TÉCNICAS DE SWITCHING

UNIDADE 4 - CONFIGURAÇÃO AVANÇADA DE *SWITCHES*

Bruno de Souza Toledo

Introdução

Caro aluno, estudaremos nessa unidade as configurações avançadas de *switches*, através da identificação de tronco e anúncios de Protocolo de Entroncamento VLAN (VTP). Estudaremos, também, o gerenciamento de enlaces redundantes, protocolo *Spanning Tree* e roteamento entre VLANs.

O uso de *links* redundantes pode acarretar uma intempérie de *broadcast* na rede. Com o uso do *Spanning Tree Protocol* (STP), que foi definido pela IEEE 802.1S, ocorre a permuta de informações entre *bridges*, para assim verificar se há *loops* e fazer outros caminhos distintos do que já havia sido verificado.

Temos, ainda, as topologias redundantes, que têm a função de prevenir contra o chamado tempo de indisponibilidade, ou *downtime* rede. O tempo de indisponibilidade surge por causa de um único *link* da rede, dispositivo ou porta, que falha, e, por meio das topologias redundantes, o responsável poderá fazer o nivelamento do custo da redundância e da disponibilidade da rede.

Isso significa que a redundância de uma rede é necessária, pois garante a sua proteção evitando a desconectividade, acarretada por erros dos componentes individuais.

Vale ressaltar que a redundância gera topologias físicas com *loops* que provocam danos em redes comutadas e, por isso, sugere-se que ela seja planejada e monitorada.

Para isso, podemos voltar a falar do *Spanning-Tree Protocol* e seu uso nas redes comutadas, que tem a função de gerar uma topologia lógica sem *loops*, utilizando de uma topologia física com *loops*. Esse protocolo é visto como um instrumento eficaz, que certifica a segurança de uma topologia redundante, sem a inseguridade dos impedimentos causados pelos *loops* de comutação ao gerenciador da rede.

Nesta unidade, você irá aprofundar esses conhecimentos, simulando a implementação EtherChannel em equipamentos, a partir de sua configuração e análise, para compreender na prática o funcionamento do protocolo *Spanning Tree* (STP). Além disso, aprenderá a analisar o roteamento entre Lans Virtuais (VLANs).

4.1 VTP: identificação de tronco e anúncios VTP

Para que a conectividade das VLANs possa ocorrer em toda a estrutura elas devem ser configuradas em cada *switch.* O protocolo VLAN Trunking Protocol (VTP), da Cisco, é utilizado para que se obtenha uma manutenção mais fácil e segura de uma VLAN em toda a rede comutada, garantindo as suas funções básicas que são distribuir e sincronizar informações de identificação das VLANs configuradas em toda a rede comutada.

O enlace tronco tem o papel de propagar as configurações determinadas em um único servidor VTP (JAVVIN, 2005).

Por padrão, quando acontece alguma modificação de VLANs, ou periodicidade de 5 minutos, os anúncios VTP são transportados em todo o domínio de gerenciamento.

Vale salientar que quando as redes de *switch*es não possuem o protocolo VTP, um

protocolo deverá ser criado manualmente pela pessoa responsável pelo gerenciamento da rede. Nesse caso, o gerenciador deverá observar o número de equipamentos e VLANs um a um e isso poderá tornar a sua atividade exaustiva, aumentando a probabilidade de erros na configuração dos equipamentos, uma vez que grandes quantidades de configurações e ajustes deverão ser feitos de acordo com as necessidades de cada momento.

É justamente para evitar isso que utilizamos o protocolo VTP, pois ele tem por característica diminuir o tempo gasto pelo administrador da rede com as configurações, uma vez que o uso desse protocolo permite que todas as informações estejam em um único *switch,* pois o VTP *Server*, distribui e sincroniza as informações para os outros *switch*es da rede.

VOCÊ SABIA?

O Trunking tem origem nas tecnologias de rádio e telefonia e foi criado para o setor corporativo, para um curto número de vias de comunicação em grande escala de usuários de telefone. No uso da tecnologia de rádio, um tronco é uma só linha de comunicação que envia vários canais de sinais de rádio. Na telefonia, o Trunking é associado com o caminho ou canal de comunicação telefônica entre dois pontos, sendo que um deles é normalmente a central telefônica. O sistema troncalizado faz o envio de mensagens de tráfego entre os canais disponíveis, tendo a vantagem de diminuir o tempo de espera do canal, pois possui um método inteligente com capacidade de gerenciamento de chamadas e sem a necessidade de intervenção do usuário.

Como você já deve ter percebido, esse método tem como principal função auxiliar na prevenção de erros de configuração e, ao mesmo tempo, diminuir a mão de obra do administrador de redes, uma vez que a configuração das VLANs será feita uma única vez no *switch* VTP Server VLANs (CISCO, 2014).

A seguir, falaremos mais sobre o VTP, visando compreender melhor o seu uso e importância para as redes.

4.1.1 VLAN Trunk Protocol *(VTP)*

É importante que você saiba que o VTP foi desenvolvido pela Cisco para gerenciar e manter a consistência de todas as VLANs configuradas na rede.
No exemplo a seguir, mostramos que no *switch* 1 foram criadas a VLAN (cor verde) e VLAN (cor azul). Assim, teremos que ingressar no *switch* 2 e criar as VLANs (cores verde e azul). Isso deverá ser feito em todos os *switches* da rede.

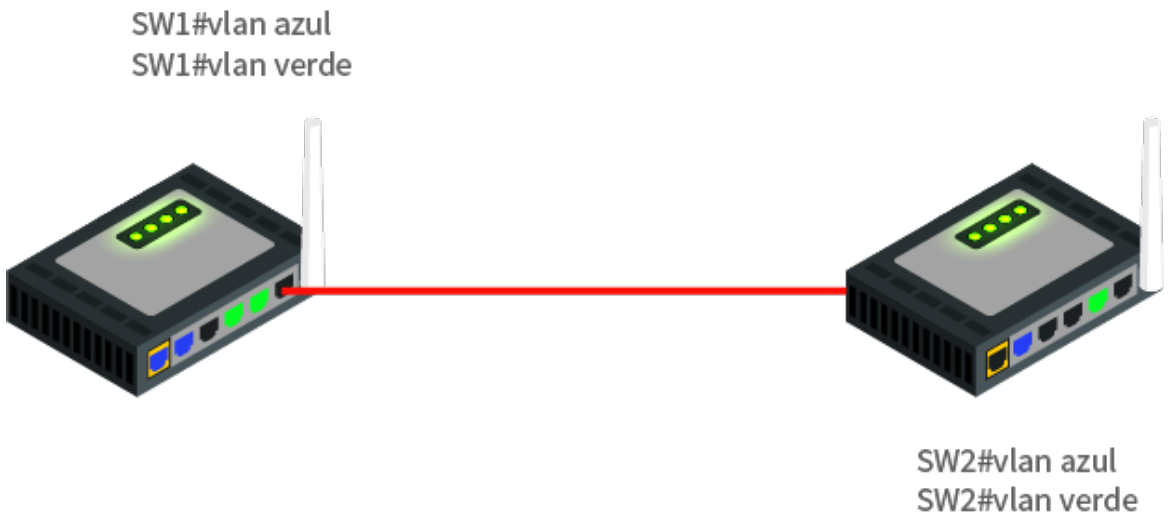


Figura 1 - VLAN Trunk Protocol.
Fonte: Elaborada pelo autor, baseado em CISCO, 2014.

Conforme vimos anteriormente, o VTP, criado pela Cisco, contribui agilizando o trabalho do administrador de rede, evitando que a configuração de equipamentos e VLANS seja feito um a um. Assim, com esse protocolo é criada a VLAN em um *switch* apenas, e ela se propagará para os demais *switches*. Portanto, um protocolo VTP é considerado um conjunto de *switches* que trocam informações entre as VLANs. Para isso, um dos *switches* faz o papel de VTP *server* (servidor), centralizando todo o processo de criação e alteração de VLANs. Os outros *switches* são considerados clientes que são administrados pelo servidor que recebe as informações e não tem permissões para alterar ou adicionar VLANs.

CASO

Até aqui vimos um pouco sobre os VTPs. No entanto, é importante alertar sobre um problema recorrente em redes reais no dia a dia das empresas. Então vamos analisar um caso hipotético, mas que é bastante comum. Suponha que tenhamos uma rede já configurada. Assim, já consideramos existentes diversas VLANs e domínio VTP. Agora, teremos que adicionar um novo *switch* nessa rede já existente. Qual seria a melhor abordagem para realizar esse procedimento? Tecnicamente poderíamos pensar em usar o *switch*, adicioná-lo na rede, ligar, configurar e então tudo estaria resolvido. No entanto, não é bem assim, pois nesse caso qualquer mudança de topologia e configuração deve ser analisada antes de ser aplicada. Quando utilizamos o VTP alguns detalhes devem ser lembrados. Imagine quem está administrando a rede, os usuários com problemas, as reclamações com serviços fora do ar!

Para resolver esse tipo de problema devemos criar novamente as VLANs no *switch* VTP *server* e deletar as VLANs indesejadas, que foram inseridas por outro *switch*. Apesar da demora, isso resolverá o problema.

Para saber mais sobre o assunto, você pode ler o artigo de Tavares (2011), acessando o seguinte endereço: <http://www.dltec.com.br/blog/cisco/vtp-vlan-trunk-protocol-estudo-de-caso-curso-ccna/>.

Algumas especificações para o funcionamento de um VTP são apresentadas pela Cisco (2014), conforme abaixo. Navegue no recurso a seguir.

Um *switch* pode trocar *frames* apenas com outros switches configurados no mesmo domínio e serão encaminhados sempre por portas de transporte (*trunk*). Ou seja, cria-se, por exemplo, um domínio Ânima e todos que estiverem nesse domínio irão receber as VLANs que foram criadas no VTP server.

As frames VTP contêm várias informações de controle, como o domínio VTP, o número de revisão da configuração, a senha do domínio e as VLANs conhecidas. As senhas devem ser definidas para que haja o aumento do

controle do domínio VTP, e todos os *switches* pertencentes a um mesmo domínio deverão ser configurados com a mesma senha.

Quando um *switch* em domínio VTP recebe uma atualização com um número de revisão mais alto que o último recebido, ele subscreve o seu banco de dados com as novas informações traduzidas pela atualização. Desse modo, cria-se uma VLAN no *switch* e o número de revisão é 1. Se outro número de revisão é criado, ele será 2, e assim por diante. Quanto mais VLANs são criadas, maior o número de revisões.

A rede tem que ser toda Cisco, por ser um protocolo proprietário.

A administração é centralizada, o que facilita o gerenciamento e controle da rede, garantindo a consistência da informação.

4.1.2 Modos de Operação VTP

Existem três modos de operação VTP: o modo cliente, o modo servidor e o modo transparente. Cada um desses modos serve para atender uma necessidade específica da rede.

O modo *server* ou modo servidor, como dito anteriormente, é o modo padrão de todos os *switches* Cisco. Ele tem que ter pelo menos um servidor em um domínio VTP, porém podemos ter outros servidores paralelos. Esse tipo de *switch* em modo servidor tem a capacidade de inserir, deletar ou alterar VLANs em um domínio VTP. Assim, quando alteramos um *switch* em modo servidor VTP ele se propaga para todo o domínio VTP com um número de revisão de atualização igual ao último número recebido mais um (+1). (CISCO, 2007).

Por outro lado, quando falamos de clientes VTP, observamos que se trata de um modo que tem função distinta do modo servidor, pois nesse caso não é possível inserir, deletar ou alterar as informações de VLANs. Uma vantagem desse modo, é a sua utilidade para quando os *switches* não possuem memória suficiente para armazenar grandes tabelas de informações de VLANs. Assim, a função dos clientes VTP é executar alterações de VLAN, enviando mensagens VTP para todas as portas de tronco. (CISCO, 2007).

Embora os *switches* no modo VTP transparente encaminhem os anúncios VTP, eles ignoram informações contidas na mensagem, pois esse funcionamento não participa do domínio VTP. Mesmo assim, ele propaga as informações do VTP do *switch* que está conectado a ele, ou seja, um *switch* transparente não pode modificar o seu banco de dados quando recebe atualizações e nem enviar uma atualização que indique uma alteração no *status* de suas VLANs.

Característica	Servidor	Cliente	Transparente
Mensagens VTP de Origem	Sim	Sim	Não
Escutar Mensagens VTP	Sim	Sim	Não
Criar VLANs	Sim	Não	Sim*
Lembrar de VLANs	Sim	Não	Sim*

* Somente tem Significado Local

Figura 2 - Comparações de Modo VTP.
Fonte: CISCO, 2006.

O VTP é sempre desativado em um *switch* transparente, a menos que seja para o encaminhamento de anúncios VTP. (CISCO, 2007).
Na figura, você pode visualizar as comparações das características entre os três modos VTP.

VOCÊ QUER VER?

O documentário *A origem dos hackers,* do canal Discovery Channel, conta a história dos primeiros *hackers* conhecidos como *phreaking*, que hackeavam linhas telefônicas e assim faziam inúmeras ligações internacionais gratuitas. O primeiro deles foi John Draper, famoso pelo nome Captain Crunch. Entre seus amigos estavam Steve Jobs e Steve Wozniak, fundadores da empresa Apple. O documentário mostra, também, como Kevin Mitnick ficou mundialmente conhecido após ser preso por atividades hackers e invasões nas redes de computadores. Você pode ver o documentário completo acessando: < https://www.youtube.com/watch?v=cgI1pesO1do>.

Agora que já conhecemos os modos de operação VTP, iremos estudar como fazer a sua configuração.

4.1.3 Configuração de VTP

A utilização do VTP reduz o trabalho de administração em uma rede comutada. Segundo a Cisco (2014), quando se configura uma VLAN nova em um servidor VTP, esta está subdivida através de todos os *switches* no domínio e, com isso, há a diminuição da necessidade de configurar a mesma VLAN em todos os lugares.

> A configuração de VLAN em uma rede de pequeno porte pode ser facilmente administrada, entretanto em grandes ambientes corporativos a administração pode resultar muito trabalhosa e complicada devido a que temos que configurar manualmente todas as VLANs em todos os switches e pode ser fácil que alguma VLAN não seja configurada em algum dos switches, sobretudo em um desenho end-to-end. No caso de uma rede de tamanho considerável é importante manter a consistência das VLANs que estamos criando, para isso é muito recomendável dispor de algum mecanismo que permita ter todos os switches sincronizados com as VLANs da rede (RABELO, 2014, p. 50).

Para ter uma configuração de VLAN em conformidade com toda a rede comutada, utiliza-se um VTP, permitindo soluções nesse tipo de rede com escalabilidade simples a outras dimensões, diminuindo assim a necessidade de configuração manual da rede.
O VTP é um protocolo proprietário Cisco de camada 2 e uma de suas funções é a troca de informação sobre VLAN entre trunks, por isso as VLANs sempre estarão sincronizadas nas bases de dados dos *switches* da rede (WEBB, 2003).
Agora chegou a hora de criarmos e configurarmos um tronco simples para VLAN em um *switch* configurado por comandos do Cisco IOS, através do *software* Packet Tracer. Primeiro você deverá configurar a porta como tronco e depois usar os comandos, conforme indicado na figura abaixo. Em seguida, especifique o encapsulamento do tronco.

```
Router#show interface fast 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
```

Figura 3 - Switch Cisco Catalyst da Série 2900XL.
Fonte: CISCO, 2006.

Você terá que verificar se o Trunking está configurado a partir do modo EXEC privilegiado do *switch*, com os comandos *show interfacesFa0/port_num* ou *show interfacestrunk.*

Nesse ponto é preciso ter alguns cuidados na hora de configurar o VTP, lembrando que o número de revisão determina o sincronismo do banco de dados das VLANs no cliente. Suponhamos que temos dois VTPs servidores em um mesmo domínio, sendo que o *switch* 1 tem número de revisão do VTP 5, enquanto o *switch* 2 está na revisão 10, o que aconteceria? Os clientes apagam todas as informações passadas pelo *switch* 1 e inserem as VLANs do *switch* 2. Portanto, ao colocar um novo *switch* na rede, é preciso observar se ele ficará como cliente, evitando assim possíveis problemas.

VAMOS PRATICAR?

Suponha que você foi contratado para ser o administrado de uma faculdade e, ao verificar essa rede, você pe instalação da rede local de computadores que inclui trê (VLAN1, VLAN2 e VLAN3) em sua topologia. As VLA segmentadas utilizando uma *switch* L2. Considere, ainda, u gerado por um computador pertencente à VLAN1, que encaminhado para um computador pertencente à VLAN situação, qual meio você utilizaria para o encaminhamento na VLAN1?

Agora que você já conheceu os diferentes tipos de VLANs e suas funcionalidades, você poderá estudar e compreender o gerenciamento de enlaces redundantes e conhecer o *Spanning Tree Protocol*.

4.2 Gerenciamento de enlaces redundantes / protocolo *Spanning Tree*

Neste tópico, falaremos sobre conexões redundantes entre *switches*, principalmente em um protocolo *Layer* 2, que faz a topologia das empresas funcionarem. Esse protocolo é o *Spanning Tree Protocole* (STP).

Observa-se que as redes de computadores são fundamentais para as empresas em suas operações. Por exemplo, a utilização de banco de dados, servidores de arquivos, Internet, intranet, entre outros, é fundamental para o melhor desempenho dos negócios. Se a rede falhar, consequentemente a produtividade da empresa cairá e, consequentemente, o contentamento dos clientes diminuirá.

Assim, existem as topologias de rede redundantes, que são concebidas para aferir que as redes fiquem em perfeito funcionamento na presença de pontos únicos de falha. Por isso, com a rede em funcionamento, evita-se que os usuários fiquem parados constantemente, pois qualquer paralização causada por falha deverá ser a mais breve possível.

Nesse sentido, é importante aprofundarmos mais o assunto sobre as redes redundantes.

4.2.1 Enlaces redundantes

Podemos afirmar que a confiabilidade aumenta com a redundância. Isso, porque uma rede baseada em *switches* ou *bridges* insere *links* redundantes entre eles para superar a falha de um único *link*. Essas ligações introduzem *loops* físicos na rede; os chamados *loops* de *bridges* são criados para o caso de um *link* falhar e outro passar a funcionar com o propósito de direcionar o tráfego.

Quando o destino do tráfego é desconhecido para um *switch*, ele submerge o tráfego por todas as portas, menos a porta que fez o seu recebimento. Assim, o tráfego de *broadcast* e/ou *multicast* também passam pelo encaminhamento de todas as portas, menos a que recebeu esse tráfego e, nesse caso, o tráfego poderá ficar preso em um *loop.* (OPPENHEIMER, 2011, tradução do autor).

No cabeçalho da camada 2, não há valor de tempo de vida (TTL), como no protocolo Internet IP na versão 4 (IPv4), por isso, se um quadro for enviado para uma topologia de *switches* para essa camada poderá ocorrer o chamado *loop* infinito, acarretando problemas tais como perda da largura de banda ou perda da rede.

Na camada 3, o tempo de vida é diminuído e o pacote é retirado quando o tempo de vida chega a zero. Isso acarreta um problema de confiabilidade, pois ele necessitará de uma topologia física que contenha *loops* de *switches* e *bridges*; mas, em contrapartida, uma rede comutada não terá *loops*.

Uma solução seria os *loops* físicos, sem a criação de uma topologia lógica que não possui *loops*, pois essa terá o tráfego destinado ao servidor "*farm*", conectado à Catalyst Cisco (Cat), Cat-5, a partir de qualquer estação de trabalho de usuário conectada à Cat-4 e passará por Cat-1 e Cat2. (LOPES, 2012).

Isso acontece mesmo que haja uma conexão física direta entre *switch*-5 e *switch*-4

> A topologia lógica sem loops criada é chamada de árvore. Essa topologia é uma topologia lógica em estrela ou em estrela estendida. Ela é a spanning-tree da rede. É uma spanning-tree (árvore de espalhamento) porque todos os dispositivos da rede podem ser alcançados ou estão abrangidos por ela. O algoritmo usado para criar essa topologia lógica sem loops é o algoritmo spanning-tree. Esse algoritmo pode levar um tempo relativamente longo para convergir. Para reduzir o tempo que uma rede leva para computar uma topologia lógica sem loops, foi desenvolvido um novo algoritmo, chamado rapid spanning-tree (LOPES, 2012, p. 301).

Kurose e Ross (2014), afirmam que um dos problemas de um projeto para segmentos de LAN interconectadas é quando um *switch* próximo ao topo da hierarquia falha, os enlaces da LAN serão desconectados.

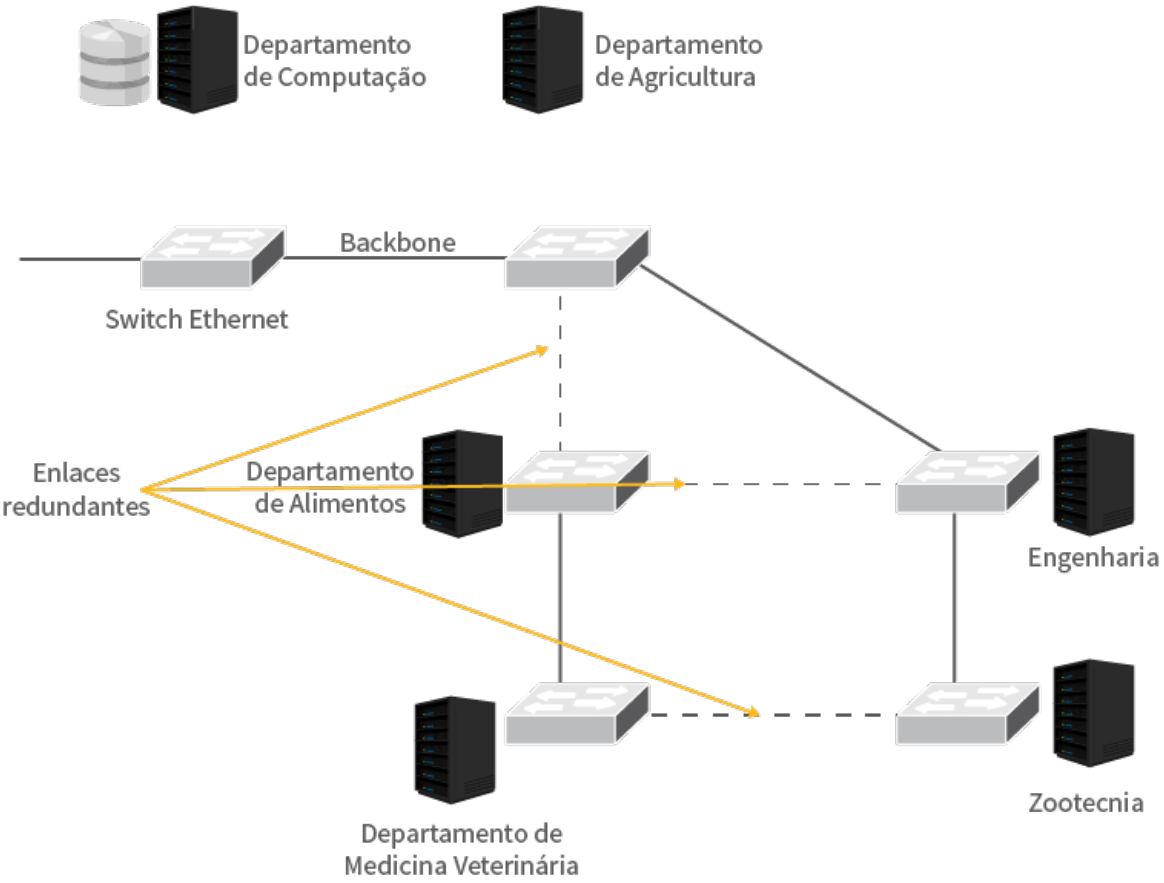


Figura 4 - Enlaces redundantes em uma rede.
Fonte: KUROSE; ROSS, 2014.

Assim, como é possível observar na figura apresentada, é recomendável a construção de redes com múltiplos trajetos entre os enlaces da rede que está sendo criada.

VOCÊ QUER LER?

A Cisco possui uma plataforma de comunicação com empresas e pessoas que querem conhecer mais sobre as redes de computadores. Nessa plataforma você encontra, fórum, suporte, treinamentos, área de *downloads*, informações sobre eventos e os parceiros da Cisco. Para mais informações acesse o site <cisco.com/c/pt_br/support/index.html>.

A seguir iremos discutir o *Spanning Tree Protocol,* para aprofundar o estudo da redundância na rede.

4.2.2 Spanning Tree Protocol (STP)

A existência de equipamentos redundantes é necessária em diversas ocasiões, assim como ligações para a elevada disponibilidade de uma rede informática. No entanto, ela gera o surgimento de *loops* na rede, prejudicando o seu desempenho.
Então, para controlar esses *loops* no nível da camada 2 do modelo OSI, surgiu o protocolo *Spanning Tree Protocol* ou STP, que é como interruptores ou pontes.
A especificação para o STP é IEEE 802.1D. A função primordial dele é garantir que não surjam laços para os caminhos redundantes, melhorando o desempenho da rede.
Para melhor compreendermos isso, vejamos como se realiza a descrição do STP. Com ele a chave é para todos os interruptores na rede para selecionar o chamado “bridge-raiz” que se altera no ponto principal na rede.

> Todas as decisões restantes na rede, tal como que porta obstruir e qual mover para o modo de encaminhamento, são feitos da perspectiva da ponte raiz. Um ambiente comutado, que seja diferente de um ambiente da ponte, trata mais provavelmente de VLANs múltiplas. Quando você executa um bridge-raiz em uma rede de comutação, você refere geralmente o bridge-raiz como o switch-raiz. Cada VLAN deve ter seu próprio bridge-raiz porque cada VLAN é um domínio de transmissão separado. Todas as raízes para VLANs diferentes podem residir em um switch único ou em vários interruptores. Os switches não filtram broadcasts e tal situação faz com que todos os broadcast recebidos numa interface de um switch sejam enviados pelas outras interfaces, exceto pela interface que foi recebida (*flooding*), podendo assim serem criados os

broadcast storms (CISCO, 2014).

Mas então como funciona o STP? De modo geral, o STP exclui de forma lógica os caminhos de comunicação. Para isso, ele insere uma "árvore de *switches*" existente na rede e escolhe o *switch* a partir da criação dessa árvore. Esse *switch* é denominado de *root bridge.* A escolha dele é por prioridade e também com base no MAC Address. Salienta-se que em uma rede deve ter apenas um *root bridge.*
A seguir, vemos o exemplo completo, conforme o Manual Switching da Cisco (2006). O Switch A é o *root bridge*, devido a menor prioridade (por omissão, a prioridade é 32768) e também o menor endereço físico (*MAC address)*.

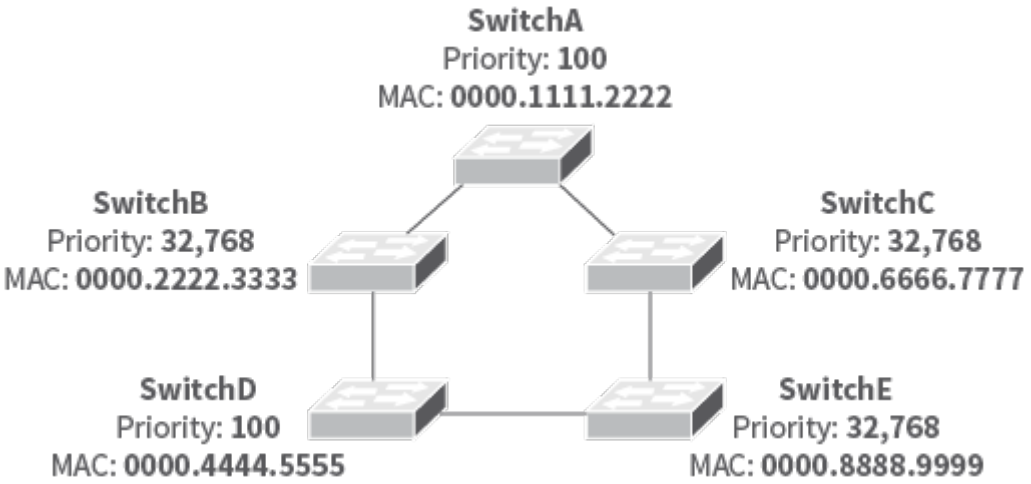


Figura 5 - Exemplo de Root Bridge.
Fonte: CISCO, 2006.

Cada *switch* em seguida, que não é *root bridge*, define qual é a sua *root port*. Ela é a opção definida de acordo com o menor custo, e a partir da análise da largura de banda para a *root bridge*. Depois de definida a *root port,* ela é colocada em modo de encaminhamento, conforme a figura.

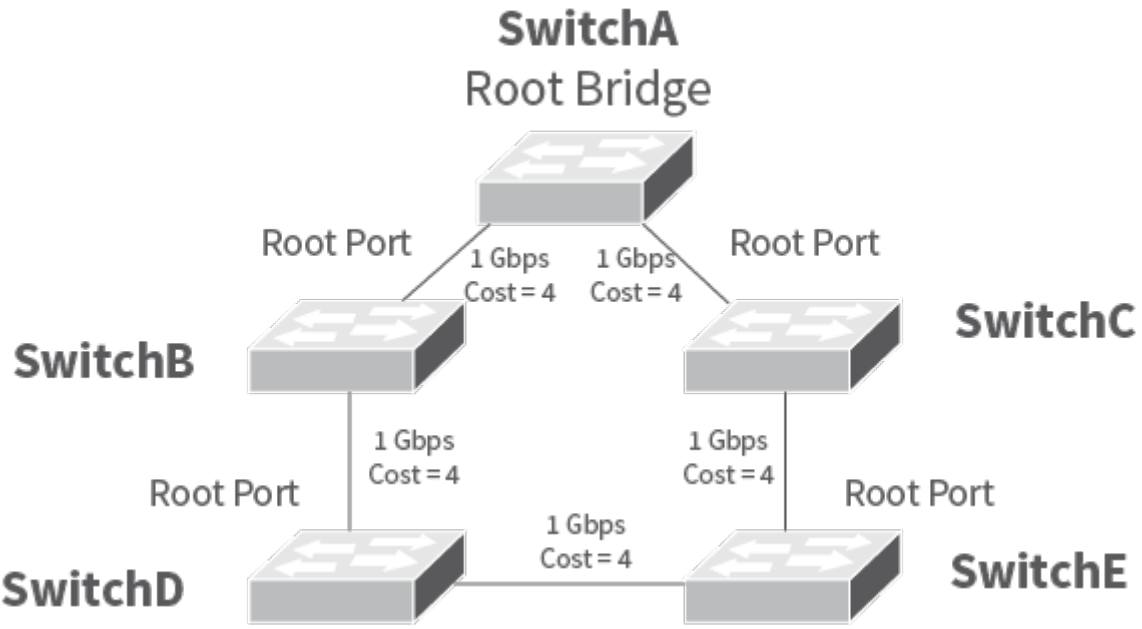


Figura 6 - Modo de encaminhamento da root bridge.
Fonte: CISCO, 2006.

É definida uma *designated bridge* em cada seguimento, que será o *switch* com menor custo até o *root bridge*, SwitchD, conforme a próxima figura. A interface de ligação com a *root bridge* é inserida no modo encaminhamento. Já a porta do SwitchE é inserida em modo de bloqueio. Com isso, há o bloqueio dos *frames* e, assim, não acontece *loops* na rede.

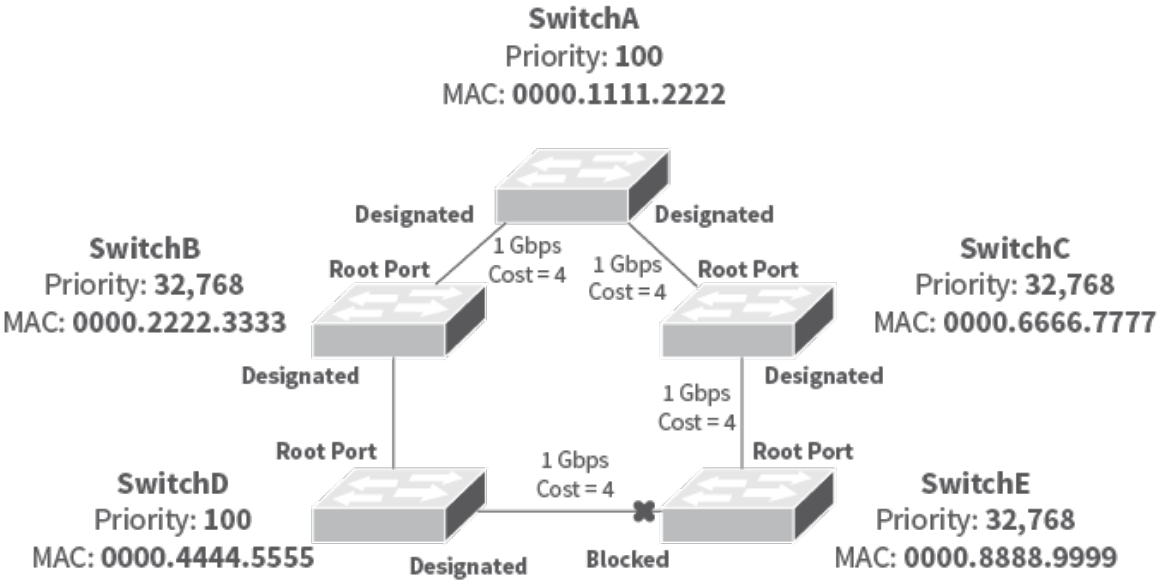


Figura 7 - Root Bridge.
Fonte: CISCO, 2006.

Podemos afirmar que o STP é um protocolo simples no quesito configuração. No entanto, devemos ter maiores conhecimentos conceituais que são necessários para a sua aprendizagem.

VAMOS PRATICAR?

Utilizando o Packet Tracer, crie um cenário de rede *switches* de 24 portas e três computadores, com os IPs 10.0.0.2 e 10.0.0.3. Verifique o mecanismo de aprendiz *switch* e a atualização da tabela MAC em caso de recon Você pode utilizar comandos básicos tais como: *show i show interfaces interface-id* e *show mac-address-table dyn* seguida, force um *loop* na rede. O intuito é aplicar na p conhecimentos de *loop* em redes visto até aqui.

No próximo tópico, apresentaremos o roteamento entre VLANs, configurando e fazendo a sua análise, além de apresentar o EtherChannel.

4.3 Roteamento entre VLANs

A partir daqui focalizaremos em como permitir a comunicação entre diversas VLANs. Vamos rotear o tráfego entre elas e, para isso, apresentaremos as técnicas utilizadas.
Lembramos que, por padrão, VLANs distintas não se comunicam, pois há domínios de *broadcast* reservados. Para essa situação é necessário usar um roteador ou um *switch* camada 3 (*multi-layer*).
A Cisco (2014), mostra que sempre que for necessário devemos criar sub-redes para cada uma das VLANs, para que haja sucesso na comunicação entre elas, pois se duas ou mais VLANs estiverem com o mesmo endereço de rede haverá transtornos posteriores no roteamento, devido a comunicação do roteador com redes distintas.
Iremos destacar aqui algumas características para uso de interfaces físicas e virtuais através de exemplos.
No uso de interfaces físicas de um roteador para cada VLAN podemos considerar, por exemplo, um ambiente com duas VLANs que iremos rotear. Para que isso ocorra, duas interfaces físicas são necessárias para o roteador. Porém, nesse procedimento iremos perceber uma adversidade, pois necessitaremos de uma interface física para cada VLAN. Assim, se pensarmos em um rede maior, devemos evitar esse tipo de técnica, pois será fundamental um ou mais roteadores com várias portas para ligar cada VLAN. Essa técnica tem a vantagem de evitar o sobrecarregamento de uma única porta. (CISCO, 2014).
Para compreender melhor esse funcionamento, pode-se usar interfaces virtuais (sub-interfaces) de um roteador para cada VLAN. Podemos exemplificar esse uso a partir de uma situação real, na qual usaremos um único cabo para conectar várias VLANs do *switch* no roteador. Para isso, é essencial que esse cabo seja configurado em um *trunk* no *switch*, pois ao ser ligado diretamente no roteador permite-se o tráfego de múltiplas VLANs.
No mercado encontramos um protocolo responsável por realizar esse *trunk*, que é o tronco dot1q. No entanto, é importante ressaltar que a Cisco, até 2007, falava que era preciso utilizar o seu proprietário, o ISL.
É permitido inserir até 256 sub-interfaces a partir de uma interface física dentro do IOS da Cisco. Contudo, com esse método pode ocorrer a sobrecarga da interface, pois todo o tráfego das VLANs terá que ser suportado e, assim, as chances de prejuízos no desempenho da rede seriam grandes. (CISCO, 2014).

4.3.1 EtherChannel

annel é uma tecnologia de agregação de *link* de porta ou arquitetura de canal usada principalmente em *switches* da Cisco. Ela é uma forma de usar a e banda em *links* redundantes de modo mais eficaz, agregando *links* em uma única conexão lógica.
Sua criação acontece entre duas e oito portas ativas Ethernet 10-Gigabit rápida, Gigabit ou portas, com um adicional de oito inativos (*failover* portas), que se tornam ativas quando as outras portas ativas falharem.
O EtherChannel é utilizado na rede de *backbone*, mas ela também é utilizada para

conexão de máquinas de usuários finais (KUROSE e ROSS, 2014).
Existem vários benefícios no uso de um EtherChannel em nossas redes comutadas: clique nos ícones a seguir.

- a) Ao usar o EtherChannel, permitimos o balanceamento de carga, pois o tráfego será direcionado em três links em vez de um.

- b) Em caso de falha em um dos enlaces físicos no EtherChannel ele continuará funcionando com os links restantes, failover automático, ou seja, se fa0/1 em nosso cenário estava inativo o EtherChannel ainda usaria fa0/2 e fa0/3.

- c) A terceira vantagem de usar EtherChannel é que ele simplifica a configuração de interfaces. Isso significa que quando ele é implementado, podemos configurá-lo como faríamos com qualquer outra interface, o que seria mais simples do que configurar as três interfaces repetidamente.

Vejamos como é o funcionamento do EtherChannel, que agrega o tráfego em todas as portas ativas disponíveis no canal.
Você deve selecionar na porta um algoritmo de *hash,* proprietário da Cisco, com base em endereços MAC de origem ou de destino, endereços IP ou números de porta TCP e UDP. O *hash* é considerado um algoritmo que mapeia grandes dados, sendo de tamanho variável para pequenos dados de tamanho fixo.
É importante salientar que o EtherChannel é tolerante a falhas, pois se um *link* falhar ele redistribuirá de forma automática todo o tráfego pelos *links* que sobraram. Isso

ocorre em menos de um segundo, sendo transparente para os aplicativos de rede e o usuário final.
Basicamente temos duas formas de trabalhar com o EtherChannel, que se constituí em dois padrões, que também são conhecidos por Protocolos de Negociação de EtherChannel, sendo eles: Clique no recurso a seguir.

1. ***Port Aggregation Protocol,*** **ou Protocolo de agregação de porta** ***(PAgP)***

   Foi desenvolvido pela Cisco e os modos portuários são definidos como automáticos ou desejáveis.

2. ***Link Aggregation Control Protocol,*** **ou Protocolo de controle de agregação de link** ***(LACP)***

   É um padrão aberto conforme definido pelo padrão IEEE 802.3ad e os modos de porta são passivos ou ativos. Passivo é o equivalente do PAGP automático e ativo é o equivalente do modo desejável PAGP.

Sobre os modos de porta LACP e PAGP, temos que:

- os pacotes de LACP da troca das interfaces de switch se conectam somente com a configuração do active ou do modo passivo. As relações sobre a configuração de modo não trocam o PAgP ou os pacotes de LACP;
- no modo ativo há uma relação em um estado da negociação ativa, em que ocorrem negociações com outras relações, com a emissão dos pacotes de LACP;
- no modo auto há uma relação passiva na negociação, em que a relação responde aos pacotes PAgP que recebe mas não começa a negociação do pacote PAgP. Esse ajuste minimiza a transmissão de pacotes PAgP;
- no modo desejável temos uma relação ativa, que começa as negociações com outras relações com a emissão dos pacotes PAgP;
- em - Força a relação em um EtherChannel sem PAgP ou LACP. Desse modo, um EtherChannel utilizável existe

somente quando um grupo de interface está conectado a outro grupo de interface sobre no modo.

- no modo passivo temos um estado passivo da negociação, que apenas esponde aos pacotes de LACP que a relação recebe, mas não começa a negociação do pacote de LACP. Esse ajuste minimiza a transmissão de pacotes LACP (CISCO, 2014, p. 3).

O STP pode ser usado com um EtherChannel e trata todos os *links* como único. Sem o uso de um EtherChannel o STP desligaria efetivamente quaisquer *links* redundantes entre os *switches* até que uma conexão fosse desativada. É por isso que o EtherChannel é mais desejável, pois permite o uso de todos os *links* disponíveis entre dois dispositivos. Os EtherChannels também podem ser configurados como troncos de VLAN. Se algum *link* único de um EtherChannel estiver configurado como um tronco de VLAN, todo o EtherChannel atuará como um tronco de VLAN, seja Cisco ISL, VTP ou IEEE 802.1Q, que são compatíveis com EtherChannel.

VOCÊ O CONHECE?

Scott Childs foi o responsável pela criação da tecnologia EtherChannel. Ele era funcionário da empresa Kalpana, no início dos anos 90. Posteriormente, essa tecnologia foi obtida pela Cisco Systems, no ano de 1994. Já em 2000, o IEEE criou o 802.3ad, que é uma versão padrão aberta do EtherChannel.

EtherChannel é composto pelos seguintes elementos-chave:

- links Ethernet - o EtherChannel funciona sobre links definidos pelo 802.3, incluindo todos os sub-padrões.

Todos os links em um único EtherChannel devem ter a mesma velocidade.

- hardware compatível - toda a linha de switches Cisco Catalyst, bem como os roteadores baseados no software Cisco IOS, suportam EtherChannel. Configurar um EtherChannel entre um switch e um computador requer suporte embutido no sistema operacional; O FreeBSD, por exemplo, suporta EtherChannel via LACP. Vários EtherChannels são suportados por dispositivo, o número depende do tipo de equipamento. Os switches Catalyst 6500 e 6000 suportam um máximo de 64 EtherChannels;
- configuração - um EtherChannel deve ser configurado usando o Cisco IOS em switches e roteadores, e usando drivers específicos ao conectar um servidor. Existem duas maneiras principais para configurar o EtherChannel. A primeira é a emissão manual de um comando em cada porta do dispositivo que faz parte do EtherChannel. Isso deve ser feito para as portas correspondentes nos dois lados do EtherChannel. A segunda maneira é usar o Cisco Port Aggregation Protocol (PAgP) para a agregação automatizada de portas Ethernet (CISCO, 2014, p. 3).

No próximo tópico, iremos aplicar configurações e análises do roteamento entre VLANs através de um simulador.

4.3.2 Configuração e análise do roteamento entre VLANs

Aprenderemos agora como configurar o roteamento entre as VLANs.
O exemplo a seguir tem como referência a LabCisco (2013), uma das fontes mais respeitáveis na área de redes de computadores.
Nesse exemplo o usuário aprenderá a configurar um *switch multi-layer* (*layer*-3), usando o Packet Tracer. Esse tipo de *switch* tem as mesmas características dos tradicionais *switches*, com o acréscimo de realizarem o roteamento de tráfego inter-redes, feito somente por roteadores. Esse *switch multi-layer* tem melhor desempenho e realiza as suas tarefas eletronicamente em *hardware*. Na figura abaixo, temos o exemplo inicial da nossa aprendizagem.

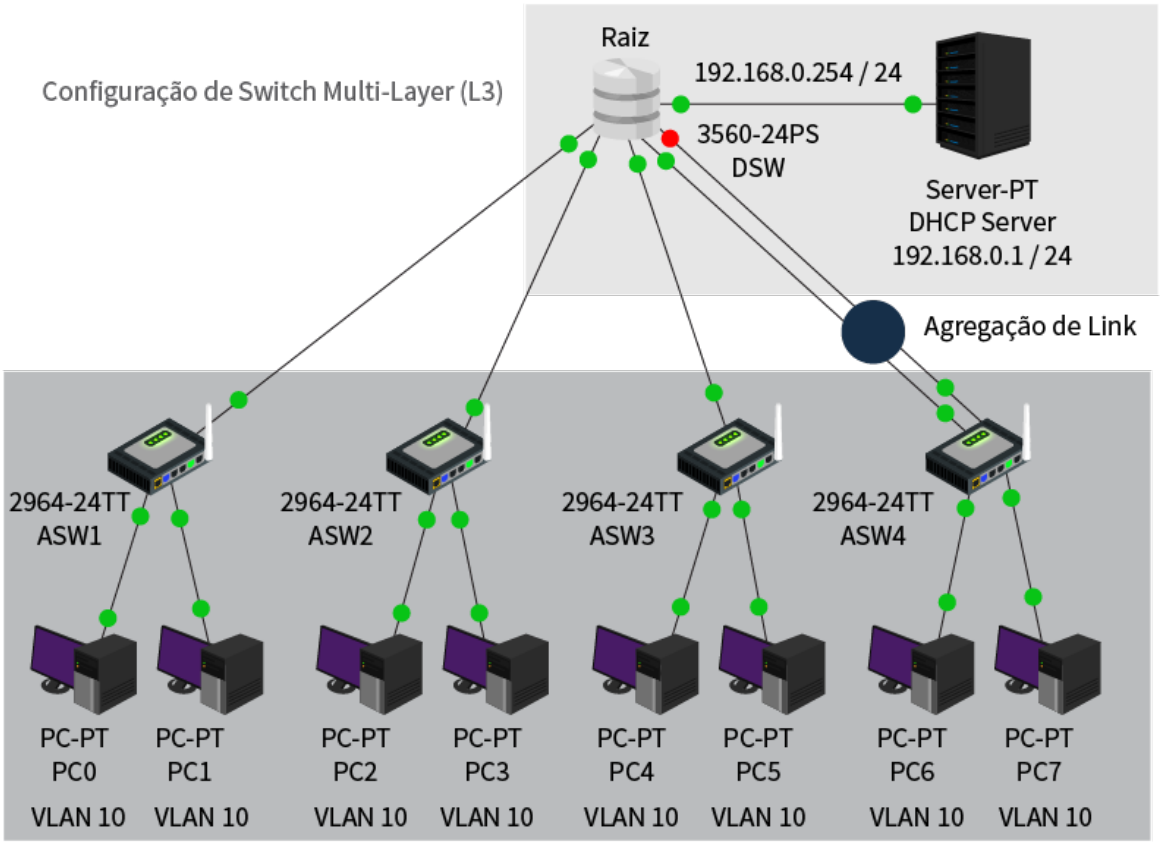


Figura 8 - Configuração de um Switch Multi-Layer.
Fonte: LABCISCO, 2013.

No cenário apresentado, observa-se 4 *switches* de acesso para conexão dos computadores. Além disso, existem duas VLANs, a VLAN10 e VLAN20. Repare que os *switches* para o acesso se conectam a um *switch multi-layer*, pois esse terá a responsabilidade de distribuição da conexão da rede e fará o roteamento inter-VLAN.

Podemos notar que os endereços de todos os computadores da sub-rede são 192.168.10.0/24 (associada à VLAN-10) e 192.168.20.0/24 (associada à VLAN-20) e, também, distribuem-se automaticamente via Protocolo de Configuração Dinâmica de Endereços de Rede (DHCP), que permite os computadores terem um endereço IP automaticamente.

O DHCP, por padrão, faz o envio de "*broadcast*" na rede, para localizar um servidor. Ou seja, um DHCP exclusivo para cada sub-rede seria necessário, no entanto isso é inviável em um ambiente com mais VLANs, além do alto custo que teria. Desse modo, faremos a instalação em uma sub-rede administrativa à parte das sub-redes 192.168.10.0/24 e 192.168.20.0/24, com encadeamento para a VLAN-1, que é padrão.

Para alcançar o servidor com o tráfego de *broadcast* gerado pelos computadores no momento da solicitação de endereços é necessário a configuração da *relay-agent* no *switch*/roteador, desse modo o tráfego de *broadcast* será reencaminhado até o endereço específico do servidor DHCP na rede administrativa.

Já temos aqui um servidor DHCP configurado com os escopos corretos. O servidor já

tem um IP 192.168.0.1/24 e seu *gateway* com o endereço 192.168.0.254. Com isso, a interface do *switch,* conectada ao servidor, será configurada para ser uma porta roteável (*layer*-3) capaz de receber esse IP, o que o faz um equipamento bastante versátil.

Com o objetivo de termos uma rede potente e equilibrada para melhor desempenho, iremos configurar de forma manual a prioridade do DSW para que ele seja a nova raiz da rede, *spanning-tree vlan ID priority 0*, conforme a primeira parte do bloco de comandos.

Mesmo sabendo que os *switches multi-layer* tem a capacidade de rotear entre redes, geralmente isso não vem por padrão ativo, e assim vamos usar o comando *ip routing* para permissão de rotear entre as redes de sua tabela de roteamento. Com isso, também vamos realizar as principais configurações de *hostname*, fazer um domínio de *switches*, além de criar VLANs, inoperar resolução de nomes, entre outras coisas.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname DSW
DSW(config)# no ip domain lookup
DSW(config)# ip routing
DSW(config)# vtp mode server
DSW(config)# vtp domain AULA
DSW(config)# vtp password SENHA
DSW(config)# vlan 10
DSW(config-vlan)# name VLAN-10
DSW(config-vlan)# vlan 20
DSW(config-vlan)# name VLAN-20
DSW(config-vlan)# exit
DSW(config)# spanning-tree vlan 1,10,20 priority 0
DSW(config)#
```

Após as configurações iniciais, converteremos a interface f0/10, que está conectada ao servidor DHCP, para uma porta roteável no *switchport* e então atribuir a ela o endereço 192.168.0.254/24, que é o endereço de *gateway* feito no servidor.

Agora, criamos duas interfaces lógicas, vinculadas a cada uma das VLANs e configuramos em cada uma delas um endereço IP, que será o *gateway* das sub-redes associadas às suas respectivas VLANs.

Nas interfaces lógicas usamos o comando *ip helper-address*, que altera o tráfego de *broadcast* gerado nas respectivas VLANs encaminhando até o endereço do servidor DHCP. Por fim, faremos a configuração das interfaces de f0/1 até f0/5, que interligam os demais *switches* de acesso para transportarem as informações de todas as VLANs em modo *trunk*.

```
DSW> enable
DSW# configure terminal
DSW(config)# int f0/10
DSW(config-if)# no switchport
DSW(config-if)# ip address 192.168.0.254 255.255.255.0
DSW(config-if)# int vlan 10
DSW(config-if)# ip address 192.168.10.254 255.255.255.0
DSW(config-if)# ip helper-address 192.168.0.1
DSW(config-if)# int vlan 20
DSW(config-if)# ip address 192.168.20.254 255.255.255.0
DSW(config-if)# ip helper-address 192.168.0.1
```

```
DSW(config-if)# int range f0/1 - 5
DSW(config-if-range)# switchport trunk encapsulation dot1q
DSW(config-if-range)# switchport mode trunk
```

Agora, o usuário pode utilizar o comando *show ip route*, que tem a função de mostrar a tabela de rotas do *switch multi-layer* e verificar que já existem as sub-redes referentes às interfaces em que já fizemos as atribuições de IPs.

Observe que na interligação entre DSW e ASW4 forçaremos dois *links* redundantes para configurar uma agregação entre eles e, assim, formar uma porta lógica, *port-channel,* equivalente à soma das duas interfaces físicas, conforme o próximo bloco de comandos.

Mas porque fazemos isso? Para uma garantia de maior largura de banda entre os *switches,* por meio do balanceamento de carga entre os *links* físicos, pois já que o STP bloqueia uma das portas, para evitar a ocorrência de *loops*, um dos *links* físicos fica ocioso, podendo comprometer o desempenho na rede.

```
DSW> enable
DSW# configure terminal
DSW(config)# int range f0/4 - 5
DSW(config-if-range)# channel-group 1 mode on
DSW(config-if-range)# end
DSW#
```

Agora vamos para a criação da *port-channel,* de forma manual, e repetiremos esse procedimento depois nas portas f0/23 e f0/24 do ASW4. Assim, perceberemos que o STP não bloqueia mais nenhum dos *links* individuais, pois ele só entenderá a existência da porta lógica a partir dessa configuração.

Pronto! O *switch multi-layer* está configurado.

Agora, vamos configurar os demais *switches* de acesso, para associar suas portas às suas respectivas VLANs.

Depois, iremos configurar os *switches* de acesso convencionais. Para a configuração dos outros *switches* de acesso faz-se apenas a inserção deles no domínio AULA (VTP) e a associação das portas com suas respectivas VLANs. Para o ASW4 configuraremos de forma manual a agregação com o DSW, conforme bloco de comandos a seguir.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname ASW1
ASW1(config)# no ip domain lookup
ASW1(config)# vtp domain AULA
ASW1(config)# vtp mode client
ASW1(config)# vtp password SENHA
ASW1(config)# interface f0/24
ASW1(config-if)# switchport mode trunk
ASW1(config-if)# interface f0/1
ASW1(config-if)# switchport mode access
ASW1(config-if)# switchport access vlan 10
ASW1(config-if)# interface f0/2
ASW1(config-if)# switchport mode access
ASW1(config-if)# switchport access vlan 20
ASW1(config-if)# end
ASW1#
Switch> enable
Switch# configure terminal
```

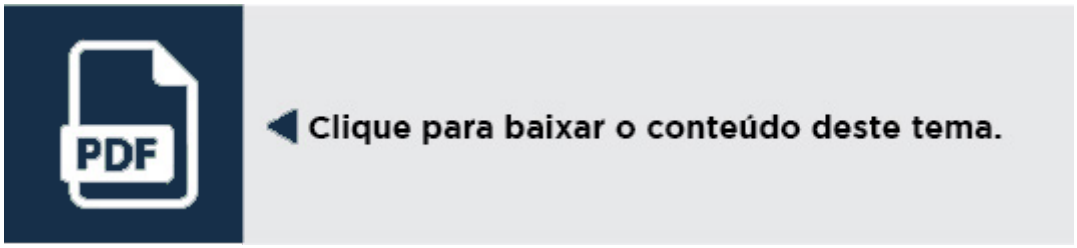
```
Switch(config)# hostname ASW2
ASW2(config)# no ip domain lookup
ASW2(config)# vtp domain AULA
ASW2(config)# vtp mode client
ASW2(config)# vtp password SENHA
ASW2(config)# interface f0/24
ASW2(config-if)# switchport mode trunk
ASW2(config-if)# interface f0/1
ASW2(config-if)# switchport mode access
ASW2(config-if)# switchport access vlan 10
ASW2(config-if)# interface f0/2
ASW2(config-if)# switchport mode access
ASW2(config-if)# switchport access vlan 20
ASW2(config-if)# end
ASW2#
Switch> enable
Switch# configure terminal
Switch(config)# hostname ASW3
ASW3(config)# no ip domain lookup
ASW3(config)# vtp domain AULA
ASW3(config)# vtp mode client
ASW3(config)# vtp password SENHA
ASW3(config)# interface f0/24
ASW3(config-if)# switchport mode trunk
ASW3(config-if)# interface f0/1
ASW3(config-if)# switchport mode access
ASW3(config-if)# switchport access vlan 10
ASW3(config-if)# interface f0/2
ASW3(config-if)# switchport mode access
ASW3(config-if)# switchport access vlan 20
ASW3(config-if)# end
ASW3#
Switch> enable
Switch# configure terminal
Switch(config)# hostname ASW4
ASW4(config)# no ip domain lookup
ASW4(config)# vtp domain AULA
ASW4(config)# vtp mode client
ASW4(config)# vtp password SENHA
ASW4(config)# interface range f0/23 - 24
ASW4(config-if-range)# switchport mode trunk
ASW4(config-if-range)# channel-group 1 mode on
ASW4(config-if-range)# interface f0/1
ASW4(config-if)# switchport mode access
ASW4(config-if)# switchport access vlan 10
ASW4(config-if)# interface f0/2
ASW4(config-if)# switchport mode access
ASW4(config-if)# switchport access vlan 20
ASW4(config-if-range)# end
```

ASW4#
Finalizamos o exemplo, deixando o último comando para verificação do *status* das configurações:
Switch# show vlan
Switch# show interface trunk
Switch# show ip interface brief
Switch# show ip route
Switch# show ether-channel summary
Switch# show ether-channel port-channel
Ótimo! Agora que fizemos todos procedimentos, esperamos que você, depois de ter visto os aspectos teóricos e práticos aqui explicitados, tenha aprendido melhor os aspectos práticos que envolvem a configuração de um *switch multi-layer* (*layer*-3).

Síntese

Nesta unidade aprofundamos nosso conhecimento sobre as técnicas de *switching* e a sua importância para as redes de computadores. Aprendemos que a redundância é essencial na rede, pois ela concede a tolerância de falhas na rede. Conhecemos também a VLAN Trunking Protocol, da Cisco, que gerencia e mantém a consistência de todas as VLANs configuradas na rede. Com isso, podemos dizer que a redundância aumenta a confiabilidade da rede.
Ao longo do capítulo percebemos que é necessário, em diversas situações, ter equipamentos redundantes e com isso surgem os *loops* na rede, que prejudicam seu desempenho. Para resolver isso, surgiu o protocolo *Spanning Tree* Protocol.
No final da unidade, fizemos a configuração e análise do roteamento entre VLANs através do simulador Packet Tracer.
Nesta unidade, você teve a oportunidade de:

- aprender a configuração avançada de *switches*;
- conhecer as configurações do VTP;
- compreender o gerenciamento de enlaces redundantes/protocolo *Spanning Tree* e roteamento entre VLANs;
- entender o uso de *links* redundantes e sua função na rede;
- configurar e analisar na prática o roteamento entre VLANs.



Bibliografia

A ORIGEM DOS HACKERS. Direção: Ralph Lee. USA. Documentário. 47 min. 2001.

Disponível em: <https://youtu.be/cgI1pesO1do (https://youtu.be/cgI1pesO1do)>. Acesso em: 17/08/2019.

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)>. Acesso em: 30/09/2019.

CONFIGURAÇÃO de Switch Multi-Layer (Layer-3). In: LABCISCO. Brasil, 14 mar. 2013. Disponível em: <http://labcisco.blogspot.com/2013/03/configuracao-de-switch-multi-layer.html (http://labcisco.blogspot.com/2013/03/configuracao-de-switch-multi-layer.html)>. Acesso em: 17/08/2019.

JAVVIN TECHNOLOGIES. Network Protocols Handbook. Saratoga: Javvin Network Inc, 2005. Disponível em: <https://ww1.prweb.com/prfiles/2005/01/25/201816 /Book2005demo.pdf. (https://ww1.prweb.com/prfiles/2005/01/25/201816 /Book2005demo.pdf.)>. Acesso em: 30/09/2019.

KUROSE, J.; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-dowm. 6. ed. São Paulo: Pearson, 2014.

LOPES, N. **Switching Basico e Roteamento Intermediário**: notas de estudo de Redes de Computadores. Módulo III. Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS). Porto Alegre, 2012. 406 p. (Programa Cisco Networking Academy). Disponível em: <https://www.docsity.com/pt/ccna-modulo-3-switching-basico-e-roteamento-intermediario/4777567/ (https://www.docsity.com/pt/ccna-modulo-3-switching-basico-e-roteamento-intermediario/4777567/)>. Acesso em: 17/08/2019.

OPPENHEIMER, P. **Top-Down Network Design.** Indianapolis: Cisco Systems, Inc., 2011. 476 p. Disponível em: <http://www.teraits.com/pitagoras/marcio /gpi/b_POppenheimer_TopDownNetworkDesign_3rd_ed.pdf (http://www.teraits.com /pitagoras/marcio/gpi/b_POppenheimer_TopDownNetworkDesign_3rd_ed.pdf)>. Acesso em: 30/09/2019.

RABELO, H. **CCNP Switch**: guia de estudos para profissionais. Belo Horizonte: Fontana Editora, 2014.

SISTEMA operacional inter-redes Cisco. In: CISCO. Brasil, 2 fev. 2006. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/ios-nx-os-software/ios-software-releases-110/13178-15.html (https://www.cisco.com/c/pt_br/support/docs/ios-nx-os-software/ios-software-releases-110/13178-15.html) >. Acesso em: 30/09/2019.

TAVARES, A. C. VTP (VLAN Trunk Protocol) – Estudo de Caso – Curso CCNA. In: DLTEC do Brasil. Curitiba, 22 dez. 2011. Disponível em: http://www.dltec.com.br/blog/cisco/vtp-vlan-trunk-protocol-estudo-de-caso-curso-ccna/ (http://www.dltec.com.br/blog/cisco/vtp-vlan-trunk-protocol-estudo-de-caso-curso-ccna/). Acesso em: 30/09/2019.

TODO o VTP domain transparente ao exemplo de configuração da migração de VTP domain do Server-cliente. In: CISCO. Brasil, 2 fev. 2007. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/lan-switching/vtp/81682-vtp-migration.html (https://www.cisco.com/c/pt_br/support/docs/lan-switching/vtp/81682-vtp-migration.html)>. Acesso em: 30/09/2019.

WEBB, K. **Construindo Redes Cisco Usando Comutação Multicamadas.** São Paulo: Pearson Education, 2003.