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

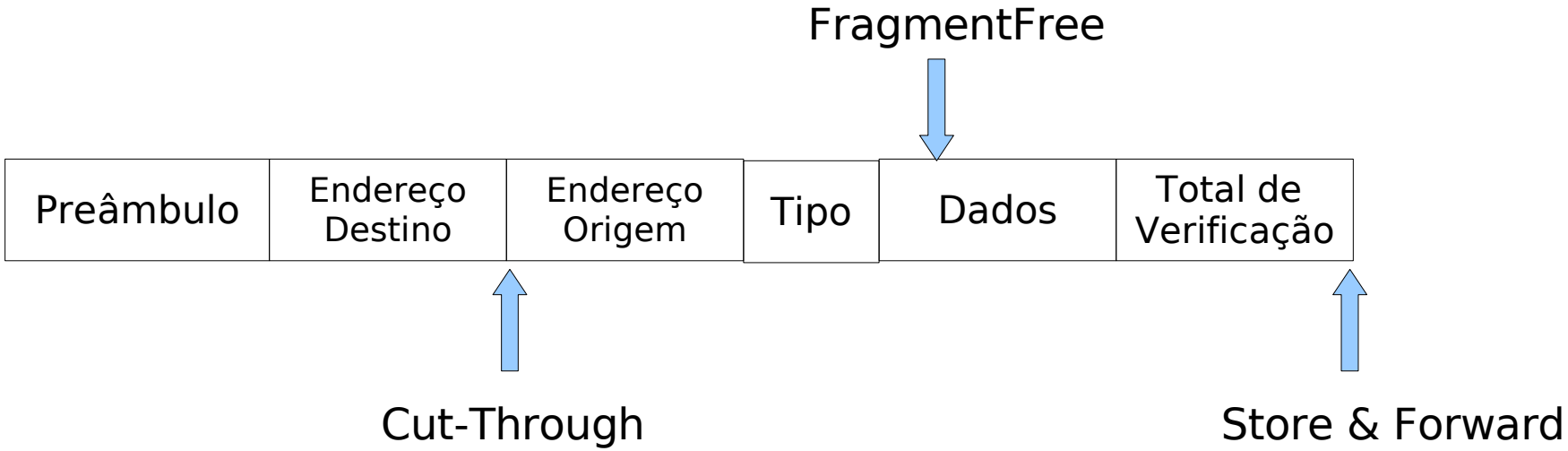
A **latência** envolvida **na comutação** de um quadro em um switch depende do modo de comutação (**switching mode**) configurado do switch.

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:

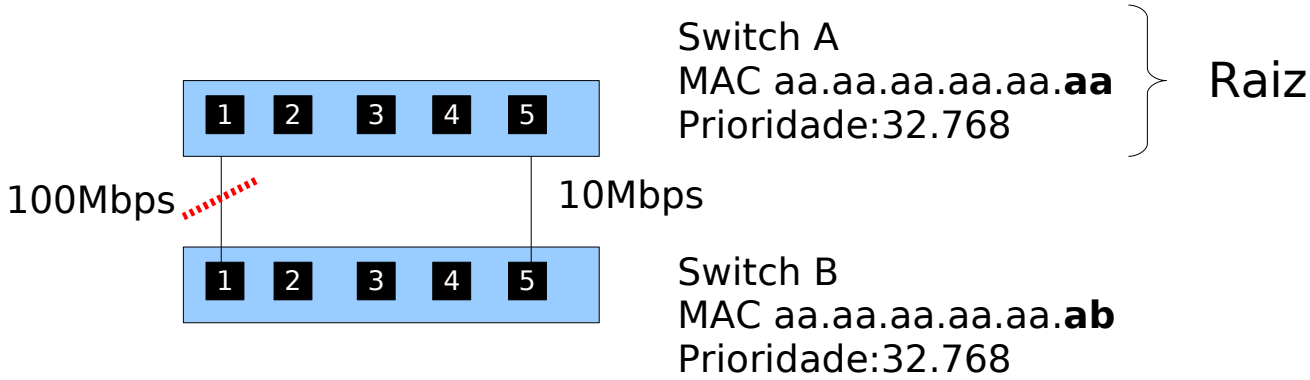
- **Bloking**: Não encaminhará quadros. Pode receber e analisar BPDUs. Todas as portas de um switch encontram-se em modo bloking quando ele é ligado;
- **Listening**: Recebe e analisa BPDUs para certificar-se de que não ocorrerão loops na rede antes de começar o encaminhamento de quadros;
- **Learning**: 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