

Switches em redes de computadores

Apresentação

As redes de comunicação são de extrema importância e apresentam objetivos, como conectar diversos dispositivos e permitir o compartilhamento de recursos com confiabilidade, segurança e contínuo foco em redução de custos. Para a composição dessas redes de comunicação, faz-se uso de diferentes dispositivos, tais como repetidores, pontes, switches, hubs, roteadores e gateways.

Nesta Unidade de Aprendizagem, você vai conhecer especificamente o comutador, ou *switch*, com suas características e funções, além de aprender sobre a criação de VLANs e suas aplicações.

Bons estudos.

Ao final desta Unidade de Aprendizagem, você deve apresentar os seguintes aprendizados:

- Explicar o funcionamento dos *switches*.
- Descrever as principais características dos *switches*.
- Apresentar a criação de VLANs e suas aplicações.

Desafio

Uma LAN (*Local Area Network*) é uma rede local, que pode ser pequena, com dois computadores conectados entre si, ou grande, com muitos dispositivos conectados. A rede de uma empresa em um único edifício é considerada uma LAN. Nessa LAN, usa-se o protocolo dominante Ethernet cabeada. A Ethernet é um padrão, publicado pelo IEEE, que descreve os protocolos, os cabos, os conectores, etc.

Buscando conectar os dispositivos e permitir o compartilhamento de recursos, uma LAN faz uso de diferentes dispositivos, tais como repetidores, *switches*, *hubs*, roteadores e *gateways*.

Levando em conta esses dispositivos, suas características e funções, na qualidade de profissional, analise o seguinte cenário:

Um prédio empresarial de cinco andares tem quatro escritórios por andar. Cada escritório contém uma tomada/soquete para ser usada por um terminal/dispositivo.

As tomadas formam uma grade retangular em um plano vertical, com distância de 4m entre elas, tanto no sentido horizontal quanto no vertical.



Exemplo de um andar com quatro escritórios e dispositivos como computadores e impressoras.

Partindo do princípio de que é possível passar um cabo entre qualquer par de tomadas, seja no sentido horizontal, seja no vertical ou diagonal, **é necessário que os escritórios tenham comunicação entre os andares**, e deve-se prezar por alta velocidade de comunicação, segurança, escalabilidade e baixo custo para a implementação de uma LAN nesse prédio.

Considerando que você foi contratado para auxiliar na implementação dessa LAN, responda:

Que solução seria a mais adequada entre os dispositivos *hub*, *switch* e roteador? Justifique a sua escolha.

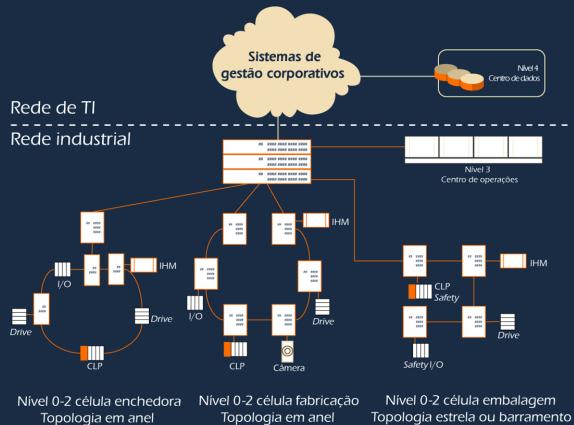
Infográfico

Trocas de informações quanto aos processos e/ou produtos em produção são necessárias em diversas corporações. Algumas informações até mesmo necessitam ser transmitidas em tempo real. Como podem existir diversas camadas desde o chão de fábrica até o centro de operações e de dados, tanto o volume de dados como a segurança destes devem ser de alto nível. Os dispositivos que atendem às demandas de comunicação dessas redes são os comutadores, ou *switches*.

Acompanhe, no Infográfico, um exemplo de utilização de *switches* como apoio na convergência dos sistemas de produção e gestão.

SWITCHES APLICADOS À CONVERGÊNCIA DOS SISTEMAS DE PRODUÇÃO E GESTÃO

O switch, ou comutador, é o dispositivo que permite encaminhar o pacote que está chegando a um de seus enlaces de comunicação de entrada para um de seus enlaces de comunicação de saída. É tipicamente utilizado em redes de acesso local, como no esquema a seguir, aplicado a empresas que têm maturidade e necessidade de convergir seus dados de produção e gestão.



Aponte a câmera para o código e accese o link do conteúdo ou clique no código para accesar.

DIFERENTES NÍVEIS

Nessa corporação se está trabalhando com níveis diretamente relacionados à **pirâmide de automação industrial**, em que a aplicação do switch é completa, ou seja, seu uso à transmissão de dados para todas as camadas, permitindo a convergência.



IMPORTÂNCIA DOS SWITCHES

Os switches, ou comutadores, podem permitir aos dispositivos conectados a comunicação em diferentes velocidades e o isolamento de tráfego. Além disso, oferecem segurança, podem ser plug-and-play ou ser configurados, permitem a criação de VLANs, melhorando todo o tráfego de dados, o uso de diferentes mídias físicas e a gestão de dispositivos e usuários, além de:

- adicionar inteligência ao gerenciamento de transferência de dados;
- permitir transferir dados somente para a conexão que necessite desses dados;
- determinar se os dados devem ou não permanecer na rede local;
- mantener os formatos dos dados transmitidos sem converter;
- reduzir os domínios de colisão, permitindo que as estações (dispositivos) não "briguem" pelo uso do meio de transmissão.

SUGESTÃO DE VLANS

VLAN 17

Sub-rede 10.17.10.0/20

Dispositivos da célula:
processo enchedora

VLAN 16

Sub-rede 10.16.10.0/20

Dispositivos da célula:
processo fabricação

VLAN 10

Sub-rede 10.10.10.0/20

Dispositivos da célula:
processo embalagem

Conteúdo do Livro

Redes existem para que dados possam ser transmitidos de um lugar a outro. As redes de comunicação são fundamentais para conectar os dispositivos e fazer o compartilhamento de seus recursos com confiabilidade e segurança.

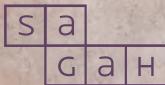
Para a compreensão desse tema, é preciso conhecer os componentes da comunicação de dados, entender como diferentes tipos de dados podem ser representados e como criar um fluxo desses dados. A comunicação de dados, nesse estudo, aplica-se a LANs, ou seja, redes locais, e que fazem uso de dispositivos denominados *comutadores* (*switches*).

Leia o capítulo *Switches* em redes de computadores, da obra *Arquitetura TCP/IP I*, para conhecer o comutador (*switch*), suas características e funções, além dos endereços, do IEEE 802.1d, dos métodos de comutação, da capacidade do *backplane* (*blocking, non-blocking*), dos *links* resilientes, do IEEE 802.3ad, do IEEE 802.1p e do espelhamento de tráfego.

Boa leitura.

ARQUITETURA TCP/IP I

Rodrigo Santarelli



SOLUÇÕES
EDUCACIONAIS
INTEGRADAS

Switches em redes de computadores

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Explicar o funcionamento dos *switches*.
- Descrever as principais características dos *switches*.
- Apresentar a criação de VLANs e suas aplicações.

Introdução

As redes de comunicação são de extrema importância, pois permitem conectar diversos dispositivos e compartilhar recursos entre eles com confiabilidade, segurança e contínuo foco em redução de custos. Para a composição dessas redes, faz-se o uso de alguns dispositivos, como repetidores, pontes, *switches*, *hubs*, roteadores e *gateways*.

Neste capítulo, você estudará sobre os *switches* em redes de computadores. Além disso, conhecerá os endereços IEEE 802.1d, IEEE 802.3ad e IEEE 802.1p, bem como os métodos de comutação, *backplane (blocking, non-blocking)*, *links resilientes* e espelhamento de tráfego. Por fim, verá como se dá a criação de VLANs (Virtual Local Area Network; ou Rede Local Virtual, em português) e quais são as suas aplicações.

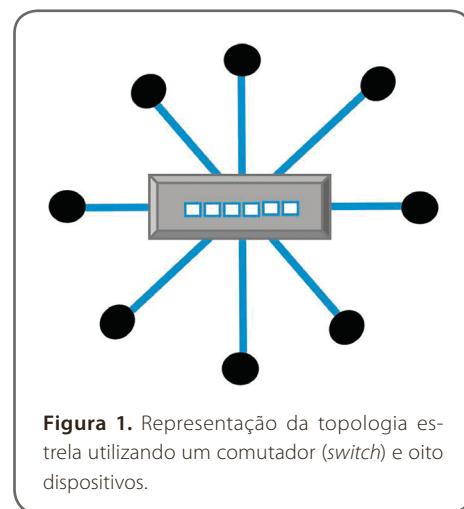
1 Funcionamento dos switches

O *switch* é um comutador de pacotes que permite encaminhar o pacote que está chegando em um de seus enlaces de comunicação de entrada para um de seus enlaces de comunicação de saída. O comutador de camada de enlace (i.e., os *switches*) é um dos dispositivos mais importantes utilizados na internet. Esse tipo de dispositivo de rede encaminha os pacotes aos seus destinos finais, sendo geralmente utilizado em redes de acesso local (TANENBAUM, 2003).

As principais vantagens dos comutadores são listadas a seguir:

- adicionam inteligência ao gerenciamento de transferência de dados;
- transferem dados somente para a conexão que necessitar deles;
- determinam se os dados devem ou não permanecer na rede local;
- mantêm os formatos dos dados transmitidos (não os convertem);
- reduzem os domínios de colisão, a fim de impedir que as estações (dispositivos) “briguem” pelo uso do meio de transmissão;
- estão associados à topologia estrela.

A Figura 1, a seguir, apresenta uma representação da topologia estrela utilizando um comutador e dispositivos conectados a ele para a realização da comunicação de dados.



De modo geral, pode-se descrever o *switch* como um dispositivo que interliga várias linhas de comunicação, encaminhando uma mensagem ao seu destino (FOROUZAN; MOSHARRAF, 2013). A **comutação** é o processo realizado na camada 2 — a camada de enlace do modelo OSI (Open System Interconnection; ou interconexão de sistemas abertos, em português) —, na qual o *switch* monta a sua tabela de encaminhamento utilizando endereços MAC (Media Access Control; ou controle de acesso de mídia, em português). Em contrapartida, os roteadores que trabalham na camada 3 (nível de rede)

analisam o endereçamento IP (Internet Protocol; ou Protocolo de Internet, em português), conforme apresentado na Figura 2. Assim, o *switch* permite conectar segmentos que pertencem à mesma rede ou sub-rede lógica.

O *switch* pode trabalhar com uma quantidade razoável de endereços MAC, que não obrigatoriamente precisam estar organizados ou em sequências, pois basta realizar uma pesquisa em sua tabela para verificar os endereços contidos no seu segmento de acesso à rede. Ele faz uma filtragem no endereço MAC do *frame* que recebeu e pode conter um *buffer* (tabela) para reter os *frames* para processamento ou ter um fator de comutação que encaminha os *frames* de forma mais rápida. O Quadro 1, a seguir, apresenta um exemplo de *buffer* com endereços MAC, suas interfaces ou portas e o horário de atualização. Alguns comutadores, denominados *switches cut-through*, foram desenvolvidos para encaminhar o *frame* assim que verificarem os endereços MAC no cabeçalho do *frame* (FOROUZAN, 2008).

Quadro 1. Exemplo de buffer com endereços MAC

Endereço	Interface/Porta	Horário
02-12-23-34-45-56	2	19h31
63-FE-F7-11-89-A3	1	19h32
7D-BA-B2-B4-91-10	3	19h36

Existem *switches* de muitas ou poucas portas de comunicação. O *switch* com menos portas pode conectar entre si redes locais, ao passo que o com mais portas permite um melhor desempenho, além de ter a possibilidade de alocar cada porta de comunicação a uma única estação ou dispositivo da rede. Dessa forma, a estação passa a possuir sua própria entidade independente, de modo que não existe tráfego concorrente, ou seja, nenhuma colisão. Com isso, ocorre a eliminação de colisões em uma LAN (Local Area Network; ou Rede de Área Local, em português) que utiliza *switches* (sem *hubs*), de modo que não existe desperdício de banda devido a colisões, pois os *switches* armazenam os *frames* e nunca transmitem mais de um *frame* em um segmento ao mesmo tempo.

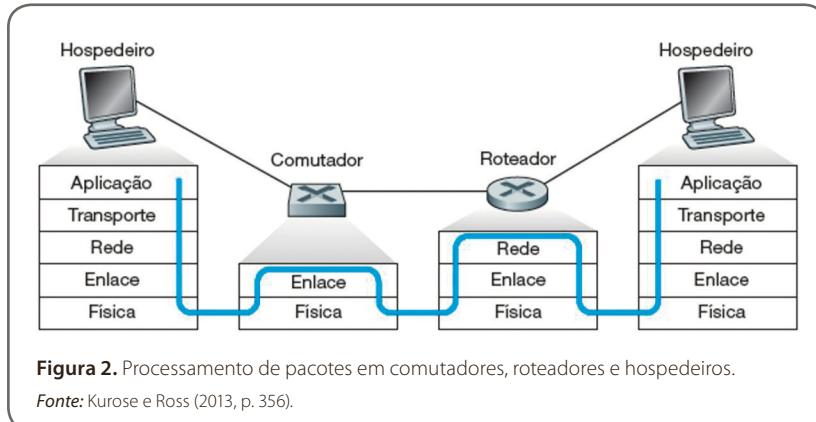


Figura 2. Processamento de pacotes em comutadores, roteadores e hospedeiros.

Fonte: Kurose e Ross (2013, p. 356).

Para melhor compreensão quanto ao funcionamento dos *switches*, torna-se relevante entender os processos de filtragem, repasse e aprendizagem automática realizados por eles. A **filtragem** é a capacidade do *switch* de determinar se um *frame* deve ser repassado para alguma interface/porta ou se deve apenas ser descartado. Esse processo advém da ideia de que as estações não devem ter conhecimento da existência da ponte (*bridge*) para que as configurações de rede se tornem mais simples. Para tanto, foi criado o conceito de **ponte transparente** no IEEE 802.1d, obedecendo aos critérios de que (I) os *frames* devem ser enviados diretamente entre as estações, (II) de que a tabela de encaminhamento deve ser aprendida e atualizada e de que (III) o sistema não deve ter *loop*.

O **repasse**, por sua vez, refere-se à capacidade do *switch* de determinar as interfaces para as quais um quadro deve ser dirigido. Tanto a filtragem como o repasse são feitos com uma tabela de comutação, a qual possui registros para alguns nós da LAN, mas não necessariamente para todos. O registro de um nó na tabela contém: (I) o endereço MAC do nó, (II) a interface do *switch* que leva em direção ao nó e (III) o horário em que o registro para o nó foi colocado na tabela.

Para melhor compreensão de como funcionam a filtragem e o repasse, suponha que um *frame* com endereço de destino AA-AA-AA-AA-AA-AA chegue ao *switch* na interface/porta “x”. O *switch* indexa sua tabela com o endereço MAC AA-AA-AA-AA-AA-AA. Assim, existem três casos possíveis, descritos a seguir.

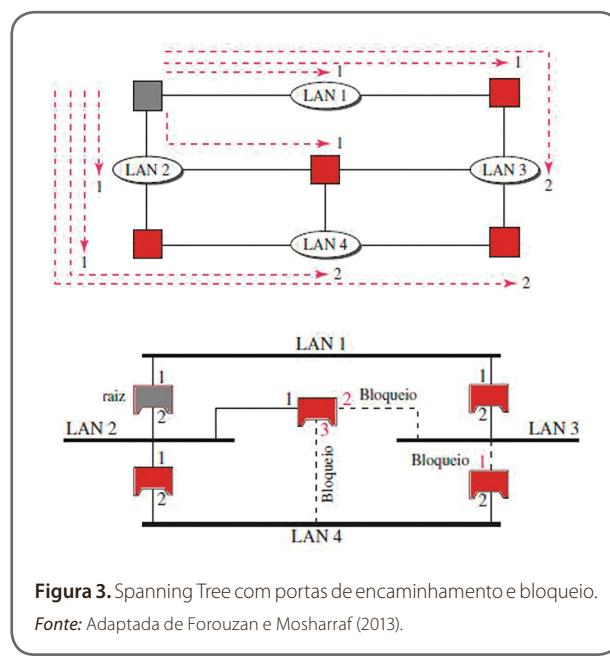
1. Não existe entrada na tabela para AA-AA-AA-AA-AA-AA. Nesse caso, o *switch* encaminha anteriormente cópias do *frame* para os *buffers* de saída de todas as interfaces, exceto a interface “x”. Ou seja, se não existe entrada para o endereço de destino, o *switch* transmite o *frame* em *broadcast*.
2. Existe uma entrada na tabela, associando AA-AA-AA-AA-AA-AA à interface “x”. Nesse caso, não existe qualquer necessidade de encaminhar o *frame* para qualquer outra interface, pois o *switch* realiza a função de filtragem ao descartar o *frame*.
3. Existe uma entrada na tabela, associando AA-AA-AA-AA-AA-AA à interface “x” ≠ “y”. Nesse caso, o *frame* precisa ser encaminhado ao segmento da LAN anexado à interface “y”. O *switch* realiza sua função de encaminhamento ao colocar o *frame* em um *buffer* de saída que precede à interface “y”.

Em se tratando dos conceitos relacionados com a filtragem, cabe alguns esclarecimentos quanto ao Protocolo IEEE 802.1d Spanning Tree. Esse protocolo é dedicado aos sistemas baseados em *switches* e permite a implementação de caminhos em paralelo para o tráfego da rede. Além disso, o Protocolo IEEE 802.1d Spanning Tree utiliza um processo de detecção de *loops* para identificar e desabilitar os caminhos menos eficientes, ou seja, aqueles com as menores larguras de banda. Desse modo, o Spanning Tree é utilizado pelos *switches* para a criação de uma topologia sem *loop* (FOROUZAN; MOSHARRAF, 2013), encontrando caminhos mais “curtos”. Esse processo ocorre devido à execução de um *software* interno ao *switch*. Ou seja, dinamicamente, o *switch* realiza o envio de mensagens especiais entre si por meio das chamadas BPDU (Bridge Protocol Data Units; ou unidades de dados de protocolo de ponte, em português), com o objetivo de atualizar o Spanning Tree quando há qualquer mudança no sistema, como, por exemplo, a falha de um dos *switches* ou a adição ou remoção de *switch*. Esse processo, ilustrado na Figura 3, apresenta as etapas descritas a seguir.

- Selecionar a raiz da árvore do Spanning Tree, o que ocorre pela escolha do *switch* que apresenta o identificador de menor valor, como, por exemplo, o identificador como o número de série do *switch*, pois são números de identificação absolutamente únicos (exclusivos).

- Encontrar o caminho mais eficiente (i.e., o mais curto) na raiz da árvore, variando entre *switch* com identificador de menor valor no momento e qualquer outro *switch* ou LAN. Em seguida, verificar o custo total da raiz até o destino; o menor custo é a referência para a criação da árvore.
- Após formar a estrutura, as portas dos *switches* são “marcadas” como portas de encaminhamento e portas de bloqueio, as quais, respectivamente, conduzem o *frame* aos *switches* que o recebem e bloqueiam os *frames* recebidos pelo *switch*.

Observe a Figura 3, na qual o *switch* “A” é identificado com o menor valor identificador, de modo que é selecionado como a raiz entre os cinco *switches* e quatro LANs que compõem a rede desse exemplo. Então, a partir do *switch* “A”, são contabilizados custos para acesso aos demais *switches* e LANs, com custo de valor 1 até os *switches* “B”, “C” e “D” e as LANs “1” e “2”, bem como custo de valor 2 até o *switch* “E” e LANs “3” e “4”. Dessa forma, foram eleitas as portas 2 e 3 do *switch* “C” como portas de bloqueio, de modo que nenhum *frame* é enviado a partir dessas portas, e o mesmo ocorre com a porta 1 do *switch* “E” (porta de bloqueio). As demais portas dos *switches* são as portas de encaminhamento, como as portas 1 e 2 dos *switches* “A”, “B” e “D”.



Observe que, além da aplicação IEEE 802.1d — uma redundância automática implementada em *switches* —, existe, em alguns fabricantes, a opção de utilizar sua própria implementação de nível de redundância de *link*, chamado de *links* resilientes. Os *links* resilientes protegem a rede contra uma falha advinda de uma conexão individual ou de um dispositivo, devido à existência de uma conexão secundária, como *backup* em *standby*, que fica inativa até que se torne necessária a conexão por esse meio. Eles compreendem um par de *links* em que se tem a conexão principal e a reserva. Assim que ocorre a falha do *link* principal, o *link* reserva assume as atividades do principal. É importante mencionar que é responsabilidade do administrador da rede realizar essa configuração. Ao escolher a funcionalidade por *links* resilientes, deve-se desabilitar a opção de uso Spanning Tree no *switch*. No entanto, existem diferentes fabricantes e ainda não há garantia de que *switches* de fabricantes diferentes possam implementar a redundância de *link* em uma mesma rede (GUTIERREZ, 2008).

A **aprendizagem automática** é a propriedade de montar uma tabela de forma automática e dinâmica, sem nenhuma intervenção de um administrador de rede ou de um protocolo de configuração. Em outras palavras, pode-se dizer que os *switches* são autodidatas. Tal capacidade é conseguida conforme as etapas apresentadas a seguir:

- inicialmente, a tabela está vazia;
- para cada *frame* recebido em uma interface, o *switch* armazena em sua tabela: (I) o endereço MAC que está no campo de endereço de fonte do *frame*, (II) a interface da qual veio o *frame* e (III) o horário corrente. Dessa maneira, o *switch* registra em sua tabela o segmento MAC no qual reside o nó remetente. Se cada nó da rede local enviar um *frame*, cada nó será registrado na tabela;
- o *switch* apagará um endereço na tabela se nenhum *frame* que tenha aquele endereço como endereço de fonte for recebido após um certo período de tempo (o tempo de envelhecimento). Desse modo, se um computador for substituído por outro, o endereço MAC do computador original será expurgado da tabela de comutação.



Fique atento

Fique atento quanto ao uso do termo **switch**, pois um *switch* pode significar coisas distintas. Quando acrescenta o nível no qual o dispositivo opera, esse termo pode se referir a um *switch* de camada 2 ou a um *switch* de camada 3. Um *switch* de camada 3 é aquele utilizado na camada de rede, sendo uma espécie de roteador. Já o *switch* de camada 2 opera nas camadas física e de enlace, sendo, assim, um comutador (FOROUZAN, 2008).

Aspectos funcionais aplicados a *switches*

Nesta subseção, serão descritos os aspectos funcionais aplicados a *switches*.

IEEE 802.3ad

O Link Aggregation é um tipo de conexão especial que roda diretamente em cima da subcamada MAC, em que os *switches* podem tratar um conjunto de conexões entre um par de dispositivos como se fossem uma conexão simples. Em alguns casos, é chamado de *trunking*, e a combinação de um conjunto de conexões também pode ser chamada de *virtual link* ou *trunk*, além de que uma porta que participa do Link Aggregation é chamada de interface de agregação (*aggregation port*). O Link Aggregation oferece alguns benefícios, como: (i) alta capacidade de conexão configurada entre um par de sistemas por combinar um grupo de conexões, ou seja, pode multiplicar a largura de banda da conexão, dependendo da quantidade de *links* que irão compor o “tronco” de portas; (ii) melhora a disponibilidade da rede, visto que, mesmo que uma falha de uma conexão subjacente em um grupo de conexões cause a redução da largura de banda, as conexões agregadas continuam funcionando (FEIT, 2000). É importante ressaltar que essas características somente funcionam se o sistema for obtido de um mesmo fabricante de *switches* e que o padrão 802.3ad é o esforço para que diversos fabricantes permitam que seus *switches* se tornem capazes da aplicação.

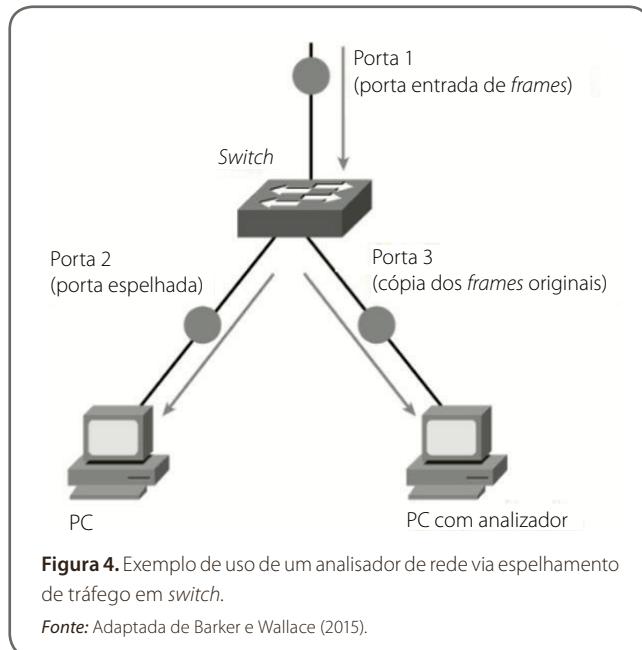
IEEE 802.1p

O IEEE 802.1p é o protocolo QoS/CoS da camada 2 da LAN para priorização de tráfego. Sua especificação permite que os comutadores da camada 2 priorizem o tráfego e realizem a filtragem dinâmica de transmissão múltipla, funcionando sobre o MAC e garantindo a não proliferação de transmissão múltipla além da camada 2 das redes comutadas. O IEEE 802.1p define oito níveis de prioridade, desde o nível 7, de maior prioridade, até o nível 0, de menor prioridade (JAVVIN TECHNOLOGIES, 2005). A IEEE recomenda:

- **Prioridade 7:** indicada quando há tráfego crítico da rede, como atualizações de tabela RIP (Routing Information Protocol; ou protocolo de informação de roteamento, em português) e OSPF (Open Shortest Path First; ou [protocolo] Aberto de Menor Rota Primeiro, em português).
- **Prioridades 6 e 5:** indicadas para aplicativos sensíveis ao atraso, como os de vídeo e voz interativos.
- **Prioridades 4, 3, 2 e 1:** devem variar de aplicativos de carga controlada, como *streaming* de multimídia e tráfego crítico aos negócios (p. ex., dados SAP), até perda de tráfego elegível.
- **Prioridade 0:** o valor zero é utilizado como padrão de melhor esforço, sendo invocado automaticamente quando nenhum outro valor é definido.

Espelhamento de tráfego

Alguns *switches* suportam a característica desejável por administradores de rede: fazer a cópia do tráfego visto de uma porta por uma outra porta com seu tráfego duplicado, em que um analisador de protocolo diretamente da porta do *switch* é conectado para monitorar o tráfego do equipamento. Assim, deve-se definir a porta do *switch* que será monitorada e o seu “espelho”, isto é, onde a porta do analisador será conectada (BARKER; WALLACE, 2015). A Figura 4, a seguir, apresenta um *switch* configurado com espelhamento de tráfego da porta 2 para a porta 3, permitindo que o analisador possa capturar os pacotes para análise via sua conexão à interface 3.



2 Principais características dos switches

Existem prós e contras quanto à aplicação de *switches* em redes de comunicação. Em suma, os *switches* são dispositivos de conexão que operam nas camadas física e de enlace de dados do modelo OSI, utilizado na internet. Eles podem ter velocidades relativamente altas de filtragem e repasse, visto que processam *frames* apenas até a camada 2 do modelo OSI. Além disso, eles possibilitam que cada estação em uma rede local tenha largura de banda dedicada a seu dispor. Com isso, há enlaces heterogêneos, uma vez que o *switch* isola um enlace do outro, e os diferentes enlaces na rede local podem operar em diferentes velocidades e ser executados através de diferentes mídias.

Os *switches* são transparentes e capazes de encaminhar e filtrar *frames*, além de construírem automaticamente a tabela de encaminhamento ao destino. Eles são do tipo *plug-and-play*, de modo que são apreciados por administradores de rede, pois não requerem a intervenção de um administrador de rede ou de um usuário. Assim, o administrador de rede que desejar instalar um *switch* não precisa fazer nada além de conectar os segmentos de LAN às interfaces/portas do *switch*. Além disso, o administrador não precisa configurar as tabelas de

comutação no momento da instalação. Outra característica dos *switches* é o fato de serem *full-duplex*, o que significa que, para qualquer enlace conectando um nó a um *switch*, ambos podem transmitir ao mesmo tempo sem colisões.

No entanto, os *switches* não bloqueiam o *broadcast*, de modo que não oferecem proteção contra “tempestades de *broadcast*”. Ou seja, permitem a transmissão de uma mensagem simultaneamente a todos os nós de uma rede, o que pode, em casos extremos, colapsar a rede inteira.

Os comutadores podem ser utilizados para redes institucionais (p. ex., rede empresarial local, rede de *campus* universitário, rede de aeroporto), visto que são redes consideradas pequenas, com algumas centenas de hospedeiros e alguns poucos segmentos de redes locais (LAN). Portanto, para essas redes, os comutadores serão satisfatórios, pois localizam o tráfego e aumentam a vazão agregada sem exigir nenhuma configuração de endereços IP (CARISSIMI; ROCHOL; GRANVILLE, 2009).

As principais características dos comutadores são listadas a seguir:

- permitem o isolamento de tráfego;
- possuem fácil utilização, bastando ligar e usar;
- não necessitam de um roteamento ótimo;
- possuem capacidade de gerenciamento;
- fornecem segurança aprimorada;
- facilitam o gerenciamento de rede (se um dispositivo não funcionar corretamente e enviar *frames* repetitivos, o *switch* pode detectar o problema e desconectar internamente o dispositivo com defeito);
- desconectam apenas o próprio nó que estava sendo utilizado até o cabo ser cortado do *switch*;
- coletam estatísticas sobre o uso da largura de banda, as taxas de colisão e os tipos de tráfego. Essas informações podem ser utilizadas para depurar e corrigir problemas, bem como para planejar como a LAN deve evoluir no futuro.

Tais características são encontradas em dispositivos de mercado, como o apresentado na Figura 5, em que pode ser visto o produto da Cisco. No mercado, existem *switches* simples, focados no uso doméstico e em redes simples, e *switches* complexos, com alta capacidade de gerenciamento, direcionados para o mercado corporativo, em que há necessidade de alto nível de processamento de dados, segurança e escalabilidade.



Figura 5. Representação de exemplo de marcado: Switches Cisco Catalyst 3850.

Fonte: Adaptada de Switches... (2020).

Ao observar a documentação do *switch*, é indicada uma série de números que mostram a capacidade de processamento/encaminhamento de pacotes do equipamento. No *backplane*, tem-se a referência de “largura do barramento” do equipamento, onde estão conectadas as portas/interfaces. Quando o barramento possui largura igual ou maior do que a soma das portas dos *switches*, afirma-se que ele é *non-blocking*, isto é, embora todas as portas estejam transmitindo ao mesmo tempo em sua velocidade máxima, o *backplane* é suficiente para dar vazão ao tráfego. Um exemplo de equipamento *non-blocking* é o Cisco 2960X-48TD-L, com LAN Base de 48 portas Gigabit + 2 TenGigabit. Esse *switch* tem 216 Gbps de *switching bandwidth* (ou *backplane*). Observe que:

- multiplicando o número de portas (48) pela velocidade (1.000) e por 2 (*full duplex*), tem-se 96 Gbps;
- somando-o às portas de *uplink* (2 portas * 10 Gbps * 2), tem-se 136 Gbps;
- somando-o à banda utilizada pelo módulo de empilhamento (80 Gbps), tem-se 216 Gbps.

No entanto, aumentar o *backplane* desse equipamento Cisco para 400 Gbps não trará benefício, uma vez que ele consegue encaminhar “apenas” 216 Gbps. Em contraponto ao equipamento *non-blocking* citado, em casos em que o *backplane* não suportar o fluxo agregado que está recebendo, ele terá de guardar na memória alguns dos *frames*, a fim de evitar o descarte deles; nesse caso, o *backplane* torna-se o gargalo da rede, o *blocking*.



Saiba mais

Os *switches* podem ser classificados quanto ao método de encaminhamento dos *frames* utilizado, como descrito a seguir.

- **Store-and-forward:** guardam cada *frame* em um *buffer* antes de encaminhá-lo para a porta de saída. Enquanto o *frame* está no *buffer*, o *switch* calcula o CRC e mede o tamanho do *frame*. Se o CRC falhar ou o tamanho for muito pequeno ou muito grande, o *frame* é descartado. Se estiver tudo certo, o *frame* é encaminhado para a porta de saída. Esse método assegura operações sem erro e aumenta a confiabilidade da rede, porém o tempo gasto para guardar e verificar cada *frame* adiciona um tempo de latência ao processamento dos *frames*.
- **Cut-through:** projetados para reduzir a latência indicada no *store-and-forward*. Esses *switches* minimizam o atraso de processamento lendo apenas os seis primeiros bytes de dados do *frame*, que contêm o endereço de destino e, logo, encaminham o pacote. No entanto, eles não detectam *frames* corrompidos causados por colisões, nem erros de CRC. Um segundo tipo de *switch cut-through*, o *fragment free*, foi projetado para eliminar esse problema, o qual sempre lê os primeiros 64 bytes de cada *frame*, assegurando que o *frame* tem, pelo menos, o tamanho mínimo.
- **Adaptative cut-through:** processam *frames* no modo adaptativo e suportam tanto *store-and-forward* quanto *cut-through*. Qualquer dos modos pode ser ativado pelo gerente da rede, ou o *switch* pode ser inteligente o bastante para escolher entre os dois métodos, baseado no número de *frames* com erro passando pelas interfaces/portas.

3 Criação de VLANs e suas aplicações

Em resposta à solicitação dos administradores de rede, que precisam atender inúmeros usuários que desejam uma maior flexibilidade quanto à sua posição geográfica de acesso à rede de comunicação de dados, os fabricantes e fornecedores de dispositivos de redes procuraram por um meio de recompor a fiação dos edifícios inteiramente em *software*. Assim, as alterações mecânicas para conectar um usuário ou um conjunto de usuários nas portas dos comutadores, trocando a conexão do cabo de uma porta para outra, deixam de ser uma prática, pois passa a ser utilizado um *software* no comutador, permitindo novos acessos do usuário. O conceito resultante é chamado de VLAN (Virtual Local Area Network; ou Rede Local Virtual, em português), padronizado pelo comitê do IEEE 802.1q (TANENBAUM, 2003). Os VLANs permitem suprir desvantagens até então comuns, listadas a seguir.

- **Falta de isolamento de tráfego:** apesar de ser possível localizar dentro de um único *switch* o tráfego de grupos, o tráfego *broadcast* ainda percorre toda a rede da instituição, de modo que limitar esse tráfego melhora o desempenho da rede local. Também é desejável limitar o tráfego *broadcast* da LAN por razões de segurança e de privacidade.
- **Uso ineficiente de switches:** imagine que, na instituição, existe a hierarquia três grupos em rede. Por uma nova necessidade, a instituição precisa ter 10 grupos. Assim, seriam necessários 10 *switches* do primeiro nível. Se cada grupo fosse pequeno, com menos de 10 usuários, um comutador/*switch* de 96 interfaces/portas seria suficiente para atender a todos, mas esse único comutador não fornecerá isolamento de tráfego.
- **Gerenciamento de usuários:** se um funcionário se locomove entre os grupos, o cabeamento físico deve ser mudado para conectar o funcionário a um *switch* diferente, visto que funcionários pertencentes a dois grupos dificultam o problema de gestão.

As VLANs se baseiam em *switches* projetados para reconhecê-las e podem ter alguns dispositivos, como *hubs* na periferia. Para configurar uma rede baseada em VLAN, o administrador da rede decide:

- quantas VLANs haverá;
- quais computadores ou outros dispositivos estarão em cada VLAN;
- qual será o nome de cada VLAN.

Em geral, as VLANs são identificadas informalmente por cores, pois, assim, é possível imprimir diagramas de cores mostrando o *layout* físico das máquinas, com os membros da LAN vermelha em vermelho, os membros da LAN preta em preto, e assim por diante. Isso permite que os *layouts* físico e lógico sejam visíveis em um diagrama único (TANENBAUM, 2003). A Figura 6, a seguir, apresenta um exemplo em diagrama com quatro redes locais físicas organizadas por duas VLANs, uma na cor preta e outra na cor vermelha, atendendo à comunicação de 15 dispositivos.

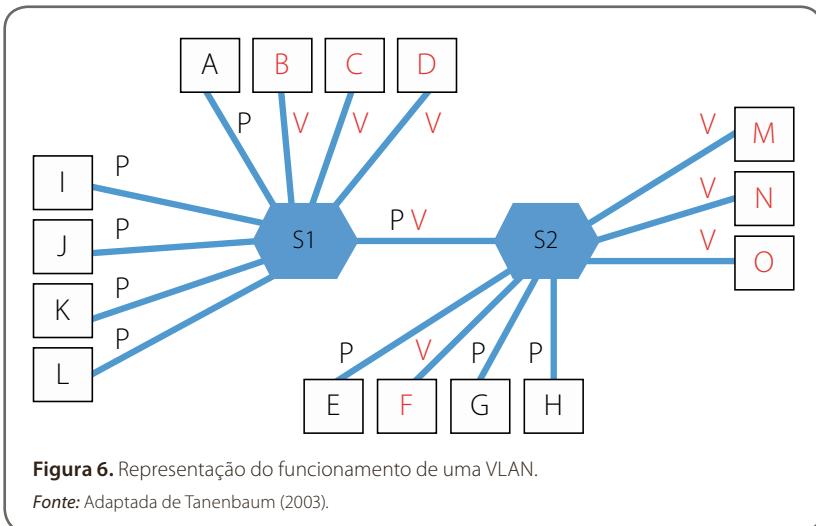


Figura 6. Representação do funcionamento de uma VLAN.

Fonte: Adaptada de Tanenbaum (2003).

Contudo, para que as VLANs funcionarem corretamente, faz-se necessário definir tabelas de configuração nos *switches*. Essas tabelas informam quais são as VLANs acessíveis através de cada uma das portas dos *switches*. Por exemplo, quando um *frame* chega da VLAN “preta”, ele é encaminhado para todas as portas marcadas com “P” caso o destino não seja identificado na tabela. Isso é válido para o tráfego comum, bem como para o tráfego de multidifusão e de difusão (*broadcast*). Em detalhe, o *switch* tem uma tabela/*buffer* listando o endereço MAC de cada dispositivo conectado, juntamente à VLAN em que o dispositivo está na rede. Sob essas condições, é possível misturar VLANs em uma LAN física, como na LAN composta pelos dispositivos A, B, C e D da Figura 6. Quando um *frame* chega, tudo que o *switch* faz é extrair o endereço MAC e procurar em sua tabela para identificar de qual VLAN ele veio.



Saiba mais

Para aprimorar seu conhecimento sobre *switches*, em seu navegador de preferência, acesse o YouTube e assista aos seguintes vídeos:

- Minicurso *switches* Huawei parte 3 – Tutoriais vídeo #02 – como configurar seu *switch* em L2;
- Configuração VLAN Switches Smart TP-Link;
- Tutorial: Como configurar os *switches* industriais Hirschmann;
- Configurando VLANs Tagueadas e não Tagueadas no Switch Ethernet SEL-2730M.



Exemplo

A seguir, confira um exemplo de itens a serem observados ao criar uma VLAN para uma empresa utilizando *switches*.

Inicialmente, faz-se necessário identificar as necessidades da rede, obtendo as informações sobre a quantidade de dispositivos que serão conectados, sejam eles computadores, impressoras ou outro dispositivo. Em seguida, é preciso saber a distância entre os dispositivos da rede e se haverá particularidades funcionais, como setores de administração e gestão, produção, compras, entre outros. Além disso, é recomendado considerar questões como escalabilidade e interesses em ampliações de departamentos e funcionários.

Após avaliar os documentos e obter as respostas da empresa, considere que se tem a necessidade de conectar 15 dispositivos, geograficamente divididos em duas áreas, com cada área dividida em outras duas subáreas. Para tanto, é preciso de uma boa resposta da rede e que haja segurança. Os grupos devem ser divididos em administração (compras, gestores, RH) e produção. Assim como na Figura 6, é possível utilizar dois *switches* (S1 e S2), de 24 portas cada, e configurar duas VLANs:

- o *switch* S1 conectado aos dispositivos A, B, C, D, I, J, K e L fisicamente;
- o *switch* S2 conectado aos dispositivos E, F, G, H, M, N e O fisicamente;
- a VLAN “Preta” (administração) conectada aos dispositivos A, E, G, H, I, J, K e L logicamente.
- a VLAN “Vermelha” (produção) conectada aos dispositivos B, C, D, F, M, N e O logicamente.



Referências

- BARKER, K.; WALLACE, K. *CompTIA Network+ N10-006 cert guide*. Indianapolis: Pearson Certification, 2015. 600 p.
- CARISSIMI, A. S.; ROCHOL, J.; GRANVILLE, L. Z. *Redes de computadores*. Porto Alegre: Bookman, 2009. 392 p. (Série Livros Didáticos Informática UFRGS, 20).
- FEIT, S. *Local area high speed networks*. Indianapolis: Sams, 2000. 665 p.
- FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. 4. ed. Porto Alegre: AMGH; Bookman, 2008. 1134 p.
- FOROUZAN, B. A; MOSHARRAF, F. *Redes de computadores: uma abordagem top-down*. Porto Alegre: AMGH; Bookman, 2013. 917 p.
- GUTIERREZ, J. *Selected readings on telecommunications and networking*. Hershey: IGI Global, 2008. 464 p.
- JAVVIN TECHNOLOGIES. *Network protocols handbook*. 2. ed. Saratoga: Javvin, 2005. 340 p.
- KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a internet: uma abordagem top-down*. 6. ed. São Paulo: Pearson, 2013. 656 p.
- SWITCHES Cisco Catalyst 3850 Series. *Cisco Systems*, San José, 2020. Disponível em: https://www.cisco.com/c/pt_br/support/switches/catalyst-3850-series-switches/series.html#~tab-models. Acesso em: 3 jun. 2020.
- TANENBAUM, A. S. *Redes de computadores*. 4. ed. Rio de Janeiro: Campus, 2003. 945 p.

Leituras recomendadas

COMO funciona um switch? Saiba como os switches são elementos essenciais da rede, que conectam seus dispositivos. *Cisco Systems*, San José, [2020?]. Disponível em: https://www.cisco.com/c/pt_br/solutions/small-business/resource-center/networking/network-switch-how.html. Acesso em: 3 jun. 2020.

CONFIGURAÇÃO VLAN Switches Smart TP-Link. [S. l.: S. n.], 2019. 1 vídeo (6 min 39 s). Publicado pelo canal TP-Link. Disponível em: <https://www.youtube.com/watch?v=UiQoK1727k8>. Acesso em: 3 jun. 2020.

CONFIGURANDO VLANs Tagueadas e não Tagueadas no Switch Ethernet SEL-2730M. [S. l.: S. n.], 2017. 1 vídeo (8 min 14 s). Publicado pelo canal SEL Brasil. Disponível em: <https://www.youtube.com/watch?v=drE1JnOKuq4>. Acesso em: 3 jun. 2020.

MINICURSO switches Huawei parte 3 – Tutoriais vídeo #02 – como configurar seu switch em L2. [S. l.: S. n.], 2019. 1 vídeo (5 min 15 s). Publicado pelo canal ClickMobile. Disponível em: <https://www.youtube.com/watch?v=768i3V9ST48>. Acesso em: 3 jun. 2020.

1.1 – TUTORIAL: Como configurar os switches industriais Hirschmann. [S. l.: S. n.], 2017. 1 vídeo (4 min 7 s). Publicado pelo canal Belden Inc. Disponível em: <https://www.youtube.com/watch?v=dRbLKUO-h8A>. Acesso em: 3 jun. 2020.



Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Encerra aqui o trecho do livro disponibilizado para esta Unidade de Aprendizagem. Na Biblioteca Virtual da Instituição, você encontra a obra na íntegra.

Conteúdo:



SOLUÇÕES
EDUCACIONAIS
INTEGRADAS

Dica do Professor

Em razão de tantos dispositivos e de tantas LANs diferentes que podem ser encontrados no mercado, é necessário um modo para configurar e interconectar as LANs. Para esse objetivo, são usados comutadores (*switches*).

Nesta Dica do Professor, acompanhe um tutorial que vai ajudá-lo a entender, de forma geral, o processo de configuração de VLAN em *switches*.



Aponte a câmera para o código e accese o link do conteúdo ou clique no código para accesar.

Exercícios

- 1) Em relação aos comutadores em LAN, além da redundância automática implementada pelo protocolo *Spanning Tree*, totalmente padronizado pelo IEEE, os fabricantes de comutadores costumam implementar um nível de redundância de *links*, chamado de *resiliência*.

Sobre os *links* resilientes, julgue as seguintes afirmações:

- I. Cada implementação quanto ao uso de *link* resiliente é proprietária, não sendo garantida a interoperabilidade entre comutadores de fabricantes diferentes.
- II. As aplicações do protocolo *Spanning Tree* e da definição de *links resilientes* podem ser aplicadas conjuntamente em um comutador.
- III. Quando o administrador da rede considerar necessário configurar o uso de *links resilientes*, a função de *Spanning Tree* deverá estar desabilitada no comutador.

Está correto o que se afirma em:

- A) I apenas.
 - B) II apenas.
 - C) III apenas.
 - D) I e II apenas.
 - E) I e III apenas.
- 2) Quanto ao método de encaminhamento dos pacotes utilizados por *switches*, tem-se um tipo de conexão especial que permite e possibilita aos dispositivos se comunicarem utilizando mais de um *link* em paralelo. Esses *links* em paralelo produzem benefícios, como a possibilidade de multiplicar a largura de banda da conexão, dependendo da quantidade de *links* que irão compor o “tronco” de portas, o *port trunk*.

Que tipo de conexão é esse?

- A) IEEE 802.3ad *Link Aggregation*.
- B) IEEE 802.1d *Spanning Tree*.

- C) Método *Store-and-Forward*.
 - D) Método *Cut-Through*.
 - E) Método espelhamento de tráfego.
- 3) Em se tratando de redes de comunicação, é prática fazer uso de *hubs*, *switches* e roteadores. Entre estes, embora um *switch* seja um comutador de pacotes do tipo armazena-e-repassa, ele é fundamentalmente diferente de um *hub* ou de um roteador, pois repassa pacotes usando endereços MAC, por exemplo.

Sobre as características dos *switches*, julgue as seguintes afirmações:

- I. São do tipo *plug-and-play*, uma propriedade que é apreciada por todos os administradores de rede, e também podem ter velocidades relativamente altas de filtragem e repasse.
- II. Seus *frames* são processados apenas até a camada 2, e, para evitar a ciclagem da transmissão de quadros, a topologia da rede de comutação está restrita a um *Spanning Tree*.
- III. Fornecem isolamento de tráfego mais robusto, controlam tempestades de *broadcast* e usam rotas mais inteligentes entre os hospedeiros da rede, além de fazerem uso de IP e camada 3 do modelo OSI.

Está correto o que se afirma em:

- A) I apenas.
 - B) II apenas.
 - C) III apenas.
 - D) I e II apenas.
 - E) I e III apenas.
- 4) As LANs empresariais modernas costumam ser configuradas hierarquicamente, com cada grupo de trabalho, ou departamento, com seu próprio *switch* de LAN conectado ao *switch* de LAN de outros grupos, por meio de uma hierarquia simples de *switches*.

Em relação ao mundo real do funcionamento dessas LANs, estão elencadas, a seguir, dificuldades do modelo implementado, que podem ou não ser resolvidas com um *switch* que suporte uma rede local virtual (VLAN):

I. Falta de isolamento do tráfego das LANs: apesar de a hierarquia localizar o tráfego de grupos dentro de um único *switch*, o tráfego *broadcast* ainda tem de percorrer toda a rede.

II. Uso ineficiente de *switches*: se, em vez de alguns poucos grupos, a empresa tivesse muitos grupos, por exemplo 10 grupos, seriam necessários 10 *switches* de conexão ao primeiro nível.

III. Gerenciamento de usuários: se um funcionário se locomove entre os grupos, o cabeamento físico deve ser mudado para conectar o funcionário a um *switch* diferente. Funcionários pertencentes a dois grupos dificultam ainda mais o problema.

Em relação a essas situações, marque a opção correta:

- A) Todas as situações são motivos para implementação de VLAN.
 - B) Nenhuma situação é motivo para implementação de VLAN.
 - C) Apenas a situação I é motivo para implementação de VLAN.
 - D) Apenas a situação II é motivo para implementação de VLAN.
 - E) Apenas a situação III é motivo para implementação de VLAN.
- 5) As redes de computadores inicialmente tinham sua divisão departamental realizada por separação física, ou seja, davam-se as separações topológicas em LANs físicas pela empresa. Porém, com o advento de VLANs, toda essa segmentação passou a ser lógica, ou seja, é possível criar diversas LANs independentemente da sua localização.

Sobre o conceito e o uso de VLANs, avalie as seguintes asserções:

I. As VLANs se baseiam em *switches* especialmente projetados para reconhecê-las.

PORTANTO

II. As VLANs precisam obrigatoriamente ter *hubs* na periferia da rede implementada.

Marque a opção correta:

- A) As asserções I e II são proposições verdadeiras, e a II é uma justificativa da I.
- B) As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa da I.
- C) A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.
- D) A asserção I é uma proposição falsa, e a II é uma proposição verdadeira.

E) As asserções I e II são proposições falsas.

Na prática

A maioria das empresas deseja ter uma LAN adequada à sua estrutura e às condições de preços. Porém, analistas e administradores de rede podem ter dificuldade em definir adequadamente os *switches* para que se possa compor a LAN de um *campus* universitário ou hospital, por exemplo.

Neste Na Prática, veja um conjunto de passos que podem ajudar na seleção de *switches* adequados a uma LAN.

ETAPAS QUE AUXILIAM NA ESCOLHA DE SWITCHES ADEQUADOS PARA UMA LAN

Juliano é administrador de rede e precisa definir os switches adequados para compor a LAN de um campus universitário. Para isso, ele vai aplicar um conjunto de passos que o ajudarão nessa escolha.

1 AVALIAÇÃO POR QUANTIDADE DE PORTAS/INTERFACES

Essa avaliação depende diretamente do projeto que Juliano está fazendo ao seu cliente: **se a demanda é por disponibilizar 200 pontos de rede, recomenda-se que sejam utilizados switches de 24 e/ou 48 portas**

Caso estejam em uma área de concentração, Juliano deve optar por 48 portas, mas, se o cliente tem departamentos não tão concentrados em uma mesma área, Juliano deve fornecer os switches de 24-portas.

A quantidade de switches, nesse caso, será a divisão de 200 por 24, o que resulta em 8,33 switches, ou seja, na necessidade de 9 switches, e uma reserva interessante de 16 portas. Caso Juliano opte por um switch de 48 portas, terá 5 switches e uma reserva de 40 portas.

2 AVALIAÇÃO POR VELOCIDADE

Existem switches para uso de conexão em fastethernet e gigabitethernet, tal como é encontrado no labem em placas de rede de conexões. Juliano sabe que a demanda é necessidade das conexões da LAN de seu cliente e sabe que são muitos os casos, se não a maioria, em que **switches de 10/100/1.000Mbps com suporte a interfaces a gigabit standerão muito bem à LAN** e a custos razoáveis.

3 SWITCHES DE CAMADA 2 OU 3

Esse passo é importante devido ao custo adicional que pode existir pelo fato de o switch suportar recursos de roteamento (switch camada 3, ou Layer 3, ou L3). Nesse caso, Juliano sabe que **switches L3 são usados para distribuição da rede, e switches L2, para a conexão aos usuários fim da rede**. Ainda sabe que os switches de camada 2 como camada de acesso têm os custos mais baixos no mercado. Independentemente disso, ele vai optar por **switches gerenciáveis, com suporte à VLAN**.

No caso da necessidade de uso de switches L3, é importante que eles suportem IPv4 e IPv6 e roteamento entre VLANs estático e dinâmico em ambas as versões do protocolo IP.

4 UPLINK: QUANTIDADE E TIPO

Juliano vai deixar as portas "normais" do switch para conexão de clientes (end points) e **optar por switches que tenham portas especiais para uplink**, como portas SFP ou RJ45. Além disso, ele pode optar por switches com 2 ou 4 interfaces uplink, podendo ainda ser UTP ou fibra óptica com módulos SFP. Além disso, ele vai escolher entre **links de par metálico ou uso de fibra, em velocidades de 1Gbps ou 10 Gbps**, dependendo da distância entre os switches.

Exemplo de 5 switches de acesso, atendendo aos 200 usuários, e 2 switches para distribuição, com uso de 10 uplink entre os switches:

5 AVALIAÇÃO POR SWITCHES INDEPENDENTES OU EMPILHADOS

Essa avaliação também depende diretamente do projeto que Juliano está fazendo ao seu cliente, pois **tanto uma configuração usando switches independentes quanto uma usando switches empilhados poderá funcionar**. Basicamente, a diferença é que, estando empilhados, em vez de os switches serem cabeados pelos uplinks, são conectados por cabos especiais a formação da pilha, formando um grupo gerenciável que pode ser o conjunto de todos os switches que compõem um. Esta pode ser a melhor solução por economizar portas, cabos e esforços de gerenciamento. Entretanto, Juliano está atento, pois, algumas vezes, não se consegue o empilhamento fazendo-se uso de diferentes fabricantes.

6 RECURSOS SOLICITADOS OU DESEJÁVEIS

Levando em conta que é possível ter nas redes vários serviços sendo executados ao mesmo tempo, como dados da Intranet e da Internet, voz e vídeo sobre IP e tráfego sem fio, Juliano lembrou de **avaliar critérios de segurança**, como **firewall**, pois faz, certamente, uso de conexão UTP de qualidade de serviço (QoS) e de um mínimo de PoE (Power over Ethernet) alimentando access-points.

7 SEGURANÇA

Por fim, Juliano está ciente de que a segurança é um item importantíssimo na definição pela compra do switch, para evitar mau funcionamento da LAN, ataques via portas do switch e acessos inadequados. Geralmente, os fabricantes indicam as melhores práticas de segurança aplicadas aos seus switches, como **desativação de serviços desnecessários, senhas fortes, uso de SSH e HTTPS para gerenciamento, proteção contra falsificação de endereço MAC, proteção contra ataque de MAC-flooding**, entre outras.

A aplicação desse conjunto de passos permitiu a Juliano atender à demanda de seu cliente com atenção aos requisitos de funcionalidade e segurança, além de permitir a avaliação de custos e escalabilidade.



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Saiba mais

Para ampliar o seu conhecimento a respeito desse assunto, veja abaixo as sugestões do professor:

Segmentação de redes com VLAN

Com a leitura deste artigo, saiba mais sobre os riscos e os problemas provenientes do uso de uma rede não segmentada, bem como sobre o conceito de VLAN, suas características, classificação e configuração.



Aponte a câmera para o código e accese o link do conteúdo ou clique no código para accesar.

VLANs: abordagem prática para criação e configuração em ambiente simulado e ambiente real

Este trabalho apresenta um objeto de aprendizagem e a utilização de VLAN. Tal objeto é implementado por um vídeo, contendo a apresentação dos conceitos, além de instruções para a criação e a configuração de VLANs em ambientes simulado e real. Confira.



Aponte a câmera para o código e accese o link do conteúdo ou clique no código para accesar.

Configuração VLAN: *Switches Smart TP-Link*

Assista a este vídeo e aprenda, passo a passo, a configurar uma VLAN em alguns modelos de switches da TP-Link.



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

IEEE 802.1p - QoS na camada MAC

No *link* a seguir, acompanhe um estudo dos protocolos descritos em IEEE (Institute of Electrical and Electronics Engineers) 802.1p, 802.1D e 802.1p, que são protocolos relacionados à camada física e de enlace.



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Configuração básica do *switch* Cisco SG30028

O SG30028 é um *switch* totalmente gerenciável, com 24 portas *Gigabit*, 4 portas *Gigabit* de *uplink* e 2 portas *Gigabit SFP* para *uplinks*. Neste vídeo, aprenda a configurá-lo.



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Configuração do *switch* em L2

Assista a este vídeo e aprenda a configurar o *switch* em L2 a partir do detalhamento das linhas de comando.



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Configuração de VLANs tagueadas e não tagueadas no switch Ethernet SEL-2730M

O tagueamento de VLANs é benéfico à rede de comunicação, pois, por meio do direcionamento, envia mensagens apenas aos equipamentos que realmente necessitam recebê-las, diminuindo o tráfego de rede e o processamento de mensagens desnecessárias. Assista a este vídeo e aprenda a configurar VLANs tagueadas e não tagueadas no switch de comunicação SEL-2730M.



Aponte a câmera para o código e accese o link do conteúdo ou clique no código para acessar.