

***TÉCNICAS DE SWITCHING***  
**UNIDADE 3 - VLAN TRUNKING  
PROTOCOL (VTP) - CONCEITOS E  
CONFIGURAÇÕES**

Andrea Karina Garcia

## Introdução

O fim do século XX trouxe vários acontecimentos que têm transformado o cenário social. Segundo Castells (2002, p. 21), “uma revolução tecnológica concentrada nas tecnologias da informação, organizadas em rede, está reorganizando a base material da sociedade, em um ritmo bastante acelerado.”

A capacidade do desenvolvimento de redes se tornou possível por causa dos avanços das telecomunicações e das tecnologias de integração de computadores em rede, ocorridos durante a década de 1970. As telecomunicações também foram transformadas pela combinação das tecnologias de nós (roteadores e comutadores eletrônicos) e novas conexões (tecnologias de transmissão).

A sociedade organizada em redes está diretamente relacionada a ideia de compartilhamento de recursos computacionais, composta por serviços compartilhados.

Você já se perguntou sobre a importância de conhecer as características técnicas das redes atuais? Elas são compostas por uma combinação de *bridges* e roteadores conectados pela Ethernet ou Token Ring. Conexões de blocos de *switches* da Camada 2, de acordo com o modelo de rede, podem ser divididos em vários domínios de broadcast, os chamados: VLANs (Virtual LANs ou redes locais virtuais).

As VLANs permitem que os administradores dividam a rede, designando determinadas portas como parte de uma rede lógica. Em outras palavras, embora vários computadores (ou dispositivos) possam estar conectados a uma mesma rede física, eles podem estar separados logicamente, a partir do uso de uma VLAN.

Quais são, no entanto, as principais ferramentas de gerenciamento de VLANs?

Nesta unidade você conhecerá uma delas, o chamado VTP (VLAN Trunking Protocol), de propriedade Cisco. Inicialmente, apresentaremos, o conceito, aplicações e configurações do VTP.

As informações de VTP são trocadas de servidores para clientes, e seu banco de dados VLAN é atualizado. Um tronco é o canal usado para o transporte de informações da VLAN de um *switch* para o outro, usando 802.1Q, ISL, 802.10 ou LANE. O gerenciamento de VTP é configurado em domínios. As VLANs podem ser usadas para implementar maior segurança, ao segmentar diferentes departamentos em segmentos separados, fazendo com que um departamento não possa espionar o tráfego de outro. O entroncamento poderia alterar poderia essa segurança, caso alguém estivesse acessando a conexão troncalizada (LIU; BARBER; DIGRANDE, 2009).

Você já ouviu falar em EtherChannel? Nesta unidade também faremos uma breve exposição dessa tecnologia, que foi desenvolvida pela Cisco Systems. O EtherChannel tem como objetivo agregar o *link* de porta, ou promover a arquitetura de canal de porta. Na prática, ele permite agrupar vários *links* Ethernet físicos, a fim de criar um *link* Ethernet lógico, com a finalidade de aprimorar a tolerância à falhas e *links* de alta velocidade entre *switches*, roteadores e servidores.

No decorrer deste estudo, você também terá a oportunidade de praticar o conteúdo estudado. Siga em frente! Bons Estudos!

### 3.1 Conceito de VTP

O VLAN Trunking Protocol (VTP) é um protocolo de propriedade da Cisco, disponível na maior parte dos produtos da série Cisco Catalyst. A função do VTP é reduzir a administração em uma rede comutada. Ao configurar um novo VLAN a um servidor VTP, por exemplo, o VLAN será distribuído a todos os interruptores do domínio. Esse mecanismo, portanto, ajudará a reduzir a necessidade de se configurar várias vezes a mesma VLAN, de modo a facilitar o gerenciamento da rede, mantendo a consistência da sua configuração.

O VTP é um protocolo de mensagens da camada 2. Para executar a adição, exclusão e renomeação de VLANs de um mesmo domínio VTP e, ao mesmo tempo, manter a consistência de sua configuração.

---

#### VOCÊ SABIA?

Analogias humanas podem ajudar a entender o conceito de protocolo. Considere perguntar a alguém as horas. De acordo com Kurose e Ross (2014), o protocolo, primeiro devemos cumprimentá-la. Implicitamente, a resposta “oi” seria a indicação de que podemos prosseguir e perguntar as horas. Outras respostas, poderiam vir a indicar falta de vontade ou incapacidade de comunicação. Ações específicas existirão em reação às respostas recebidas ou a outros eventos, ou, após certo tempo, podemos inclusive não ter nenhuma resposta, por exemplo. Se as pessoas executarem protocolos diferentes, eles não interagem e nenhum trabalho útil pode ser realizado. Isso também é válido para redes.

---

O VTP faz uso de quadros de troncos, ou seja, um domínio VTP – ou domínio de gerenciamento de VLAN – é composto por um ou mais dispositivos de rede que compartilham o mesmo nome de domínio VTP e estão interconectados com troncos. Sendo assim, o VTP permite a elaboração de alterações centralizadas, as quais serão comunicadas a todos os outros *switches* da rede, minimizando a possibilidade de surgimento de inconsistências a partir das alterações. Configurações incorretas ou inconsistentes podem resultar em violações da segurança, tais como: nomes de VLAN duplicados, especificações incorretas do tipo de VLAN, entre outros problemas (CISCO,

2014).

O primeiro passo seria verificar as VLANs atuais de uma rede, antes de criar novas VLANs em um *switch*, a partir da instalação de um domínio de gerenciamento VTP, pois: 1) cada *switch* participa de um único domínio de gerenciamento VTP; 2) todo *switch*, dentro do mesmo domínio de gerenciamento, compartilha suas informações de VLAN; 3) *switches* em domínios diferentes, portanto, não compartilham informações VTP.

Um domínio VTP é composto por um ou mais dispositivos interconectados, que compartilham do mesmo nome de domínio VTP. As informações globais da VLAN são propagadas através de portas-troco conectadas a um *switch*, sendo que cada *switch* pode ser configurado para participar de apenas um domínio VTP.

Cada *switch* da família Catalyst, segundo Webb (2003, p. 98), anunciará em suas portas-tronco:

- O domínio de gerenciamento;
- O número da versão de configuração;
- as VLANs conhecidas e respectivos parâmetros.

Também, os *switches* podem ser configurados para que não aceitem informações VTP. Sendo assim, os *switches* são capazes de encaminhar as informações VTP recebidas em portas-troco, a fim de verificarem se os outros *switches* receberão a atualização, sem realizar alterações no seu banco de dados, e sem enviar alteração de estado na VLAN. Esse é o chamado modo transparente.

Os domínios de gerenciamento são definidos, por padrão, em um modo não seguro. Isto é, sem o uso de senha, pois, ao acrescentar uma senha, altera-se o domínio de gerenciamento para o modo seguro, mas antes de se fazer uso do modo seguro, sugere-se que haja a configuração de uma senha para cada *switch* do domínio de gerenciamento.

A figura abaixo traz um exemplo de operações VTP de adição e exclusão. Nesse caso, o C5000-3 transmite uma entrada na base de dados VTP, com acréscimos e exclusões no C5000-1 e C5000-2.

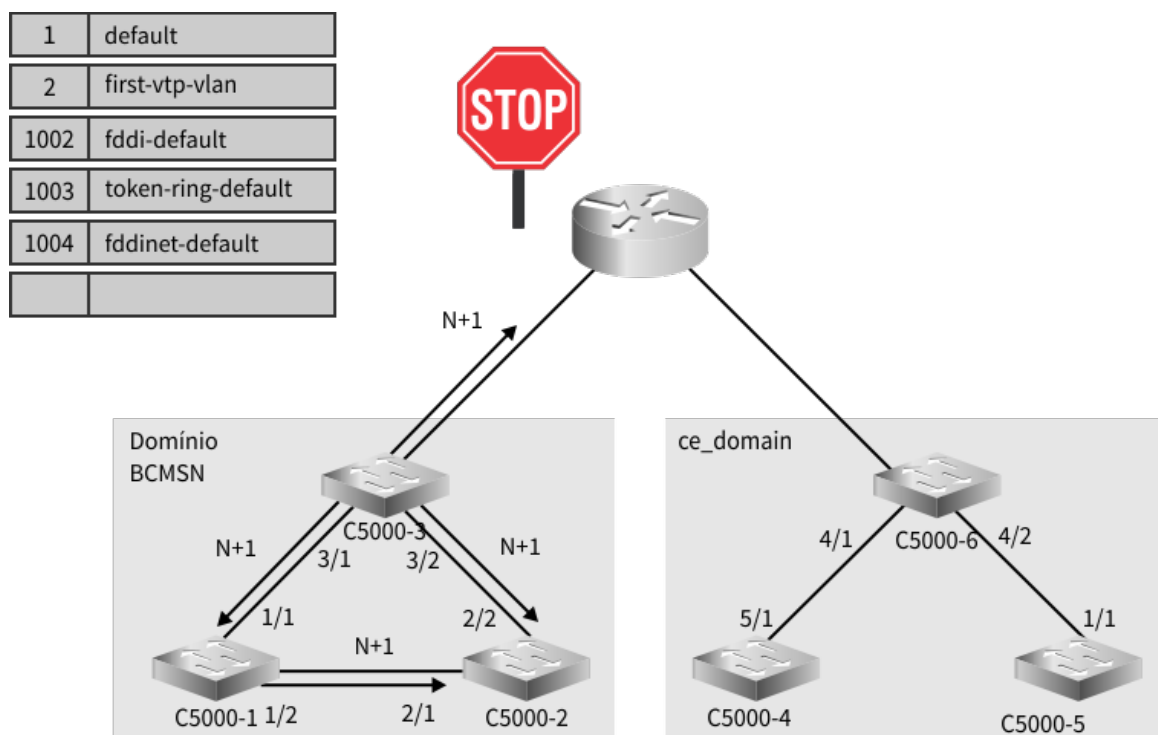


Figura 1 - Entradas na base VTP são transmitidas para outros switches no mesmo domínio.

Fonte: WEBB, 2003, p. 99.

A base de dados é configurada com um número de revisão equivalente a  $N+1$  (notificação + 1), de modo a indicar que um número de versão maior corresponde às informações de VLANs mais recentes que a cópia armazenada. Então, sempre que um *switch* receber uma atualização, com um número de revisão maior, ele substituirá as informações armazenadas pelas novas informações enviadas pela atualização VTP (CISCO, 2014).

---

## VOCÊ O CONHECE?

Robert Metcalfe e David Boggs foram pioneiros no desenvolvimento tecnológico nos Estados Unidos. Eles foram responsáveis pela criação da Ethernet, uma arquitetura de interconexão para redes locais, baseada no envio de pacotes.

---

A preparação de um *switch* para entrar em um domínio VTP pode ser realizada de acordo com as seguintes etapas:

<b>Etapas 1</b>	Digite o comando <b><i>clear config all</i></b> para remover a configuração existente, lembrando que o número de versão do VTP não será apagado.
<b>Etapas 2</b>	Desligue e ligue novamente a energia do switch, para limpar a NVRAM ( <i>Non Volatile Random-Access Memory</i> ) do VTP. Essa operação fará com que o número da versão retorne a 0 (zero), fazendo com que o novo switch propague informações incorretas.
<b>Etapas 3</b>	Determine o modo de operação VTP do switch e inclua tais informações de domínio VTP a ele. Caso seja definido o modo servidor, o padrão e mais comum, é preciso certificar-se que a configuração do número de versão foi definida para 0, antes de acrescentar o switch ao domínio VTP.

Quadro 1 - Etapas para preparação de um switch para entrar em um domínio VTP.  
Fonte: Elaborado pela autora, baseado em WEBB, 2003.

Há três tipos de operação VTP: servidor, cliente e transparente. O modo servidor VTP é considerado o padrão. O comutador permanece no estado de domínio, sem gerenciamento, até que um anúncio seja recebido, através de um *link* de tronco. Outra opção seria configurar o domínio de gerenciamento. Além do modo servidor, pode-se configurar um *switch* da família Catalyst para operar nos seguintes modos VTP:

Servidor (Server)
Servidor VTP é o modo padrão. Ele permite criar, alterar e excluir VLANs. Ademais, possibilita especificar outros parâmetros de configuração, como a versão VTP e a poda VTP, para todo o domínio VTP. Os servidores VTP anunciam a sua configuração para os outros switches, do mesmo domínio VTP, e sincronizam a configuração de VLANs com os outros switches, tendo como base os anúncios recebidos através de enlaces de tronco.
Cliente (Client)
Os clientes VTP possuem comportamento semelhante aos servidores VTP. Contudo, ele não permite criar, alterar ou excluir VLANs em um cliente VTP.
Transparente (Transparent)
Os switches VTP transparentes não participam do VTP. Ou seja, assim como ele não anuncia a sua configuração VLAN, da mesma forma não sincroniza a sua configuração VLAN, com base nos anúncios recebidos.
Desligado (Off)
No modo VTP desligado, o funcionamento de um dispositivo se assemelha ao modo VTP transparente. No entanto, não é capaz de encaminhar anúncios VTP.

Quadro 2 - Modos VTP que podem operar um Switch família .

Fonte: Elaborado pela autora, 2019.

### 3. 1. 1 Anúncios e mensagens VTP

No VTP, cada *switch* é responsável por anunciar o seu domínio de gerenciamento e o número da versão da configuração, bem como as informações sobre as VLANs conhecidas e os parâmetros em suas portas-tronco. Esses são os chamados anúncios VTP.

Os quadros de anúncios VTP são enviados para um grupo de dispositivos (conhecido como endereço *multicast*), que permite a transmissão dessa informação para múltiplos destinatários de maneira simultânea.

Dessa forma, todos os dispositivos vizinhos recebem a mesma informação. Isso significa que todos os dispositivos, pertencentes a um mesmo domínio de gerenciamento, serão informados sobre quaisquer novas VLANs que sejam configuradas no dispositivo de transmissão. Em outras palavras, as informações serão apreendidas automaticamente pelos outros dispositivos no mesmo domínio de gerenciamento (CISCO, 2014).

Cada anúncio é iniciado tendo 0 como o número da versão de configuração. À medida que alterações são executadas, o número da versão é aumentado em uma unidade ( $n+1$ ). Os anúncios nas VLANs padrão baseiam-se nos tipos de cabo e as portas do usuário não são configuradas como troncos VTP.

Podemos considerar que há dois tipos de anúncios e três tipos e mensagens, conforme o quadro:

<b>Tipos de anúncios</b>	<ul style="list-style-type: none"><li>· Requisições de clientes que desejam informações no momento da inicialização.;</li><li>· Respostas de servidores.</li></ul>
<b>Tipos de mensagens</b>	<ul style="list-style-type: none"><li>· Requisições de anúncios por clientes.</li><li>· Anúncios de sumários.</li><li>· Anúncios de subconjuntos.</li></ul>

Quadro 3 - Tipos de anúncios e mensagens VTP.

Fonte: Elaborado pela a autora, baseado em WEBB, 2003.

Nas requisições de anúncios por clientes, os clientes requisitam informações de VLAN e o servidor responde com um índice e um anúncio de subconjuntos. Os anúncios de sumários acontecem a cada 300 segundos na VLAN1, e sempre que ocorrer qualquer alteração na topologia. Finalmente, os Anúncios de subconjuntos trazem informações detalhadas sobre VLANs.

A demonstração da figura a seguir, ajudará a ilustrar a diferença entre os tipos de conteúdo dos anúncios VTP.



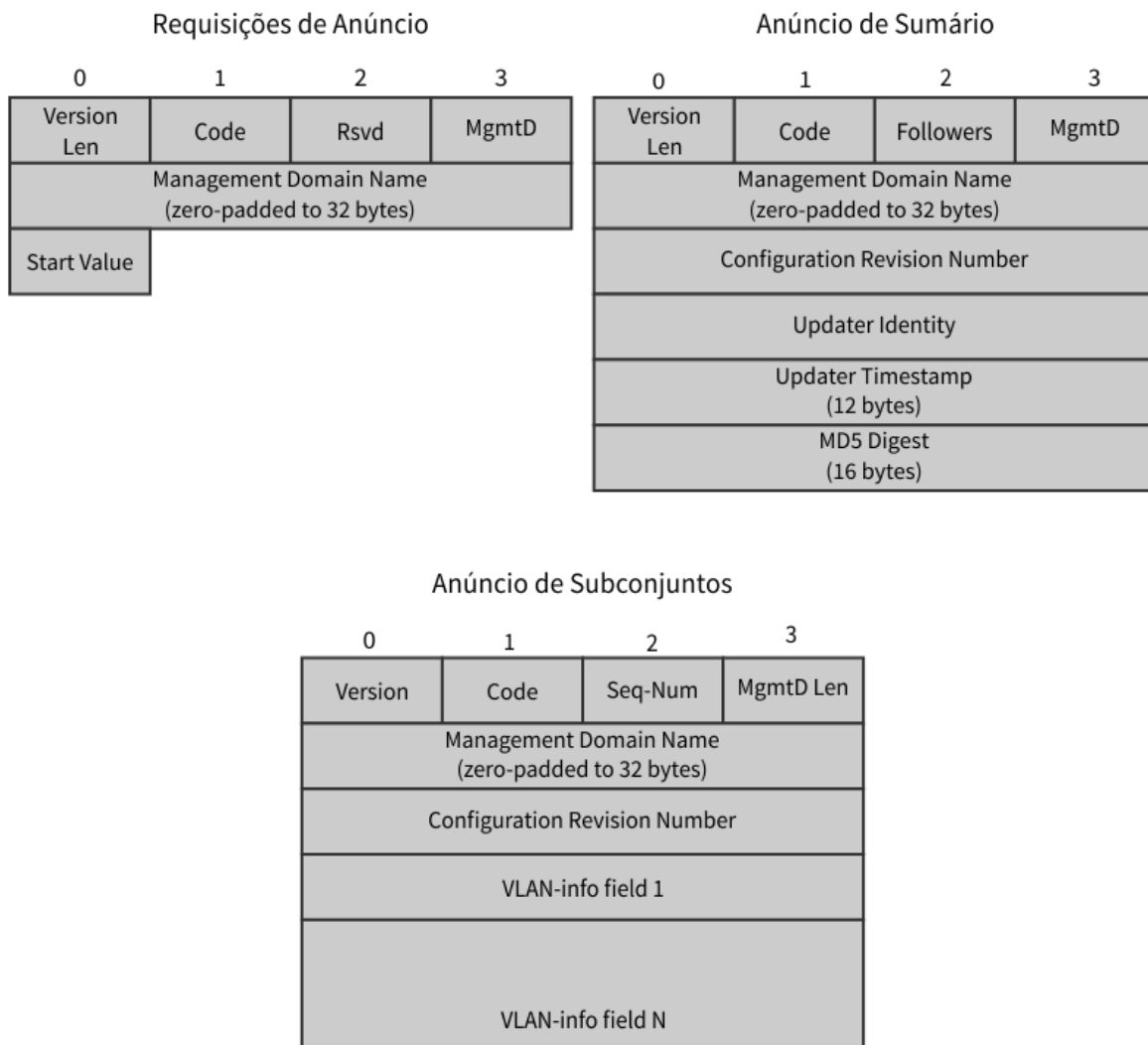


Figura 2 - Os três tipos de anúncios VTP – requisições, sumários e subconjuntos.

Fonte: WEBB, 2003, p. 101.

Ainda, os anúncios podem exibir informações como as descritas abaixo. Clique e confira!

•

Management Domain Name (Nome do  
Domínio de Gerenciamento).

•

Configuration      Revision      Number  
(Número de Versão da Configuração).

•

## MD5 Digest.

•

## Updater Identity (Identidade do Atualizador).

Identificando o nome do domínio de gerenciamento, anúncios com nomes diferentes serão ignorados. O número de versão da configuração serve de parâmetro para identificar a configuração. Quanto maior o número, mais recente será a configuração. O *MD5 Digest* é a chave que é enviada com o VTP, quando uma senha for a ele atribuída. A atualização será ignorada, caso a chave não coincida. A identidade do atualizador do *switch* é a responsável pelo envio do anúncio de sumário VTP.

É importante salientar que o número de versão da configuração é um dos componentes mais importantes nos anúncios VTP. Sempre que um servidor VTP alterar a sua base de dados, será acrescido o número da versão em uma unidade ( $n+1$ ). Então, o servidor anunciará à sua base de dados o novo número de versão da configuração. Caso o número seja maior do que o número armazenado nos outros dispositivos do domínio VTP, o *switch* fará uma requisição para que o atualizador envie um anúncio de subconjuntos. O anúncio de subconjuntos exibe detalhes das VLANs, armazenados pelo atualizador na sua NVRAM. Os *switches* farão as alterações em suas bases de dados, a partir das novas informações anunciadas.

### 3. 1. 2 Diretrizes de configuração VTP

Antes de dar início à configuração, sugere-se que algumas etapas sejam cumpridas (CISCO, 2014):

Etapa 1	Determinar o número de versão VTP que será executado em seu ambiente.
Etapa 2	No caso de inserção de um novo switch, é imprescindível estabelecer se ele será membro de um domínio de gerenciamento existente, ou se um novo domínio deverá ser criado para ele. Se o domínio de gerenciamento já existir, o próximo passo será criar o seu nome e senha.
Etapa 3	Escolher um modo VTP para o switch.

Quadro 4 - Etapas para a configuração de VTP.

Fonte: Elaborado pela autora, baseado em CISCO, 2014.

Duas versões VTP diferentes podem ser executadas no seu domínio de gerenciamento: o VTP versão 1 e o VTP versão 2, lembrando que ambas não são capazes de operar em conjunto. O VTP versão 1 é considerado o modo padrão.

Clique nas setas e aprenda mais sobre o tema.

Já para definir o modo do seu *switch*, o comando será:

O funcionamento de um para outro não difere muito, a não ser pelo fato de que o VTP versão 2 tem a capacidade de introduzir o apoio para VLAN de *token ring*. O *Token Ring* é um protocolo de redes que opera na camada física e de enlace e que circula numa topologia em anel, com três *bytes*, em que as estações devem aguardar sua recepção para depois realizar a transição.

Ao configurar um *switch* no domínio para o VTP versão 2, faz-se necessário configurar todos os *switches* no domínio de gerenciamento para o VTP versão 2. Para a alteração do número de versão VTP, utilize o comando *set vtp v2 enable*.

De acordo com Webb (2003, p.104), para criar um domínio de gerenciamento ou unir-se a um domínio de gerenciamento, utiliza-se seguinte comando (WEBB, 2003, p. 104):

```
Switch (enable) set vtp domain nome-do-domínio password senha
```

```
Switch (enable) set vtp domain nome-do-domínio mode [server | cliente | transparente]
```

O primeiro *switch Catalyst* do domínio de gerenciamento deve ser definido para o modo servidor, para que outros *switches* possam ser adicionados posteriormente. Sendo assim, os *switches* adicionais serão capazes de obter as informações de VLAN do primeiro *switch*.

É importante ressaltar que é indispensável que haja um servidor, no mínimo.

Caso haja outros *switches Catalyst* no seu domínio de gerenciamento, defina o modo do seu *switch* para cliente e, em seguida, desligue o *switch*. Essa medida é indicada para evitar que o novo *switch* propague informações incorretas sobre a sua rede.

Opta-se pelo modo transparente, se o *switch* não for compartilhar informações de VLAN com outros *switches* da rede, permitindo que VLANs sejam criadas, excluídas e renomeadas, sem que tais alterações sejam propagadas para os outros *switches*.

Utiliza-se o comando *set vtp domain* para alterar o modo VTP de local para servidor (WEBB, 2003, p. 105), sendo ele: Switch (enable) set vtp domain bcmsn\_block2 mode server VTP domain bcmsn\_block2 has been modified.

O comando *show vtp domain* é útil para verificar o número de versão da configuração atual.

```
switch (enable) show vtp domain
```

Domain Name	Domain Index	VTP Version	Local Mode Password
-----	-----	-----	-----
bcmsn_block2	1	2	server -
Vlan-count	Max-vlan-storage	Config Revision	Notifications
-----	-----	-----	-----
33	1023	0	disabled
Last Updater	V2 Mode	Pruning	PruneEligible on Vlans
-----	-----	-----	-----
172.20.52.124	disabled	disabled	2-1000

Figura 3 - Exemplo do comando `show vtp domain`.

Fonte: WEBB, 2003, p. 105.

A figura acima traz um exemplo de uso do comando `show vtp domain`, com a configuração mostrada anteriormente.

### 3. 1. 3 Poda de VTP

Os *broadcasts*, por padrão, são enviados para cada um dos *switches* que tenha um enlace de tronco, de modo a sobrecarregar a VLAN, mesmo que o *switch* não tenha nenhuma porta nesta VLAN. Isso quer dizer que os enlaces de tronco transmitem o tráfego de *broadcast* que, posteriormente será descartado pelo *switch*.

A fim de aprimorar o uso da largura de banda da rede e, por consequência, reduzir a retransmissão de tráfego desnecessários – como *broadcasts*, *multicasts* e *unicasts* desconhecidos – há a chamada poda VTP (VTP *pruning*). Por padrão, a poda VTP fica desativada (CISCO, 2014).

A Figura a seguir mostra uma rede de *switches* com a poda VTP desativada. Dessa forma, a Porta 1 do *Switch* 1 e a Porta 2 do *Switch* 4 foram atribuídas à VLAN 10. Além disso, um *broadcast* é emitido do *host* conectado ao *Switch* 1.

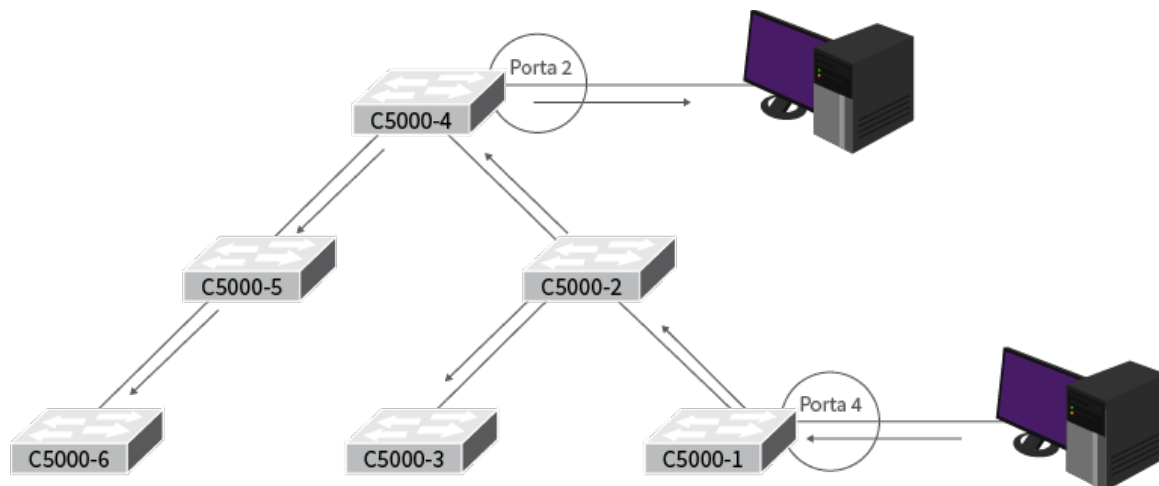


Figura 4 - Uma rede de switches com a poda VTP desativada.

Fonte: WEBB, 2003, p. 107.

O Switch 1 retransmite o *broadcast* e, por conseguinte, todos os switches desta rede o recebem; embora os Switches 3, 5 e 6 não tenham portas na VLAN 10.

A próxima figura traz a mesma rede comutada, mas, desta vez, com a poda VTP ativada.

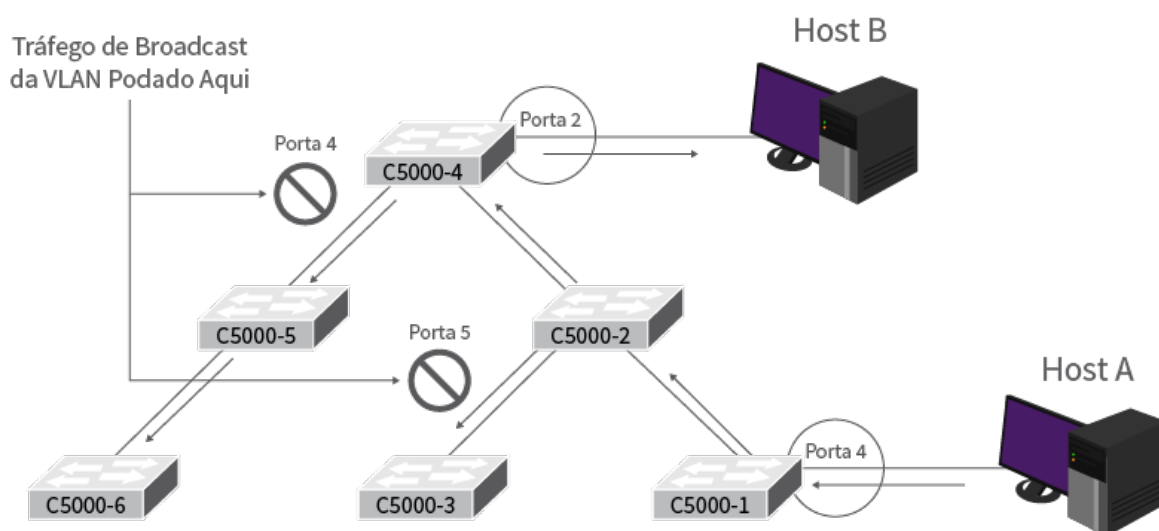


Figura 5 - Uma rede de switches com a poda VTP ativada.

Fonte: WEBB, 2003, p. 107.

O tráfego de *broadcast* do Switch 1 não é encaminhado para os Switches 3, 5 e 6, pois o tráfego para a VLAN 10 foi podado nos enlaces indicados. Isto é, nas portas 5 (no switch 2) e 4 no (switch 4).

Ao ativar a poda VTP em um servidor VTP, permite-se a poda em todo o domínio de seu respectivo gerenciamento.

As VLANs de 2 a 1000, por padrão, são passíveis de poda. O VTP *pruning* não poda o tráfego de VLANs que não sejam passíveis de poda. Por exemplo, a VLAN1 nunca é passível de poda.

```
switch (enable) show trunk 1/1
```

Port	Mode	Encapsulation	Status	Native vlan
1/1	desirable	isl	trunking	1

Port	Vlans allowed on trunk
1/1	1-100,250,500-1005

Port	Vlans allowed and active in management domain
1/1	1,521-524

Port	Vlans in spanning tree forwarding state and not pruned
1/1	1,521-524

Figura 6 - O comando `show trunk` verifica se as VLANs são podadas.

Fonte: WEBB, 2003, p. 108.

Existe também a opção de tornar determinadas VLANs passíveis ou não passíveis de poda no dispositivo. O comando `show trunk` é utilizado para a verificação das VLANs, se são podadas ou não. A figura acima demonstra o que pode resultar desse comando.

---

## VAMOS PRATICAR?

Até aqui você aprendeu que para executar a adição, e renomeação de VLANs de um mesmo domínio VTP e, a tempo, manter a consistência de sua configuração, o VTP funciona em quadros de troncos. Ou seja, um domínio VTP – ou de gerenciamento de VLAN – é composto por um ou mais dispositivos de rede que compartilham o mesmo nome de domínio VTP e estão interconectados com troncos. Sendo assim, o VTP possibilita a elaboração de alterações centralizadas, as quais serão comunicadas a todos os outros *switches* da rede, minimizando a possibilidade de surgimento de inconsistências a partir das alterações. Configurações incorretas ou inconsistentes podem resultar em violação de segurança, tais como: nomes de VLAN duplicados, especificações incorretas do tipo de VLAN, entre outros problemas. (CISCO, 2014). Também demonstramos que pode-se configurar um *switch* Cisco Catalyst para operar nos seguintes modos VTP:

**Servidor (*Server*)** – Servidor VTP é o modo padrão. Ele permite alterar e excluir VLANs. Ademais, possibilita especificar parâmetros de configuração, como a versão VTP e a poda de todo o domínio VTP. Os servidores VTP anunciam a sua configuração para os outros *switches*, do mesmo domínio VTP, e sincronizam a configuração de VLANs com os outros *switches*, tendo como base os anúncios recebidos através de enlaces de tronco.

**Cliente (*Client*)** – Os clientes VTP possuem comportamento semelhante aos servidores VTP. Contudo, ele não permite alterar ou excluir VLANs em um cliente VTP.

**Transparente (*Transparent*)** – Os *switches* VTP transparentes participam do VTP. Ou seja, assim como ele não anuncia sua configuração VLAN, da mesma forma não sincroniza sua configuração VLAN, com base nos anúncios recebidos.

**Desligado (*Off*)** – No modo VTP desligado, o funcionamento do dispositivo se assemelha ao modo VTP transparente. No entanto, ele não permite encaminhar anúncios VTP. (WEBB, 2003).

Você também aprendeu que os *broadcasts*, por padrão, são encaminhados para cada um dos switches que tenha um enlace de tronco, a fim de carregar a VLAN, mesmo que o switch não tenha nenhuma interface nesta VLAN. Isso quer dizer que os enlaces de tronco transportam tráfego de broadcast que, embora seja posteriormente descartado pelo switch. A fim de aprimorar o uso da largura de banda e, por consequência, reduzir a retransmissão de tráfego desnecessário – como *broadcasts*, *multicasts* e *unicasts* desconhecidos – é realizada a poda VTP (*VTP pruning*). (CISCO, 2014).

Após aprender e revisar todos esses passos, com as respectivas configurações, te convidamos a exercitar os conhecimentos adquiridos. Procure analisar o conteúdo estudado e identificar

executando as diretrizes e configurações aprendidas situação real. As questões que seguem são norteadoras para a construção de seu conhecimento. Ao respondê-las, faça em forma de um passo-a-passo, descrevendo detalhadamente o funcionamento das operações.

1. Explique como o VTP permite a propagação dos dados por meio das redes.
  2. Enumere os modos de operação VTP e descreva o funcionamento de cada qual.
  3. Como funciona a poda VTP?
- 

Ao finalizar o tópico 3.1, você aprendeu sobre o conceito e a função do VTP, que é reduzir a administração em uma rede comutada. Ao configurar uma nova VLAN a um servidor VTP, a VLAN será distribuída a todos os interruptores do domínio, de modo a facilitar o gerenciamento da rede, mantendo a consistência da sua configuração. Você também aprendeu que a poda VTP consiste em aprimorar o uso da largura de banda da rede e, por consequência, reduzir a retransmissão de tráfegos desnecessários – como *broadcasts*, *multicasts* e *unicasts* desconhecidos.

Desse modo, o VTP, segundo Webb (2003, p. 97), fornece as seguintes vantagens:

- consistência da configuração de VLAN em toda a rede;
- esquema de mapeamento atravessando *backbones* de cabeamento misto, mapeando VLANs Ethernet a uma VLAN em um *backbone* de alta velocidade (como ATM LANE ou FDDI), que permite que uma VLAN exista em um tronco sobre cabeamento misto;
- rastreamento e monitoramento preciso de VLANs;
- anúncio dinâmico de VLANs adicionadas à rede;
- configuração *plug-and-play* ao acrescentar novas VLANs.

## 3.2 EtherChannel: conceitos e VTP com EtherChannel

O EtherChannel é uma tecnologia desenvolvida pela Cisco que tem como objetivo agrupar vários *links* de porta, ou promover a arquitetura de canal de porta. Na prática, ele agrupa vários *links* Ethernet físicos, a fim de criar um *link* Ethernet lógico, com a finalidade de aprimorar a tolerância à falhas e links de alta velocidade entre *switches*, roteadores e servidores. O EtherChannel é usado em redes de *backbone*, principalmente, mas pode também ser utilizado para conectar máquinas de usuários finais.



---

## VOCÊ QUER VER?

A Cisco Systems é uma companhia transnacional dos Estados Unidos. A principal atividade da Cisco é a criação de soluções para redes e comunicações, com destaque na fabricação e venda de roteadores e *switches*. Assista ao vídeo *Cisco History Timelin*, disponível no site da Cisco, sobre a trajetória da empresa, de 1984 a 2013. Você poderá vê-lo acessando: [https://www.cisco.com/c/pt\\_br/about.html?socialshare=lightbox1](https://www.cisco.com/c/pt_br/about.html?socialshare=lightbox1) (https://www.cisco.com/c/pt\_br/about.html?socialshare=lightbox1)>.

---

Podem ser criadas entre duas e oito portas *Fast*, *Gigabit* ou *10-Gigabit Ethernet* ativas, mais oito portas inativas (*failover*) que se tornam ativas, quando alguma das ativas anteriormente falhar. A maior vantagem sobre o uso de um EtherChannel refere-se à largura de banda. Além de oferecer a estabilidade de largura de banda *full-duplex*, entre 200 Mbps e 800 Mbps, também proporciona o compartilhamento de carga e redundância, promovendo o balanceamento de carga e gerenciamento de cada enlace, ao distribuir o tráfego através dos vários enlaces do canal (CISCO, 2014).

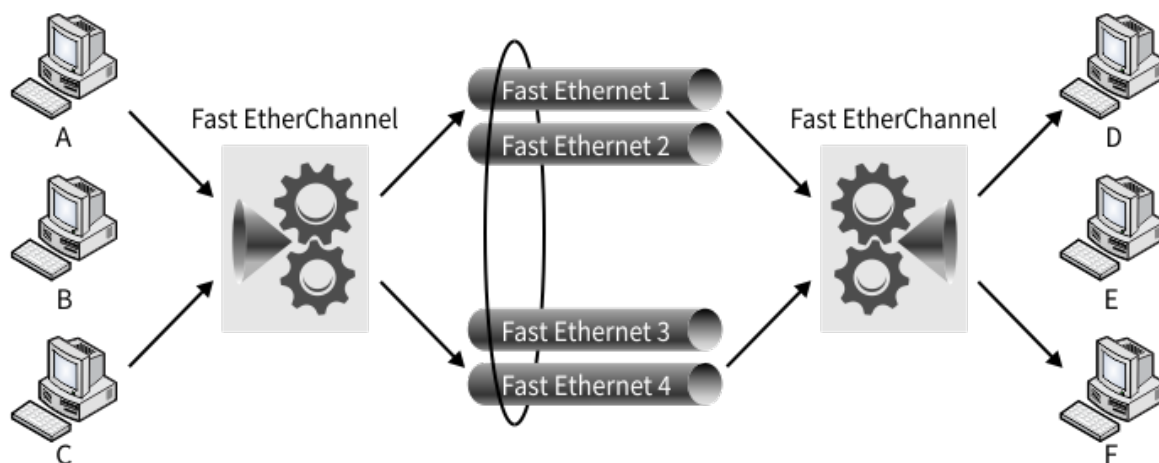


Figura 7 - Enlaces paralelos Fast Ethernet.

Fonte: WEBB, 2003, p. 147.

Dessa forma, pressupõe-se uma mistura de tráfego, pois as diversas velocidades não se limitam apenas a um único aplicativo. O tráfego *unicast*, *multicast* e *broadcast* é distribuído por meio dos enlaces do canal. Para tanto, o EtherChannel fornece a redundância, caso exista uma falha no enlace. Caso um enlace seja perdido, o tráfego será roteado novamente para outro enlace, e a convergência será transparente para o usuário.

Ao configurar um EtherChannel, todos os adaptadores que compõem o canal passam a compartilhar o mesmo endereço da Camada 2. Nesse contexto, o EtherChannel torna-se transparente, por reconhecer uma única conexão lógica.

O EtherChannel é bastante escalonável, à medida que aproveita a fiação já existente. Todos os *switches* da Cisco suportam a tecnologia EtherChannel, portanto, podem ser utilizados em todos os níveis da rede, para criar *links* de largura de banda mais altos, de acordo com a necessidade de tráfego da rede.

---

## VOCÊ QUER VER?

*Black Mirror* é uma série de TV britânica de ficção científica, criada por Charlie Brooker. O enredo aborda as consequências trazidas pelas novas tecnologias de informação e comunicação. Ao *The Guardian*, Brooker declarou: “Se a tecnologia é uma droga – e parece ser – então, quais são, mais precisamente, os seus efeitos colaterais? Essa área, entre o prazer e o desconforto, é onde *Black Mirror* se passa. Para assistir a esse episódio, acesse: <<https://www.netflix.com/search?q=black%20mirror> (<https://www.netflix.com/search?q=black%20mirror>)>.

---

O Fast EtherChannel e o Gigabit EtherChannel, segundo Webb (2003, p. 147), usam um algoritmo de distribuição de carga com base no endereço MAC (*Media Access Control*) de destino, de acordo com a figura abaixo:

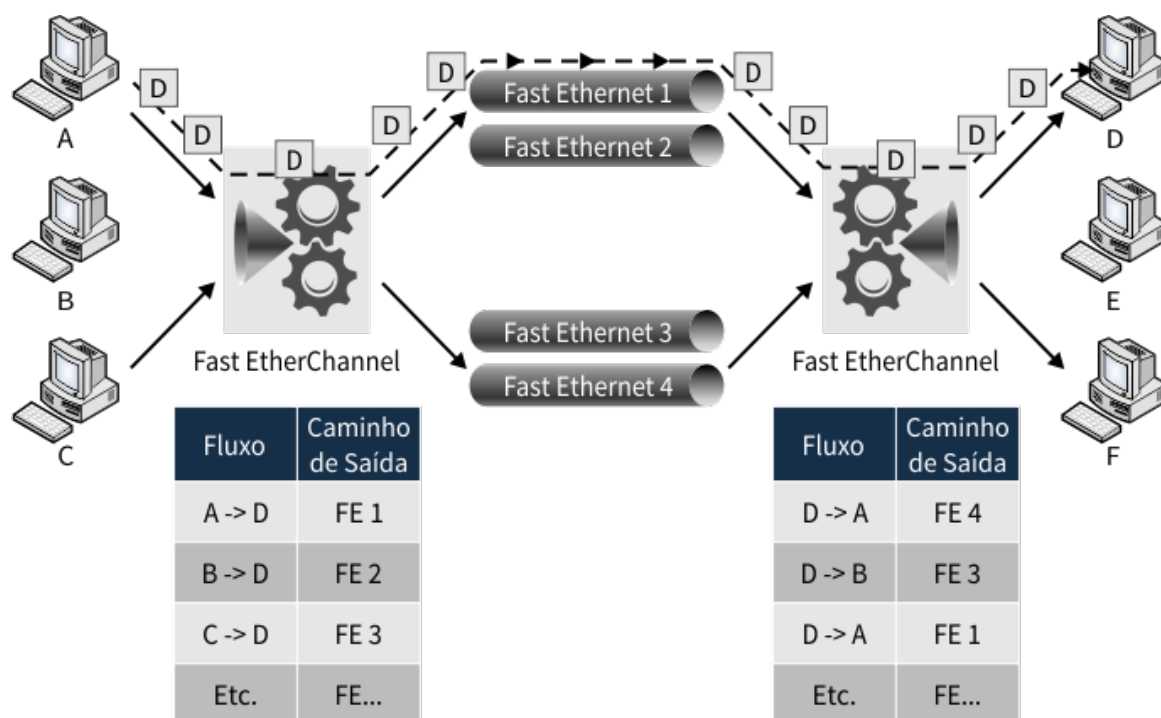


Figura 8 - Fast EtherChannel e Gigabit EtherChannel usam a distribuição de carga para compartilhar os enlaces.

Fonte: WEBB, 2003, p. 147.

Agora, clique nas abas abaixo para conhecer mais sobre o tema.

<b>Bundle</b>	<i>Bundle</i> é um grupo de enlaces gerenciados pelo processo Fast EtherChannel. Essa tecnologia permite a distribuição estática de carga nas conexões de enlaces múltiplos. Quando um enlace falha, o <i>Ethernet Bundle Controller</i> (EBC) informa a entrada <i>Enhanced Address Recognition Logic</i> (EARL) sobre a falha.
<b>EARL</b>	Dessa forma, o EARL interpretará todos os endereços por ele apreendidos no enlace como obsoletos. Tais condições permitem que o EBC e o EARL recalculam o par de endereços destino-origem em um enlace diferente. Assim que o endereço de origem consultar, e o destino responder, o endereço será assimilado por outro enlace.
<b>PAgP</b>	O PAgP ( <i>Port Aggregation Protocol</i> ) tem como finalidade auxiliar na criação de enlaces Fast EtherChannel. Ele é capaz de identificar quem são seus vizinhos, bem como seu potencial de agrupamento, repassando essa informação para os vizinhos indicados.

Depois de determinar os enlaces ponto-a-ponto, paralelos e bidirecionais, o protocolo

agrupa as portas que possuem o mesmo ID e a mesma capacidade de agrupamento do dispositivo vizinho, em um único canal.

O PAgP possui algumas restrições. Por exemplo, ele não forma um grupo nas portas que estão configuradas para VLANs dinâmicas (criadas e alteradas dinamicamente via *software*, através de um servidor e de um banco de dados dos membros das VLANs). Todas as portas do canal devem pertencer a mesma VLAN. Ou, ainda, podem ser configuradas como portas-tronco.

### 3.2.1 Diretrizes para a configuração do EtherChannel

É importante que algumas diretrizes sejam seguidas para a configuração do EtherChannel, para que não haja falhas nas portas. Algumas portas podem ser desativadas automaticamente, caso erros ocorram, a fim de evitar loops de rede, entre outros problemas.

1	Atribua todas as portas de um canal à mesma VLAN. Outra opção seria configurá-las como portas-tronco;
2	Se o canal for configurado como tronco, altere todas as portas do canal para o modo tronco também, para uma e outra porta do enlace;
3	Configurar todas as portas de um canal para que operem na mesma velocidade, bem como em modo duplex ( <i>full</i> ou <i>half</i> );
4	Ao optar pela limitação do <i>broadcast</i> nas portas, configure-o com um limite de porcentagem, para evitar o descarte de pacotes <i>unicast</i> quando a capacidade de <i>broadcast</i> é ultrapassada;
5	Se o canal for composto de portas-tronco, as VLANs, em seu conjunto, deverão receber permissão em todas suas portas. Em contrapartida, se o conjunto permitido não for o mesmo, para todos os troncos do canal, as portas-tronco irão ignorar os pacotes destinados à VLAN não permitida. Nas portas que a VLAN receber permissão, o tráfego continuará sendo transmitido;
6	Sugere-se que as portas de um canal não sejam configuradas como portas de VLANs dinâmicas, para que não afete o desempenho do switch;
7	Conferir se a segurança da porta está desativada nas portas do canal;
8	Ativar todas as portas de um canal, para que não ocorram falhas de enlace;
9	Certificar se todas as portas em um canal têm a mesma configuração, nas duas pontas do canal;
10	O <i>hardware</i> que controla os canais dos switches Catalyst 5XXX trabalha no sentido de evitar que certas portas (ou grupos de portas) formem canais;
11	Verificar se uma placa de linha tem a capacidade de compor um canal em um switch Catalyst 5XXX (WEBB, 2003, p. 149):  Switch>(enable)show port capabilities [ módulo/porta ]

Quadro 5 - Algumas diretrizes para a configuração do EtherChannel.

Fonte: Elaborado pela autora, baseado em WEBB, 2003.

Para finalizar, é importante frisar que determinadas condições devem ser cumpridas com rigor, para que o grupo EtherChannel esteja ativo. Caso contrário, as portas podem ser desativadas automaticamente.

### 3.2.2 PortFast, UplinkFast e BackboneFast: conceito e configuração

O *Spanning Tree Protocol* (STP) é um protocolo executado em todas as portas de um *switch*. Na prática ele determina que cada porta aguarde alguns segundos, antes de permitir o envio de dados.

Com o intuito de minimizar problemas decorrentes de protocolos como esse, algumas medidas podem ser tomadas, como a implementação do *PortFast*. Vale lembrar que o *PortFast* deve ser usado apenas em conexões de servidores ou em estações de trabalho, vide ilustração abaixo. Caso contrário, corre-se o risco de criar um *loop* na rede.

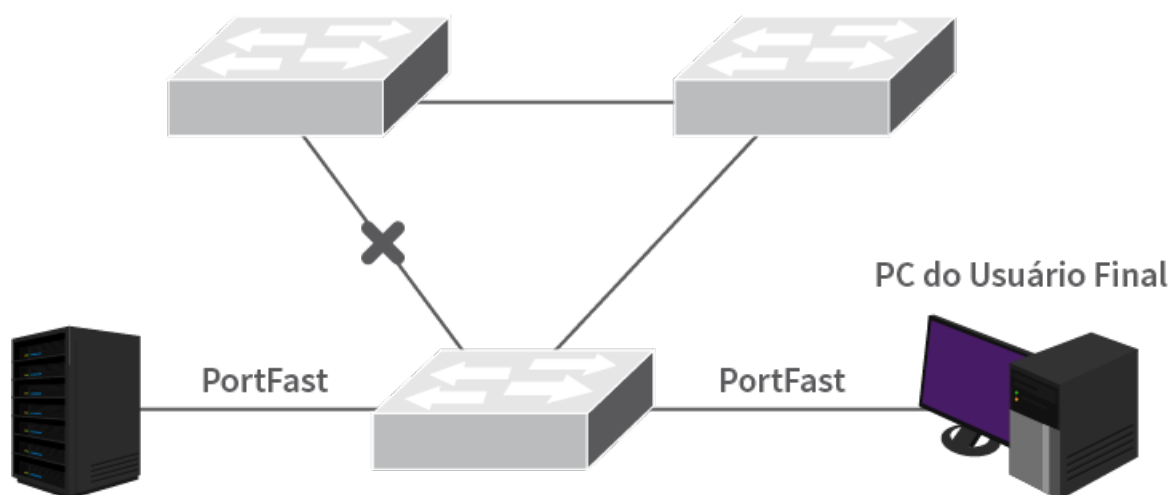


Figura 9 - A implementação do PortFast diminui o tempo que uma porta fica nos estados de escuta e de aprendizado.

Fonte: WEBB, 2003, p. 150.

O STP atua na garantia da manutenção de uma topologia sem *loops*. Para que o mecanismo de convergência não acarrete demora no processo, o *UplinkFast* pode ser implementado. Ele permite que uma porta de um *switch* no estado bloqueado dê início ao encaminhamento dos pacotes, assim que falhas sejam detectadas no enlace.

Um grupo de *uplink* é formado a partir da porta raiz (responsável pelo encaminhamento) e um conjunto de portas no estado bloqueado. Sendo assim, o grupo de *uplink* terá a competência para indicar um caminho alternativo, no caso de falhas no enlace.

O recurso STP *UplinkFast* foi projetado para atuar somente com *switches* da camada de acesso. No exemplo abaixo, o *switch* de acesso tem dois *uplinks* para a camada de distribuição.

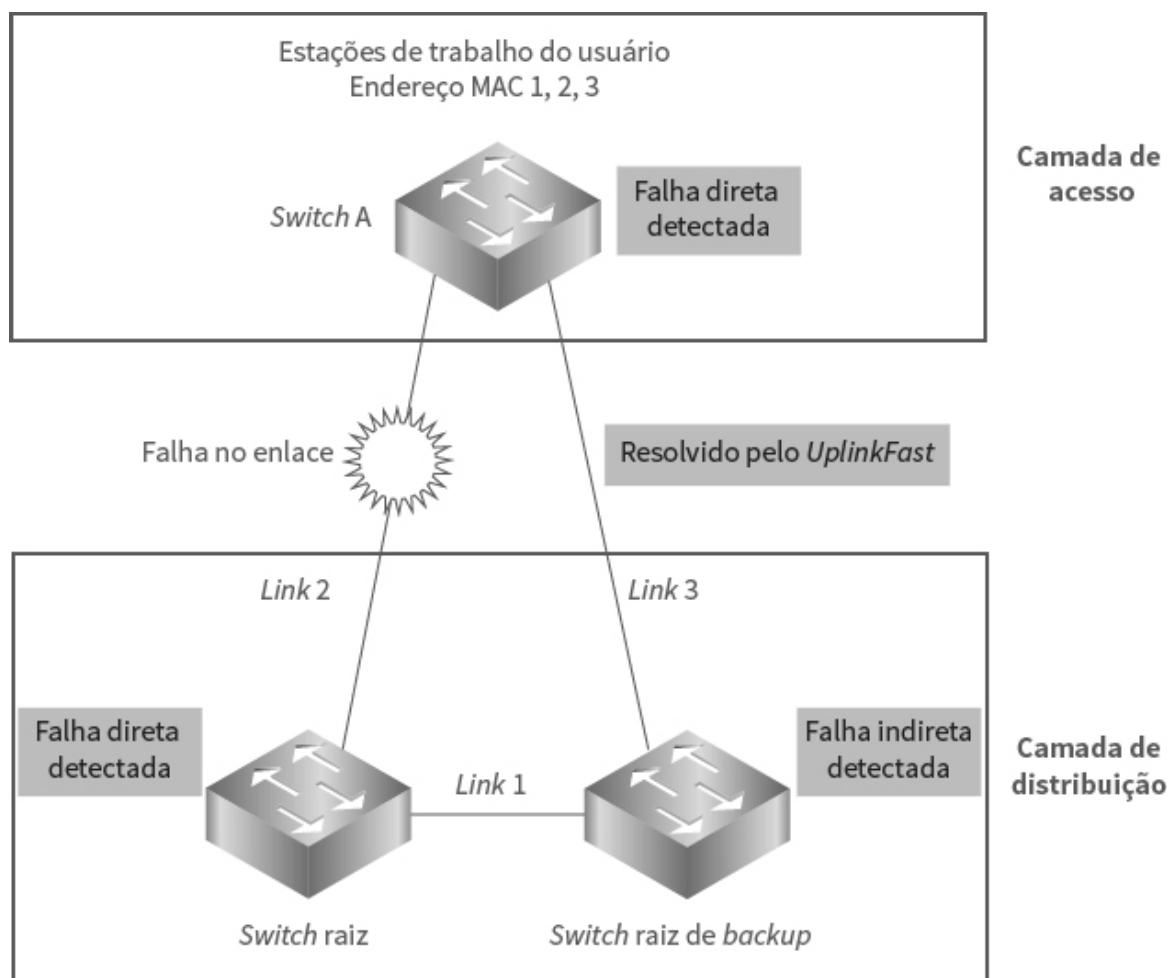


Figura 10 - Visualização do funcionamento do Uplink Fast.

Fonte: WEBB, 2003, p. 152.

No exemplo acima, um dos *uplinks* foi bloqueado pelo STP, por ser redundante. O *switch*, ao constatar que o enlace ativo fora derrubado, fará com que o *UplinkFast* permita que a porta bloqueada passe para o estado de encaminhamento. Consequentemente, o tempo de convergência será reduzido.

O *BackboneFast* é acionado em um *switch* quando uma porta raiz, ou uma porta em estado bloqueado, recebe uma BPDUs (*Bridge Protocol Data Unit*) inferior. Isso significa que algum enlace indireto falhou. Isto é, que a *bridge* escolhida perdeu a conexão com a *bridge* raiz. Nessas condições, o *switch* procura sugerir um caminho alternativo para a *bridge* raiz. Clique e confira!

•

Se a BDPUs inferior chegar a uma porta em estado bloqueado, a porta raiz e outras portas que estiverem no estado

bloqueado tornar-se-ão rotas alternativas para a bridge raiz.

.

Se a BDPU inferior chegar à porta raiz, as portas que estiverem no estado bloqueado servirão como caminhos alternativos para a bridge raiz.

.

Se a BDPU inferior chegar à porta raiz e não existirem portas no estado bloqueado, o switch entenderá que a conectividade com o bridge raiz foi perdida. Vencendo o prazo de vida na raiz, outro switch será considerado o raiz, conforme as regras do Spanning Tree.



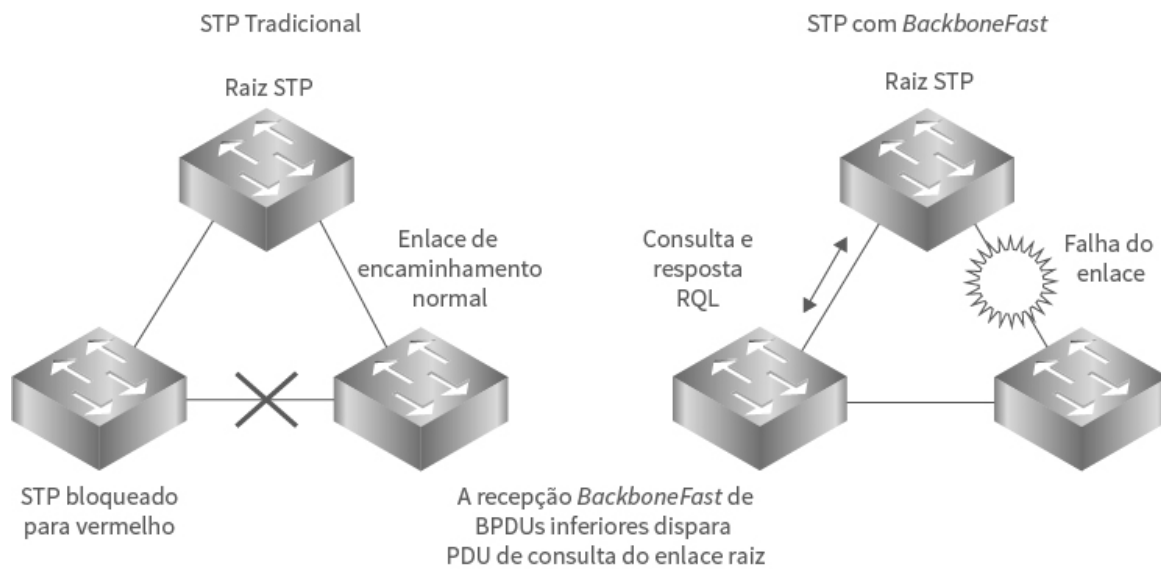


Figura 11 - Exemplo de uma falha de enlace indireto.

Fonte: WEBB, 2003, p. 155.

Ao finalizar o tópico 3.2, você aprendeu que o EtherChannel é uma tecnologia que permite agregar o *link* de porta, ou promover a arquitetura de canal de porta e que o PAgP (*Port Aggregation Protocol*) tem como finalidade auxiliar na criação de enlaces Fast EtherChannel.

---

## VAMOS PRATICAR?

Como vimos até aqui, o EtherChannel é uma tecnologia desenvolvida pela Cisco que tem como objetivo agregar o *link* de rede para promover a arquitetura de canal de porta. Na prática, ele agrupa vários *links* Ethernet físicos, a fim de criar um *link* lógico, com a finalidade de aprimorar a tolerância a falhas e de alta velocidade entre *switches*, roteadores e servidores.

Já o Protocolo de Agregação de Porta (PAgP), auxilia na configuração de enlaces Fast EtherChannel, sendo capaz de identificar os seus vizinhos, bem como seu potencial de agrupamento, e repassar esta informação para os vizinhos indicados. (WEBB, 2003).

Considerando a breve revisão de conteúdo que apresentamos, te convidamos a exercitar os conhecimentos adquiridos analisando o conteúdo estudado, tendo em vista a importância do conhecimento em uma situação real de configuração e, por seu conhecimento prático, procure responder as questões a seguir.

1. O que é o EtherChannel e para que ele serve?
  2. Qual a finalidade do Protocolo de Agregação de Porta (PAgP)?
- 

## 3.3 Desafios em ambientes simulados

---

Depois de ter estudado a parte teórica sobre o VLAN Trunking Protocol (VTP) e o EtherChannel, é hora de materializar o conhecimento construído, a fim de aprimorá-lo na prática.

O exemplo proposto por Webb (2003, p. 109-118), mostrará para você como configurar VLANs em cada um dos *switches* da camada de acesso, bem como criar VLANs nos segmentos que fazem a conexão entre os *switches* da camada de distribuição e, também, camada de núcleo. Além disso, demonstrará como configurar troncos em todos os *uplinks* dos *switches* da camada de distribuição para os *switches* da camada de acesso.

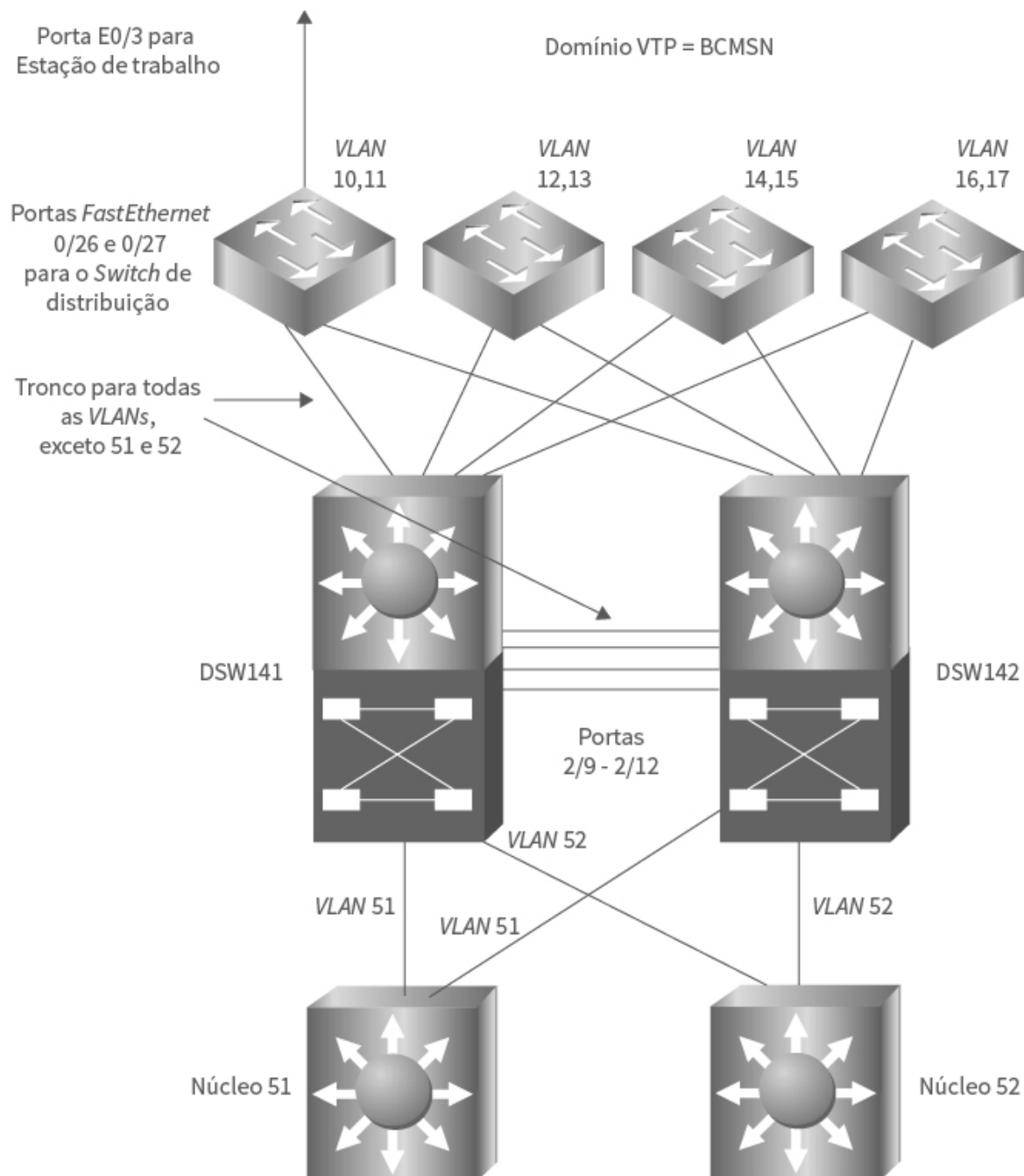


Figura 12 - Valores das VLANs e os nomes de domínio VTP.

Fonte: WEBB, 2003, p. 110.

A lista de comandos abaixo servirá para auxiliar você, sobre os comandos do *switch* de acesso.

*Comandos do switch de acesso.*

Comando	Descrição
<b>interface</b>	Seleciona uma interface a ser configurada.
<b>trunk</b>	Permite a criação de troncos em uma interface Fast Ethernet.
<b>no trunk-vlan</b>	Não deixa o tráfego VLAN ser transportado por um tronco.
<b>vlan</b>	Define a configuração da VLAN.
<b>vlan-membership</b>	Define a configuração de associação a VLANs.
<b>vtp nome</b>	Define o nome de domínio VTP.
<b>vtp modo</b>	Coloca o switch no modo VTP escolhido (server, client ou transparent).
<b>vtp password senha</b>	Define uma senha para o domínio VTP (opcional).
<b>show vtp</b>	Exibe as informações de configuração VTP.
<b>show run</b>	Exibe as informações de configuração.
<b>Ctrl-Shift-6-x</b>	Sequência de escape.

Figura 13 - Comandos do switch de acesso.

Fonte: WEBB, 2003, p. 110 -111.

A lista de comandos abaixo servirá para auxiliar você, sobre os comandos do *switch* de distribuição.

*Comandos do switch de distribuição.*

Comando	Descrição
<b>enable</b>	Entra no modo privilegiado.
<b>set port</b> <i>módulo/portas</i>	Define os parâmetros da porta.
<b>set vlan</b> <i>num-vlan</i> [ <i>nome</i> ]	Cria uma VLAN Ethernet (se você não especificar um tipo, o padrão será Ethernet).
<b>set vlan</b> <i>num-vlan</i> <i>módulo/portas</i>	Atribui porta(s) à VLAN.
<b>set trunk</b> <i>módulo/portas</i> [ <i>on off desirable auto nonegotiate</i> ] [ <i>vlan</i> s] [ <i>tipo-de-tronco</i> ]	Configura as portas-tronco.
<b>clear trunk</b> <i>módulo/portas</i> <i>vlan</i> s	Limpa o tronco.
<b>set vtp domain</b> <i>nome</i>	Define o nome de domínio VTP.
<b>set vtp mode</b> <i>modo</i>	Coloca o switch no modo VTP escolhido (server, client ou transparent).
<b>set vtp password</b> <i>senha</i>	Define uma senha para o domínio VTP (opcional).
<b>show vlan</b>	Mostra as VLANs que estiverem configuradas no switch.
<b>show vtp domain</b>	Exibe as informações de configuração VTP.
<b>Ctrl-Shift-6-x</b>	Seqüência de escape.

Figura 14 - Comandos do switch de distribuição.

Fonte: WEBB, 2003, p. 111.

As figuras trazem os valores das VLANs e os nomes de domínio VTP que você poderá consultar quando for estudar o nosso estudo de caso, mais adiante.

### **3.3.1 Etapas para configurar o domínio VTP, VLANs e troncos nos dispositivos da camada de acesso.**

Para poder configurar o domínio VTP, VLANs e troncos nos dispositivos da camada de acesso, você precisará: 1) colocar o *switch* de acesso em um domínio de gerenciamento; 2) ativar os troncos no switch de acesso; 3) criar e nomear VLANs nos *switches* da camada de acesso; 4) fazer a atribuição de VLANs a portas no *switch* da camada de acesso.

Etapas para colocar o *switch* de acesso em um domínio de gerenciamento.

- Da área de trabalho do PC, faça um *telnet* para o switch de acesso.

- No modo de configuração global, digite o comando `vtp modo`, para alterar o modo VTP. Altere para servidor.
- No modo de configuração global, digite o comando `vtp domain nome`, para atribuir um nome de domínio ao seu switch de acesso.
- No modo privilegiado, digite o comando `show vtp` para verificar o nome de domínio e o modo VTP.

```
VTP version: 1
Configuration revision: 0
Maximum VLANs supported locally: 1005
Number of existing VLANs: 0
VTP domain name      : BCMSN
VTP password         :
VTP operating mode   : Server
VTP pruning mode     : Disabled
VTP traps generation : Enabled
Configuration last modified by: 172.16.4.41 at 00-00-0000 00:00:00
```

Figura 15 - Resultado do comando `show vtp`.

Fonte: WEBB, 2003, p. 112.

Etapas para ativar os troncos no switch de acesso.

- Da área de trabalho do PC, faça um *telnet* para o seu switch de acesso.
- No modo de configuração global, digite o comando `interface fast 0/26`, para entrar no modo de configuração de interface.
- No modo de configuração de interface, digite o comando `trunk on`, para ativar o uso de troncos.
- No modo de configuração de interface, digite o comando `no trunk vlan 51-52`, para remover as VLANs 51 e 52 do tronco.
- No modo de configuração global, digite o comando `interface fast 0/27`, para entrar no modo de configuração de interface.
- No modo de configuração de interface, digite o comando `trunk on`, para evitar o uso de troncos.
- No modo de configuração de interface, digite o comando `no trunk vlan 51-52`, para remover as VLANs 51 e 52 do tronco.
- No modo privilegiado, verifique se o uso de troncos está ativado, a partir do comando `show trunk` tronco. Em seguida, digite o valor A para a porta-tronco 0/26, e o valor B para a porta-tronco 0/27.

```
ASW21#show trunk A
DISL state: On, Trunking: On, Encapsulation type: ISL
ASW21#show trunk B
DISL state: On, Trunking: On, Encapsulation type: ISL
```

Figura 16 - Resultado do comando show trunk.

Fonte: WEBB, 2003, p. 113.

- No modo privilegiado, verifique se o uso de troncos foi configurado para *FastEthernet 0/26* e *0/27*, a partir do comando *show run*, conforme a figura abaixo. No modo privilegiado, verifique se o uso de troncos foi configurado para *FastEthernet 0/26* e *0/27*, a partir do comando *show run*, conforme a figura abaixo.

```
interface FastEthernet 0/26
    duplex full
    !
    trunk On
    no trunk-vlan 51 52
    !
    description "Trunk link to primary DSW121"
    !
interface FastEthernet 0/27
    duplex full
    !
    trunk On
    no trunk-vlan 51 52
    !
    description "trunk link secondary to DSW122"
```

Figura 17 - Resultado do comando show trunk.

Fonte: WEBB, 2003, p. 113

Etapas para criar e nomear VLANs nos switches da camada de acesso.

- Da área de trabalho do PC, faça um *telnet* para o seu switch de acesso atribuído.
- No modo de configuração global, digite o comando *vlan name nome-vlan* para criar uma nova VLAN.
- No modo privilegiado, digite o comando *show vlan*, para exibir os parâmetros das VLANs configuradas no *switch*.

- Usando o valor da sua VLAN, digite o comando `show vlan número-vlan`, para exibir os detalhes de parâmetros para VLAN que você configurou. Digite o comando `show vlan`, para que sejam relacionadas todas as VLANs existentes no *switch*.

```
ASW41#show vlan 10
```

VLAN	Name	Status	Ports
10	Usergroup10	Enabled	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	Trans1	Trans2
10	Ethernet	100010	1500	0	0	0	Unkn	0	0

```
ASW41#
```

Figura 18 - Resultado do comando `show vlan`.

Fonte: WEBB, 2003, p. 114.

Etapas para a atribuição de VLANs a portas no *switch* da camada de acesso.

- No modo de configuração global, digite o comando `interface e 0/1`, para entrar no modo de configuração de interface.
- No modo de configuração de interface, digite o comando `vlan-membership static número vlan` para atribuir a interface à VLAN apropriada.
- Refaça as etapas 1 e 2, para atribuir interfaces Ethernet a todas as VLANs especificadas.
- No modo privilegiado, digite o comando `show run`.



```
(texto apagado)
interface Ethernet 0/2
  vlan-membership static 10
!
interface Ethernet 0/3
interface Ethernet 0/3
  duplex full
  vlan-membership static 42
  description "To PC42"
!
interface Ethernet 0/4
  vlan-membership static 10
!
```

Figura 19 - Resultado do comando `show run`.

Fonte: WEBB, 2003, p. 115.

- No modo privilegiado, digite o comando `show vlan`.

```
ASW21#show vlan
VLAN Name      Status      Ports
-----
1  default      Enabled     AUI, A, B
10 Usergroup41  Enabled     1-6
11 Usergroup45  Enabled     7-12
```

Figura 20 - Resultado do comando `show vlan`.

Fonte: WEBB, 2003, p. 115.

No caso descrito a seguir, você conhecerá um desafio real enfrentado em um projeto de gerenciamento de roteamento.

## CASO

Jennifer Rexford é professora no departamento de Ciência da Computação da Princeton University. Sua pesquisa tem o amplo objetivo de tornar as redes de computadores mais fáceis de projetar e administrar. Kurose e Ross (2014, p.578) apresentam um projeto importante da carreira de Jennifer, contando os seus desafios. Quando ela era pesquisadora na AT&T, foi projetada uma nova forma de gerenciar o roteamento nas redes de *backbone* dos ISPs. O gerenciamento de rede seria mais simples e mais flexível se os operadores da rede pudessem exercer controle direto sobre o modo como os roteadores repassam o tráfego com base em uma visão em nível de rede da topologia e do tráfego. Sendo assim, a plataforma de controle de roteamento poderia calcular as rotas para todo o *backbone* da AT&T em um único computador comercial, e poderia controlar roteadores legados sem modificação.

---

Até aqui, você teve a oportunidade de conhecer detalhadamente as etapas para configurar o domínio VTP, VLANs e troncos nos dispositivos da camada de acesso. Agora, passaremos a estudar as configurações dos *switches* de distribuição com o domínio VTP e troncos.

### **3.3.2 Etapas para configurar os switches de distribuição com o domínio VTP e troncos.**

Para poder configurar os *switches* de distribuição com o domínio VTP e troncos, você precisará: 1) colocar o *switch* de distribuição em um domínio de gerenciamento VTP; 2) ativar os troncos e limitar os intervalos de VLANs nos *switches* de distribuição; 3) ativar o uso de troncos entre os *switches* de distribuição; 4) criar e configurar parâmetros globais para as VLANs de núcleo no *switch* da camada de distribuição.

Etapas para colocar o *switch* de distribuição em um domínio de gerenciamento VTP.

- No modo privilegiado, digite o comando `set vtp domain nome mode` modo, para atribuir o nome de domínio e o modo VTP. Especifique server para o modo VTP.
- No modo privilegiado, digite o comando `show vtp domain`, para verificar a sua configuração.

Domain Name	Domain Index	VTP Version	Local Mode	Password
BCMSN	1	2	Server -	
Vlan-count	Max-vlan-storage	Config Revision	Notifications	
5	1023	0	disabled	
Last Updater	V2 Mode	Pruning	PruneEligible on Vlans	
disabled	disabled	2-1000		

Figura 21 - Resultado do comando `show vtp domain`.

Fonte: WEBB, 2003, p. 116.

Etapas para ativar os troncos e limitar os intervalos de VLANs nos switches de distribuição.

- No modo privilegiado, digite o comando `set trunk módulo/porta on isl`, para ativar o uso de troncos na porta de distribuição, a qual está conectada ao seu switch de acesso.
- No modo privilegiado, digite o comando `clear trunk módulo/porta`, para limitar o tráfego VLAN no tronco. Os intervalos de VLANs permitidas serão: 1-50 e 53-1005.
- No modo privilegiado, digite o comando `show trunk`, para verificar a sua configuração.

```
DSW121 (enable) show trunk
```

Port	Mode	Encapsulation	Status	Native vlan
2/1	on	isl	trunking	1
2/2	on isl trunking 1			
2/3	on	isl	trunking	1
2/4	on isl trunking 1			

(texto apagado)

Port	Vlans allowed on trunk
2/1	1-50,53-1005
2/3	1-50,53-1005

(texto apagado)

Port	Vlans allowed on trunk
2/1	1-50,53-1005
2/2	1-50,53-1005
2/3	1-50,53-1005
2/4	1-50,53-1005

(texto apagado)

Figura 22 - Resultado do comando `show trunk`.

Fonte: WEBB, 2003, p. 116.

Etapas para ativar o uso de troncos entre os switches de distribuição.

- No modo privilegiado, digite o comando `set trunk módulo/porta on isl`, para ativar o uso de troncos entre dois switches de distribuição. Será necessário repetir esse comando para as quatro conexões de tronco.
- No modo privilegiado, digite o comando `show trunk`, para verificar a sua configuração.

```
DSW141> (enable) show trunk
```

Port	Mode	Encapsulation	Status	Native vlan
-----	-----	-----	-----	-----
(texto apagado)				
2/9	on	isl	trunking	1
2/10	on	isl	trunking	1
2/11	on	isl	trunking	1
2/12	on	isl	trunking	1

Port	Vlans allowed on trunk
-----	-----
(texto apagado)	
2/9	1-50,53-1005
2/10	1-50,53-1005
2/11	1-50,53-1005
2/12	1-50,53-1005

Figura 23 - Resultado do comando `show trunk`.

Fonte: WEBB, 2003, p. 117.

- No modo privilegiado, digite o comando `clear trunk 2/9-12 intervalo-de-vlans`, para limitar o tráfego VLAN permitido.

### 3.3.3 Etapas para criar e configurar parâmetros globais para as VLANs de núcleo no switch da camada de distribuição.

Abaixo apresentamos algumas das etapas para criação e configuração de VLANs de núcleo de switch da camada de distribuição.

- No modo privilegiado, digite o comando `set vlan número-vlan name nome-vlan`, para criar a VLAN de núcleo.
- No modo privilegiado, digite o comando `set vlan número-vlan módulo/portas`, para atribuir as portas de núcleo a sua VLAN nativa.
- No modo privilegiado, digite o comando `set port name módulo/porta "To core xx"`, para atribuir um nome às portas de núcleo, para as quais xx poderá ser 51 ou 52.
- No modo privilegiado, digite o comando `show port`, para verificar a sua configuração.

```
DSW141> (enable) show port
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
-----	-----	-----	----	-----	-----	-----	-----
(texto apagado)							
2/9	"To core51"	disabled	51	normal	auto	auto	10/100BaseTX
2/10	"To core51"	disabled	51	normal	auto	auto	10/100BaseTX
2/11	"To core52"	disabled	52	normal	auto	auto	10/100BaseTX
2/12	"To core52"	disabled	52	normal	auto	auto	10/100BaseTX
(texto apagado)							

Figura 24 - Resultado do comando show port.

Fonte: WEBB, 2003, p. 118.

O exemplo de Webb (2003, p. 109-118) ajudou você a concretizar e a elucidar, mais ainda, seus conhecimentos sobre o VLAN Trunking Protocol (VTP)? A partir dessa demonstração, agora você é capaz de configurar VLANs em *switches* da camada de acesso; criar VLANs nos segmentos que fazem a conexão entre os *switches* da camada de distribuição e camada de núcleo; configurar troncos em todos os *uplinks* dos *switches* da camada de distribuição para os *switches* da camada de acesso.

## Síntese

Finalizamos aqui mais uma unidade da disciplina Técnicas de Switching. Nela você pode aprofundar seus conhecimentos sobre o VTP (VLAN Trunking Protocol) e o EtherChannel, a partir de uma relação entre teoria e prática.

Nesta unidade, você teve a oportunidade de:

- aprender que a função do VTP é reduzir a administração em uma rede comutada. Ao configurar um novo VLAN a um servidor VTP. O VLAN será distribuído a todos os interruptores do domínio, de modo a facilitar o gerenciamento da rede, mantendo a consistências da sua configuração;
- usar um *switch* da família Catalyst para operar nos seguintes modos VTP: 1) servidor; 2) cliente; 3) transparente. E que há dois tipos de anúncios VTP: 1) requisições de clientes que desejam informações no momento da inicialização; 2) respostas de servidores e três tipos de mensagens VTP: 1) requisições de anúncios por clientes; 2) anúncios de sumários; 3) anúncios de

subconjuntos;

- conhecer que a poda VTP consiste em aprimorar o uso da largura de banda da rede e, por consequência, reduzir a retransmissão de tráfego desnecessários – como *broadcasts*, *multicasts* e *unicasts* desconhecidos.
- compreender que O EtherChannel é uma tecnologia que permite agregar o *link* de porta, ou promover a arquitetura de canal de porta, com a finalidade de aprimorar a tolerâncias a falhas e *links* de alta velocidade entre switches, roteadores e servidores.
- o PAgP ( *Port Aggregation Protocol*) tem como finalidade auxiliar na criação de enlaces Fast EtherChannel. Ele é capaz de identificar quem são seus vizinhos, bem como seu potencial de agrupamento, repassando esta informação para os vizinhos indicados.



◀ Clique para baixar o conteúdo deste tema.

## Bibliografia

BLACK mirror. Criação Charlie Brooker. Série original Netflix. S.l.: Media Rights Capital; Panic Pictures, 2011. Disponível em: <<https://www.netflix.com/search?q=black%20mirror>>. Acesso em: 17/08/2019.

CASTELLS, Manuel. **A sociedade em rede**. 6. ed. São Paulo: Paz e Terra, 2002.

COMO entender o VLAN Trunk Protocol (VTP). In: CISCO. Brasil, 29 set. 2014. Disponível em: <[https://www.cisco.com/c/pt\\_br/support/docs/lan-switching/vtp/10558-21.html](https://www.cisco.com/c/pt_br/support/docs/lan-switching/vtp/10558-21.html) ([https://www.cisco.com/c/pt\\_br/support/docs/lan-switching/vtp/10558-21.html](https://www.cisco.com/c/pt_br/support/docs/lan-switching/vtp/10558-21.html))>. Acesso em: 17/08/2019.

LIU, D.; BARBER, B.; DIGRANDE, L. VLAN Trunking Protocol. In: **Cisco CCNA/CCENT**. Elsevier, 2010.

KUROSE, J.; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem *top-down*. 6ª edição. Pearson, 2014.

WEBB, K. **Construindo redes Cisco usando comutação multicamadas**. Pearson Education do Brasil, 2003.