Camada Enlace

Luiz Arthur

A camada de enlace de dados é a segunda camada tanto do modelo OSI quanto do modelo TCP/IP. A camada de enlace trata de algoritmos que permitem uma comunicação eficiente e confiável entre dois computadores adjacentes, ou seja, duas máquinas fisicamente conectadas por meio de um canal de comunicação que funciona conceitualmente como um fio (cabo coaxial, par-trançado, linha telefônica, ou um canal sem fio).

Em principio parece que a camada de enlace não é importante e cuida de problemas triviais, mas infelizmente, **os circuitos de comunicação produzem erros ocasionais**. Além disso, eles têm uma taxa de dados finita, e há um retardo de propagação diferente de zero entre o momento em que o bit é enviado e o momento em que ele é recebido. Essas limitações têm implicações importantes para a eficiência da transferência de dados e **os protocolos usados para comunicações devem levar todos esses fatores** em consideração.

A camada de enlace de dados executa diversas funções específicas. Dentre elas estão as seguintes:

Fornece uma interface de serviço bem definida à camada de rede;
• Lidar com **erros** de transmissão;
• Fornecer **controle** de acesso ao meio;
• Regular o fluxo de dados, de tal forma que receptores lentos não sejam atropelados por transmissores rápidos.

A camada de enlace de dados recebe os pacotes da camada de rede e os encapsula em quadros para transmissão, cada **quadro** contém um **cabeçalho** (header) de quadro, um campo de **carga útil**, que conterá o pacote, e um final (trailer) de quadro.

A camada de enlace de dados pode ser projetada de modo a oferecer diversos serviços, que podem variar de sistema para sistema. Três possibilidades razoáveis oferecidas com freqüência são:

•Serviço **sem conexão** e sem confirmação;

•Serviço **sem conexão** e **com confirmação**;

•Serviço **orientado a conexões** com confirmação;

A maior parte das LANs utiliza serviços sem conexão e sem confirmação na camada de enlace de dados, ficando isto a cargo das camadas superiores. O segundo método é útil em canais não confiáveis, como os sistemas sem fio. O terceiro método tem uso em algumas redes WANs.

Para oferecer serviços à camada de rede, a camada de enlace deve usar o serviço fornecidos a ela pela camada física. O que a camada física faz é aceitar um fluxo de bits brutos e tentar entregá-lo ao destino. Não há uma garantia de que esse fluxo de bits seja livre de erros. Assim a camada de enlace é responsável por detectar e, se necessário, corrigir erros.

Em muitos casos, os **processos** da camada **física** e da camada de **enlace** de dados **estarão** geralmente **funcionando em um processador dentro de um chip especial de E/S de rede**, e o código da camada de rede estará na CPU principal, porém outras implementações também são possíveis.

Exemplos de protocolos da Camada de Enlace

Um protocolo da camada de enlace é o protocolo **HDLC** (High-level Data Link Control), que é um protocolo clássico orientado a bits, cujas variantes foram utilizadas durante décadas em muitas aplicações, apesar de um pouco antigo. O HDLC e seus sucessores são **derivados** do protocolo de enlace utilizado primeiro no mundo dos computadores de grande porte da **IBM**: O protocolo **SDLC** (Synchronous Data Link Control - controle de enlace de dados síncrono), depois de desenvolvido este foi submetido ao **ANSI** e este modificou e transformou o SDLC no **ADCCP** (Advanced Data Communication Control Procedure – procedimento de controle de comunicação de dados avançados), e a **ISO** alterou o SDLC, para transformá-lo no HDLC (controle de enlace de dados de alto nível), este também teve variações levando a chamar de **LAP** (Link Access Procedure) como parte do padrão de interface de rede X.25. A característica mais interessante dos padrões é que há muitos deles para escolher. Além disso, se você não gostar de nenhum, você poderá simplesmente esperar pelo modelo do próximo ano.

Esses protocolos se baseiam nos mesmos princípios. Todos são orientados a bits e todos utilizam a técnica de inserção de bits para transferência de dados. Eles diferem apenas em pequenos e irritantes detalhes.

Os protocolos orientados a bits, tem o seguinte formato: Um conjunto de **Flags** que indica o inicio e final do quadro; o campo **Endereço** para identificar um dos vários terminais, ou em redes ponto-a-ponto esse campo é utilizado para fazer distinção entre comandos e respostas; O campo **Controle** é usado para números de seqüência, confirmações e outras finalidades.

01111110	Endereço	Controle	Dados	Verificação	01111110

O campo **Dados** pode conter qualquer informação; O campo **soma de verificação** é uma variação do código de redundância cíclica; O quadro é delimitador por outra flag, sendo que nas linhas ponto-a-ponto ociosa, as seqüências de flags são transmitidas de forma contínua. Apesar de sua ampla utilização, o HDLC está longe de ser perfeito.

Redes com canais Ponto-a-Ponto

A Internet consiste em máquinas individuais (hosts e roteadores) e na infra-estrutura de comunicação que as conecta. Dentro de um único prédio, as LANs são bastante utilizadas para interconexões, mas **grande parte da infra-estrutura geograficamente distribuída é construída a partir de linhas privadas ponto-a-ponto.**

Na prática, a comunicação **ponto-a-ponto** é utilizada principalmente em duas situações. Na primeira delas, milhares de organizações têm uma LAN ou mais, cada uma com um determinado número de hosts e um roteador. Com freqüência, os roteadores são interconectados por uma LAN de backbone. Em geral, todas as conexões com o mundo exterior passam por um ou dois roteadores que têm linhas privadas (também chamadas de linhas dedicadas) **ponto-a-ponto com roteadores distantes**. São esses roteadores e suas linhas privadas que compõem as sub-redes de comunicação, nas quais a Internet se baseia.

A segunda situação em que as linhas ponto-a-ponto executam uma função importante na Internet diz respeito aos milhões de indivíduos que estabelecem **conexões domésticas com a Internet utilizando modems** e linhas telefônicas com acesso por discagem.

Tanto para a conexão de linha privada entre roteadores quanto para a conexão com acesso por discagem entre o host e o roteador, é necessário o uso de um **protocolo de enlace de dados ponto-a-ponto** na linha para cuidar do enquadramento, do controle de erros e de outras funções da camada de enlace.

Point-to-Point Protocol - PPP

A Internet precisa de um protocolo ponto-a-ponto para diversos fins, inclusive para cuidar do tráfego de roteador para roteador e de usuário doméstico para ISP (provedor de serviços da Internet). Esse protocolo é o **PPP (Point-to-Point Protocol – protocolo ponto-a-ponto)**, este **trata da detecção de erros**, aceita vários protocolos, permite que endereços IP sejam negociados em tempo de conexão, **permite a autenticação** e inclui muitas outras características.

O PPP dispõe de três recursos:

•Um método de enquadramento que **delineia** de forma não ambígua o **fim de um quadro e o início do quadro seguinte**. O formato do quadro também lida com a detecção de erros;

•Um protocolo de **controle de enlace** usado para **ativar linhas**, **testá-las**, negociar opções e **desativá-las** novamente quando não forem mais necessárias. Esse protocolo é denominado LCP (**Link Control Protocol** – protocolo de controle de enlace). Ele admite circuitos síncronos e assíncronos, e também codificações orientados a bytes e a bits.

•**Uma maneira de negociar as opções da camada de rede** de modo independente do protocolo da camada de rede a ser utilizada. O método escolhido deve ter um NCP (Network Control Protocol – protocolo de controle de rede) diferente para cada camada de rede aceita.

O **formato de quadro PPP foi definido** de modo a ter uma aparência **semelhante ao formato de quadro HDLC**, pois não há motivo algum para a definição de um novo padrão. A principal diferença entre o PPP e o HDLC é que **o PPP é orientado a caracteres**, e não a bits. O **PPP não** oferece uma **transmissão confiável** com o uso de números de seqüência e confirmações como padrão, mas em redes sem fio podemos utilizar o PPP modificado para este tipo de recurso.

Flags 01111110	Endereço	Controle	Protocolo	Carga útil	Verificação	Flags 01111110

Todos os quadros PPP começam pelo byte de **flag**, que indica o inicio de um quadro.

O **campo endereço**, que sempre é definido como o valor binário 111111111, indicando que todas as estações devem aceitar o quadro. A utilização desse valor evita o problema da necessidade de atribuição de endereços de enlace de dados.

O **campo controle** tem o valor 00000011. Esse valor indica um quadro não numerado, ou seja, o PPP não oferece transmissão confiável e confirmações como padrão. Em ambientes ruidosos como em redes sem fio, pode ser utilizada a transmissão confiável que emprega o modo numerado, mas na prática é raramente utilizado.

O **campo Protocolo** informa o tipo de pacote que se encontra no campo Carga útil. Ele indica, por exemplo, se a carga útil leva dados do protocolo IP, IPX, etc.

O campo **Carga útil** tem comprimento variável, podendo se estender até o tamanho máximo negociado. Se o comprimento não for negociado na configuração da linha, será empregado o comprimento padrão de 1.500 bytes. Porerá haver um preenchimento logo após a carga útil, caso seja necessário.

O **campo Total de verificação**, que normalmente tem 2 bytes, embora seja possível negociar um total de verificação de 4 bytes.

Em suma, o PPP é um mecanismo de enquadramento multiprotocolo, adequado para a utilização de modems, em linhas seriais e em outras camadas físicas.

Redes com canais de difusão

As **redes** podem ser divididas em **duas categorias**: as que usam conexão **ponto-a-ponto** e as que utilizam **canais de difusão**.

A maioria das rede de computadores, principalmente as **locais**, **utilizam canais de difusão**. Em qualquer rede de difusão, a questão fundamental é determinar quem tem direito de usar o canal quando há uma disputa por ele. Na literatura, os canais de difusão às vezes são referidos como canais de multi-acesso ou canais de acesso aleatório.

Os protocolos usados para determinar **quem será o próximo a usar a rede em um canal de multi-acesso** pertencem a uma subcamada da camada de enlace de dados, chamada **sub-camada MAC (Medium Access Control)**, que é especialmente importante em LANs.

O problema central em redes por difusão é definir como alocar um único canal de difusão entre usuários concorrentes.

Dentre os padrões mais importantes do IEEE na camada de enlace estão o padrão **802.3** mais conhecido como **Ethernet**, o **802.11** (LAN sem fio), e ainda estão engatinhando dois outros padrões o **802.15** (Bluetooth) e o **802.16** (MAN sem fio).

O 802.3 e o 802.11 têm camadas físicas diferentes e subcamadas MAC diferentes, **mas convergem para a mesma subcamada de controle de enlace lógico (Logical Link Control) IEEE 802.2**, e portanto têm a mesma interface para a camada de rede.

Ethernet

A história começa no primitivo Havaí, no início da década de 1970. Onde era impossível estender cabos no mar para interligar as linhas para a comunicação em rede. A única solução que eles encontraram foi o rádio de ondas curtas.

No qual, cada terminal do usuário estava equipado com um pequeno rádio que tinha **duas freqüências**: **ascendente** (até o computador central) e **descendente** (a partir do computador central). Quando o usuário queria entrar em contato com o computador, ele transmitia um pacote contendo os dados no canal ascendente. Se ninguém mais estivesse transmitindo naquele momento, o pacote provavelmente chegava e era confirmado no canal descendente. **Se houvesse disputa pelo canal ascendente**, **o terminal perceberia a falta de confirmação e tentaria de novo**. Tendo em vista que só havia um transmissor no canal descendente (o computador central), nunca ocorria colisões nesse canal. Esse sistema, chamado ALOHANET, funcionava bastante bem sob condições de baixo tráfego, mas fica fortemente congestionado quando o tráfego ascendente era pesado.

Quase na mesma época, um estudante chamado Bob Metcalfe e juntamente com seu amigo David Boggs, projetaram e implementarão a primeira rede local, baseada na rede havaiana. O sistema foi chamado **Ethernet**, uma menção ao éter luminoso, através do qual os antigos diziam que a radiação eletromagnética se propagava (mas a radiação se propaga no vácuo). No caso da Ethernet, o meio de transmissão não era o vácuo, mas um cabo coaxial grosso (o éter) com até 2,5 Km de comprimento (com repetidores a cada 500 metros. **Até 256 máquinas podiam ser conectadas ao sistema por meio de transceptores presos ao cabo. O sistema funcionava a 2,94 Mbps**.

Mas a **Ethernet tinha um aperfeiçoamento importante em relação à ALOHANET**: **antes de transmitir, primeiro um computador inspecionava o cabo para ver se alguém** mais já estava transmitindo. Nesse caso, o computador ficava impedido até a transmissão atual terminar (isto é chamado de CSMA/CD - Carrier Sense Multiple Acess with Collision Detection).

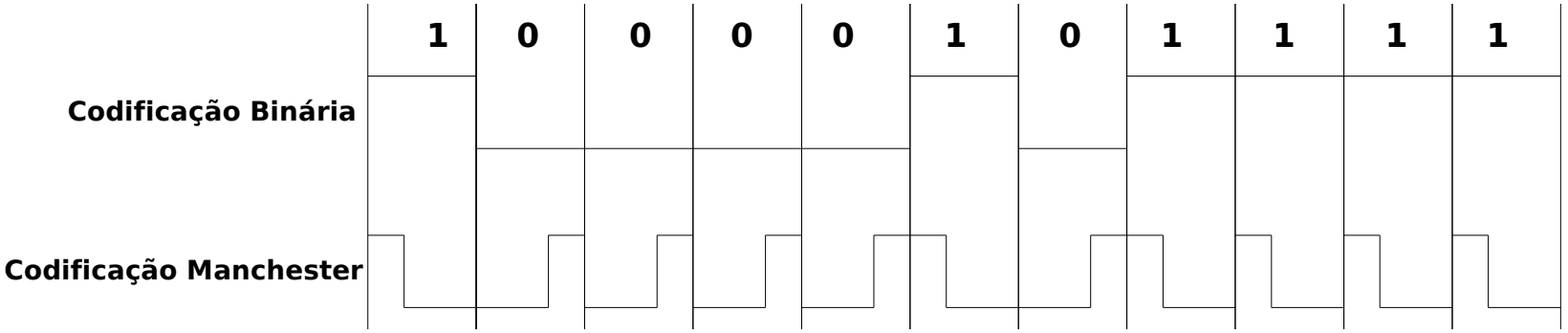
Isso evitava interferências com transmissões em andamento, o que proporcionava uma eficiência muito maior. A **ALOHANET não funcionava assim** basicamente porque era **impossível para um terminal em uma ilha detectar a transmissão de um terminal em outra ilha distante**, problema este enfrentado por computadores em redes sem fio atuais.

Apesar da escuta do computador antes de transmitir, **ainda surge um problema**: o que acontece se dois ou mais computadores esperarem até a transmissão atual se completar e depois todos começarem a transmitir ao mesmo tempo? A solução é fazer cada computador se manter na escuta durante sua própria transmissão e, **se detectar interferência, bloquear o éter para alertar todos os transmissores**. Em seguida, recuar e esperar um tempo aleatório antes de tentar novamente. Se ocorrer uma segunda colisão, o tempo aleatório de espera será duplicado e assim por diante, até separar as transmissões concorrentes e dar uma a uma delas a chance de iniciar sua transmissão.

Desde o seu surgimento a Ethernet não parou mais de se desenvolver e ainda está em desenvolvimento. Surgiram novas versões a 100Mbps, 1000Mbps e a velocidades ainda mais altas 10000Mbps, por exemplo.

Porém a Ethernet (IEEE 802.3) não é o único padrão de LAN. O comitê IEEE também padronizou um barramento de símbolos (**802.4, token bus**) e um anel de símbolo (**802.6, token ring**). O símbolo seria a passagem de um pequeno pacote chamado símbolo ou tokem (ficha) de um computador para outro. Um computador só podia transmitir se tivesse a posse do símbolo, e isso evita colisões. Porém, esses padrões basicamente desapareceram.

Uma rede **Ethernet utiliza a codificação manchester** para identificar o inicio e o fim de cada bit. Na codificação Manchester, cada período de bits é dividido em dois intervalos iguais. Um bit 1 binário é enviado quando a voltagem é definida como alta durante o primeiro intervalo, e como baixa no segundo intervalo. Um bit 0 binário é exatamente o oposto: primeiro baixo, e depois alto. Esse esquema garante que cada período de bit terá uma transição na parte intermediária tornando fácil para o **receptor sincronizar-se com o transmissor**. Uma **desvantagem** da codificação Manchester é que ela **exige duas vezes mais largura de banda** que a codificação binário direta, pois os pulsos são a metade da largura.



A estrutura original de quadros Ethernet DIX (DEC, Intel, Xerox) começa com um **Preâmbulo** de 8 bytes, cada um contendo o padrão de bits **10101010**. A codificação Manchester desse padrão produz uma onda quadrada, a fim de permitir a sincronização entre o clock do receptor e o clock do transmissor. Tanto o transmissor quanto o receptor, devem permanecer sincronizados durante todo o restante do quadro, usando a codificação Manchester para controlar os limites de bits.

O quadro contém dois **endereços**, um para o **destino** e um para a **origem**. O padrão permite endereços de 2 e de 6 bytes, mas os parâmetros definidos para o padrão de banda básica de 10 Mbps usam somente os endereços de 6 bytes. O bit de alta ordem do endereço de destino é **0** para **endereços comuns** e **1** para endereços de **grupos**. Os endereços de grupos permitem que diversas estações escutem um único endereço. Quando um quadro é enviado para um endereço de grupo, todas as estações do grupo o recebem. A transmissão para um grupo de estações é chamada de multidifusão (**multicast**). O endereço que consiste em todos os bits 1 é reservado para difusão (**broadcast**).

Em seguida, vem o **campo Tipo**, que **informa ao receptor o que fazer** com o quadro. **Vários protocolos** da camada de rede **podem estar em uso** ao mesmo tempo na mesma máquina; assim, ao chegar um quadro Ethernet, o núcleo de processamento Ethernet tem de saber a qual protocolo da camada de rede deve entregar a carga util do quadro. O campo Tipo **especifica** que **processo** deve receber o quadro.

Depois, vêm os **dados**, com **até 1500 bytes**. Para tornar mais fácil a distinção entre quadros válidos e lixo, o padrão Ethernet **exige** que os quadros válidos tenham **pelo menos 64 bytes** de extensão, do endereço de destino até o campo de total de verificação, incluindo ambos. Se a parte de dados de um quadro for menor que 46 bytes, o **campo Preenchimento será usado para preencher o quadro até o tamanho mínimo**.

O último campo Ethernet é o **Total de verificação**. Ele é efetivamente um código de **hash** de 32 bits dos dados. Se alguns bits de dados forem recebidos com erros (devido ao ruído no cabo), o total de verificação quase certamente estará errado, e o erro será detectado. O algoritmo do total de verificação é um **CRC (Cyclic Redundancy Check)**. Ele simplesmente realiza a **detecção de erros, não a correção** de erros antecipada.

Evolução da Ethernet

A princípio, 10 Mbps parecia ser o paraíso, da mesma forma que os modems de 1200 bps pareciam ser o paraíso para os primeiros usuários de modems acústicos de 300 bps. Porém, a novidade se dissipou com rapidez. Mas o mercado ainda precisava de LANs mais rápidas (devido as aplicações).

Foi nesse ambiente que o IEEE reuniu o comitê do 802.3 em 1992, com instruções para produzir uma LAN mais rápida. Uma das propostas era manter o 802.3 exatamente como estava, e apenas torná-lo mais rápido.

As **três principais razões** pelas quais o comitê do 802.3 decidiu **continuar** com uma rede **Ethernet** aperfeiçoada foram:

1. A necessidade de manter a **compatibilidade** retroativa com as LANs Ethernet existentes.
2. O **medo** de que um **novo protocolo** criasse **problemas** imprevistos.
3. O desejo de **terminar o trabalho** antes que a tecnologia mudasse.

O trabalho foi feito rapidamente (pelas normas dos comitês de padronização) e o resultado, o 802.3u, foi oficialmente aprovado pelo IEEE em junho de 1995. Tecnicamente, o 802.3u não é um padrão novo, mas um adendo ao padrão 802.3 existente (para enfatizar sua compatibilidade retroativa). Como todos o chamam **Fast Ethernet**, em vez de **802.3u**, também faremos o mesmo.

A idéia básica por trás do **Fast Ethernet** era simples: manter os antigos formatos de quadros, interfaces e regras de procedimentos, e **apenas reduzir o tempo de bit de 100*ns* para 10*ns***. Tecnicamente, teria sido possível fazer isto apenas **reduzindo o tamanho dos cabos** 10Base2 e 10Base5, **mas** isto **não** seria muito **interessante**.

Entretanto, algumas decisões ainda precisavam ser tomadas, sendo a mais importante delas os **tipos de fios que seriam aceitos**, **e os cabos coaxiais não eram a escolha**.

Um dos concorrentes era o par trançado da categoria 3. A principal desvantagem do par trançado da categoria 3 é sua incapacidade para transportar sinais de 200 megabauds (100 Mbps com codificação Manchester) por 100 metros, a distância máxima entre o computador e o hub especificada para 10Base-T. Por outro lado, a fiação de par trançado da categoria 5 é capaz de tratar 100 metros com facilidade, e a fibra pode ir muito mais longe que isso. Decidiu-se permitir as três possibilidades.

Nome	**Cabo**	**Tam. Máx de segmento**	**Vantagens**
100BaseT4	Par trançado	100 m	Utiliza UTP cat-3
100BaseTX	Par trançado	100 m	Full-duplex cat-5
100BaseFx	Fibra óptica	2.000 m	Full-duplex.

Para a fiação da **cat**egoria **5**, o projeto **100Base-TX é mais simples**, porque os fios são capazes de manipular velocidades do clock de até **125 MHz**. São usados somente **dois pares trançados** por estação, um que vai para o hub e outro que sai do hub. O 100Base-TX é um sistema **full-duplex**; as estações podem transmitir a 100 Mbps e receber a 100 Mbps, ao mesmo tempo. Com freqüência, o 100Base-TX e o 100Base-T4 são referidos em conjunto como 100Base-T.

A tinta mal havia secado no padrão Fast Ethernet quando o comitê 802 começou a trabalhar em uma Ethernet ainda mais rápida (1995). Ele foi denominado **Ethernet de gigabit** e foi ratificado pelo IEEE em 1998, com o nome **802.3z**. Os objetivos do comitê do 802.3z eram essencialmente os mesmos do comitê 802.3u: tornar a Ethernet 10 vezes mais rápida, mantendo a compatibilidade retroativa com todos os padrões Ethernet existentes.

Existe também o padrão **10 Gb Ethernet**, definido pela recomendação IEEE **802.3an**, neste padrão só é suportado o modo full-duplex.

Então temos basicamente os padrões:

- Ethernet ou IEEE 802.3 com velocidades de 10Mbps;
- Fast Ethernet ou IEEE 802.3u com velocidades de 100Mbps;
- Gigabit Ethernet ou IEEE 802.3z com velocidades de 1.000Mbps;
- 10 Gigabit Ethernet ou IEEE 802.3an com velocidades de 10.000Mbps

Camada de enlace sem fio

A demanda cada vez maior, por **portabilidade**, **mobilidade**, **conveniência**, convergência entre tantos outros atrativos oferecidos atualmente pelos sistemas de comunicação sem fio, ou até mesmo a simples idéia de entrar em um escritório e magicamente seu notebook se conectar à Internet sem nenhum fio faz com que cada dia mais e mais pessoas invistam em dispositivos sem fio.

Atualmente a Wireless Local Area Networking ou simplesmente **WLAN** é uma tecnologia desenvolvida ao longo da década de 90 pelo IEEE, mas ainda está em fase de amadurecimento, principalmente em questões relacionadas com qualidade de serviço e segurança.

Assim, à comercialização de WLANs por várias empresas não demorou, e o IEEE teve de padronizar este tipo de rede para que estas fossem compatíveis. Ao padrão de LANs sem fio deu-se o nome de **802.11**, e um apelido comum para este é **WiFi** (Wireless Fidelity). Tal padrão proposto tinha de funcionar em dois modos:

•Na presença de uma **estação base**, neste toda a comunicação deveria passar por um ponto de acesso comum aos hosts da rede.

•Na ausência de uma estação base, este modo é chamado de interligação de redes **ad hoc** e não requer um ponto de acesso como o primeiro caso, no modo ad hoc os hosts podem comunicar entre si diretamente.

Mas para desenvolver este novo padrão sem fio o **IEEE teve de abordar alguns pontos críticos** dentre estes estão:

(i) descobrir uma banda de **freqüência** adequada que estivesse **disponível**, de preferência em todo o mundo;
(ii) lidar com o fato de que os **sinais de rádio têm um alcance finito**;
(iii) assegurar que a **privacidade dos usuários** seja mantida;
(iv) compreender as implicações de **mobilidade** dos computadores;
(v) e por fim, construir um sistema com **largura de banda** suficiente para ser economicamente viável.

Bem no inicio da padronização das redes sem fio a Ethernet já havia dominado o mercado de redes locais, e assim o comitê decidiu tornar **o 802.11 compatível com a Ethernet** tornando possível enviar um pacote IP pela WLAN, mas mesmo assim existe diferenças a serem tratadas de uma rede com fio e uma rede sem fio, são elas:

• A chance de **colisão em uma rede sem fio é muito maior** do que em uma rede com fio, isto se dá devido ao meio de transmissão, o ar.

• Existe a possibilidade de **objetos** sólidos **refletirem o sinal de rádio**, de forma que o sinal pudesse ser recebido várias vezes (atenuação multiponto).

• Os **softwares** dos usuários em sua grande maioria **não estão ciente** da **mobilidade** do host.

Consciente destes problemas **em 1997 a WLAN 802.11 começou a funcionar a 1Mbps ou 2 Mbps**, é claro que as pessoas reclamaram que isto era muito lento, já que o padrão da época para redes com fio era no mínimo 10 Mbps. Desta forma, surgiram dois novos padrões:

• Um que utiliza uma faixa de freqüências mais larga e funcionava em velocidades de **54 Mbps** na banda de 5 Ghz utilizando a técnica OFDM (Orthogonal Frequency Division Multiplexing), que foi chamado de **802.11a**;

• Outro o padrão **802.11b** que utiliza a mesma faixa de freqüências que o 802.11, mas emprega a técnica de modulação HR-DSSS (High Rate Direct Sequence Spread Spectrum) para alcançar **11 Mbps** na banda 2,4 GHz. Este padrão emprega bandas de freqüência **ISM** (Instrumentation, Scientific & Medical), compreendem três segmentos do espectro reservado para uso **sem a necessidade de licença**, sendo as freqüências disponíveis 902 a 928 Mhz, 2400 a 2483,5 Mhz e 5.725 a 5.850 MHz.

• Com o passar do tempo o comitê 802 apresentou ainda outra variante, o **802.11g**, que utiliza a técnica de modulação do 802.11a (OFDM), mas emprega a faixa de freqüência do 802.11b (2.4Ghz), atualmente este tem se tornado o padrão mais procurado.

Sendo que, a camada física corresponde muito bem à camada física do modelo OSI em todos os padrões, mas a **camada de enlace** de dados em todos os protocolos 802 **se divide em duas ou mais subcamadas**.

No 802.11, a **subcamada MAC (Medium Access Control) determina como o canal é alocado**, isto é, quem terá oportunidade de transmitir em seguida. Acima dela, encontra-se a **subcamada LLC (Logical Link Control), cujo trabalho é ocultar as diferenças entre as diversas variações do 802** e torná-las indistinguíveis no que se refere à camada de rede.

O **protocolo da subcamada MAC** do 802.11 é bastante diferente do protocolo Ethernet, devido à complexidade inerente do ambiente sem fio, em comparação com o de um sistema fisicamente conectado. Com a Ethernet, uma estação só precisa esperar até o éter ficar inativo e começar a transmitir. Se não receber de volta uma rajada de ruído dentro dos primeiros 64 bytes, é quase certo que o quadro tenha sido entregue corretamente. No caso das **LANs sem fios**, essa situação não ocorre, por que **nem todas as estações estão dentro do alcance de rádio umas das outras**, as transmissões realizadas em uma parte de uma célula podem não ser recebidas em outros lugares na mesma célula. Como resultado desses problemas, o 802.11 não utiliza o CSMA/CD, como faz o padrão Ethernet.

Para lidar com esse problema, o 802.11 admite dois **modos de operação**. O primeiro, chamado de **DFC** (Distributed Coordination Function – **Função de coordenação distribuída**), que não usa nenhuma espécie de controle central (seria um esquema parecido com o Ethernet). O outro, chamado **PCF** (Point Coordination Function – **Função de coordenação de ponto**), que utiliza a estação base para controlar toda a atividade em sua célula. Todas as implementações devem aceitar DCF, mas PCF é opcional.

O **DCF utiliza** um protocolo chamado **CSMA/CA** (CSMA with Collision Avoidance – CSMA com abstenção de colisão), sendo que este protocolo utiliza tanto detecção do canal físico quanto a do canal virtual. O CSMA/CA **admite dois métodos** de operação.

• No primeiro método, quando uma estação quer transmitir, ela **escuta o canal**. **Se** ele estiver **ocioso**, a estação **simplesmente começará a transmitir**. Ela não escuta o canal enquanto está transmitindo, mas emite seu quadro inteiro, que pode muito bem ser destruído no receptor devido à interferência. Se o canal estiver ocupado, a transmissão será adiada até o canal ficar inativo. Se ocorrer uma colisão, as estações que colidirem terão de esperar um tempo aleatório, e então tentarão novamente mais tarde. Caso tudo corra bem durante a transmissão a estação receptora envia uma confirmação da entrega do pacote.

• O outro modo de operação do CSMA/CA se baseada no MACAW e **emprega a detecção de canal virtual**. Este exemplo funciona da seguinte maneira. Um host A quer transmitir para um host B. E C é um host dentro do alcance de A. E o Host D é uma estação dentro do alcance de B, mas não dentro do alcance de A. O protocolo começa quando o host A decide transmitir dados para o host B. Ele **inicia a transmissão enviando um quadro RTS** para o host B, a fim de solicitar permissão para enviar um quadro. Quando recebe essa solicitação, o host B pode decidir conceder a permissão e, nesse caso, **envia de volta um quadro CTS**. Após a recepção do CTS, o host A envia seu quadro e **inicia um timer ACK**. **Ao receber** corretamente o quadro de dados, o host B **responde com um quadro ACK**, concluindo a troca de quadros. Se o timer ACK de host A expirar antes do quadro ACK voltar a ele, o protocolo inteiro será executado novamente.

No pondo de vista dos hosts C e D. O host C está dentro do alcance de A, e então pode receber **o quadro RTS**. Se o fizer, host C perceberá que alguém vai transmitir dados em breve e assim, para o bem de todos, **desiste de transmitir** qualquer coisa até a troca ser concluída (isto é feito a partir de informações do RTS). Após este tempo ele reivindica uma espécie de canal virtual, indicado por NAV (Network Allocation Vector – vetor de alocação de rede).

O host D não escuta o RTS, mas escuta o CTS, e assim também reivindica o sinal NAV para ele próprio. Observe que os sinais NAV não são transmitidos; eles são apenas lembretes internos de que a estação deve se manter inativa por um determinado período de tempo.

Se um **quadro for longo** demais, ele terá bem pouca chance de chegar sem **danos** e é provável que tenha de ser retransmitido. Para lidar com o problema de canais ruidosos, o **802.11 permite que os quadros sejam fragmentados** em partes menores, cada uma com seu próprio total de verificação. Depois que um canal é adquirido com o uso de RTS e CTS, vários fragmentos podem ser enviados em seqüência e é chamada rajada de fragmentos. A fragmentação aumenta o throughput, restringindo as retransmissões aos fragmentos defeituosos, em vez de retransmitir o quadro inteiro. O tamanho do fragmento não é fixado pelo padrão, mas é um parâmetro de cada célula e pode ser ajustado pela estação base.

O outro modo permitido o **PFC**, no qual a **estação base efetua o polling das outras estações**, **perguntando se elas têm algum quadro a enviar**. Tendo em vista que **a ordem de transmissão é totalmente controlada pela estação base** em modo PCF, **não ocorre nenhuma colisão**. O padrão prescreve o mecanismo de polling, mas não a freqüência de polling, a ordem de polling, ou mesmo se todas as estações precisam receber um atendimento idêntico.

O mecanismo básico consiste na **difusão** periódica pela estação base **de um quadro de baliza**. O quadro de baliza contém **parâmetros** do sistema, **como seqüências de saltos** (hops) e **tempos de parada**, **sincronização** de clock, etc. Ele também **convida** novas **estações** a se inscreverem no serviço de polling. Depois que uma estação se inscreve para receber o serviço de polling a uma certa taxa, ela tem a **garantia efetiva de uma certa fração da largura de banda**, tornando possível assim oferecer garantias de qualidade de serviço.

Redes sem fio também **tem** mecanismos para conservar recursos de baterias em dispositivos móveis sem fio, já que tem **limitações quanto a bateria**.

O padrão 802.11 define três diferentes **classe de quadros em trânsito**: dados (duração, endereço de origem de destino, endereço de origem e destino dos AP das células, seqüências), controle (versão do protocolo, tipo, sub-tipo, MF) e gerenciamento (origem destino apenas dos hosts sem fio, RTS, CTS, ACK). Cada um deles tem um cabeçalho com uma variedade de campos usados na subcamada MAC.

O padrão 802.11 estabelece que **cada LAN sem fio compatível deve fornecer nove serviços**. Esses serviços estão divididos em **duas categorias**: cinco **serviços de distribuição** e quatro **serviços da estação**. Os serviços de distribuição se relacionam ao gerenciamento da associação a célula e à interação com estações situadas fora da célula. Em contraste, os serviços da estações se relacionam à atividade dentro de uma única célula.

Os cinco **serviços de distribuição são fornecidos pelas estações base** e lidam com a mobilidade das estações à medida que elas entram e saem das células, conectando-se e desconectando-se das estações base. Esses serviços são apresentados a seguir:

•**Associação**: Esse serviço é usado pelas **estações móveis para conectá-las às estações base**. Em geral, ele é usado imediatamente após uma estação se deslocar dentro do alcance de rádio da estação base. Ao chegar, ela anuncia sua identidade e seus recursos. Os recursos incluem as taxas de dados admitidas, a necessidade de serviço PCF (polling) e requisitos de gerenciamento da energia.

•**Desassociação**: Usado antes da estação desligar ou sair, a estação base também pode usá-lo.

•**Reassociação**: Uma estação pode mudar sua estação base usando este serviço. Esse recurso é útil para estações móveis que se deslocam de uma célula para outra.

•**Distribuição**: Esse serviço determina **como rotear quadros enviados à estação base**. Se o destino for local para a estação base, os quadros poderão ser enviados **diretamente pelo ar**. Caso contrário, eles terão de ser encaminhados pela **rede fisicamente conectada**.

•**Integração**: Cuidará de conversão do formato 802.11 para o formato exigido pela rede de destino.

Os quatro serviços restantes são serviços intra-células, ou seja, dentro de uma única célula. Eles são usados depois que ocorre a associação, e são descritos a seguir:

•**Autenticação**: Como a comunicação sem fio pode ser enviada ou recebida facilmente por estações não autorizadas, **uma estação deve se autenticar antes de ter permissão para transmitir dados**. Depois que uma estação móvel é associada pela estação base (aceita em sua célula), a estação base envia um quadro de desafio especial para ver se a estação móvel conhece a **chave secreta (senha)** que foi atribuída a ela. Se o resultado for correto, a estação móvel será completamente aceita na célula.

•**Desautenticação**: Quando uma estação autenticada anteriormente quer deixar a rede, ela é desautenticada.

•**Privacidade**: Administra a **criptografia** e a descriptografia.

•**Entrega de dados**: Por fim, a transmissão de dados é o objetivo, e assim o 802.11 oferece naturalmente um meio para transmitir e receber dados, sendo que o 802.11 não tem garantia de serviço e as camadas mais altas devem ligar com a detecção e a correção de erros.

Ainda no que se refere a redes sem fio, atualmente temos as redes **WPANs** (Wireless Personal Area Networks) que estão se tornando mais e mais comuns, essas **transmitem a taxas de dados mais baixas e cobrem distâncias menores**. A tecnologia **Bluetooth**, por exemplo, permite taxas de transmissão de até **1Mbps** e atinge uma distância nominal de até **10 metros**. As WPANs são utilizadas para substituir os cabos de conexão entre equipamentos pessoais portáteis (telefones, pagers, laptops) e também permitir acesso à Internet.

Como citado anteriormente o Bluetooth é uma tecnologia WPAN que esta se destacando, o Bluetooth fornece conexão sem fio a curta distâncias, desenvolvida inicialmente pela Ericsson (1994) com o objetivo de substituir os cabos que conectavam estes dispositivos ganhou o suporte da Intel, IBM dentre outras empresas de renome. O Bluetooth opera na faixa de freqüência de **2,4 a 2,482 GHz** e adotou o espalhamento espectral por salto de freqüência de modo a garantir comunicação robusta em uma faixa de freqüência compartilhada com outras aplicações como o WiFi.

O Bluetooth apresenta vantagens em relação a conexão via infravermelho pois suporta vários dispositivos e não exige visada direta entre transmissor e receptor. Apesar de ser padronizada pelo **IEEE 802.15** esta assemelha-se mais a um barramento como um USB, mas é wireless.

Com uma avaliação rápida do que o bluetooth, é constituído de uma **piconet**, que consiste em um nó mestre e até sete nós escravos ativos, situados dentro de uma distância de 10 metros. Porém, se existir muitas piconets na mesma sala elas podem até mesmo ser conectadas por um nó de ponto, sendo então denominadas de **scatternet**.

O sucesso do Bluetooth depende agora de sua adoção em larga escala, gerando volumes que tornem insignificantes o custo de sua acréscimo a dispositivos portáteis. Caso isto não ocorra ele poderá ser eclipsado por soluções que oferecem taxas de dados mais altas e mais opções de conectividade como o WiFi.

Para finalizar as **WLANs** estão ficando cada vez mais populares e um número crescente de edifícios de escritórios, aeroportos e outros lugares públicos estão sendo equipados com redes sem fio. Não há dúvidas que o 802.11 causará uma revolução na computação e no acesso à **Internet**. É provável que o 802.11 faça pela Internet o que os notebooks fizeram pela computação: **torná-la móvel**.

Mas ainda existe **outro padrão o 802.16** que permite velocidades de aproximadamente **54 Mbps**, podendo chegar a **75 Mbps**, a uma distância de **6 Km a 9 Km**, este é conhecido comercialmente como **WIMAX** (que na verdade é um fórum de empresas, semelhante ao WiFi) e promete revolucionar a indústria de acesso de banda larga, pois fornecem desempenho equivalentes aos dos tradicionais meios com fio como DSL, cable modem ou E1/T1 porém com tecnologia sem fio.

Switching

A comutação (switching) na camada de Enlace é **baseada no endereço de hardware**, o que significa que o endereço MAC da placa de rede do dispositivo é utilizado para filtragem de rede. Switches utilizam chips especiais, chamados "ASICS" (Application Specific Integrated Circuits), para formar e manter as tabelas de filtragem (filter tables).

Switches são rápidos porque **não analisam** informações pertinentes à **camada de Rede**, analisando, em seu lugar, os endereços de hardware dos quadros (frames) antes de decidir pelo encaminhamento ou abandono desse quadro.

O que torna a **comutação** na camada de Enlace tão **eficiente é a não-modificação de dados**, apenas no frame que o encapsula. Como nenhuma modificação no pacote é realizada, o processo de comutação é muito mais rápido e menos suscetível a erros do que o processo de roteamento existente na camada de Redes.

A comutação na camada de Enlace pode ser utilizada para conectividade entre grupos de trabalho e para a **segmentação da rede**, ou **quebra dos domínios de colisão**. Ela aumenta a largura de banda disponível para cada usuário, uma vez que cada conexão (interface) disponibilizada pelo switch representa seu próprio domínio de colisão. Devido a esse fator pode-se conectar múltiplos dispositivos em cada interface.

A **comutação** na camada de Enlace, entretanto, **possui algumas limitações**. O modo correto de se criar redes comutadas eficientes é certificando-se que os usuários permanecerão ao menos 80% de seu tempo no segmento local.

Redes comutadas quebram domínios de colisão, entretanto, **a rede ainda é um grande domínio de broadcast**, o que pode limitar o tamanho da rede, assim como causar problemas de performance. Assim, pacotes em broadcast e multicast pode vir a ser problemas sérios à medida que a rede cresce.

Devido a este e a outros fatores, **switches** da camada de Enlace **não podem substituir completamente os roteadores** da camada de Redes em uma *internetwork*.

Processo de aprendizagem de endereços físicos pelos switches

Todo switch forma uma tabela, chamada de **tabela MAC**, que **mapeia** os endereços de hardware (**MAC** Address) dos dispositivos às **portas** (interfaces) às quais eles se encontram conectados. Assim, que um switch é ligado, essa tabela encontra-se vazia.

Quando um **dispositivo inicia uma transmissão** em uma porta do switch recebe um quadro, o switch armazena o endereço de hardware do dispositivo transmissor em sua tabela MAC, **registra**ndo **a interface à qual esse dispositivos está conectado.**

Em um primeiro momento, o switch não tem outra opção a não ser "inundar" a rede com esse quadro, uma vez que ele ainda não possui em usa tabela MAC o registro da localização do dispositivo destinatário. Esse tipo de transmissão é conhecida como **broadcast**.

Se um determinado dispositivo **responder** a essa mensagem de broadcast enviando um frame de volta, **o switch irá**, então, capturar o endereço de hardware (MAC) desse dispositivo e **registrá-lo em sua tabela MAC**, associando o endereço MAC desse dispositivo à interface (porta) que recebeu o quadro.

O switch tem agora dois endereços em sua tabela MAC, **podendo assim estabelecer uma conexão ponto-a-ponto** entre os dois dispositivos. Isso significa que os quadros pertencentes a essa transmissão serão encaminhados apenas aos dois dispositivos participantes. Nenhuma outra porta do switch irá receber os quadros, a não ser as duas portas mapeadas.

É essa a grande diferença entre switches e hubs. **Em uma rede composta por hubs, quadros são encaminhados a todas as portas, o tempo todo, criando um grande domínio de colisão.**

Se os dois dispositivos **não se comunicarem** com o switch novamente **por** um determinado **período** de **tempo**, o switch irá **deletar** os endereços de usa tabela MAC, mantendo-a assim a mais atualizada possível.

Tipos de Comutação

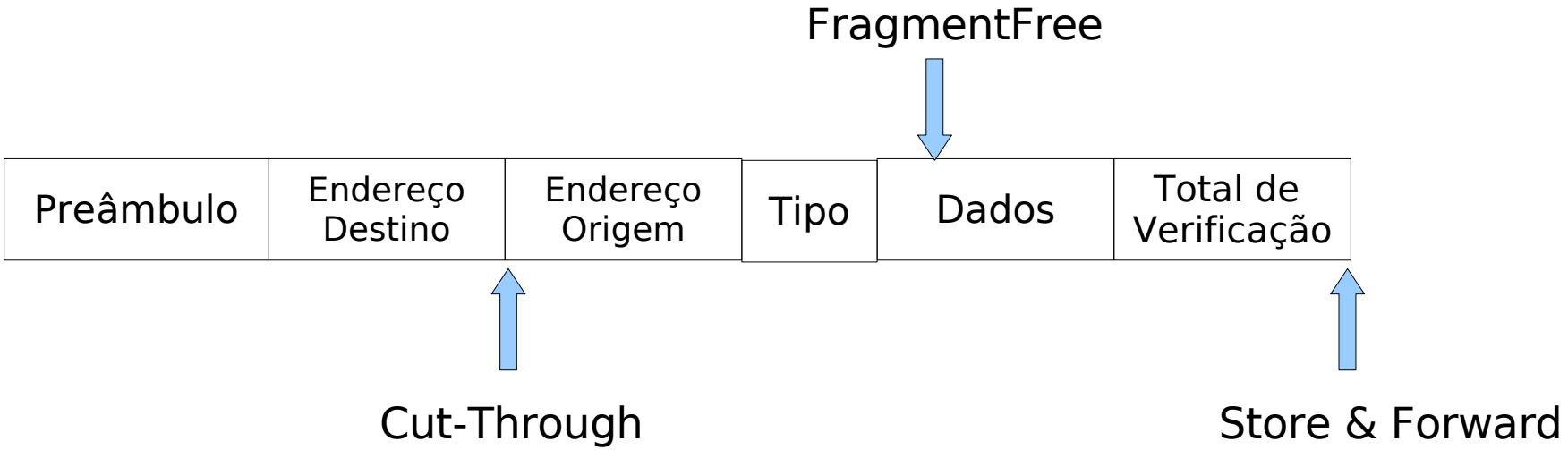
A **latência** envolvida **na comutação** de um quadro em um switch depende do modo de comutação (**switching mode**) configurado do switch.

Existem basicamante, **três tipos de comutação**:

- **Store and forward** – Neste modo como o nome diz “armazene e encaminhe”, esse modo de comutação faz com que o **quadro** seja, em um primeiro momento, **completamente recebido e armazenado** no buffer do switch. Em seguida, uma checagem de erros (CRC – Cyclic Redundant Check) é efetuada e, finalmente, o endereço de destino é localizado na tabela MAC. Este é o **método mais lento** entre os três apresentados aqui;

- **Cut-through** (tempo real): Esse é o **modo predominante** quando se fala em comutação **em LANs**. O Cut-through o switch **copia apenas o endereço de destino** (os primeiros 7 bytes seguindo o campo Preamble) para seu buffer. Logo após, o endereço do hardware de **destino é localizado** na tabela MAC, a interface de saída é determinada e **o quadro é encaminhado** ao seu destino. Esse modo provê **baixa latência**, pois o encaminhamento do quadro começa assim que o endereço de destino é identificado e a interface de saída determinada;

- **FragmentFree** (cut-through modificado): Esse modo é uma **modificação** do **cut-through**, pois **aguarda a passagem da janela de colisão** (collision window de **64 bytes**) antes de encaminhar o pacote. Seu funcionamento é assim, **pois se considera a alta probabilidade de que, se um quadro possui algum erro, este será identidicado nos 64 bytes iniciais**. Portanto, o modo FragmentFree promove uma checagem de erros mais confiável, acrescentando muito pouco à latência do processo.



Esquemas de inibição de loops em comutadores

O estabelecimento de conexões (links) **redundantes** é sempre uma boa idéia entre switches. Redundância, nesse caso, é usada para evitar a completa queda da rede no caso de falha de um link (cabo par trançado, por exemplo).

Embora a redundância em links possa ser extremamente útil, **tal redundância pode trazer mais problemas** do que resolvê-los. Uma vez que os **quadros** podem ser **propagados** através de **todos** os **links** redundantes simultaneamente, um fenômeno chamado **loop** pode ocorrer, além de outros problemas, como:

• Caso nenhum esquema de inibição de loops de rede seja implantado, os **switches** poderão **propagar quadros continuamente** na rede. Esse fenômeno é chamado de *broadcast storm* (tempestade de broadcast);

• Aumento das chances de um **dispositivo receber múltiplas cópias** de mesmo quadro, uma vez que esse quadro pode chegar de diferentes segmentos simultaneamente;

• A **tabela MAC ficará "confusa"** sobre a localização (interface) de um determinado dispositivo, uma vez que o switch pode **receber determinado quadro de mais de um link**. Pode ocorrer de o switch não encaminhar o quadro, uma vez que estará constantemente atualizando sua tabela MAC com a localização do hardware transmissor. Esse fenômeno é conhecido como *trashing* da tabela MAC;

• Um dos maiores problemas é a geração de **múltiplos loops**, ou seja, um loop dentro de outro. Se uma tempestade de broadcast então ocorrer, o switch ficará sem condições de desempenhar a comutação de pacotes, literalmente **"travando" a rede**.

Uma solução para o problema de loop é com o **Protocolo Spanning Tree (STP)**, criado pela DEC (Digital Equipment Corporation) e homologado posteriormente pela IEEE como **802.1d** e não é compatível com a versão original do protocolo criado com o DEC.

O papel principal do **STP é evitar que loops** ocorram em redes de camada de Enlace. O STP monitora constantemente a rede identificando todos os links em atividade e **certificando-se que loops de rede não ocorram**, **através da desativação de links redundantes**. O modo como o protocolo STP faz isso é "elegendo" um **switch-raiz** (*root bridge*) responsável pela definição de toda a topologia da rede.

Em uma rede, apenas um switch-raiz pode existir. Todas as interfaces ou portas do switch-raiz são denominadas "**portas designadas**" (*designated ports*) e **encontram-se** sempre no **modo de operação denominado "modo de encaminhamento"** (*forwarding-state*). Interfaces operando em modo de encaminhamento **podem tanto enviar quanto receber dados**.

Os **outros switches** presentes na rede são denominados **não-raiz** (*non-root bridges*). No caso desses switches, a porta com "menor custo" (determinada pela largura de banda do link em questão) ao switch-raiz é chamada de "porta-raiz" (*root-port*) e também se encontrará em modo de encaminhamento, podendo enviar e receber dados. As portas restantes com menor custo ao switch-raiz serão denominadas "**portas designadas**".

Se em uma rede **com diversos switches o custo de duas ou mais portas for o mesmo**, **o ID** (número de identificação) do switch **deverá ser usado** e será considerada **designada** a porta referente ao switch com o menor ID. O valor de ID padrão para todos os dispositivos rodando o STP do IEEE é 32.768. As portas restantes serão consideradas portas **não-designadas**. Estas se encontrarão em modo bloqueio (*blocking mode*), não podendo enviar ou receber dados.

Switches e bridges rodando **STP** trocam informações através do protocolo Bridge Protocol Data Units (**BPDU**). O BPDUs enviam mensagens de configuração via quadros em broadcast. O ID de cada switch é enviado aos outros dispositivos através das BPDUs.

Modos de operação das portas de um switch

Os modos de operação de switches e bridges rodando em STP podem variar entre quatro modos:

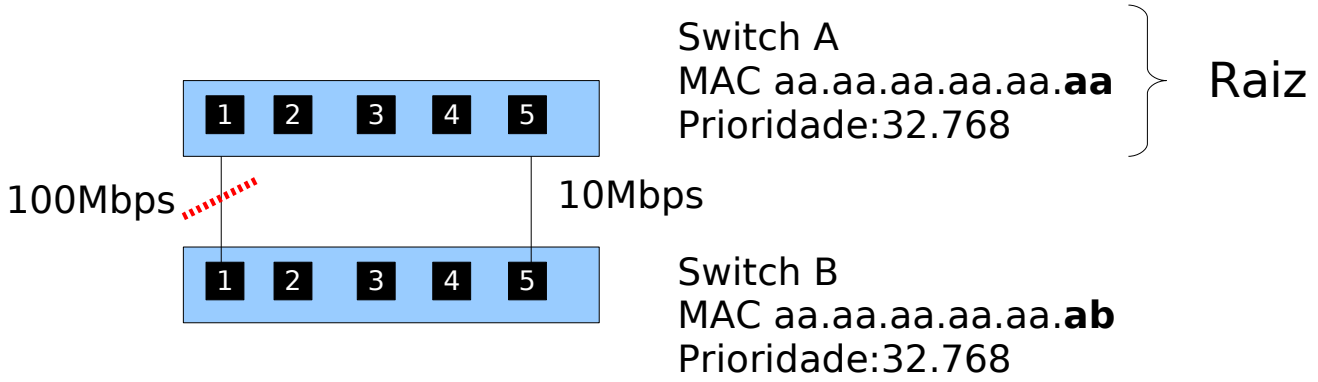
- **Bloking**: Não encaminhará quadros. Pode receber e analisar BPDUs. Todas as portas de um switch encontram-se em modo bloking quando ele é ligado;
- **Listening**: Recebe e analisa BPDUs para certificar-se de que não ocorrerão loops na rede antes de começar o encaminhamento de quadros;
- **Learning**: Registra os endereços dos hardwares conectados às interfaces e forma a tabela MAC. Não encaminha quadros, ainda;
- **Forwarding**: Envia e recebe quadros.

Tipicamente, **switches** se **encontram ou no modo blocking ou forwarding**. Uma porta no modo **forwarding** é tida como tendo o **menor custo ao switch-raiz**.

Entretanto, **se a topologia de rede se alterar** (devido a uma falha) todas as portas conectadas em redundância de um switch retornarão aos **modos listening e learning**.

O modo blocking é usado para impedir o acontecimento de loops de rede. Uma vez que o switch determina o melhor caminho ao switch-raiz, todas os portas entrarão em modo blocking. **Portas em modo blocking podem receber BPDUs**.

Se um switch por alum motivo determinar que uma porta em modo blocking deve tornar-se uma posta designada, ela entrará em modo listening, analisando todas as BPDUs recebidas para certificar-se de que não criará um loop uma vez que entre em modo forwarding.



Virtual LANs – VLANs

Em uma **rede comutada**, a rede **é plana** (flat), ou seja, **todos os pacotes broadcast transmitidos são "enxergados" por todos os dispositivos conectados à rede**, mesmo que um dispositivo não seja o destinatário de tais pacotes.

Uma vez que o processo de **comutação na camada de Enlace segrega domínios** de colisão, criando segmentos individuais para cada dispositivo conectado ao switch, as restrições relacionadas à distância impostas pelo padrão Ethernet são reduzidas, significando que redes geograficamente podem ser construídas.

Quanto maior o número de usuários e dispositivos, **maior o volume de broadcast** e pacotes que cada dispositivos tem de processar transitando na rede.

Outro problema inerente às redes comutadas é a **segurança**, uma vez que todos os usuários "enxergam" todos os dispositivos.

Perceba que apesar de o tamanho dos domínios de broadcast ser reduzido, seu número aumenta. Isso é lógico se você lembrar que antes do uso de VLANs tínhamos apenas um grande domínio de broadcast. Conforme VLANs vão sendo criadas, o número domínios broadcast aumenta, porém o tamanho de cada novo domínio é menor que o domínio original.

Com a criação de **VLANs**, é possível **resolver** uma boa parte dos **problemas** associados à comutação na camada de enlace. Eis algumas das razões para se criar LANs Virtuais:

- **Redução** do tamanho e aumento do número de **domínios de broadcast**;
- **Agrupamentos lógicos de usuários** e de recursos conectados em portas administrativamente definidas no switch;
- VLANs podem ser organizadas por localidade, função, departamento, etc, independentemente da localização física dos recursos;
- Melhor **gerenciabilidade** e aumento de **segurança** da rede local (LAN);
- **Flexibilidade** e **escalabilidade**.

Redução do tamanho dos domínios de Broadcast

Os roteadores, por definição, matêm as mensagens de broadcast dentro da rede que os originou. **Switches**, por outro lado, **propagam** mensagens de **broadcast** para todos os seus segmentos. Por esse motivo, chamamos uma rede comutada de “plana”, porque se trada de um grande domínio de broadcast.

Um **bom administrador** de redes deve certificar-se de que a rede esteja devidamente **segmentada** para evitar que problemas em um determinado segmento se propaguem para toda a rede.

A maneira mais eficaz de se **conseguir isso** é através da **combinação** entre **comutação** e **roteamento**. Uma vez que o custo dos switches vem caindo, é tendência real que as empresas substituam hubs por switches.

Em uma **VLAN**, todos os dispositivos são membros do mesmo domínio de broadcast. As **mensagens de broadcast**, por padrão, **são barradas** de todas as portas em um switch que não sejam membros da mesma VLAN.

Roteadores devem ser usados em conjunto com switches para que se estabelaça a comutação **entre VLANs**, o que impede que mensagens de broadcast sejam propagadas por toda a rede.

Gerenciabilidade e aumento de segurança em LANs através de switches

Um dos grandes problemas com redes planas é a segurança que é implementada através dos roteadores. A segurança é gerenciada e mantida pelo roteador, porém **qualquer um que se conecte localmente à rede tem acesso aos recursos disponíveis** naquela VLAN específica.

Outro problema é que qualquer um pode **conectar um analisador em um hub** e, assim, ter acesso a todo tráfego daquele segmento de rede.

Ainda outro problema é que **usuários podem se associar** a um determinado **grupo** de trabalho simplesmente **conectando** suas estações ou laptops a um **hub** existente, ocasionando um “caos” na rede.

Através da criação de VLANs, os administradores adquirem o controle sobre cada porta e cada usuário. O administrador controla cada porta e quais recursos serão alocados a ela. Se a comunicação inter-VLANs é necessária, restrições em um roteador podem ser implementadas. Restrições também podem ser impostas a endereços MAC, protocolos e a aplicações.

Switches possibilitam uma flexibilidade e escalabilidade mais que os roteadores. Através da utilização de switches é possível agrupar usuários por grupos de interesse, que são conhecidos como **VLANs organizacionais**, mas lembre-se mesmo com todo este recurso os **switchers não podem substituir os roteadores**, já que por exemplo, para a comunicação inter-VLAN é necessário obrigatoriamente o uso de roteadores.

Tipos de associações VLAN

VLANs são tipicamente criadas por um administrador de redes, que designa determinadas portas de um switch para uma determinada VLAN. As VLANs podem ser classificadas como:

- **Associação estática**: O modo mais comum e seguro de se criar uma VLAN é estaticamente. A porta do switch designada para manter a associação cm uma determinada VLAN fará isso até que um administrador mude a sua designação. Esse método de criação de VLANs é fácil de implementar e monitorar, funcionando bem em ambientes no qual o movimento de usuários dentro de uma determinada rede é controlado.

- **Associação dinâmica**: Estas determinam a designação de uma VLAN para um dispositivo automaticamente. Através do uso de softwares específicos de gerenciamento, é possível o mapeamento de endereços de hardware (MAC), protocolos e até mesmo aplicações ou logins de usuários para VLANs específicas, assim se por exemplo, o usuário de um laptop usar uma porta A ou B o seu endereço MAC sempre estará associado a uma mesma VLAN. Embora este método simplifique muito a vida do administrador uma vez que o banco de dados MAC x VLAN esteja formado, um esforço considerável é exigido inicialmente, na criação do mesmo.

Identificação de VLANs

VLANs podem ser espalhar por uma “malha” de switches interconectados. Os **switches** desse emaranhado **devem** ser capazes de **identificar os quadros** e as respectivas **VLANs** às quais estes pertencem.

Para isto foi criado o recurso **frame tagging** (etiquetamento de quadro), assim os switches podem direcionar os quadros para as portas apropriadas.

Para implementar esta técnica **existem dois tipos de links (portas)** em um ambiente comutado (portas em switch):

- **Links de acesso – access links**: Que são apenas parte de uma VLAN e são tidos como a VLAN nativa. **Qualquer dispositivo conectado a uma porta ou link de acesso não sabe a qual VLAN pertence**. O dispositivo apenas assumirá que é parte de um domínio de broadcast, sem entender a real topologia da rede. Os switches removem qualquer informação referentes às VLANs dos quadros antes de enviálos a um link de acesso. Dispositivos conectados a links de acesso não podem se comunicar com dispositivos fora de sua própria VLAN, a não ser que um roteador faça o roteamento dos pacotes;

- Links de transportes – trunk links: Também denominados uplinks, **podem carregar informações sobre múltiplas VLANs**, sendo usados para conectar switches a outros switches, routeadores ou mesmo a servidores. Links de Transporte são suportados em Fast ou Gigabit Ethernet, mas não pode ser suportado em redes 10BaseT Ethernet. Links de transporte são utilizados para transportar VLANs entre dispositivos e podem ser configurados para transportar todas as VLANs ou somente algumas. Links de Transporte ainda possuem uma VLAN nativa (default – VLAN1), que é utilizada para gerenciamento em caso de falhas.

O **processo de "entroncamento"** de links **permite colocar uma única porta como parte de múltiplas VLANs**, isto é bastante comum na conexão quando se que conectar um servidor que prove serviço a várias VLANs sem usar um roteador. Também é comum o uso de entroncamentos na conexão entre switches (uplink), já que os links de transporte podem transportar informações sobre algumas ou todas as VLANs existentes através de um único link (porta) física.

Ao se criar uma porta de transporte, informações sobre todas as VLANs são transportadas através dela, por padrão. VLANs indesejadas devem ser manualmente excluídas do link para que suas informações não sejam propagadas através dele.

Frame tagging

Um switch conectado a uma rede de grande porte necessita fazer um acompanhamento dos usuários e quadros que atravessam o aglomerado de switches e VLANs. O processo de identificação de quadros associa, de forma única, uma **identificação a cada quadro**. Essa identificação é conhecida como **VLAN ID** ou **VLAN color**.

Métodos de identificação de VLANs

Existem alguns métodos de identificação de VLANs, dois métodos muito usados são: o ISL e o 802.1q.

ISL (Inter-Switch Link)

Exclusivo aos switches Cisco, o **encapsulamento** ISL pode ser utilizado às interfaces de switches, de roteadores e de servidores, para seu entroncamento. O servidor truncado é membro de todas as VLANs simultaneamente, o que significa que os usuários não precisam atravessar um dispositivo de camada 3 para ter acesso a ele, reduzindo a complexidade e aumentando a performance da rede.

O método **ISL literalmente escapsula quadros Ethernet com informações sobre VLANs**. Essa informação, adicionada ao encapsulamento do quadro, permite a multiplexação de VLANs por meio de apenas um link de transporte.

O ISL é um método externo de identificação, ou seja, **o quadro original não é alterado**, sendo apenas encapsulado por um cabeçalho ISL. Uma vez que o quadro é encapsulado, apenas dispositivos (ou interfaces) compatíveis com ISL estarão habilitados e decodificá-dos. Assim dispositivos não ISL que recebam um quadro ISL iram achar que o quadro está corrompido.

É importante entender que o encapsulamento ISL apenas ocorre se o quadro for encaminhado a uma porta de transporte (trunk link) e o encapsulamento é removido caso o quadro seja encaminhado a uma porta de acesso.

Para para **gerenciar** e manter a consistência de todas as **VLANs** configuradas em uma rede pode ser usado o **protocolo VTP** (Virtual Trunk Protocol), sendo necessário também a criação de um servidor VTP, assim todos os servidores que necessitem compartilhar informações sobre VLANs devem utilizar a mesma identificação de domínio.

IEEE 802.1q

Criado pelo IEEE para ser um método padrão para identificação de quadros, esse é o método padrão para identificação de quadros, esse método insere um campo específico dentro do quadro, responsável pela identificação da VLAN.

O padrão de **quadro Ethernet não possui campos sobressalentes**, então o que fazer para identificar as VLANs, lembrando que alterar o quadro implica em vários problemas com os placas de redes compatíveis com o padrão Ethernet.

O comitê 802 do IEEE enfrentou esse problema em 1995 e depois de muita discussão, o IEEE fez o impensável e mudou o cabeçalho do padrão Ethernet. O **novo formato foi publicado no padrão 802.1q**, emitido em 1998. O novo formato contém uma tag de VLAN, é claro que com esta solução não temos que jogar as placas de redes Ethernet padrão fora!

A chave para a solução é perceber que os campos VLAN só são realmente usados pelas pontes e switches, e não pelas máquinas dos usuários, então apenas as pontes e switches devem reconhecer o 802.1q.

Assim, como a origem não gera os campos VLAN, quem o fará? A resposta é que o primeiro switch capaz de reconhecer a VLAN que tocar um quadro incluirá esses campos, e o último dispositivo do percurso os removerá.

Porém, como saber à qual VLAN pertence cada quadro? Bem, o primeiro switch poderia atribuir um número de VLAN a uma porta, examinar o MAC, etc.

Esperá-se que em um futuramente as novas placas tal como Gigabit Ethernet suportem o 802.1q.

Ao quadro 802.1q foi adicionado o **campo tag** que possui um campo **identificador de VLAN**, que indica a que campo o quadro pertence.

Um campo de 3 bits de **Prioridade**, que não tem nenhuma relação com a VLAN, mas como a alteração do formato do quadro não acontece sempre foram adicionados campos extras, tal campo pode ser **usado para informar a prioridade do quadro**, usado por exemplo para dizer que um quadro é de voz, ou outra informação em tempo real que deve ter um certo nível de prioridade de entrega.

O último bit é o **CFI** (Canonical Format Indicator – indicador de formato canônico) que foi originalmente criado para indicar endereços MAC little-endian versus endereços MAC big-endian, mas esse uso se perdeu em outras controvérsias e também não tem relação com VLANs.

fim