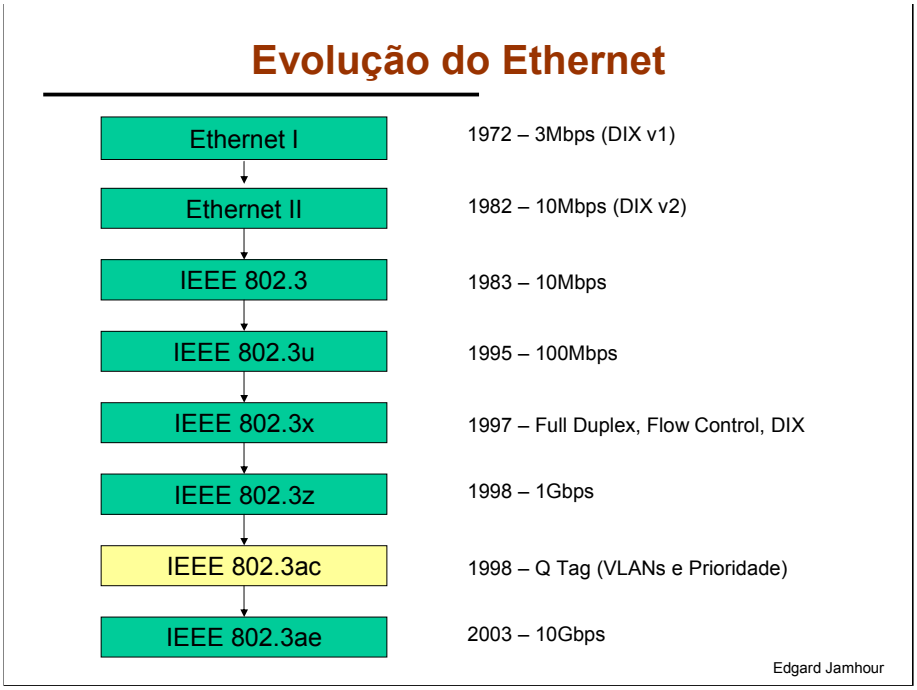
VLANs Ethernet

Edgard Jamhour

O objetivo deste módulo é apresentar o conceito de VLANs (Redes LANs Virtuais) e sua aplicação tanto com o objetivo de melhorar o desempenho quanto a segurança de uma rede IP.

A fim de facilitar a compreensão de como o Ethernet foi expandido para suportar VLANs, esse módulo começa com uma revisão sobre a padronização e o formato dos quadros Ethernet.

Nesse módulo será visto também o conceito de Spanning Trees, como fazer balanceamento de carga com VLANs e Spanning Trees e aspectos do endereçamento IP na presença de VLANs.



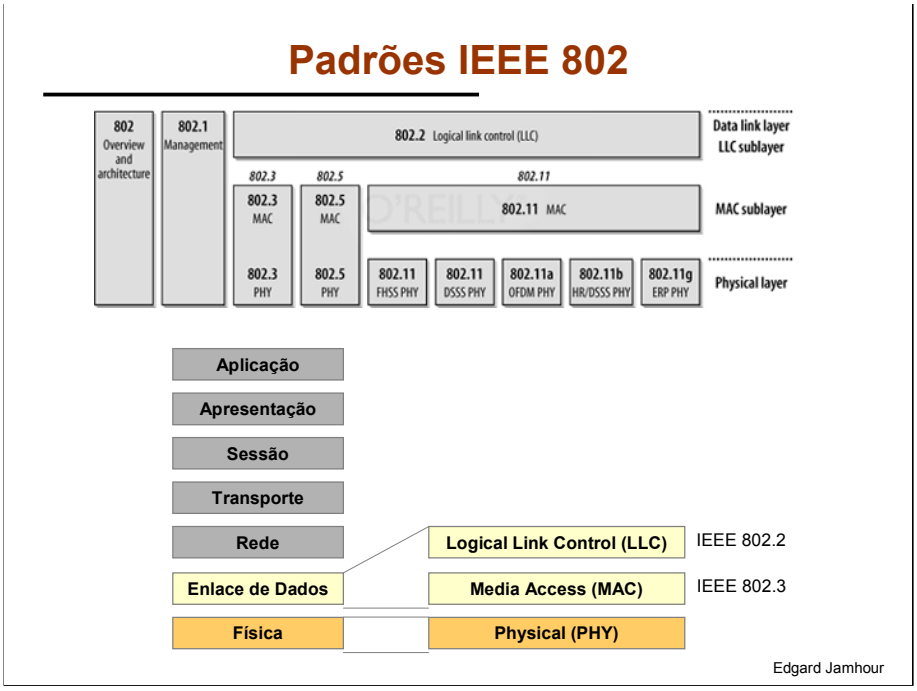
Inicialmente desenvolvida como uma alternativa de baixo custo para implementação de pequenas redes de computadores no início dos anos 70, a tecnologia Ethernet evolui muito em seus quase 40 anos de existência. O projeto inicial do Ethernet foi desenvolvido por Robert Metcalfe, então funcionário da Xerox, durante o período de 1970 a 1976.

A primeira versão proposta ficou conhecida como Ethernet I, e funcionava numa velocidade de aproximadamente de 3 Mbps. Apesar de ainda incipiente, esta versão do Ethernet já utilizava o método CSMA/CD (Carrier Sense Multiple Access with Collision Detection) como método de controle de acesso ao meio.

Em 1980, as empresas Xerox, Digital e Intel se uniram a fim de elaborar um padrão de fato para o Ethernet, com o objetivo de comercializá-lo. O padrão resultante ficou conhecido como Ethernet II, e utiliza um formato de quadro denominado DIX (em homenagem as empresas criadoras do Ethernet). O formato DIX é utilizado até hoje. Como curiosidade, nesse período, o Robert Metcalfe saiu da Xerox, e fundou a 3Com, que se tornaria um grade fornecedor de adaptadores de rede Ethernet.

Em 1985, o Ethernet foi padronizado pela ANSI/IEEE, sob a denominação IEEE 802.3. Essa padronização definiu um novo formato de quadro denominado IEEE 802.3 LLC. Existem algumas diferenças entre o formato IEEE e o formato DIX, mas os formatos são compatíveis, de forma que hoje, ambos os formatos são encontrados em redes Ethernet. De fato, uma revisão na especificação do Ethernet em 1997, denominada IEEE 802.3x, passou a aceitar o formato DIX também dentro do padrão IEEE.

Em 1998 uma especificação IEEE introduziu um novo campo para os quadros DIX e LLC. Esse novo campo, conhecido como Q Tag, permitiu utilizar os conceitos de VLANs (Redes Locais Virtuais) e prioridade com a tecnologia Ethernet.



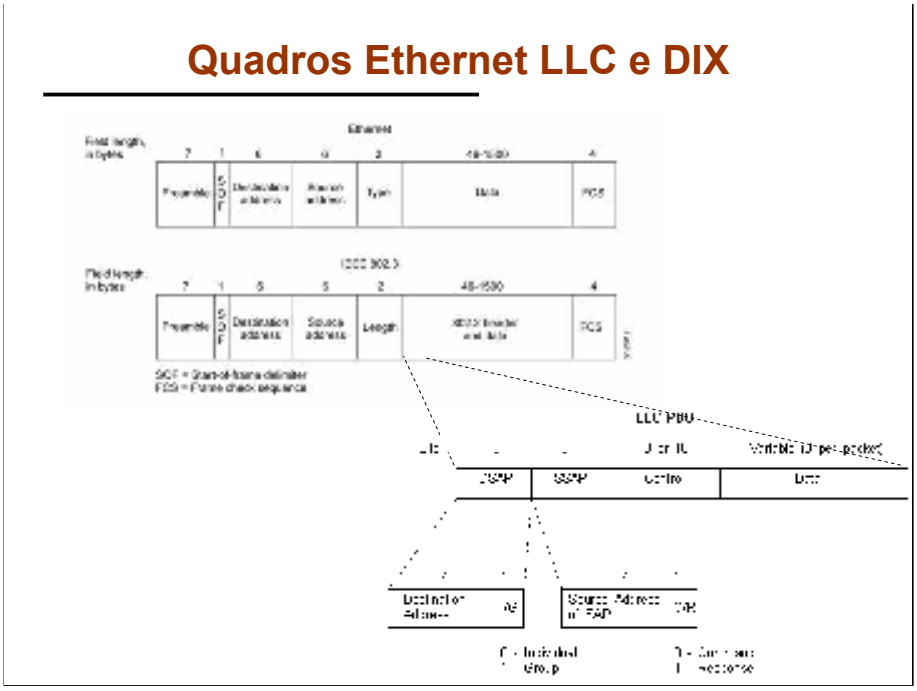
O padrão IEEE 802.3 que define o Ethernet faz parte a uma família de padrões mais ampla denominado IEEE 802.

A família IEEE 802 inclui tecnologias já bem antigas como o Ethernet (IEEE 802.3) e o Token-Ring (IEEE 802.5). Ela inclui também várias tecnologias recentes (principalmente as tecnologias sem fio), como WiFi (IEEE 802.11), o WiMax (IEEE 802.16) e as tecnologias para PAN (Personal Area Network), como o IEEE 802.15 (BlueTooth e ZigBee).

As tecnologias IEEE 802 correspondem as camadas de Enlace (2) e Física (1) do modelo OSI. Por exemplo, no caso do Ethernet, a camada física define padrões para tipos de cabo (por exemplo, par trançado ou fibra), velocidades de operação e a representação física (ótica ou elétrica) do sinal a ser transmitido.

O IEEE 802.2 define também uma subdivisão da camada de enlace em duas subcamadas: LLC: Logical Link Control e MAC: Medium Access Control. Observe pela figura que a sub-camada LLC é comum para as várias tecnologias de transmissão e a subcamada MAC é específica para cada tecnologia. A sub-camada LLC para todas as tecnologias é definida por um padrão único denominado IEEE 802.2.

A subcamada LLC não existe no Etherenet II. Na verdade, a existência dessa sub-camada é a única diferença entre o Ethernet II e o IEEE 802.3.



A figura ilustra o formato genérico dos quadros Ethernet, que serve tanto para o formato DIX quanto para o formato LLC. A diferença entre os dois formatos está apenas no campo Length/Type. O formato DIX utiliza o campo Type que identifica o conteúdo transportado pelo quadro. O formato LLC utiliza o campo Length que indica o tamanho do quadro.

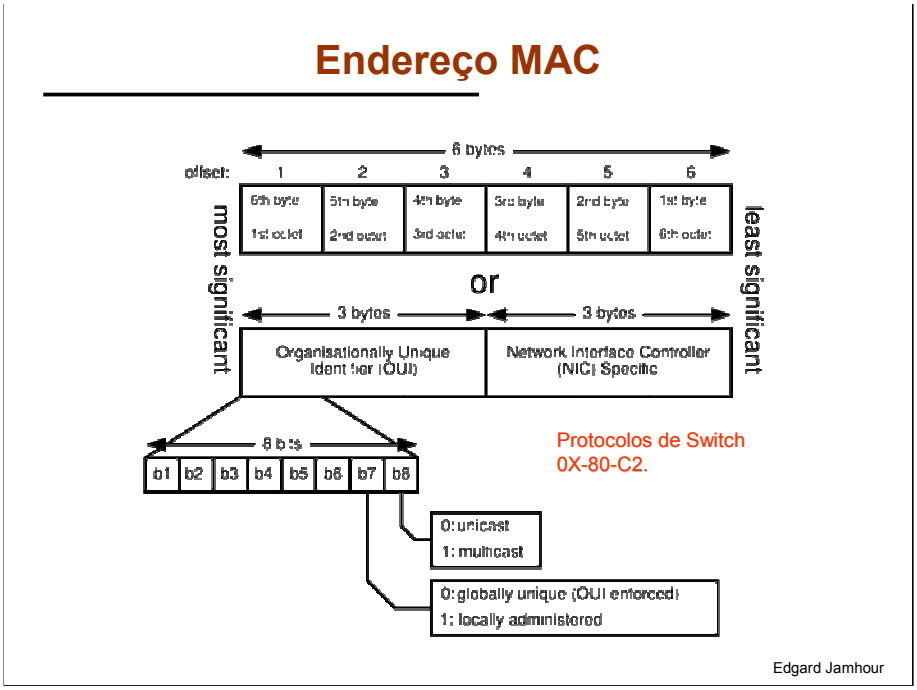
A sub-camada LLC possui um cabeçalho de 3 ou 4 bytes localizado no início do campo de dados do quadro Ethernet. A utilização dos endereços SAP (Service Access Point) permite endereçar múltiplos serviços sobre um único endereço MAC, de forma similar ao que as portas TCP/UDP fazem para o IP. O LLC é comum em protocolos de rede de baixo nível usados pelos Switches, como o BPDU (visto na seqüência deste módulo).

Os quadros Ethernet definem um tamanho mínimo e um tamanho máximo para o campo de dados. O tamanho mínimo é definido de forma a garantir que uma estação transmissora tenha tempo de detectar uma colisão antes do final da transmissão de um quadro. O tamanho máximo que pode ser transportado por um quadro em uma dada tecnologia de enlace é denominado “máxima unidade transportável (MTU). No caso do Ethernet, o MTU é de 1500 bytes. A camada superior ao Ethernet (no caso, o IP) precisa garantir que nenhum pacote acima de 1500 bytes seja enviado para camada Ethernet. Isso é conseguido através de um processo denominado fragmentação IP.

Para permitir que uma interface de rede interprete corretamente os dois tipos de quadro Ethernet é adotada a seguinte convenção para o campo Length/Type:
Valores até 1500: O quadro é do tipo LLC, e o significado do campo é Tamanho (Length)
Valores acima de 1500: O quadro é do tipo DIX, e o significado do campo é Tipo (Type)

Note que os tipos de protocolo transportados pelo Ethernet são sempre números de tamanho superior a 1500. Por exemplo: IP = 2048 (0x800), ARP=2053(0x806)

O campo PRE não costuma aparecer nas representações em alto nível dos quadros Ethernet. Ele corresponde a informações de preâmbulo utilizados para sincronização e delimitação dos quadros.



O padrão IEEE 802 define 2 tipos de endereços MAC: Administrados Localmente (Locais) e Universais. Os endereços locais são definidos livremente pelo administrador da rede, mas eles devem seguir a convenção de que o valor do segundo bit mais significativo do endereço (indicado como b7 na figura) deve ser igual a 1. Os endereços universais são globalmente únicos, pois identificadores OUI (Identificadores Únicos de Organizações) são alocados pelo IEEE para os fabricantes de dispositivos de rede. Por exemplo, a Xerox recebeu os OUIs de 00-00-00 até 00-00-09.

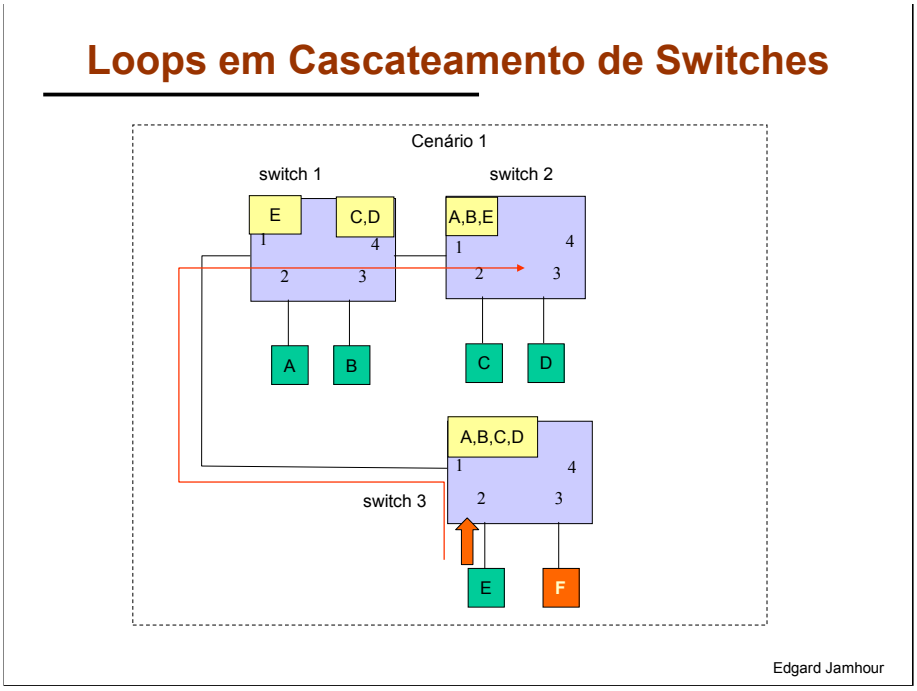
Os endereços MAC podem ser ainda individuais ou em grupo (controlado pelo bit 8 na figura). Os endereços de grupo permitem enviar um único quadro para múltiplos destinos simultaneamente, e podem ser do tipo broadcast ou multicast.

Nem todos os endereços universais podem ser usados para identificar adaptadores de rede. Um OUI foi alocado para uso exclusivo de protocolos padronizados para switches, como o “Spanning Tree”, e não pode ser usada por nenhum fabricante.

O OUI reservado para protocolos de switch é 0X-80-C2. Esse OUI inclui endereços do tipo unicast (quando X=0) e grupo (quando X=1).

Em alguns casos, o quadro recebido por um switch no formato multicast deve ser interpretado apenas localmente, e não deve ser repassado para os demais switches da rede. Em outros casos, o quadro precisa ser repassado. Esse controle é feito pela divisão do bloco de endereços de protocolos padronizados em 2 sub-grupos denominados: filtrado (não propaga multicast) e padrão (propaga multicast).

Faixa do modo filtrado: de 01-80-C2-00-00-00 até 01-80-C2-00-00-0F
Faixa do modo padrão: de 01-80-C2-00-00-10 até 01-80-C2-FF-FF-FF



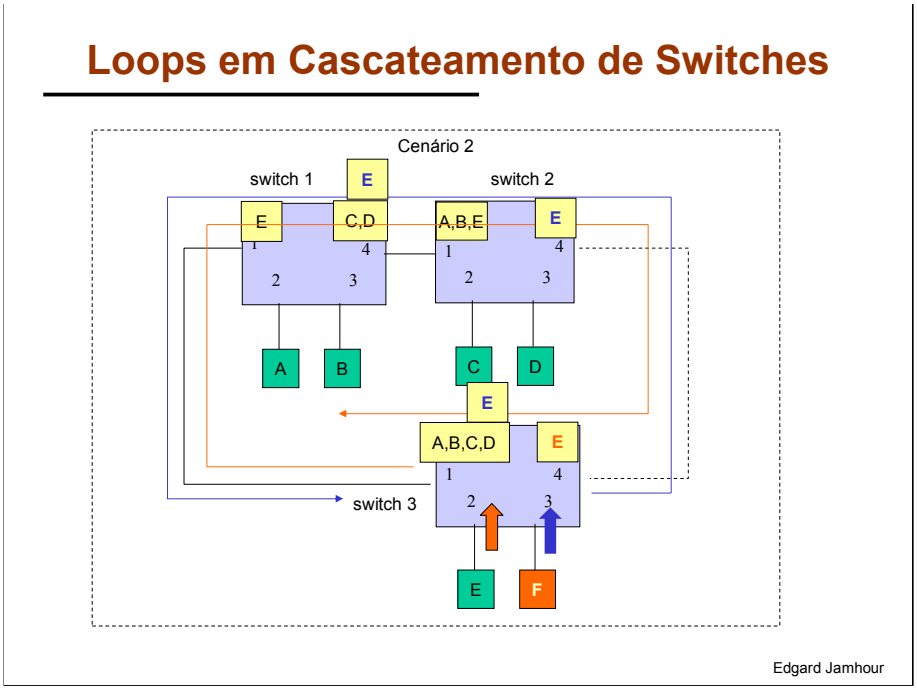
Quando switches são conectados em cascata, um cuidado especial deve ser tomado para que não sejam criados laços fechados (loops) entre os switches. Para entender porque loops são problemáticos para switches, vamos primeiramente relembrar seu funcionamento.

Os switches criam tabelas de encaminhamento escutando os endereços MAC de origem dos quadros enviados para suas portas. Quando o switch precisa entregar um quadro para um endereço MAC que ele ainda não conhece, ele encaminha o quadro para todas as suas portas.

Por exemplo, considere inicialmente o cenário 1 da figura, que não possui loop. Após um certo período, o switch entra num estado estável, onde a posição de todos os endereços MAC é conhecida. Suponha que o computador E no switch 3 deseja enviar um pacote para um computador novo da rede, digamos o computador F na figura.

Como o computador F ainda é desconhecido, o switch 3 vai enviar o quadro para todas as suas portas, incluindo a porta de cascateamento com switch 1. Como o switch 1 também não conhece F, ele envia o quadro para todas as suas portas, incluindo a porta de cascateamento com o switch 2. A mensagem é recebida por todos os computadores nos três switches, mas só o computador F que possui o endereço MAC solicitado irá interpretar a mensagem.

OBS. Em redes IP, o caso em que um computador envia um quadro endereçado para um endereço MAC desconhecido raramente acontece. Por exemplo, o computador E, antes de enviar um quadro para F, enviaria uma mensagem ARP Request em broadcast, informando o endereço IP e solicitando o endereço MAC de F. Na prática, o percurso dessa mensagem em broadcast seria o mesmo de um quadro com MAC desconhecido.



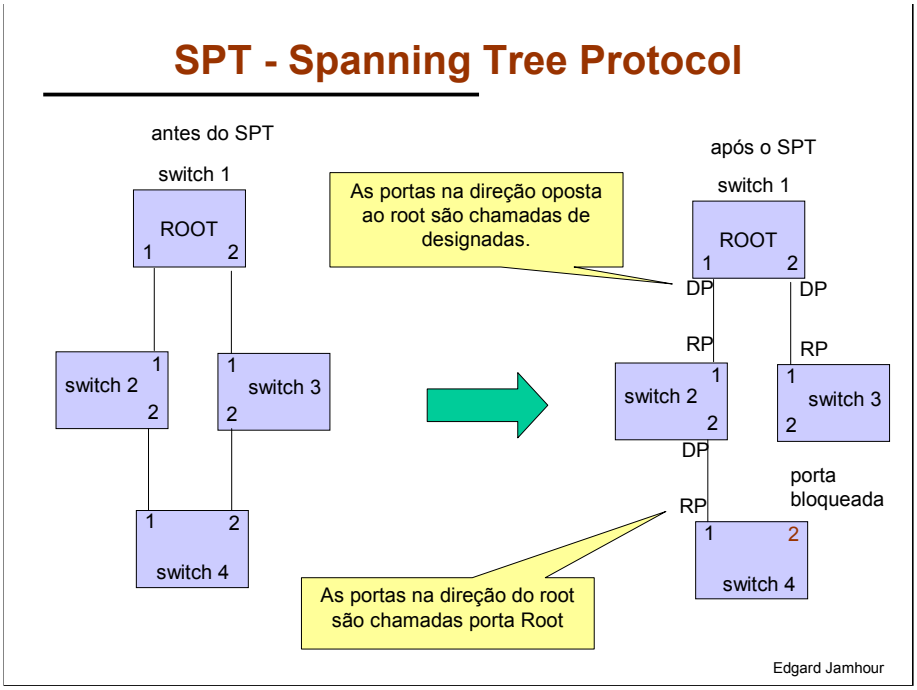
Considere agora o cenário 2, onde um loop foi criado, inserindo-se uma nova conexão entre os switches 2 e 3.

Vamos considerar novamente o caso em que o computador E envia um quadro para o computador F, ainda desconhecido na rede. Para ilustrar o efeito do loop, vamos seguir inicialmente o quadro enviado pela porta 1 do switch 3. Ao receber o quadro, o switch 1 vai considerar que o computador E é acessível pela porta 1. Como ele não conhece a localização de F, ele vai encaminhar o quadro para todas as suas portas.

O quadro enviado para o switch 2 vai fazer com que ele considere que o computador E está acessível pela sua porta 1. Novamente, como o switch 2 não conhece a localização de F, ele vai encaminhar o quadro para todas as suas portas, fazendo que o quadro retorne ao switch 3, mas agora, pela porta 3.

O mesmo processo acontece também com o caminho inverso, isto é, para o quadro encaminhado para porta 4 do switch 3. Observe que o laço faz com que a posição do computador E esteja presente em várias portas do switch, levando a loops no caso de algum computador transmitir para E.

Como os quadros circulam eternamente pelo laço fechado, o processo leva rapidamente a saturação completa da capacidade de todas as portas do switch, levando a um congestionamento completo da rede.



Os switches utilizam um protocolo para detectar e eliminar automaticamente laços fechados (loops). Esse protocolo é denominado “Spanning Tree Protocol - SPT”.

O STP é um protocolo de camada 2, e ele deve ser executado em todos os switches da rede. O princípio do SPT é que somente um caminho ativo pode existir entre 2 estações na rede. Caso mais de um caminho seja descoberto, determinadas portas do switch são bloqueadas por software a fim de eliminar o loop.

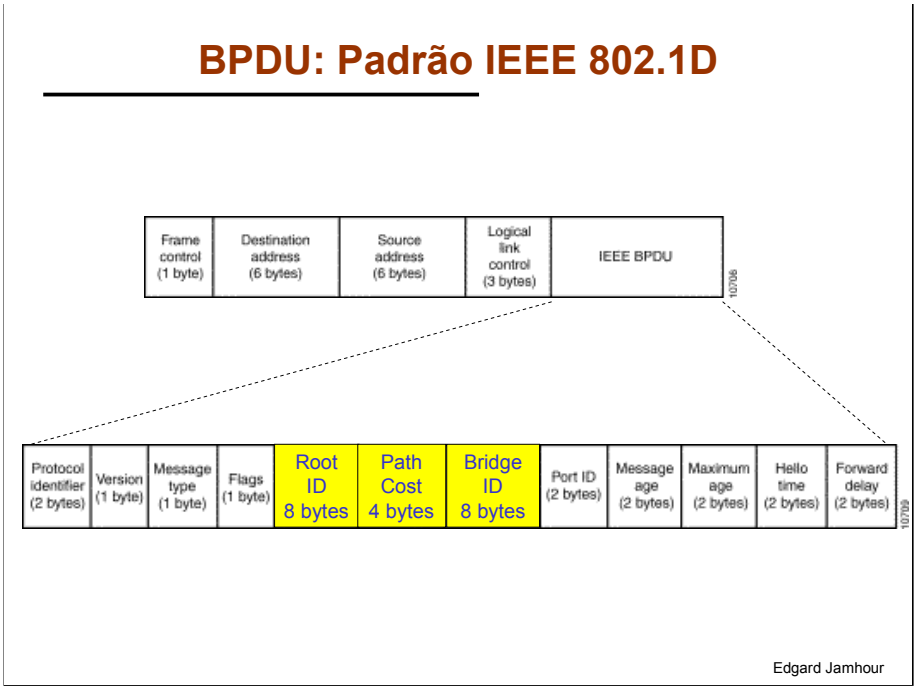
Quando o SPT é utilizado numa rede com switches, a topologia resultante é sempre uma árvore, que por definição não possui loops, o que justifica o nome do protocolo.

A estratégia consiste em eleger um dos switches da rede como Root, e construir a árvore determinando o menor caminho entre cada um dos demais switches e o Root.

As mensagens geradas pelo STP são denominadas “Bridge Protocol Data Unit - BPDU”. Essas mensagens utilizam endereços MAC em multicast na faixa de 0x0180C20000000 até 0x0180C20000010. Observe que a faixa de endereços MAC utilizada pelo STP corresponde ao OUI reservado para operação de switches em modo filtrado.

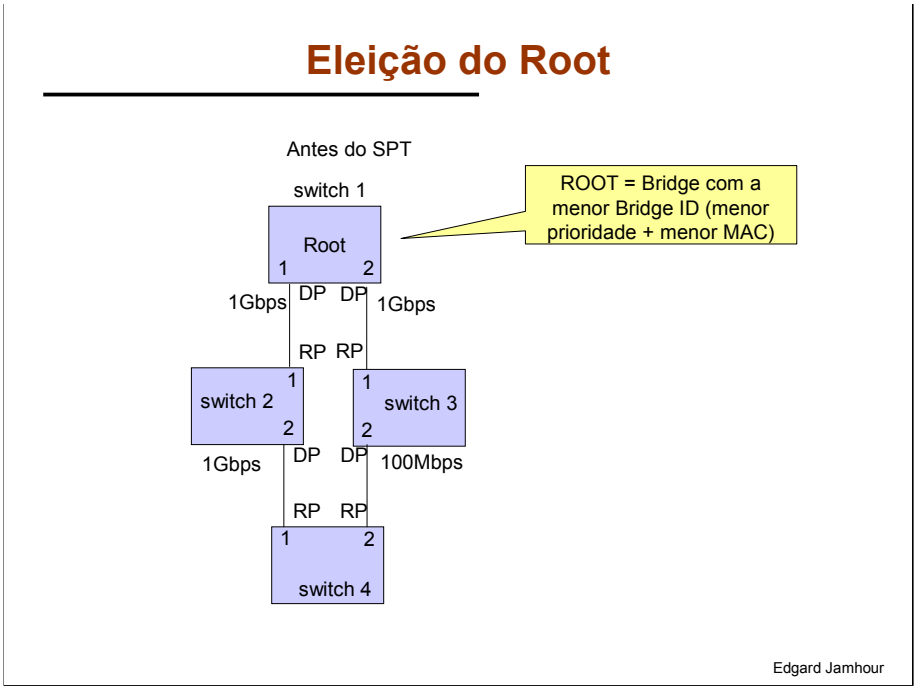
STP funciona continuamente, de maneira a refletir mudanças de topologia na rede. Se SPT estiver ativo, os pacotes multicast recebidos com esses endereços são interpretados localmente pelos switches, mas não serão encaminhados.

Se SPT estiver inativo, os quadros BPDU são encaminhados para outros switches, como se fossem endereços de multicast desconhecidos.



Numa rede STP, todos os switches possuem um identificador (ID) formado por 8 bytes, sendo 2 bytes de prioridade (configurável) e 6 bytes de um endereço MAC universal (atribuído pelo fabricante). No switch, esse identificador é denominado **Bridge ID**. Além do seu próprio ID, cada switch precisa conhecer o ID do switch root da rede. Isso é feito através de um processo de eleição, descrito na seqüência dessa unidade.

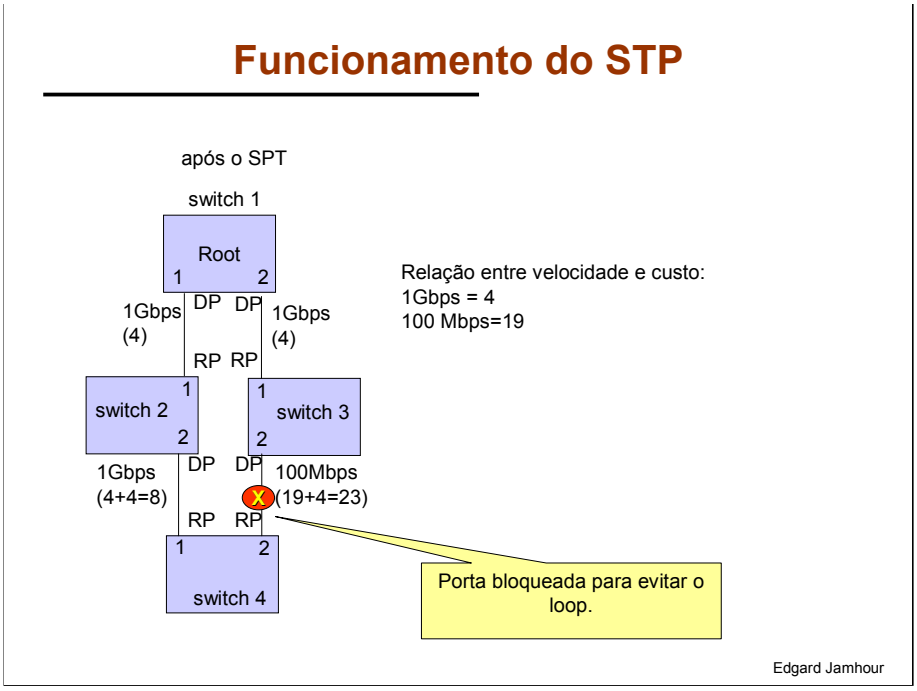
Todas a mensagens BPDU enviadas por um switch informam o seu próprio ID (campo Bridge ID), o ID do root da rede (campo **Root ID**) e o custo do melhor caminho que ele conhece para enviar um quadro até o root (campo **Root Path Cost**). Esses três campos são os mais importantes para compreender o funcionamento do STP. O formato desses campos e dos demais campos da mensagem BPDU estão descritos resumidamente a seguir.
Protocol Identifier: 0 (SPT)
Version: 0 (ST)
Message Type: 0 (Configuration)
Flags: Topology change (TC), Topology change acknowledgment (TCA)
Root ID: 2-Byte Prioridade + 6-Byte MAC da Bridge
Root Path Cost: 4-Bytes custo da Bridge até o root.
Bridge ID: 2-Byte Prioridade + 6-Byte MAC da Bridge
Port ID: 2 Bytes (usado para escolher a porta a ser bloqueada em caso de loop)
Message Age: Tempo decorrido desde que a mensagem repassada foi enviada pelo Root
Maximum Age: Idade a partir do qual a mensagem deve ser ignorada
Hello Time: Intervalo entre mensagens da root bridge
Forward Delay: Tempo que a bridge deve esperar antes de mudar de estado em caso de mudança de topologia.



O primeiro acontecimento importante numa rede com STP é a eleição do Root (raiz). Inicialmente, todos os switches se consideram Root. Eles então enviam, por todas as suas portas, mensagens BPDU com os campos Root ID e Bridge ID idênticos e um custo (campo Root Path Cost) proporcional a velocidade de sua porta.

Quando um switch recebe uma mensagem com um Root ID inferior ao seu, ele aceita o novo switch como Root. Caso o Root ID seja superior ao seu, ele simplesmente ignora. Conforme vimos, o ID do switch é composto por dois números: prioridade + endereço MAC. Por default, a prioridade de todos os switches é 32768 e a eleição do Root é feita pelo MAC.

Como o MAC é determinado pelo fabricante, pode acontecer que a escolha feita automaticamente para o Root não seja a mais apropriada para a rede (por exemplo, um switch periférico ou de baixa capacidade pode acabar sendo eleito como Root). Para evitar que isso aconteça, o administrador deve reduzir a prioridade do switch que ele deseja que seja o Root.



A construção da árvore de switches é feita a partir de mensagens BPDU enviadas pelo switch Root. Por exemplo, na figura, o switch 1 (Root) envia uma mensagem BPDU para os switches 2 e 3, informando que ele é o Root e que custo para chegar até ele é 4. O valor do custo é uma função da velocidade da porta do switch, e pode ser configurado pelo administrador. Por exemplo, a Cisco define o valor padrão de 4 para as portas de Gigabit-Ethernet (1Gbps) e 19 para as portas de Fast-Ethernet (100 Mbps).

O switch 2, propaga a mensagem recebida pelo Root para o switch 4, indicando seu próprio ID no campo Bridge-ID e aumentando o custo do caminho até a raiz para 8, devido ao custo de sua própria interface. O switch 3 faz o mesmo, só que o custo indicado para o caminho até a raiz é 23, pois a velocidade de sua conexão com o switch 4 é de apenas 100Mbps.

Dessa forma, o switch 4 recebe duas ofertas de conexão até o root. De acordo com o STP apenas uma pode ser aceita. Então o switch 4 aceita a oferta de menor custo, e bloqueia a porta que faz conexão com o switch 3, evitando assim a ocorrência do loop.

Configuração Default

Feature	Default Setting
Enable state	Enabled on VLAN 1. For more information, see the "Supported Spanning-Tree Instances" section on page 18-10.
Spanning-tree mode	PVST+. (Rapid PVST+ and MSTP are disabled.)
Switch priority	32768.
Spanning-tree port priority (configurable on a per-interface basis)	128.
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128.
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Spanning-tree timers	Hello time: 2 seconds. Forward-delay time: 15 seconds. Maximum-aging time: 20 seconds. Transmit hold count: 6 BPDUs

Edgard Jamhour

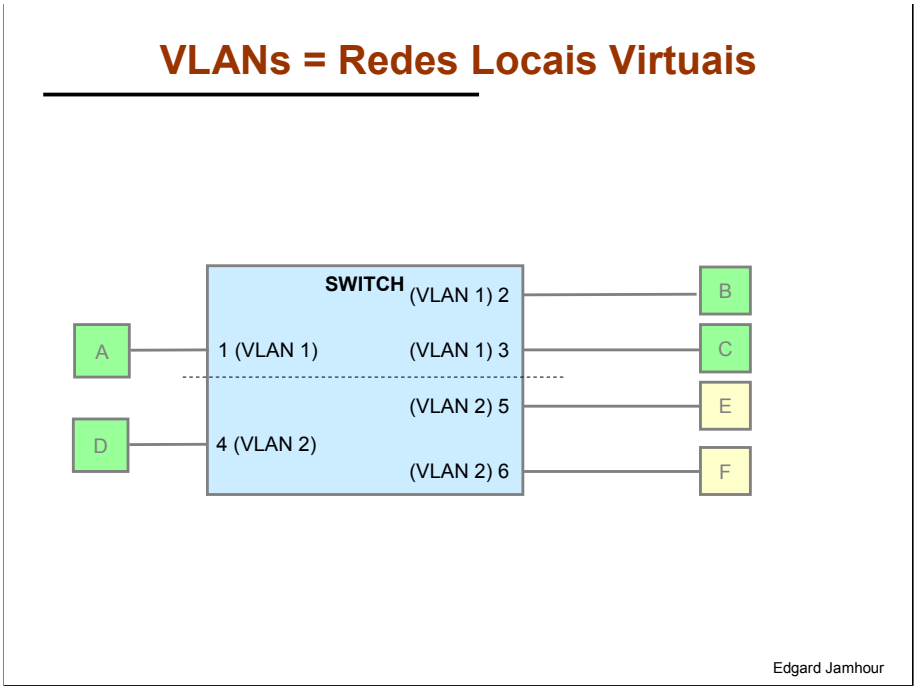
Muitos fabricantes definem uma configuração padrão que permite que o switch entre em um modo de funcionamento aceitável, mesmo que o administrador não altere nenhum dos parâmetros do switch.

A tabela acima mostra a configuração padrão para os switches da Cisco, modelo 2950. Observe que o STP é habilitado por default, mas apenas para VLAN 1. Como veremos adiante, existem um relacionamento estreito entre o funcionamento do Spanning Tree e a utilização de VLAN (Redes Locais Virtuais) em switches Ethernet.

Dessa forma, existem algumas variantes do STP, de acordo com a forma como o protocolo interage com VLANs. Por exemplo, a sigla PVST significa (Per-VLAN Spanning Tree), e é um mecanismo que permite utilizar todos os caminhos existentes entre os switches, para efeito de balanceamento de carga, ao invés de simplesmente bloquear as portas dos switches que provocam laços fechados.

Observe que na tabela, tanto o switch quanto as portas possuem uma prioridade padrão. Como explicado, a prioridade do switch é utilizada na eleição do Root. A prioridade das portas é utilizada quando o switch recebe oferta de múltiplos caminhos até o root, por portas diferentes, mas todas com o mesmo custo. Nesse caso, a porta com menor prioridade é eleita, e as demais são bloqueadas.

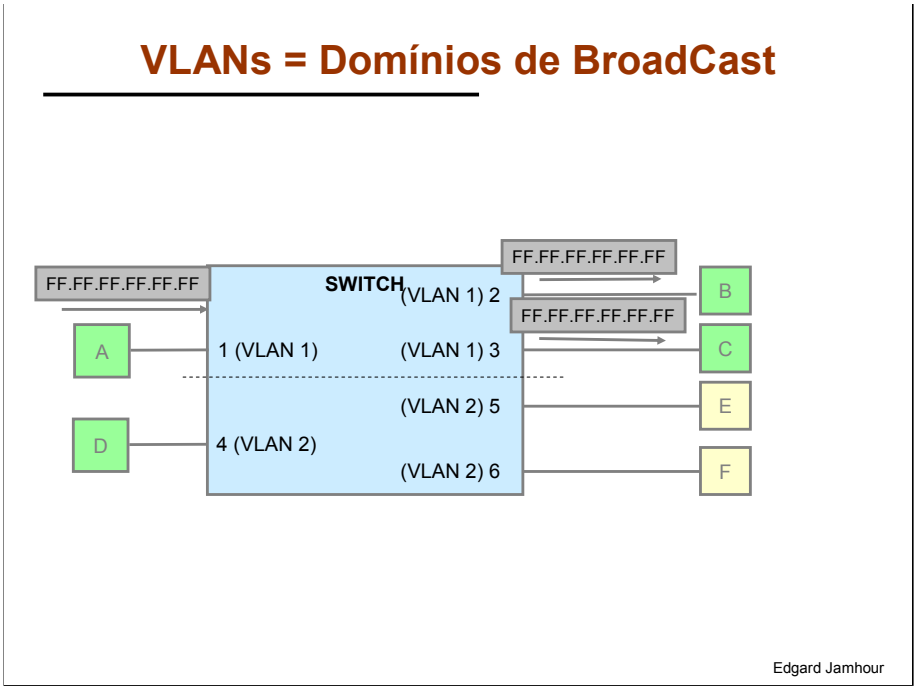
A tabela mostra também a sugestão da Cisco para o custo das portas, em relação as velocidades disponíveis. Note que pela tabela sugerida, é mais vantajoso escolher um caminho que passa por três switches com portas de 1000Mbps (4 enlaces = custo 16) , do que um caminho direto até o Root, mas usando uma porta de 100Mbps (1 enlace = custo 19). Contudo, se o caminho com portas de Gigabit-Ethernet for formado por 4 switches (5 enalces = custo 20), então é melhor escolher o caminho direto de Fast-Ethernet.



Na medida em que a velocidade do Ethernet começou a aumentar e a utilização de switches passou a ser mais comum, surgiu a necessidade de criar novos mecanismos para flexibilizar como as redes Ethernet eram organizada em uma empresa. As VLANs surgiram em 1998, e tornaram-se rapidamente um mecanismo essencial para organização de redes Ethernet, tanto para aumentar seu desempenho quanto para aumentar sua segurança.

A fim de entender a finalidade das VLANs, é preciso inicialmente relembrar o funcionamento do switch. Nós sabemos que após um processo inicial de aprendizagem, o switch passa a encaminhar os quadros recebidos em uma de suas portas apenas para a porta em que o computador que possui o MAC de destino indicado no quadro estiver conectado. Isso é verdade para a maioria dos caso, menos quando o MAC de destino for desconhecido ou for o MAC especial de broadcast “FF-FF-FF-FF-FF-FF”. Quando um quadro com um destino broadcast é recebido pelo switch, ele será propagado para todas as demais portas, incluindo as portas usadas para cascatear o switch com demais switches da rede.

Infelizmente, a presença de quadros broadcast é bastante comum na rede. Por exemplo, o protocolo ARP (Address Resolution Protocol) usado para resolver endereços MAC a partir de endereços IP, sempre utiliza mensagens em broadcast. Muitos outros protocolos, como o DHCP, também fazem isso. Como resultado, se fizermos uma rede Ethernet muito grande cascateando muitos switches, o nível de broadcast será também muito alto, reduzindo consideravelmente o desempenho da rede.

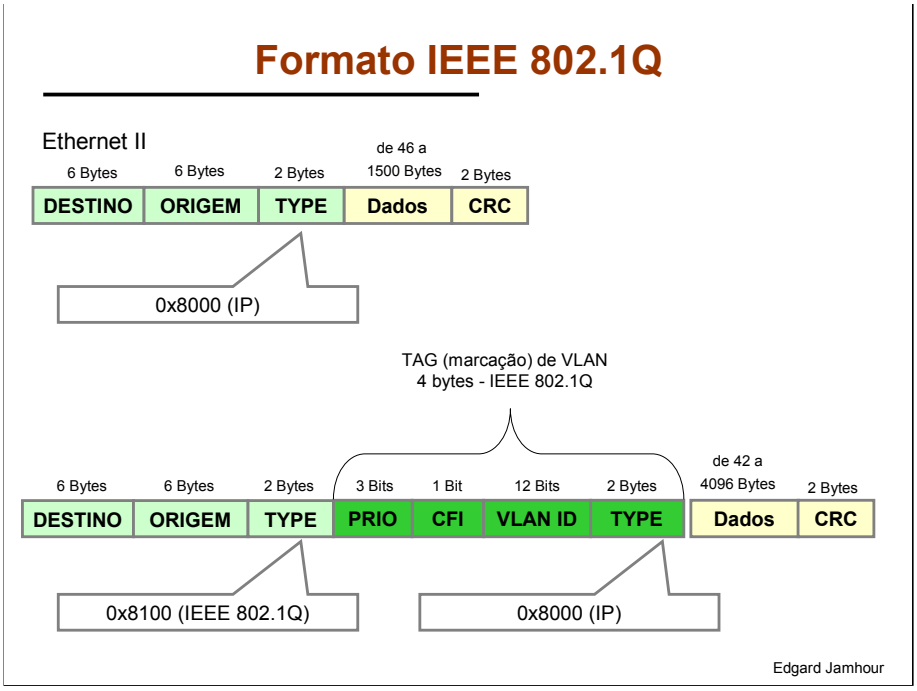


As VLANs resolvem o problema de congestionamento da rede por broadcast introduzindo um mecanismo que permite dividir os switches em múltiplos domínios de broadcast. Para ilustrar esse princípio, considere o switch mostrado na figura.

De acordo com o conceito de VLANs, é possível associar cada uma das portas do switch a um TAG de VLAN (um número entre 1 e 4096). As portas que tem o mesmo TAG constituem uma VLAN ou domínio de broadcast.

Por exemplo, na figura, o switch foi dividido em duas VLANS. A VLAN 1 inclui as portas de 1 a 3, e a VLAN 2 inclui as portas de 4 a 6.

Se o computador A enviar um quadro em broadcast, este quadro será propagado apenas para as portas da VLAN 1. Se o computador D enviar um quadro em broadcast, o quadro será propagado apenas para as portas da VLAN 2.



A fim de suportar o conceito de VLANs, o IEEE elaborou inicialmente os seguintes padrões: IEEE 802.1Q e IEEE 802.1p.

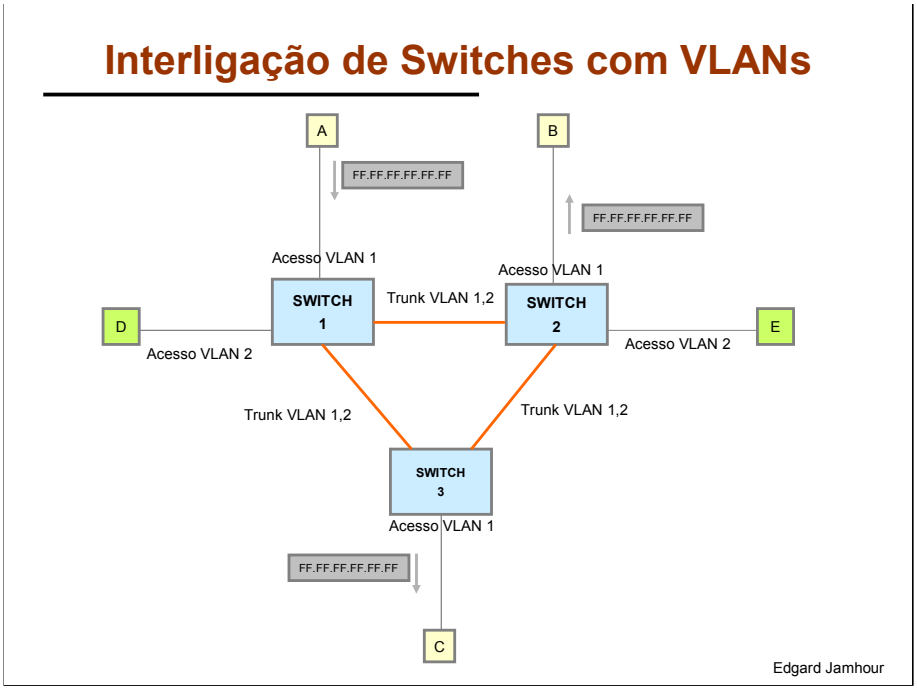
O padrão IEEE 802.1Q define o funcionamento de VLANs, e define uma extensão no formato dos quadros Ethernet, incluindo mais quatro bytes de cabeçalho, conforme indicado na figura. A extensão definida pelo IEEE 802.1Q introduziu os seguintes campos:
- PRIO: campo de prioridade com 3 bits (define 8 valores possíveis de prioridade)
- CFI: campo “Canonical Format Indicator” (valor 0 para quadros Ethernet)
- VLAN ID: identificador de VLANs (valor de 1 a 4096)
- TYPE: indica o tipo de protocolo transportado pelo quadro de VLAN

Observe que o campo TYPE já existia no quadro Ethernet sem TAG. Todavia, a fim de permitir que os equipamentos possam interpretar quadros com ou sem a extensão de VLAN, o tipo 0x8100 foi definido para identificar os quadros no formato IEEE 802.1Q. O verdadeiro identificador do conteúdo do quadro foi transferido para o segundo campo Type, que informa, por exemplo, que o quadro está transmitindo um pacote IP (que tem o valor de tipo 0x8000).

Observe também que devido aos 4 bytes adicionais, o MTU (Máxima Unidade Transportável no campo de dados) do quadro Etherenet foi reduzido de 1500 para 1496 bytes.

O campo PRIO define também um novo conceito para os quadros Ethernet, que é o conceito de classe de serviço (Class of Service - COS). Esses campos permitem priorizar quadros Ethernet que transportam tráfego do tipo tempo-real (que não suporta atraso muito elevado) sobre outros tipos de tráfego que podem ser entregues com uma prioridade mais baixa. As classes de serviço e os respectivos valores padronizados para os bits do campo PRIO são definidos no padrão IEEE 802.1p.

A existência do bit CFI indica também que a intenção do IEEE é que a extensão de VLANs pudesse ser usada em outros protocolos da família IEEE 802, como o Token-Ring.



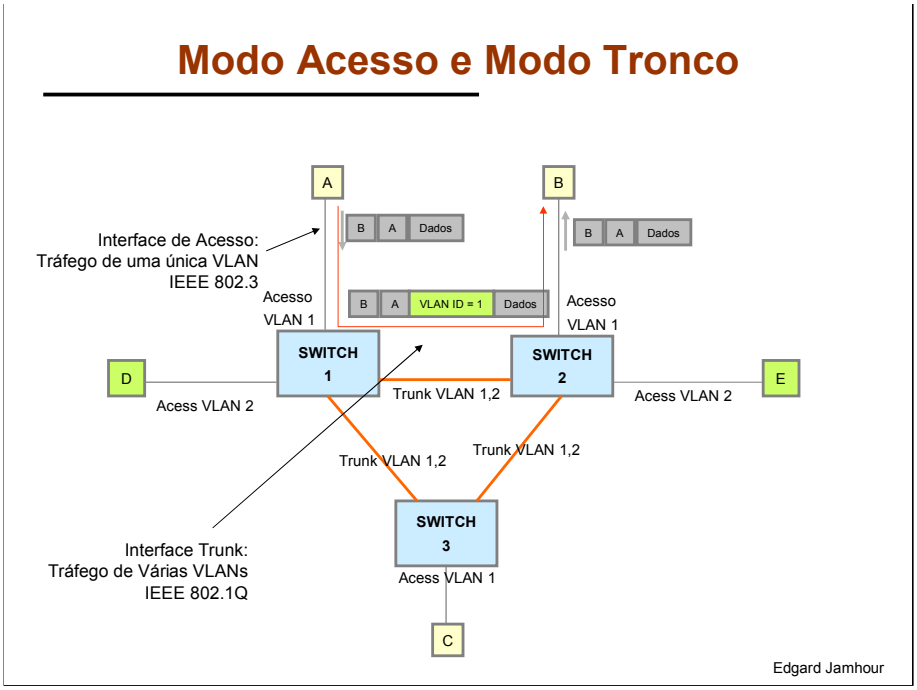
O conceito de VLAN e domínios de broadcast estende-se ao caso onde os switches são conectados em cascata, como o cenário mostrado na figura. O cenário é formado por três switches interligados, os quais são configurados com duas VLANs. Os computadores A, B e C pertencem a mesma VLAN, apesar de estarem conectados a switches distintos. Se o computador A enviar uma mensagem em broadcast, ela será propagada para os demais switches, mas apenas para as portas que também pertencerem a VLAN 1.

O mecanismo de VLANs é bastante flexível, e permite organizar os computadores em domínios de broadcast distintos, independentemente de sua conexão física. Observe que o computador D mesmo estando no mesmo switch que A não recebe o broadcast, enquanto que B e C em switches distintos recebem.

Conforme indicado na figura, as portas dos switches podem operar de dois modos distintos: modo acesso (**Access**) e modo tronco (**Trunk**).

Um porta em modo acesso pertence a uma única VLAN. Esse tipo de porta é usado para conectar computadores, e opera com quadros no formato padrão, IEEE 802.3 ou Ethernet 2. Observe que este formato não possui nenhum tipo de especificação de VLAN.

Uma porta em modo tronco é utilizada para conectar dois switches. Nesse caso, a porta pode pertencer a múltiplas VLANs, e opera com quadros no formato IEEE 802.1Q.



Quando uma porta do switch configurada como acesso recebe um quadro marcado como IEEE 802.1Q ela o descarta. Apenas portas configuradas como tronco é que são capazes de interpretar quadros com marcação de VLAN.

Quando dois switches estão conectados, suas portas de conexão precisam estar configuradas no modo tronco. Se uma porta estiver em modo tronco e a outra não, não haverá comunicação. Alguns switches, como os da Cisco, utilizam um protocolo proprietário que permite detectar se a porta do switch está ligada a um computador ou a um outro switch. Caso ele detecte que a porta está ligada a outro switch, ele automaticamente configura essa porta em modo trunk.

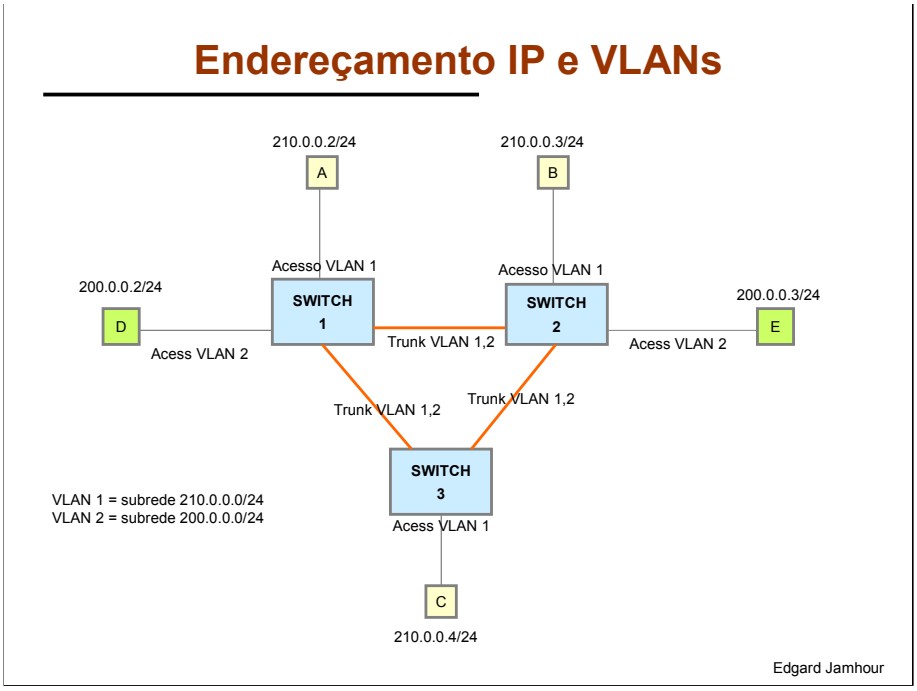
Para entender a distinção entre as portas operando em modo acesso e modo tronco, imagine que o computador A enviou um quadro para o computador B.

O quadro originalmente enviado por A não tem nenhuma informação de VLAN. Ao entrar no switch 1, o quadro recebe a marcação de VLAN e é propagado para o switch 2 pela porta tronco no formato IEEE 802.1Q.

O switch 2 recebe o quadro marcado pela sua porta tronco, determina para qual porta deverá enviar o quadro. Como a porta de destino está no modo acesso, ele remove a marcação de VLAN e entrega o quadro no formato IEEE 802.3 ou Ethernet 2 para o computador B.

Uma porta tronco, geralmente, não aceita quadros sem marcação (com exceção da Native VLAN, conceito discutido mais adiante nessa apostila). Dessa foram, se você ligar um computador numa porta trunk é provável que ele perca o acesso a rede.

Em alguns sistemas operacionais, como no Linux, é possível configurar a placa de rede para enviar pacotes com marcação de VLAN. Neste caso, é necessário que a porta do switch ao qual o computador esteja conectado funcione em modo tronco.

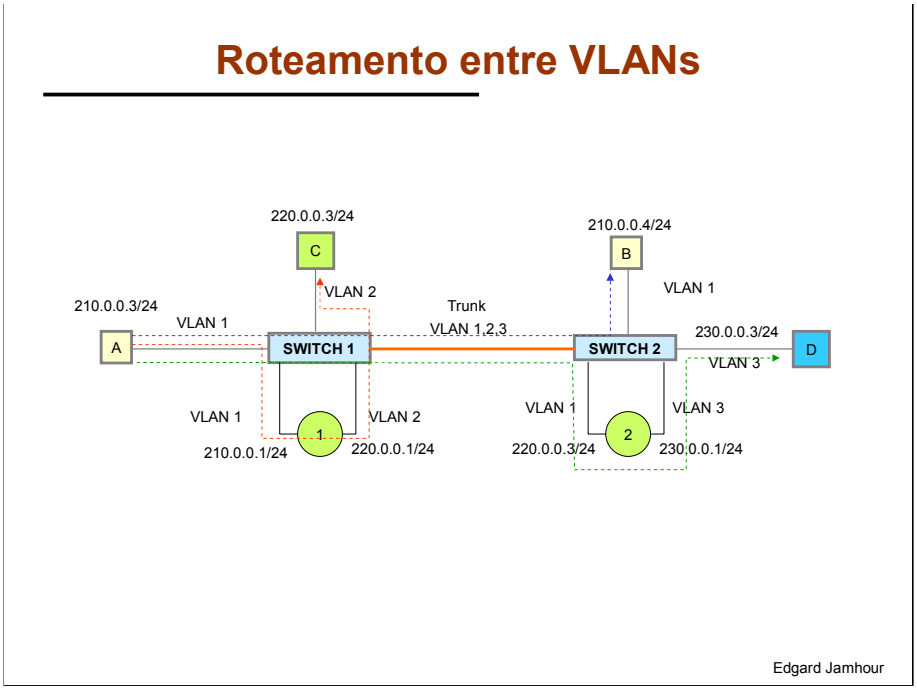


A divisão em VLANs afeta como a atribuição de endereços IPs é feita na rede. Para todos os efeitos, as propriedades de uma VLAN são as mesmas de uma LAN, isto é:
a) Computadores na mesma VLAN devem possuir o mesmo identificador de rede
b) Cada VLAN deve possuir um identificador de rede distinto

Observe na figura que os computadores A e D, apesar de estarem conectados no mesmo switch, pertencem a sub-redes distintas. Já os computadores A e B, que estão em switches distintos, na verdade, pertencem a mesma sub-rede. Conforme enfatizado anteriormente, o mecanismo de VLAN permite que o administrador organize a rede Ethernet de forma independente de como os computadores estão fisicamente conectados.

Observe que computadores em VLANs distintas não podem se comunicar diretamente. É necessário interligar as VLANs através de roteadores para que computadores em VLANs distintas não fiquem isolados. Isso é verdade mesmo que você atribua endereços da mesma sub-rede para VLANs distintas.

Essa propriedade é muito explorada nas empresas para impor políticas de segurança entre os computadores da rede. Considere por exemplo o cenário de uma Universidade que possui duas redes: uma rede acadêmica e uma rede administrativa. A rede acadêmica está disponível para professores e alunos, e consiste principalmente na possibilidade de acesso a recursos na Internet. A rede administrativa, por outro lado, disponibiliza sistemas como folhas de pagamento e emissão de boletos de mensalidade. Por questões de segurança, não se deseja, por exemplo, que um computador em um laboratório tenha acesso ao sistema de folha de pagamentos da Universidade. Isso pode ser controlado utilizando-se VLANs distintas para as duas redes. Ao obrigar que o tráfego entre as VLANs passe por um roteador, é possível utilizar mecanismos como Firewalls para controlar qual tráfego é permitido e qual tráfego é proibido entre as duas redes.



A comunicação entre computadores situados em VLANs distintas só é possível por intermédio de roteadores. Existem várias maneiras de conectar os roteadores aos switches. Caso os roteadores utilizados não tenham suporte a VLANs, é possível utilizá-los apenas com portas no modo acesso. Para ilustrar esse conceito considere a rede mostrada na figura.

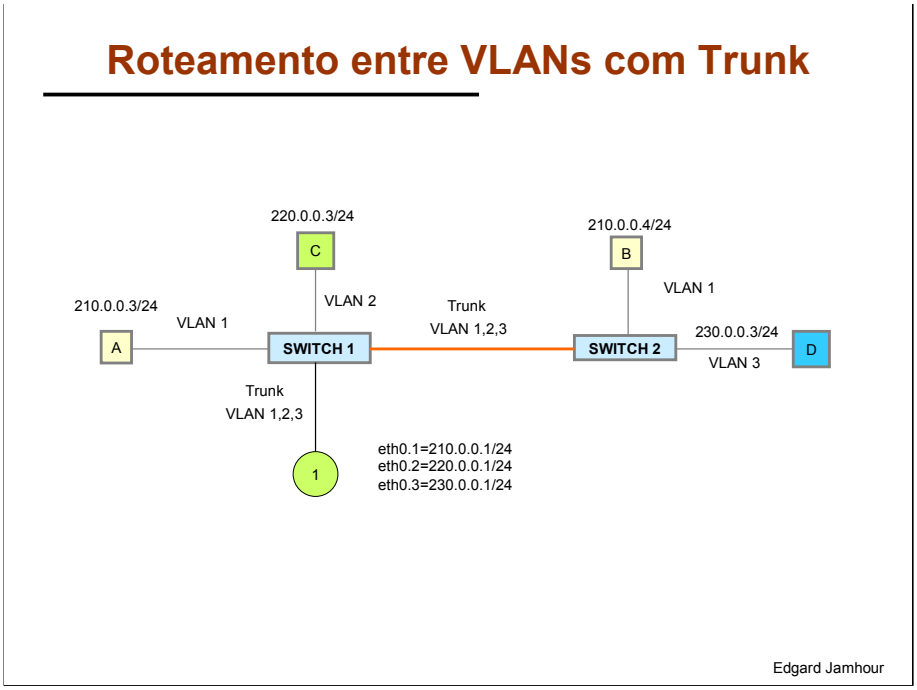
O switch 1 possui um computador na VLAN 1 (A) e outro na VLAN 2 (C). O switch 2 possui um computador na VLAN 1 (B) e ouro na VLAN 3 (D). Como existem três VLANs na rede, é necessário utilizar um switch para conectar a VLAN 1 na VLAN 2 e outro switch para conectar a VLAN 1 na VLAN 3.

O roteador utilizado para conectar duas VLANs precisa ter uma interface conectada a cada VLAN. Por exemplo, o roteador 1 tem uma interface na VLAN 1 e outra na VLAN 2. O roteador 2 possui uma interface na VLAN 1 e outra na VLAN 3.

A figura mostra qual o caminho de seguido por um pacote enviado pelo computador A (VLAN 1) para C (VLAN 2). Observe que o pacote passa pelo roteador 1. Nesse processo, a porta do switch que envia o pacote para o roteador 1 remove a marcação de VLAN 1 do quadro, e a porta do switch que recebe o quadro vinda do roteador 1 insere a marcação no quadro correspondente a VLAN 2.

Quando o computador A (VLAN 1) envia um pacote para o computador B (VLAN 1), o quadro pode ser propagado pela porta trunk sem passar por nenhum roteador.

Quando o computador A (VLAN 1) envia um pacote para o computador D (VLAN 3), o quadro é enviado com a marcação de VLAN 1 pela porta trunk até o roteador 2. O quadro que sai do roteador 2 possui a marcação de VLAN 3. Finalmente, o quadro que chega ao computador D tem sua marcação removida pela porta do switch.



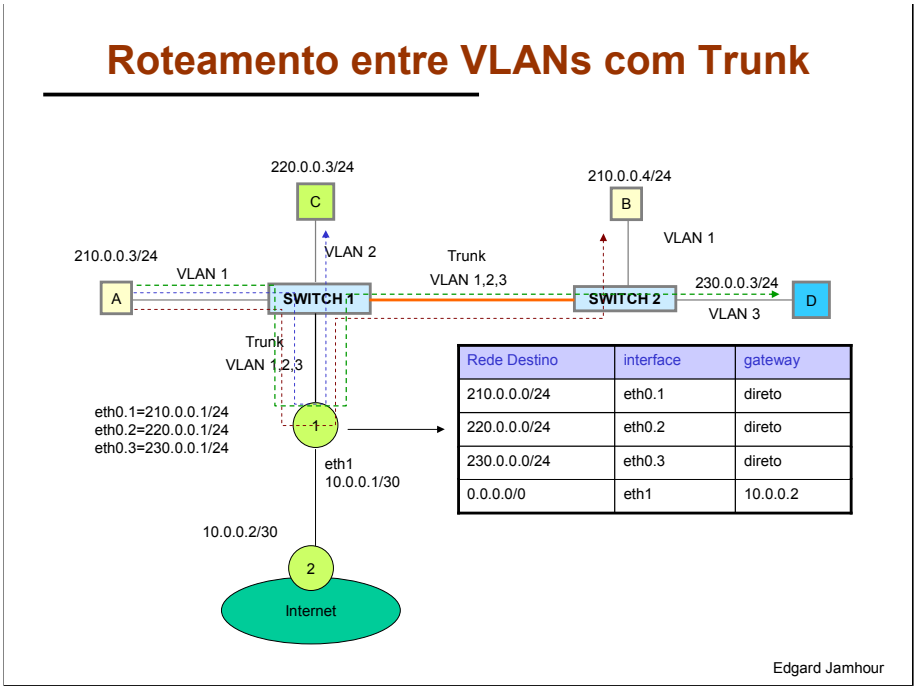
Caso o roteador possua suporte a VLAN, é possível fazer uma conexão mais simples entre os roteadores e os switches. Um roteador com suporte a VLAN é um roteador que permite colocar suas interfaces em modo tronco.

Nesse modo, a interface do roteador é capaz de emitir pacotes com marcação de VLAN e pode ser conectada a uma porta de switch também configurada em modo tronco. Internamente, o roteador permite associar diversas interfaces virtuais (VI) a uma mesma porta física. Por exemplo, o roteador 1 da figura pode ser um computador Linux com uma única interface de rede configurada em modo tronco.

A interface física do Linux (eth0) pode ser dividida em várias interfaces virtuais, cada uma pertencente a uma VLAN distinta. A denominação que cada interface recebe é do tipo "**interface_fisica.VLAN**". Por exemplo, a denominação **eth0.1** refere-se a interface virtual 1 na porta física eth0. Similarmente, a denominação **eth0.2** refere-se a interface virtual 2 na porta física **eth0**, e assim por diante.

Cada interface virtual possui um endereço IP que pertence a mesma subrede da VLAN da interface. Dessa forma, um roteador com uma única interface física pode servir de intermediário para interconectar todas as VLANs presentes na rede (contudo, por questões de desempenho, é possível usar mais roteadores se desejado).

O roteador 1 é o gateway padrão para todos os computadores da rede, mas cada computador usa o endereço da interface virtual correspondente a sua VLAN. Por exemplo, o gateway padrão dos computadores A e B é eth0.1, mas o gateway padrão do computador C é eth0.2.



A tabela de roteamento do roteador 1 determina para qual das interfaces virtuais o pacote será encaminhado em função da rede de destino, conforme indicado na figura.

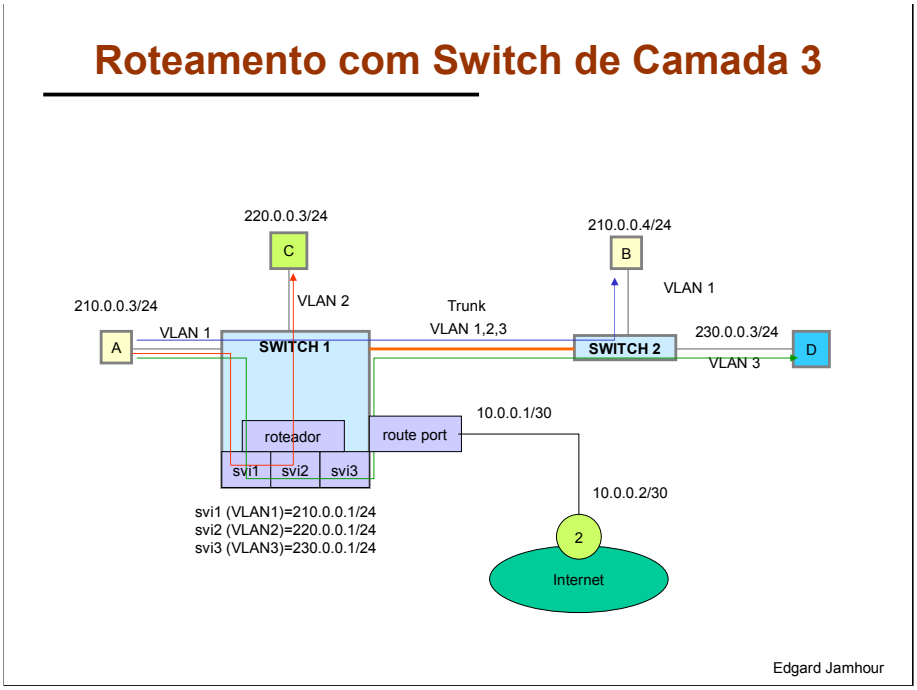
Por exemplo, considere o cenário onde o computador A (VLAN 1) envia um pacote para o computador D (VLAN 3). O pacote enviado por A chega ao roteador 1 com a marcação de VLAN 1, e por isso é recebido para interface eth0.1 do roteador.

A interface do roteador remove a marcação de VLAN do quadro e encaminha para o módulo de roteamento. Consultando a tabela, o módulo de roteamento decide que para enviar um pacote situado na rede 230.0.0.0/24 ele deve encaminhá-lo pela sua interface eth0.3.

O pacote enviado para eth0.3 é encapsulado em um quadro com a marcação de VLAN 3 pelo próprio roteador, e encaminhado para o switch 2 através da porta tronco entre os dois switches.

O switch 2 então decide que vai enviar o quadro para o computador D, conectado em uma porta em modo acesso. Para isso, ele remove a marcação e entrega um quadro Ethernet 2 para o computador D.

Observe que o roteador 1 pode também ser usado para conectar a rede de VLANs com a Internet.



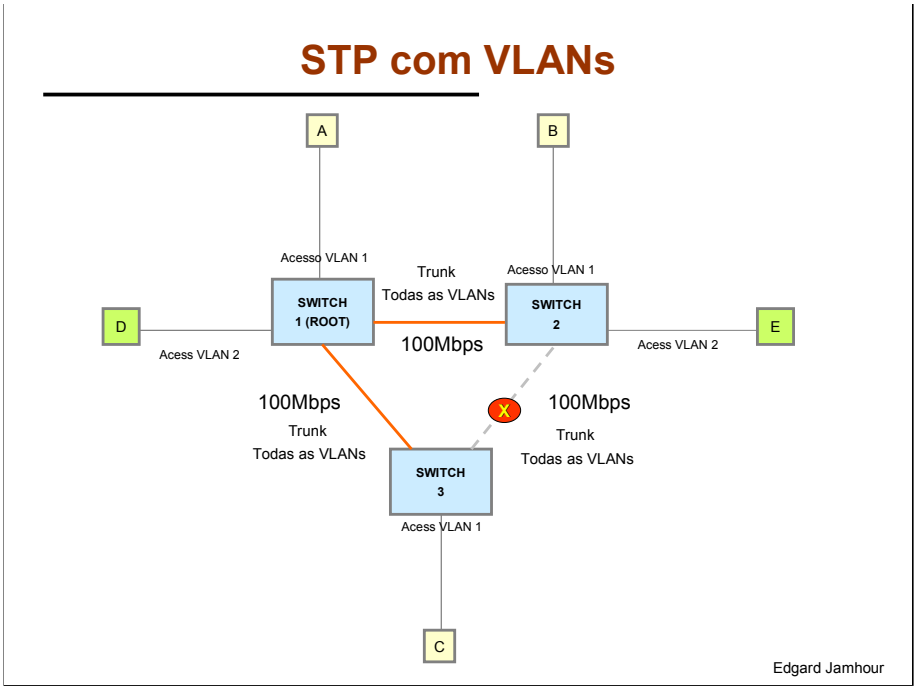
A terceira forma de interconectar as VLANs consiste em utilizar um switch de camada 3, isto é um switch com capacidade de roteamento.

Usualmente, um switch de camada três permite criar interfaces virtuais denominadas SVI (Switch Virtual Interface) para cada VLAN existente. As SVI se comportam como interfaces físicas, tendo inclusive endereço MAC. O administrador de rede deve atribuir um endereço IP para cada SVI, de acordo com a sub-rede associada a VLAN da interface. Os computadores devem utilizar os endereços das SVI como seus gateways padrão, de acordo com a VLAN ao qual pertencem.

Esse princípio é ilustrado na figura. Observe que o switch 1 é um switch de camada 3, enquanto que o switch 2 é um switch de camada 2, sem funções de roteamento. Os computadores da VLAN 1 usam o endereço IP de SVI1 como gateway, os da VLAN 2 usam o endereço IP de SVI2 e os da VLAN 3 usam o endereço IP de SVI3.

O funcionamento usando o roteador virtual interno ao switch é similar ao funcionamento do roteador com porta trunk, descrito anteriormente. Por exemplo, quando o computador A (VLAN 1) deseja enviar um pacote para o computador D (VLAN 3) ele endereça o quadro para o seu gateway padrão com a marcação de VLAN 1. O roteador interno ao switch recebe o quadro pela sua porta SVI1 e determina que o pacote deve ser encaminhado para a porta SVI3. Um novo quadro com a marcação de VLAN 3 é então criado, e enviado pela porta trunk até o switch2. O switch 2 retira a marcação de VLAN e entrega o quadro para o computador D.

As SVI não são acessíveis externamente. Para conectar a rede de VLANs com a Internet, alguns switches oferecem a possibilidade de criar portas de roteador (Route Port - RP) mapeadas em portas físicas do switch. Essa portas podem ou não ser mapeadas em VLANs. A figura ilustra também esse conceito.



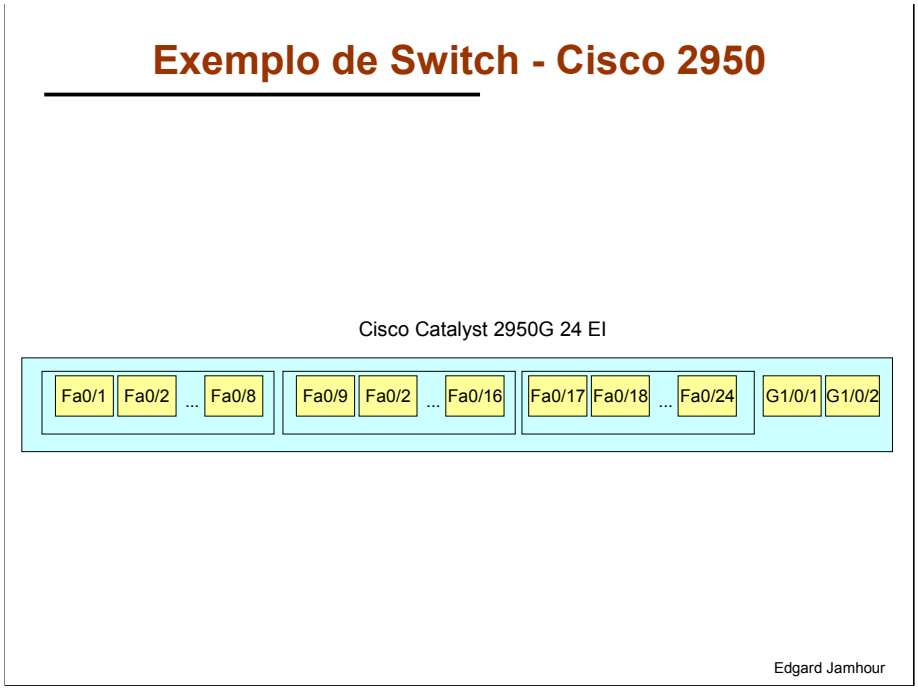
Vamos agora analisar como seria o funcionamento do protocolo de Spanning Tree (STP) na presença de VLANs. Para isso, considere o cenário mostrado na figura. Como a rede de switchs apresenta um laço fechado, se considerarmos um protocolo de STP insensível a VLANs, um dos enlaces entre os switches deveria ser eliminado. Por exemplo, na figura, suponha que todos os enlaces possuem a mesma velocidade (100Mbps). Se o switch 1 for escolhido como root, então o enlace entre os switches 2 e 3 será bloqueado.

Na prática, isso vai fazer com que os recursos da rede fiquem sub-utilizados, pois todas as vezes que algum computador no switch 2 desejar se comunicar com o switch 3, ele será encaminhado pelo root, quando seria mais eficiente utilizar o enlace direto entre os dois switches.

Felizmente, quando VLANs são utilizadas, existem variantes do STP que permitem utilizar todos os enlaces disponíveis na rede de switches simultaneamente, sem correr o risco de criar laços fechados.

O princípio utilizado por essas variantes do STP é vincular as portas trunk a VLANs específicas ao invés de todas as VLANs. Dessa forma, o algoritmo STP poderá criar uma árvore de switches independentes para cada switch.

Essa variantes do STP é denominada PVSTP (Per-VLAN Spanning Tree Protocol).



Para facilitar a apresentação dos próximos exemplos, vamos considerar um switch de mercado: o Catalyst da Cisco, modelo 2950G, com 24 portas do tipo Fast-Etherent e 2 portas do tipo Gigabit-Ethernet.

Nesses switches, as portas são identificadas por labels do tipo Slot/Port. O Slot é um módulo conceitual do switch. As séries mais simples de switch só possuem um slot identificado como 0. Um slot de portas Fast-Ethernet é denominado Fa0. O slot de portas Gigabit-Ethernet é denominado G1/0. As portas são identificadas pela sua posição no chassis, numerado da esquerda para direita, como indicado na figura.

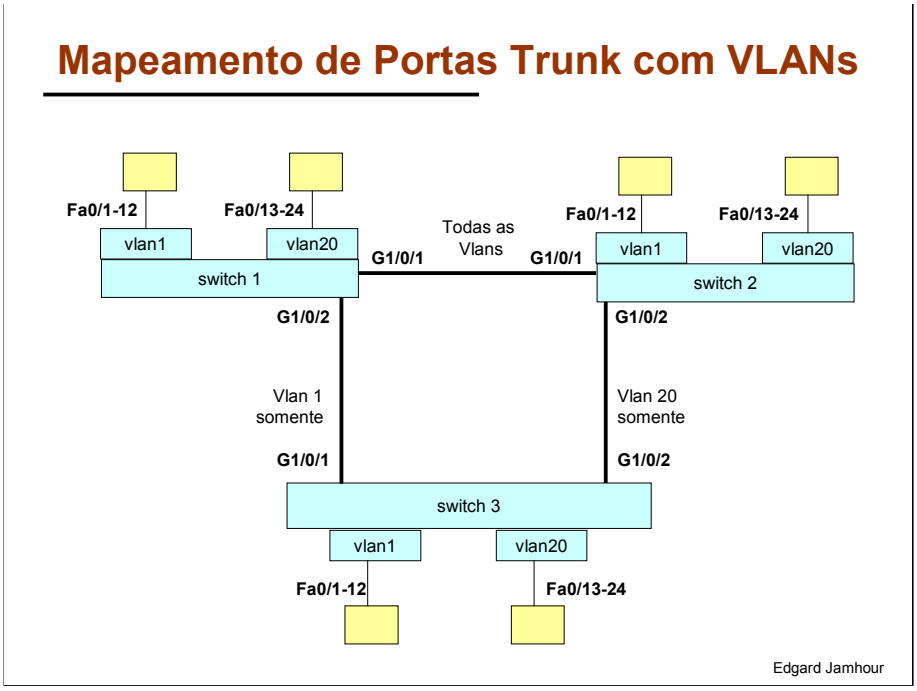
Os switches da Cisco podem ser configurados por telnet. O CISCO IOS possui uma sintaxe bastante simples de configuração, que é imitada por alguns softwares livres, como o Quagga, que permite criar um roteador completo em Linux, que será utilizado num módulo mais avançado do curso.

A seqüência de comandos básica para associar uma porta em VLAN no modo acesso é mostrada a seguir:

```
enable

#após esse comando o switch irá solicitar a senha de administrador

configure terminal
  interface Fa0/2
    switchport mode access
    switchport access vlan 2
  end
```



Por default, cada porta tronco pode ser utilizada por todos as VLANs do switch. Na configuração default, supondo que o switch 1 é o root, o enlace entre os switches 2 e 3 seria bloqueado.

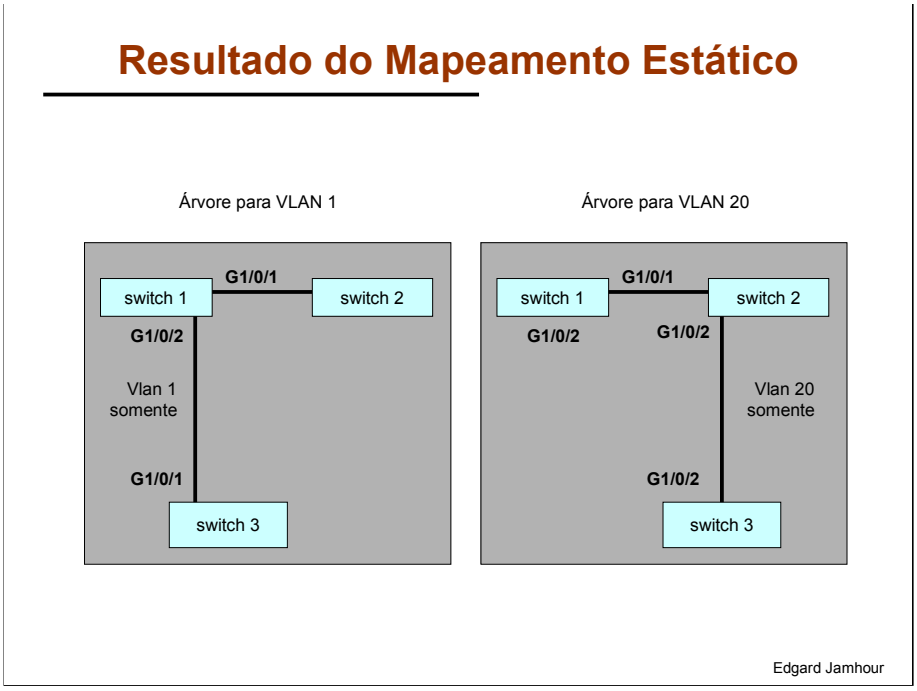
Todavia, é possível restringir o uso das VLANs para portas tronco específicas. Isso permite efetuar um engenharia de tráfego na rede de switches, controlando por quais enlaces cada tipo de tráfego irá percorrer.

No cenário mostrado na figura, os computadores conectados a rede de switches estão em duas Vlans (1 e 20). Os computadores estão ligados por portas de Fast-Ethernet, e os switches estão conectados por portas de Gigabit-Ethernet.

A fim de evitar o bloqueio das portas entre os switches 2 e 3, foram feitas as seguintes restrições de tráfego nas portas trunk:
Portas trunk entre os switches 1 e 2: transporta as Vlans 1 e 20
Portas trunk entre os switches 1 e 3: transporta apenas a Vlan 1
Portas trunk entre os switches 2 e 3: transporta apenas a Vlan 20

A seqüência de comandos para restringir o uso das Vlans nas portas trunk é bastante simples. Por exemplo, para limitar a porta trunk do switch 2 conectada ao switch 3 para apenas transportar quadros da Vlan 20, a seguinte seqüência de comandos deve ser usada:

```
configure terminal
  interface Gi/0/2
    switchport trunk allowed vlan remove all
    switchport trunk allowed vlan add 20
  end
```



A figura mostra a configuração resultante da rede após o protocolo Spanning Tree (STP) ter alcançado a convergência.

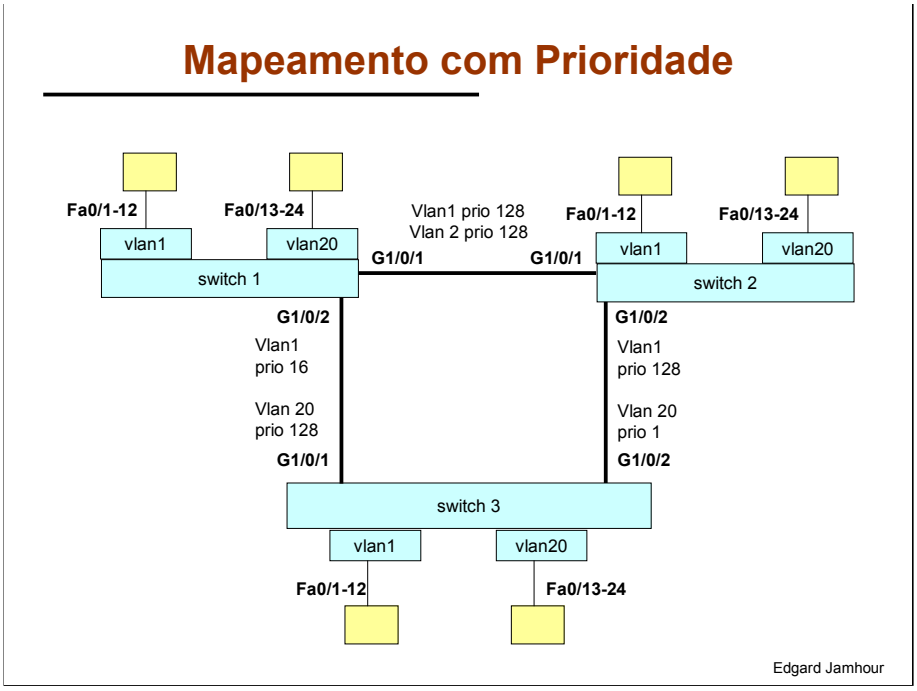
Observe que quando as VLANs são utilizadas, a configuração resultante é uma árvore de switches independente para cada VLAN existente na rede. Cada árvore de VLAN funciona como no STP original, isto é, a configuração resultante não tem dois caminhos entre dois computadores quaisquer na rede.

No caso da árvore para VLAN 1, o caminho entre os switches 2 e 3 não interfere na VLAN 20, e por isso, não gera um laço fechado entre os switches.

O mesmo acontece com a árvore para VLAN 2, pois o caminho entre os switches 1 e 3 não interface na VLAN 1, e por isso não gera um laço fechado entre os switches.

Observe que essa estratégia permite que todos os switches se falem diretamente, o que não acontece na estratégia default, onde as portas trunk permitiam todas as VLANs, o que obrigava que o tráfego entre os switches 2 e 3 passasse sempre pelo switch 1.

Essa estratégia baseada no mapeamento estático de VLANs com as portas tronco tem uma grande desvantagem. Ela não permite a reorganização automática do fluxo de dados quando uma enlace tronco é danificado. Por exemplo, se o enlace entre os switches 1 e 2 for danificado, os computadores pertencentes a VLAN 1 no switch 3 ficarão isolados. Isto é, mesmo existindo um caminho alternativo entre o switch 3 e o switch 2, ele não poderá ser usado devido a restrição estática.



Uma alternativa mais adequada que o mapeamento estático é priorizar a utilização de certas VLANs em certas portas, ao invés de bloquear sua utilização. Essa estratégia permitirá uma "migração" das VLAN para portas tronco alternativas no caso de falhas nos enlaces da rede. Isto é, se não houver falha, teremos uma árvore distinta para cada VLAN, mas em caso de falha, as árvores poderão ser fundidas.

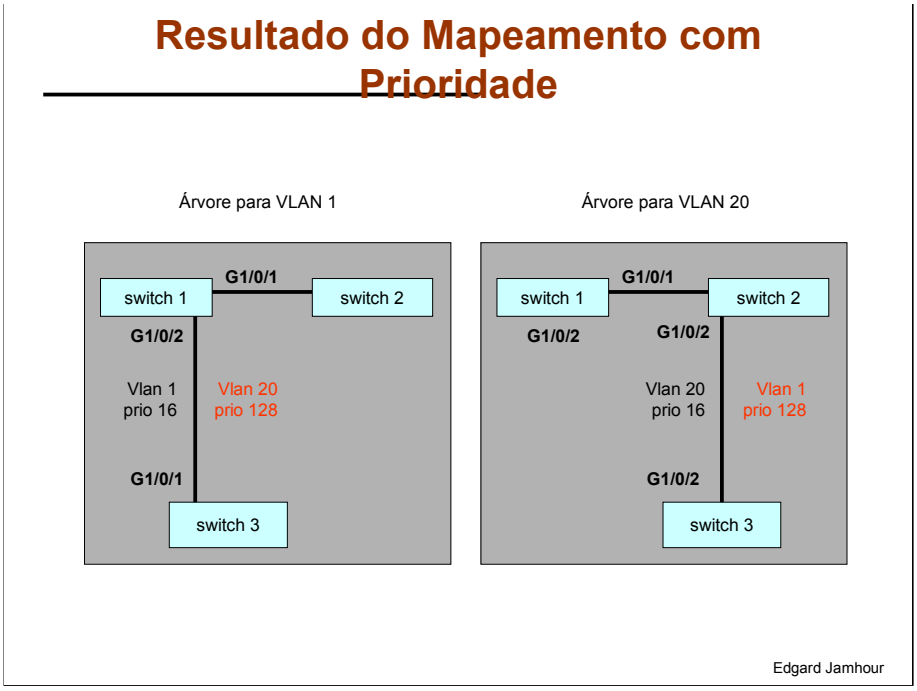
Por default, a prioridade de utilização de VLANs em portas trunk é 128. Essa prioridade poderá ser reduzida de maneira a induzir que o protocolo STP escolha uma VLAN específica em uma dada porta tronco.

Para ilustrar esse conceito, considere o cenário mostrado na figura. O enlace entre os switches 1 e 3 foi configurado de forma que a Vlan 1 tenha prioridade mais baixa (16). Similarmente, o enlace entre os switches 2 e 3 foi configurado de forma que a Vlan 20 tenha prioridade mais baixa.

A configuração da prioridade de utilização de uma VLAN em uma porta tronco é bastante simples. Abaixo é mostrada a seqüência de comandos necessária para atribuir a prioridade 16 para Vlan 1 e a prioridade 128 para Vlan 20 na porta G1/0/2 do switch 1.

```
configure terminal
  interface G1/0/2
     spanning-tree vlan 1 port-priority 16
     spanning-tree vlan 20 port-priority 128
     exit
```

Observe que se a prioridade da Vlan 20 não foi alterada em relação a configuração padrão, a atribuição da prioridade 128 para ela não é realmente necessária.



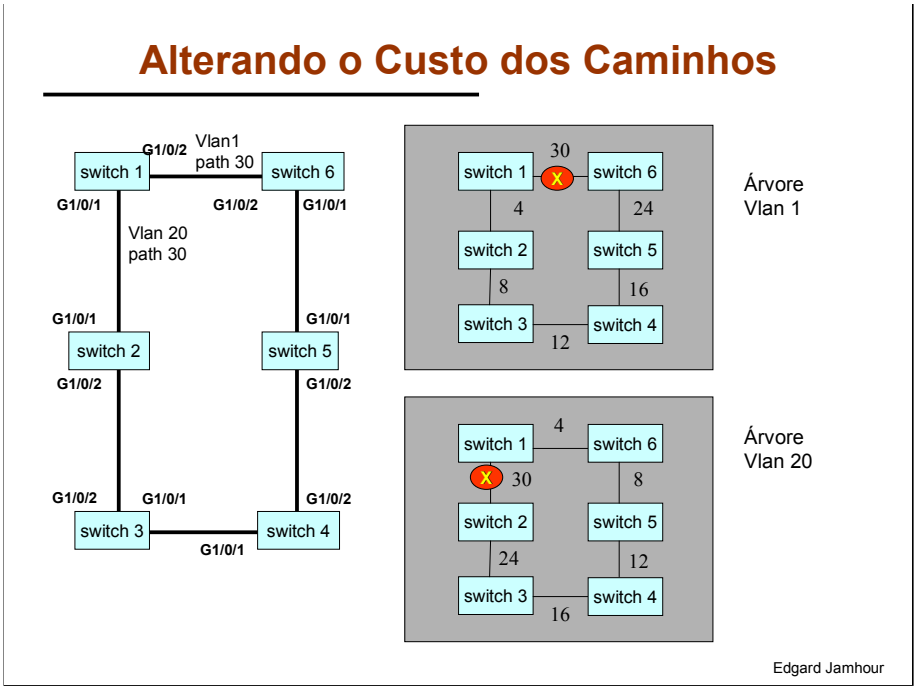
A figura mostra a configuração resultante da rede após o protocolo Spanning Tree (STP) ter alcançado a convergência.

A princípio, o resultado alcançado é idêntico ao caso estático. Para o caso da árvore da Vlan 1, o STP bloqueou a utilização do tronco entre os switches 1 e 3 para a VLAN 20, devido a esta ter uma prioridade mais baixa. De forma similar, na árvore da Vlan 20, a Vlan 1 foi bloqueada no tronco entre os switches 2 e 3.

Contudo, agora, em caso de falha, as Vlans poderão migrar de tronco. Por exemplo:
- Se o enlace entre os switches 1 e 3 falhar, a Vlan 1 será habilitada no tronco entre os switches 2 e 3.
- Se o enlace entre os switches 2 e 3 falhar, a Vlan 20 será habilitada no tronco entre os switches 1 e 3.
- Se o enlace entre os switches 1 e 2 falhar, a Vlan 1 será habilitada no tronco entre os switches 2 e 3 e a Vlan 20 será habilitada no tronco entre os switches 1 e 3.

Note que esse processo acontece automaticamente, sem a necessidade de intervenção do administrador da rede. A razão disso é que o STP continua rodando continuamente mesmo após sua convergência original.

Então em caso de falha, o switch pára de receber mensagens BPDU de seu vizinho por uma determinada porta, e assume que o caminho até o root passando por ele não está mais disponível. Assim, uma porta alternativa, que estava bloqueada será re-avaliada, e se esta não provocar um laço fechado, ela será desbloqueada. O tempo default para os switches iniciarem sua reconfiguração em caso de falha é de 20 segundos.



Uma outra maneira de fazer mapeamento dinâmico de Vlans com as portas trunk é utilizar um custo diferenciado para cada Vlan nas portas do switch. Como vimos, o custo padrão associado as portas do switch é definido de acordo com a velocidade da porta, da seguinte maneira: Porta Ethernet: 100, Porta Fast-Ethernet: 19 e Porta GigaBit-Ethernet: 4.

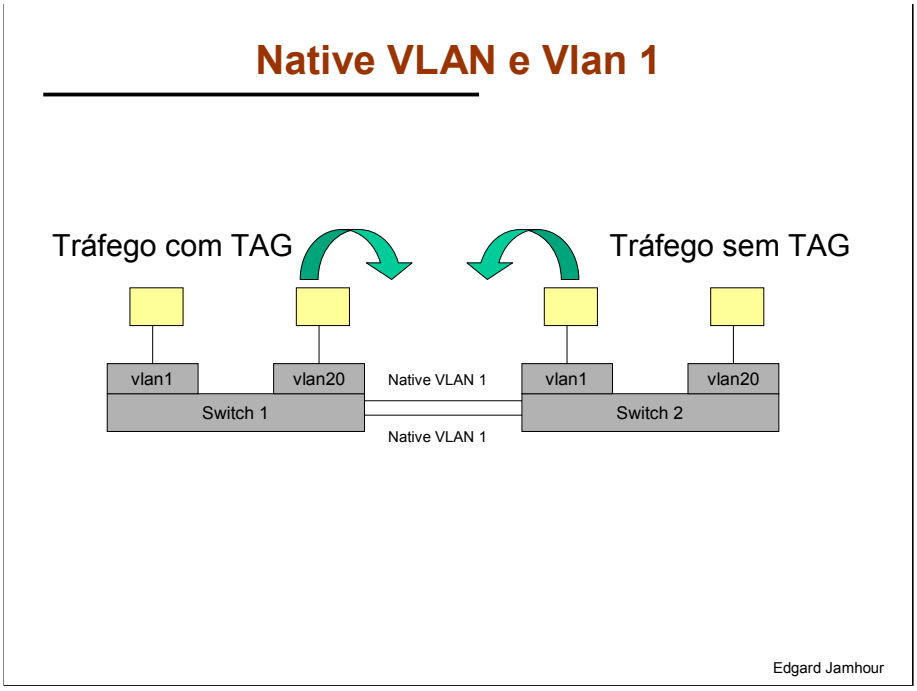
No caso de haver troncos redundantes para o mesmo caminho, o STP irá selecionar o caminho com o menor custo (i.e., maior velocidade). Por default, o valor do custo é o mesmo para todas as VLANs, mas pode ser alterado para prover balanceamento de carga.

Esse principio é ilustrado na figura. Observe que o custo padrão das portas Gigabit-Ethernet do switch 1 foi alterado de acordo com as Vlans. A porta G1/0/1 teve o custo associado Vlan 20 alterado para 30 e a porta G1/0/2 teve o custo associado a Vlan 1 alterado para 30. A figura mostra o resultado obtido pelo STP levando-se em conta a diferenciação de custos por Vlan, considerando-se que o switch 1 é o root.

Observe que o custo dos caminhos até o root são diferentes para a Vlan 1 e a Vlan 20, o que leva a um bloqueio diferente das portas nesse caso. O efeito é similar ao conseguido com a diferenciação por prioridade, mas o método é mais flexível.

A seqüência de comandos para alterar o custo padrão associado a velocidade de uma porta é muito simples. A seqüência abaixo mostra como alterar o custo associado as duas portas tronco do switch 1.

```
configure terminal
  interface G1/0/1
    spanning-tree vlan 20 cost 30
    end
  interface G1/0/2
    spanning-tree vlan 1 cost 30
    end
  exit
```



Você vai observar que alguns sistemas, como o caso do Linux, dão um aviso de que a VLAN 1 pode não funcionar com certos switches.

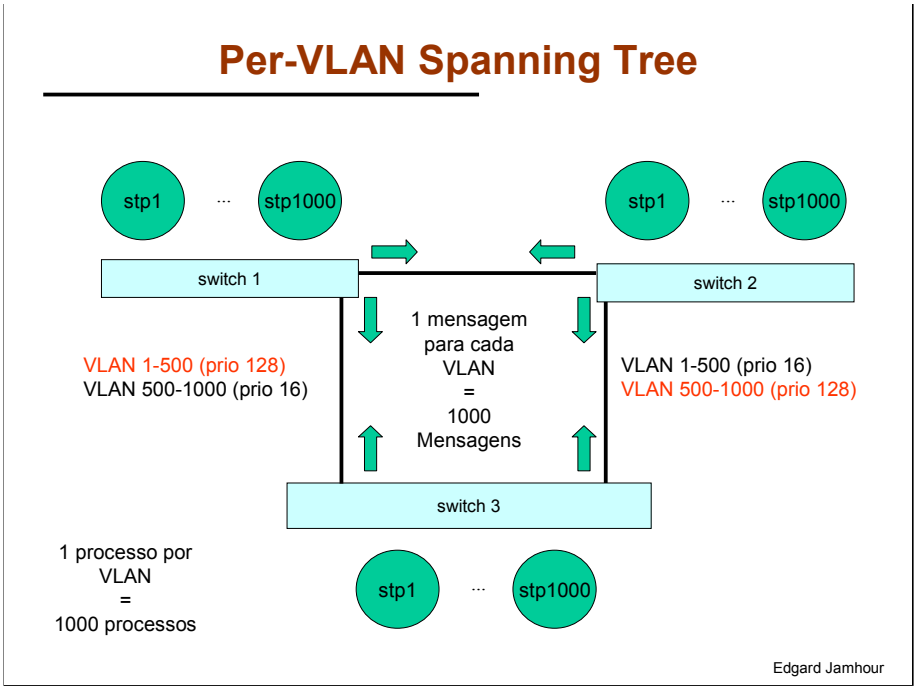
De fato, a VLAN 1 é uma VLAN particular, que pode causar alguns problemas em alguns cenários de aplicação. A razão para isso está associado ao conceito de Native VLAN.

Uma porta tronco está sujeita a dois tipos de tráfego: com TAG, resultante do tráfego de VLANs de um switch para outro e sem TAGs, resultante do tráfego gerado por protocolos intra-switch, como o protocolo de configuração de portas tronco da Cisco.

O tráfego sem TAGs é associado a Native VLAN (VLAN Nativa) da porta tronco. A fim de haver negociação entre portas tronco é necessário que elas pertençam a mesma Native VLAN. Por default, a Native VLAN das portas troncos é VLAN 1.

O tráfego direcionado de uma VLAN para a porta tronco não receberá o cabeçalho de VLAN, se seu código coincidir com a Native VLAN do switch. Dessa forma, se a VLAN 1 for utilizada nesses casos, ela não receberá a marcação IEEE 802.1Q, o que pode criar algumas confusões no funcionamento da rede.

Dessa forma, uma prática comum é utilizar apenas a numeração 2 em diante para as VLANs.



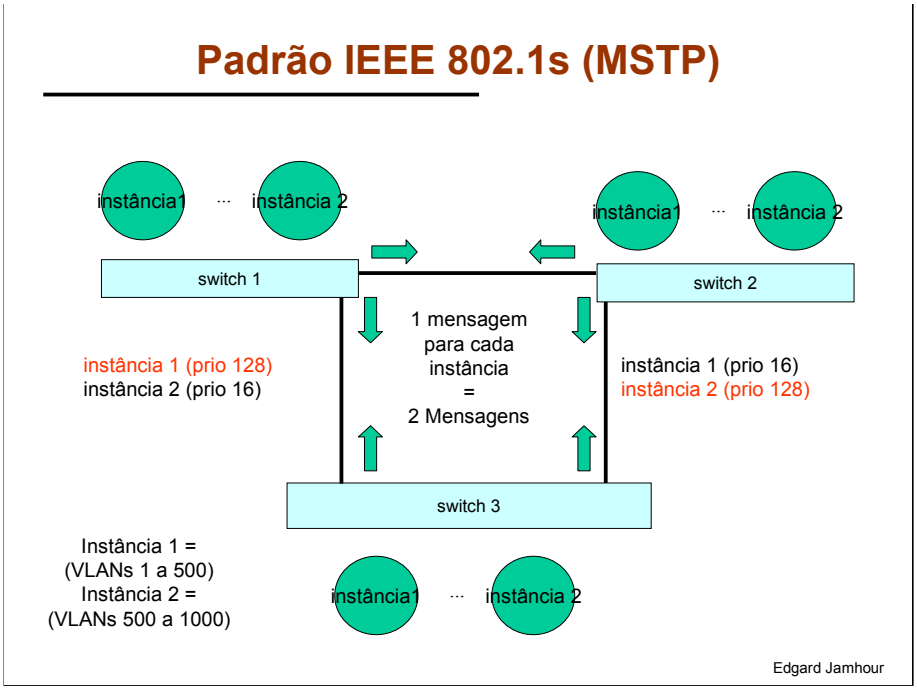
O protocolo de STP originalmente definido pelo IEEE data de 1998, e foi padronizado pela sigla IEEE 802.1D. Esse protocolo permite criar apenas uma instância de STP para todas as VLANs. Esse método é conhecido como CST (Common Spanning Tree), e não permite efetuar nenhum dos métodos de balanceamento de carga entre as portas tronco discutidos anteriormente.

O IEEE definiu também uma outra variante do protocolo STP sob a sigla IEEE 802.1W. Essa variante é comummente referenciada como “Rapid Spanning Tree Protocol - RSTP”, pois ele introduz várias melhorias no protocolo original a fim de fazer com que a convergência para uma nova árvore em caso de falha seja bem mais rápida.

A implementação da Cisco para o protocolo STP segue uma outra variante, denominada PSVT+ (Per-VLAN Spanning Tree). Conforme ilustrado na figura, o PSVT cria uma instância independente do protocolo STP para cada VLAN existente no switch. Isso permite criar uma árvore de Spanning-Tree independente para cada VLAN, e utilizar os mecanismos de balanceamento de carga discutidos anteriormente.

Esse método, contudo, apresenta uma limitação de desempenho. Quando um switch tem múltiplas VLANs, a negociação para cada VLAN é feita de forma independente das demais. Isso implica, por exemplo, que se houverem 1000 VLANs numa rede de switches, teremos 1000 vezes mais mensagens BPDU do que se tivéssemos uma única VLAN.

Igualmente, cada instância do protocolo STP que roda no switch consome memória, fazendo com que na prática, a quantidade máxima de VLANs suportada pelos switches seja bastante inferior ao número de 4096. No caso da Cisco, a quantidade máxima de instâncias de STP é de 128, o que implica, que a rede de switches pode suportar no máximo 128 VLANs.



A fim de prover maior escalabilidade, o IEEE definiu uma outra variante do protocolo Spanning-Tree denominada Multiple Spanning Tree Protocol (MSTP). O MSTP é padronizado pela sigla IEEE 802.1.s.

O MSTP cria o conceito de instâncias, que permitem agrupar múltiplas VLANs que deverão seguir o mesmos caminhos de enlaces tronco. As mensagens do MSTP são diferentes das mensagens do STP original, e por isso recebem a denominação de MSTP BPDUs. Esse novo formato de mensagem permite transportar as novas informações de instâncias usadas pelo protocolo.

Na implementação da Cisco, é possível criar até 65 instâncias MSTP numa rede, sendo que cada instância pode agrupar um número ilimitado de VLANs.

Por exemplo, o cenário anterior poder ser resolvido usando o MSTP criado-se duas instâncias. A instância 1 englobaria as VLANs de 1 a 500 e a instância 2 englobaria as VLANs de 500 a 1000. Usando essa abordagem, em cada switch, seriam criadas apenas duas instâncias de STP. Cada instância poderia então ser mapeada em um enlace tronco diferente, usando qualquer dos esquemas discutidos anteriormente (no exemplo, foi usando o esquema de priorização de porta).

A seqüência de comandos para criar instâncias é bastante simples, como forma o exemplo a seguir:

```
configure terminal
  spanning-tree mst configuration
    instance 1 vlan 1-500
    instance 2 vlan 500-1000
    spanning-tree mode mst
    end
```

Na Cisco, o modo de spanning-tree padrão é o PVST+, pois considera-se que cenários com número excessivo de VLANs não é muito usual.

Conclusão

Neste módulo vimos que, na prática, redes grandes formadas pela interligação de múltiplos switches não poderão funcionar se não forem segmentadas. Isso é decorrente da grande quantidade de mensagens em broadcast que são geradas na rede, e que não são filtradas pelas portas dos switches.

Existem duas formas de segmentar uma rede. A primeira, é utilizar switches distintos, não cascateados, interligados por roteadores. A segunda é utilizar VLANs. A estratégia baseada em VLANs é muito mais flexível, pois ela permite segmentar a rede baseado em critérios lógicos e não físicos, como na primeira abordagem.

Atualmente, além das vantagens proporcionadas para o desempenho da rede, as VLANs também são muito usadas por razões de segurança, pois é possível obrigar que o tráfego entre duas VLANs quaisquer na rede seja sempre filtrado por um firewall.

Neste módulo vimos também que os conceitos de Protocolo de Spanning-Tree (STP) e VLANs são combinados a fim de prover mecanismos de engenharia de tráfego e balanceamento de carga em redes de grande porte..