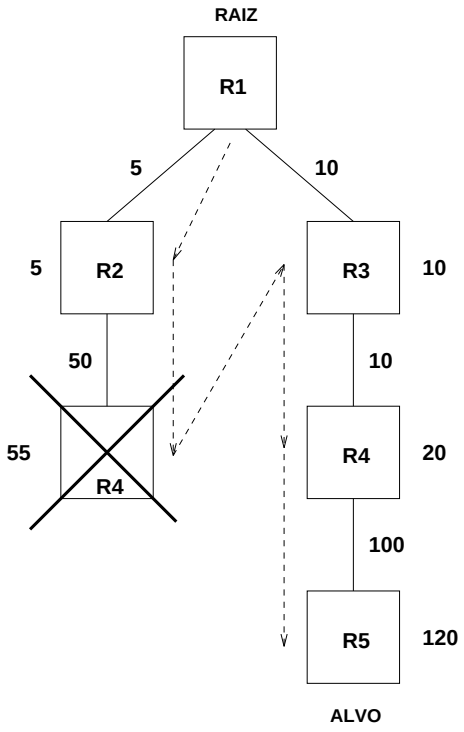


Figura 7.20: Busca SPF. A linha pontilhada representa a ordem de geração dos nós.

O encapsulamento é padronizado para várias redes de interconexão. No caso de datagramas IP, seu encapsulamento é definido para X.25 (RFC 1356), Frame Relay (RFC 1490) e ATM (RFC 1483).

7.5.1 Encapsulamento de IP Sobre X.25

Nesta seção vamos analisar como se processa a interconexão de LANs TCP/IP através de uma WAN X.25. Roteadores utilizados na interconexão implementam a RFC 1356[3] que trata do encapsulamento de PDUs de rede (IP, IPX, etc.) sobre redes X.25.

A RFC 1356 prevê que a abertura de conexões X.25 ocorra "sob demanda", isto é, o lado X.25 do roteador abre uma conxão X.25 para outro roteador sempre que um datagrama necessitar ser rotado para tal destino. Conexões abertas são encerradas em duas situações:

[3]Entitulada *Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode.*

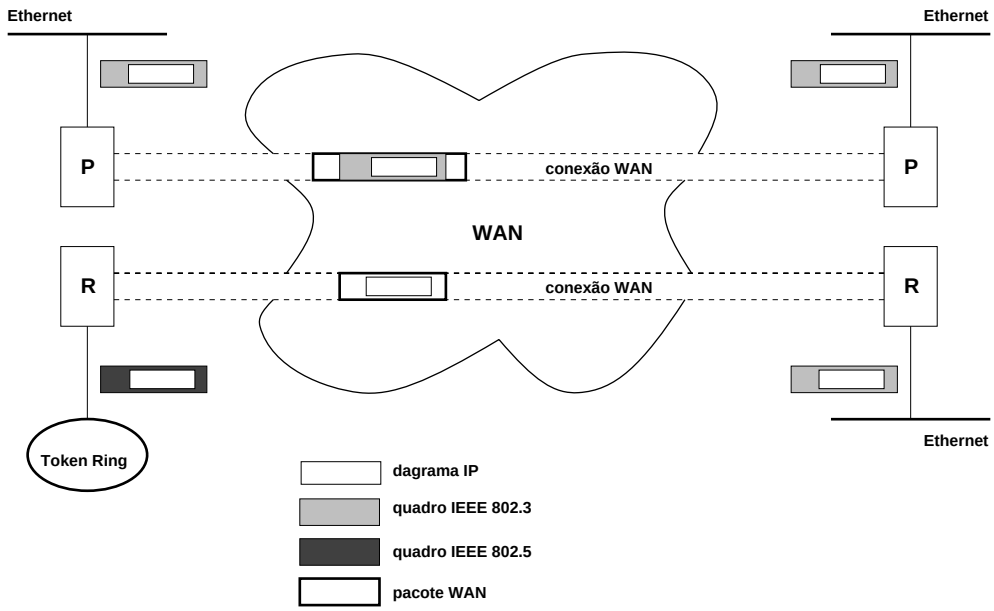


Figura 7.21: Encapsulamento de quadros MAC e pacotes de rede.

1. após certo período de inatividade (tipicamente 90 segundos);
2. quando o número máximo de conexões abertas para determinada interface for atingido.

Datagramas IP são transportados em sequências de pacotes X.25 (o bit M é utilizado para fragmentar datagramas em múltiplos pacotes X.25). O tamanho dos datagramas encapsulados pode variar entre 576 (Internet default) e 1600 bytes.

Durante o estabelecimento da conexão o campo DADOS DO USUÁRIO é utilizado para indicar o protocolo de rede sendo encapsulado (figura 7.22-b). Esta identificação se dá através do indentificador NLPID (eventualmente seguido do identificador SNAP).

O encapsulamento nulo também é especificado (figura 7.22-c). Neste caso o primeiro byte do campo de dados (e os próximos cinco, caso o SNAP seja utilizado) especifica o protocolo encapsulado.

A figura 7.23 ilustra o transporte de um datagrama IP sobre uma rede X.25.

O roteador ao aceitar uma conexão verifica a partir do NLPID se é capaz de manipular o protocolo encapsulado. Caso não seja, o pedido de estabelecimento de conexão é rejeitado.

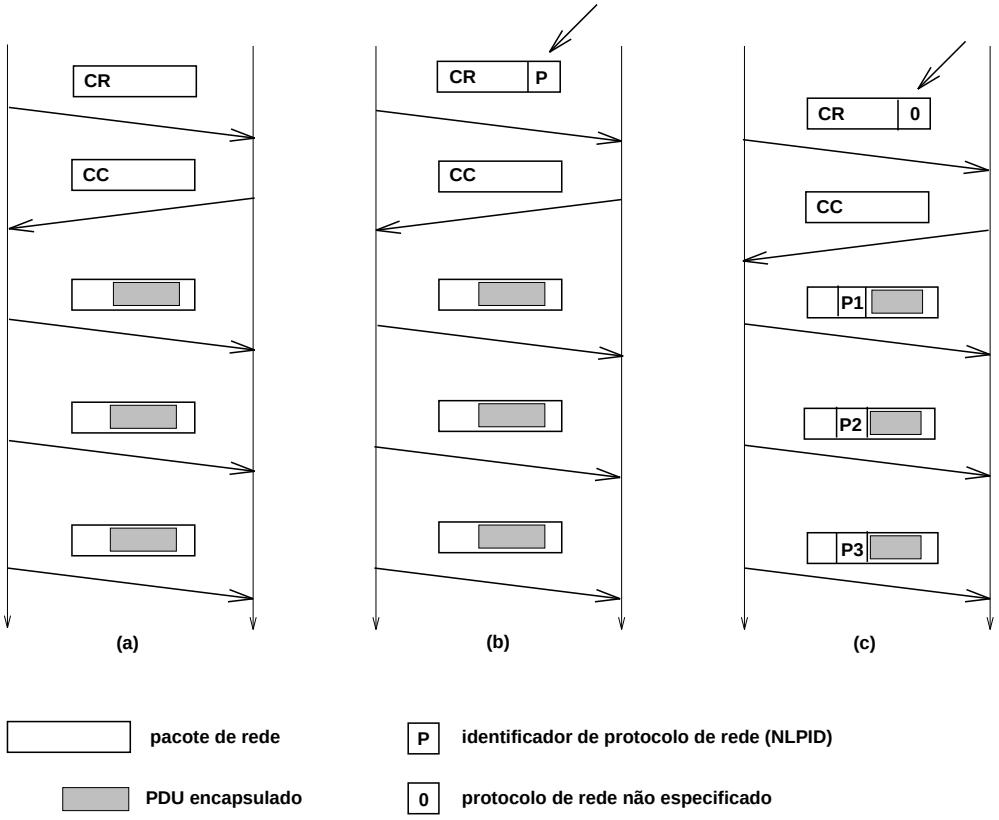


Figura 7.22: Tipos de encapsulamento: implícito (a); negociado na abertura da conexão (b); e nulo (c).

Certas particularidades do X.25 tais como pacotes de controle tipo interrupção, bit Q (Qualifyed Data) e bit D (confirmação fim-a-fim) não são empregadas no encapsulamento.

Uma questão importante é o mapeamento de endereços. Um datagrama IP carrega o endereço IP de destino. O roteador ao receber o datagrama necessita abrir (ou utilizar) uma conexão X.25 para outro roteador (na rede X.25) capaz de entregar o datagrama à subrede IP de destino. Entretanto, roteadores na rede X.25 utilizam endereçamento X.121 o que resulta no problema: como mapear endereços IP em X.121 ? A tabela 7.2 ilustra uma tabela de roteamento. Esta tabela pode ser estática ou permanentemente atualizada por algum algoritmo de roteamento dinâmico.

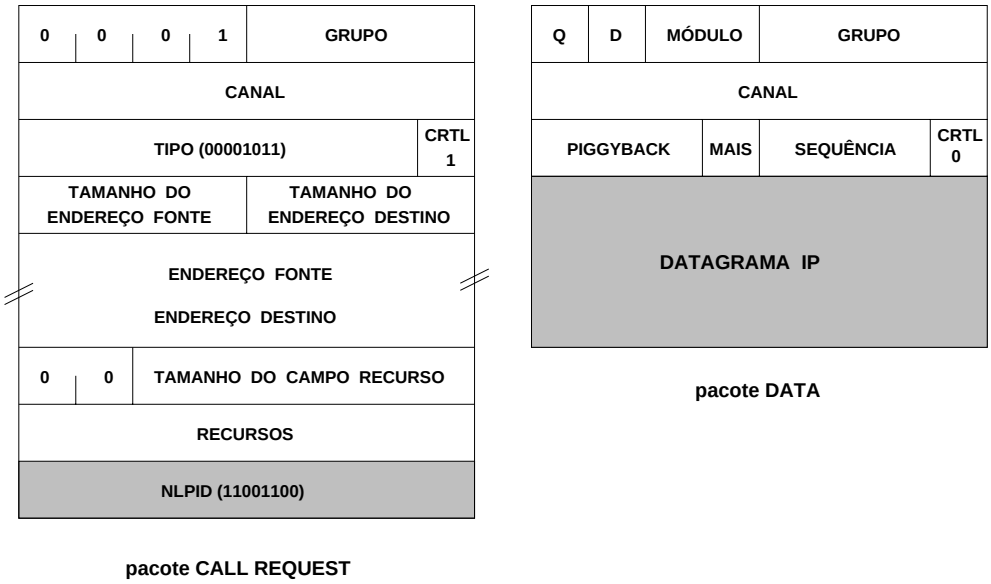


Figura 7.23: Encapsulamento IP sobre X.25 (RFC 1356).

subrede destino	endereço X.121	custo
214.194.97.0	-	0
214.194.97.64	75511787593	1
214.194.97.128	75521784566	1

Tabela 7.2: Tabela de roteamento do roteador servindo à subrede 214.194.97.0. O Endereço X.121 pode ser substituido por um identificador de conexão no caso de circuitos permanentes. O custo neste exemplo é dado pelo número de *hops*.

7.5.2 Encapsulamento de IP Sobre Frame Relay

Encapsulamento de IP sobre redes Frame Relay é especificado pela RFC 1490[4] Redes frame Relay usualmente operam com conexões permanentes estabelecidas por ocasião da contração do serviço. Neste caso o encapsulamento negociado (figura 7.22-b) não é empregado. A filosofia de encapsulamento segue àquela do X.25 para encapsulamento nulo: cada quadro Frame Relay carrega um quadro MAC ou pacote de rede identificados por NLPID ou SNAP. A figura 7.24 ilustra um quadro Frame Relay transportando um datagrama IP.

Endereços IP são mapeados em conexões Frame Relay de forma estática ou dinâmica.

[4]Entitulada *Multiprotocol Interconnect over Frame Relay.*

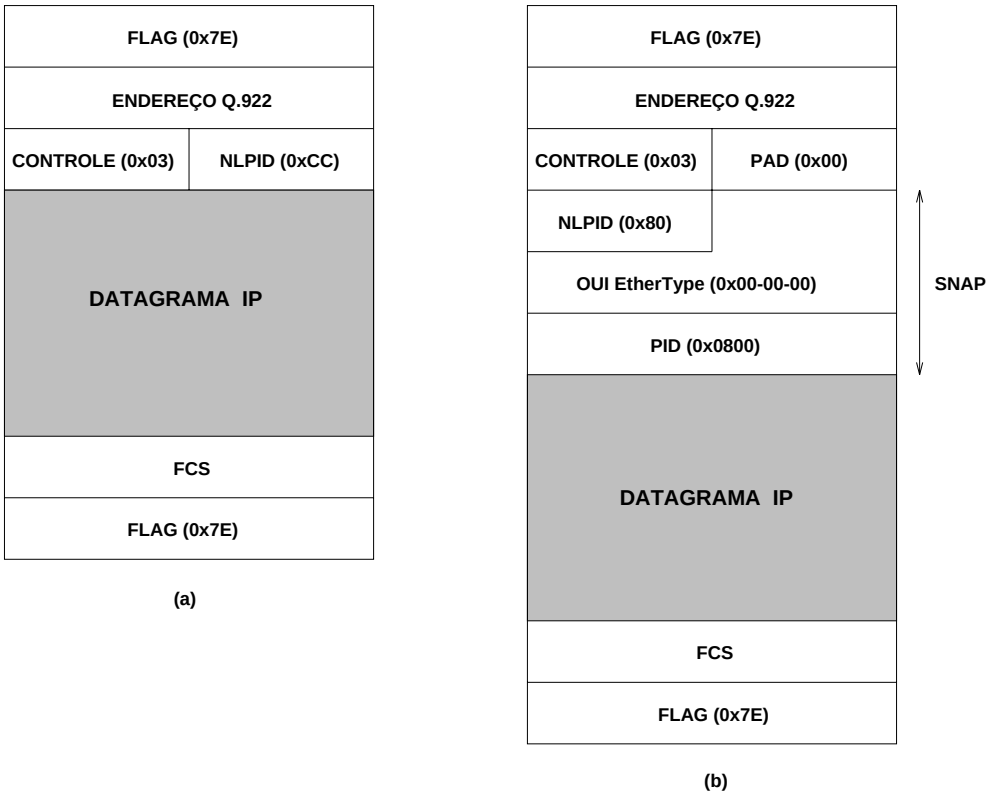


Figura 7.24: Encapsulamento IP sobre Frame Relay (RFC 1490): identificação via NLPID (a) e SNAP (b).

7.5.3 Considerações Sobre Desempenho

Encapsulamento em geral causa perda de desempenho das aplicações que fazem uso dos protocolos encapsulados. Isto se dá pelo *overhead* introduzido pelo cabeçalho dos protocolos de comunicação. Seja o exemplo do aplicativo TELNET que provê terminal remoto em redes TCP/IP. TELNET utiliza o protocolo de transporte TCP que por sua vez utiliza o protocolo de rede IP. Caso o IP seja encapsulado numa conexão X.25 temos a situação dada pela figura 7.25. Na figura nota-se que praticamente um terço da carga do pacote X.25 (pacote padrão de 128 bytes) é composta de cabeçalhos.

Algumas alternativas para minimizar o *overhead* introduzido pelo encapsulamento são:

- utilizar um pacote WAN de maior tamanho;

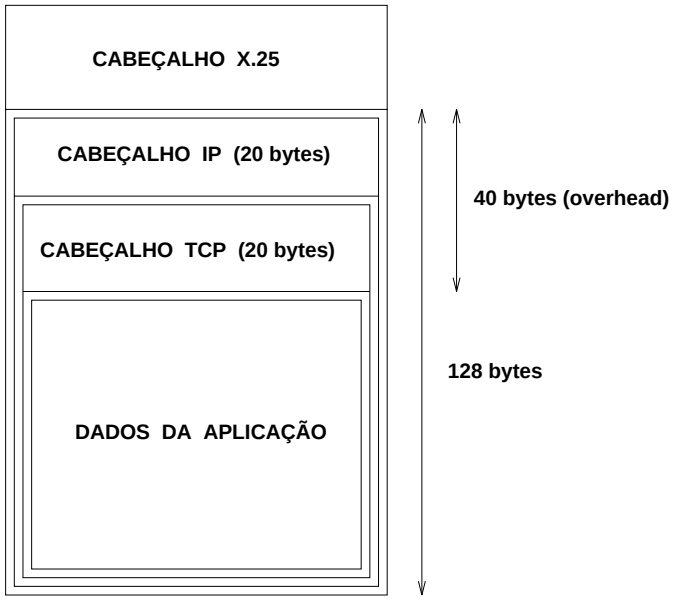


Figura 7.25: *Overhead* introduzido pelo encapsulamento.

- compactar os cabeçalhos dos protocolos encapsulados[5];
- compactar os dados da aplicação.

Infelizmente a eficácia de tais medidas depende da natureza da aplicação.

[5]Alguns roteadores efetuam esta compactação.