DUBCAMADA DE ACESSO AO MEIO

A subcamada MAC da camada de enlace

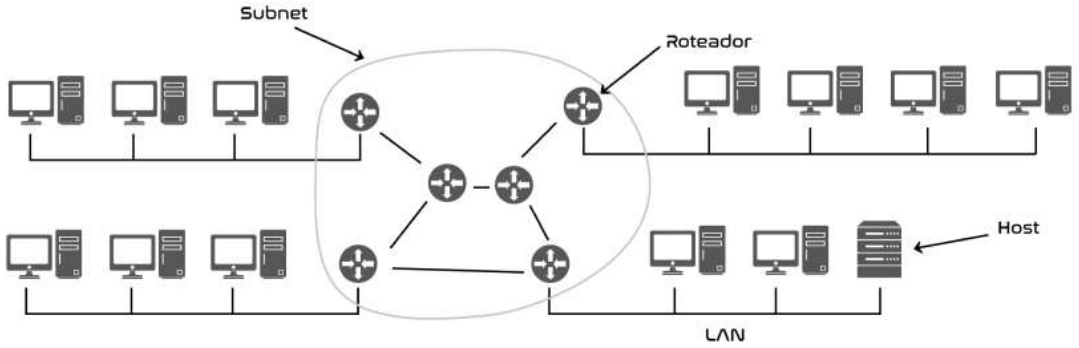
Camada MAC

Serviços da camada MAC

Como vimos, a camada de enlace é subdividida em duas subcamadas: **LLC (Controle de Enlace Lógico) e MAC (Controle de Acesso ao Meio)**, para lidar com o problema de acesso em enlaces multiponto, tema deste módulo. Vamos conferir?

A imagem abaixo ilustra uma rede de computadores composta de quatro redes locais (LANs) conectadas por uma sub-rede. Na sub-rede, os roteadores são conectados por enlaces ponto a ponto, enquanto nas LANs as estações estão ligadas a enlaces multiponto.

Os enlaces ponto a ponto são dedicados e o fluxo de informação segue sempre de um único transmissor a um único receptor. Já os enlaces multiponto são de uso compartilhado entre transmissores e receptores diferentes.



Rede de computadores com quatro redes locais (LANs) conectadas por uma sub-rede e empregam enlaces multiponto (broadcast).

Nas ligações multiponto, o enlace é compartilhado por diversas estações, porém, para que uma transmissão seja recebida com sucesso pela estação receptora, é necessário que cada estação transmissora envie seus dados em momentos diferentes.

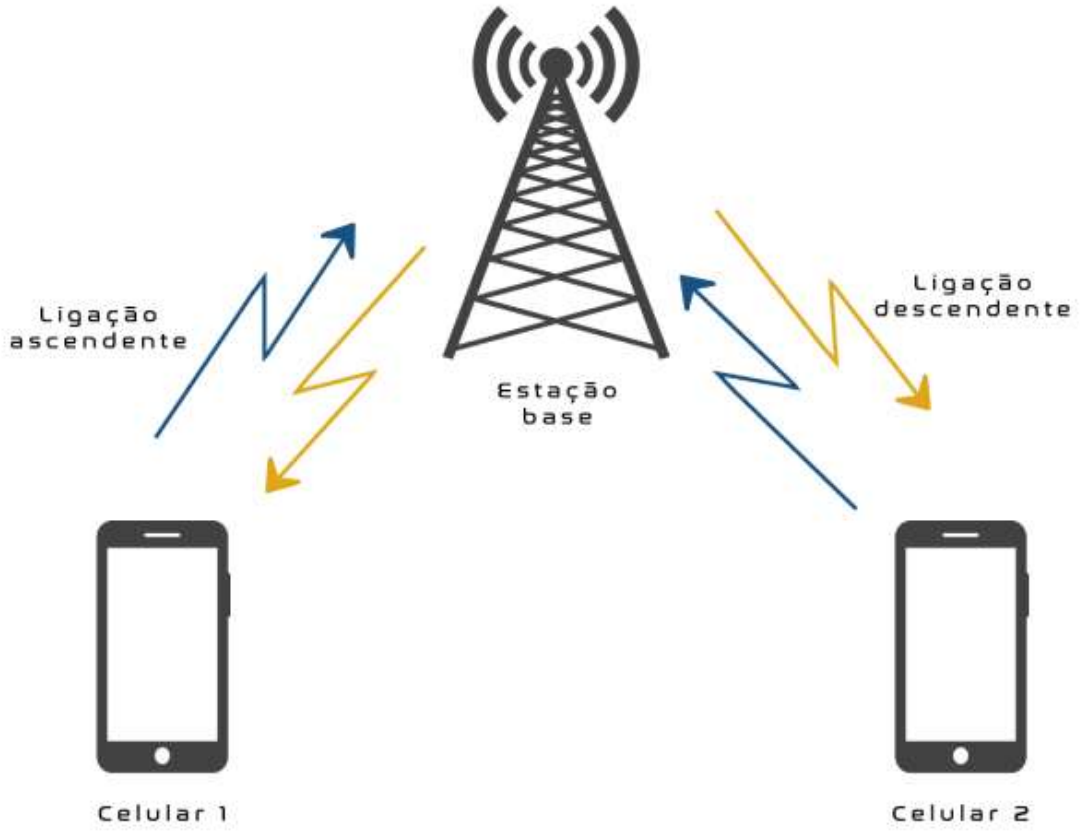
Havendo mais de uma transmissão ao mesmo tempo no enlace multiponto, a estação receptora não terá condições de decodificar o sinal – fenômeno conhecido como **colisão**.

Dessa forma, em enlaces multiponto, é necessário haver uma regra de acesso a fim de organizar as transmissões, evitando (ou minimizando), com isso, as colisões.

O uso do recurso compartilhado, no caso o enlace multiponto, requer o emprego de protocolos de controle de acesso ao meio, o que constitui a principal função da subcamada MAC.

Em suma, o controle de acesso ao meio se faz necessário sempre que houver contenção (disputa) de múltiplas estações pelo acesso ao meio de transmissão.

Exemplo de uso compartilhado do enlace:



Redes móveis celulares nas quais o uplink (canal de subida dos terminais celulares para a estação-base) é compartilhado pelos usuários móveis.

Controlando o acesso ao meio

Como solucionar os problemas

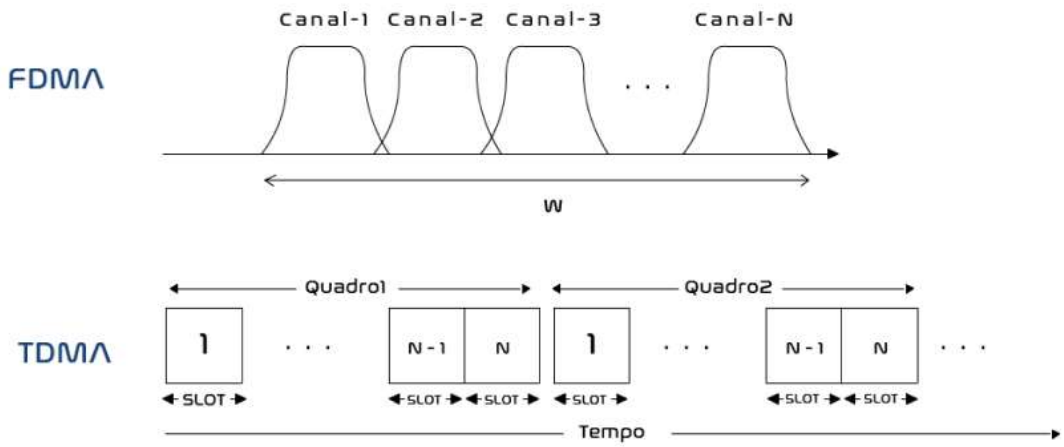
As soluções para o problema de compartilhamento de enlaces entre múltiplas estações podem ser divididas em três grandes grupos:

Alocação estática
Contenção
Acesso ordenado

Protocolos baseados em alocação estática

Alocação estática

A imagem abaixo apresenta duas técnicas de alocação estática bastante comuns:



Técnicas de alocação estática do canal (FDMA e TDMA).

Entenda suas diferenças:

1. FDMA (Acesso Múltiplo por Divisão em Frequência)

   A largura de banda *W* do enlace compartilhado é dividida em *N*, formando, assim, *N* canais individuais. Cada estação transmissora, ao ingressar no sistema, recebe a alocação estática de um desses subcanais e pode utilizá-la de forma exclusiva com o seu par até o momento de desconexão.

2. TDMA (Acesso Múltiplo por Divisão no Tempo)

A divisão ocorre em função do tempo, onde o tempo de uso do canal é dividido em *N* fatias (ou *slots*) de tempo. Cada estação recebe um *slot* designado a ela para as suas transmissões com a estação receptora.

Apesar de resolver o problema de compartilhamento do enlace, as técnicas de alocação estática, como as ilustradas anteriormente, apresentam algumas desvantagens:

- Existe um número máximo de estações que podem ser atendidas pelo sistema. No exemplo, esse número é representado por *N*. Com a chegada de mais uma estação ao sistema (*N+1*), ela será bloqueada por falta de recursos.
- Nessas técnicas, é comum haver desperdício de recursos. Imagine que determinada estação é alocada para utilizar determinado canal. Se essa estação, em algum momento, não tiver nada a transmitir, o canal ficará ocioso e não poderá ser utilizado por outra estação. Como o tráfego de dados ocorre em rajadas (períodos de muita atividade seguidos por períodos de silêncio), essas técnicas podem causar desperdícios significativos de recursos.

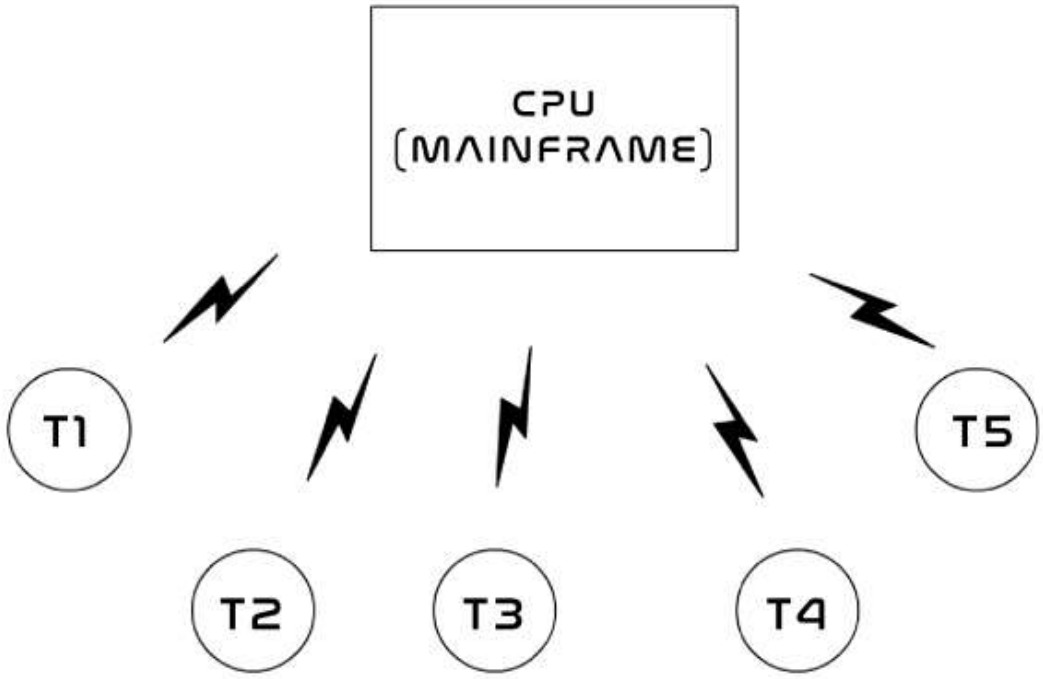
Tradicionalmente, elas são mais empregadas para o tráfego telefônico (voz), daí o seu uso ter sido mais difundido em redes de telefonia fixa e em redes de telefonia celular.

Protocolos baseados em contenção

Um dos primeiros protocolos a empregar a contenção como técnica de compartilhamento do enlace foi o protocolo **ALOHA**, no início da década de 1970, na Universidade do Havaí (ABRAMSON, 2009).

A imagem abaixo ilustra o cenário de aplicação do protocolo **ALOHA** na época. Existia uma unidade central de processamento (um computador mainframe) que deveria ser acessada por terminais remotos espalhados pela universidade.

Observe que, nesse caso, ambos compartilhavam os recursos da CPU e do canal sem fio para as transmissões e acesso à CPU.



Cenário de aplicação do protocolo ALOHA.

A solução empregada para o acesso ao meio físico foi bastante direta. Se determinado terminal tivesse algo a transmitir, ele simplesmente faria isso usando a sua interface rádio sem qualquer tipo de regra ou restrição. Caso houvesse também outro terminal na mesma situação, a colisão seria certa. Nesse caso, o que precisaria ser feito era o tratamento da colisão.

O terminal a transmitir não sabia se a transmissão seria bem-sucedida ou não (colisão); tudo o que ele tinha a fazer era aguardar a confirmação (ACK) enviada no sentido contrário pela estação central (na imagem, CPU). Quando a confirmação era recebida, o terminal entendia que a transmissão foi um sucesso. Caso contrário, o terminal ficava ciente de que houve uma colisão com a transmissão de outro terminal.

O protocolo ALOHA determinava, então, que, em uma situação de colisão, o terminal precisaria sortear um número aleatório de espera e só poderia tentar novamente a transmissão após esse tempo. Como os intervalos de tempo de espera para cada terminal eram sorteados aleatoriamente, os terminais acabariam transmitindo em momentos diferentes, evitando novas colisões.

A solução empregada pelo protocolo ALOHA era bastante simples, e isso ocasionava baixo desempenho para a rede como um todo. O melhor desempenho teórico do protocolo ALOHA pode ser calculado como 18%, ou

seja, na melhor hipótese, apenas 18% dos casos seriam caracterizados como transmissões bem-sucedidas (TANENBAUM, 2011).

O baixo desempenho do protocolo ALOHA motivou o desenvolvimento de protocolos mais elaborados:

S-ALOHA

A ideia imediata era reduzir os eventos em que as colisões pudessem ocorrer. Levando isso em consideração, foi desenvolvido o S-ALOHA (ALOHA com *slots* de tempo). Assim, o terminal só poderia transmitir algo sempre no início de cada *slot*, fazendo com que o número de eventos de colisão ocorresse apenas nesses momentos. O desempenho do S-ALOHA era duas vezes maior do que o desempenho do ALOHA, mas, ainda assim, isso era considerado muito baixo.

CSMA

Na tentativa de reduzir as colisões, foi desenvolvido o protocolo CSMA (acesso múltiplo com detecção de portadora). Para reduzir os eventos de colisão, os terminais que empregam o CSMA “escutam” o meio físico antes de transmitir e só realizam a transmissão ao perceberem que o meio está livre, ou seja, não existe outro terminal transmitindo naquele momento (não foi possível detectar a presença de algum sinal no meio).

As colisões ainda podem ocorrer no CSMA se o meio estiver livre e mais de um terminal estiver “escutando” o meio antes de transmitir. Com o meio livre, esses terminais transmitem ao mesmo tempo, gerando a colisão. A detecção de um evento de colisão acontece tal como no ALOHA, ao aguardar a confirmação ACK do terminal receptor. Havendo colisão, os terminais aguardam um intervalo de tempo sorteado aleatoriamente. Depois disso, tentam iniciar novamente a transmissão.

Na verdade, o CSMA é uma família de protocolos que podem ter variações quanto ao momento de iniciar uma transmissão no canal. Na imagem abaixo, relaciona em um gráfico o desempenho dos protocolos ALOHA, S-ALOHA e as variações do CSMA em um sistema teórico com cem terminais (TANENBAUM, 2011).

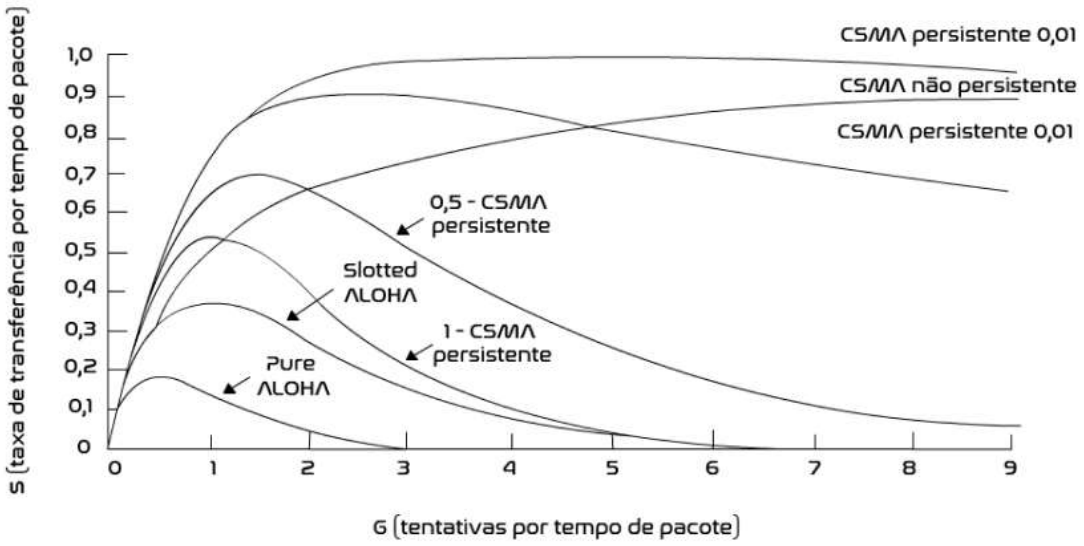


Gráfico: Desempenho dos protocolos para um sistema com cem terminais Tanebaum, 2011.

No eixo das ordenadas, o parâmetro S indica a proporção de eventos de transmissão com sucesso (de 0 a 1 ou, analogamente, de 0% a 100%), e, no eixo das abcissas G, a intensidade de tráfego que os terminais impõem ao canal (quantidade de pacotes de dados enviados pelos terminais a cada tempo).

Pode-se observar que a curva do ALOHA (na imagem, ele é chamado de *Pure ALOHA*) é a curva mais baixa e apresenta o seu pico (melhor resultado) em torno dos 18%, conforme já mencionado. É interessante observar também que, à medida que o *G* (intensidade de tráfego) aumenta, o desempenho do ALOHA diminui até entrar em pleno colapso – desempenho praticamente nulo. O mesmo ocorre para outras curvas, mas tal ponto de colapso é atingido para valores de intensidade de tráfego cada vez maiores, indicando melhores desempenhos em situações de mais alta carga. O destaque fica mesmo para o 0.01 *persistent CSMA*, que apresenta, no cenário teórico de estudo, um desempenho de quase 100% (TANENBAUM, 2011).

Outro protocolo da família do CSMA que vale a pena destacar é o CSMA/CD (acesso múltiplo com detecção de portadora e detecção de colisão), que foi padronizado pelo IEEE por meio da série IEEE802.3 (ETHERNET), para ser utilizado em redes locais cabeadas.

O CSMA/CD emprega uma função de detecção antecipada de colisão. Em vez de aguardar pela mensagem de reconhecimento (ACK), o CSMA/CD é capaz de perceber a ocorrência de uma colisão no momento em que o terminal estiver transmitindo o seu próprio pacote de dados. Assim, é possível interromper antecipadamente uma transmissão que não teria sucesso. Essa

detecção antecipada reduz os tempos de colisão, que ficariam ocupando desnecessariamente o canal.

Protocolos de acesso ordenado

Na última categoria de protocolos, encontramos aqueles que garantem o acesso ordenado ao meio físico e, portanto, são livres de colisões.

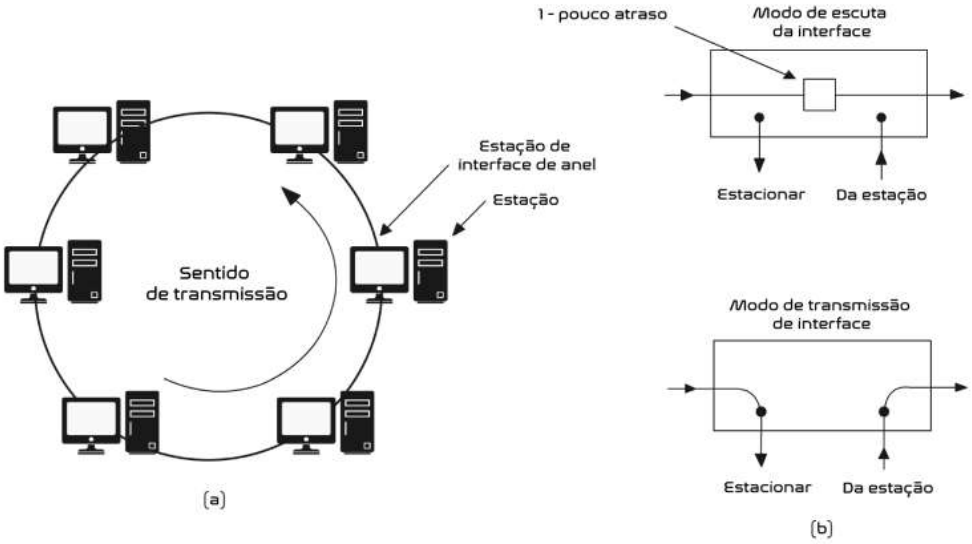
São várias as possibilidades dentro dessa categoria, mas nos concentraremos nos protocolos que utilizam passagem de permissão.

Permissão nada mais é do que um quadro especial que circula pela rede. Com isso, a estação que capturar a permissão terá o direito de realizar a transmissão.

Todas as outras estações que não possuem a permissão ficam impedidas de realizar uma transmissão no enlace compartilhado. Após a sua transmissão, a estação devolve a permissão para a rede, a fim de que outra estação consiga transmitir.

Dois protocolos de passagem de permissão foram padronizados pelo IEEE:

***Token ring* (passagem de permissão em anel)**



Token ring. (a) Rede de passagem de permissão em anel; (b) Diagrama do funcionamento da interface de cada estação.

Podemos observar na imagem acima a topologia da rede em anel e o diagrama de funcionamento da interface, que serão descritas a seguir.

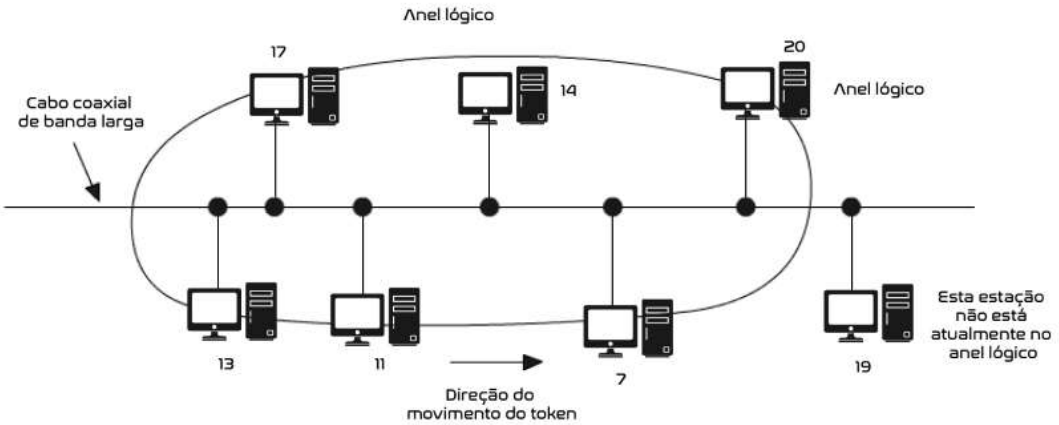
a) Topologia de rede de passagem de permissão em anel: As estações são conectadas em uma estrutura topológica em anel para que a permissão (*token*) possa circular pelo anel. Quando a estação deseja transmitir, ela captura a permissão e realiza a sua transmissão. Após esse momento, ela libera novamente a permissão para circular pelo anel e permitir que outra estação possa também receber a permissão e realizar a sua transmissão.

b) Diagrama do funcionamento da interface de cada estação: A imagem acima mostra o comportamento padrão da interface durante o modo de escuta do barramento em anel, enquanto a imagem inferior ilustra a interface da estação quando no modo de transmissão. Durante a transmissão, a estação abre a interface com o anel para capturar o *token* e também para inserir o seu quadro de informação no barramento.

O padrão IEEE 802.5 *token ring* especifica ainda uma série de modos de operação para o anel e as funções de gerência necessárias para o controle do *token*, contribuindo, assim, para o bom funcionamento da rede.

Token Bus (passagem de permissão em barra)

As redes de passagem em permissão em barra, padrão IEEE 802.4, são semelhantes às redes em anel, porém as estações são conectadas em um barramento. Elas caracterizam um bom exemplo de topologia física (conexão física das estações) em barra e topologia lógica (dada pelo funcionamento do protocolo) em anel, conforme ilustra a imagem a seguir.



Funcionamento do *Token Bus*.

A motivação para a padronização de tais redes veio do setor industrial e fabril, que opera com as suas máquinas em linhas de produção, o que exige como pré-requisito uma rede com topologia em barra.

Nas redes *token bus*, as estações possuem um número de identificação (endereço físico) e cada estação conhece os endereços das estações vizinhas. Assim como no *token ring*, existe um quadro especial de controle (*token*) que regula o acesso ao meio de transmissão. A estação que possui o *token* (uma por vez – não há colisões) tem garantia de transmissão por determinado espaço de tempo. O token “circula” pelas estações no sentido decrescente dos endereços, formando um anel lógico.

Embora as tecnologias *token ring* e *token bus* não sejam mais utilizadas em redes locais, as soluções são elegantes e foram cuidadosamente especificadas e padronizadas.

O estudo das soluções se justifica, pois as técnicas de passagem de permissão têm emprego amplo na área de redes, principalmente em problemas de compartilhamento e alocação de recursos entre múltiplos usuários.