Sistemas de Conectividade

Aula 13 - Redes Virtuais - Vlans - Parte 1

Apresentação

Na aula passada você estudou computadores virtuais usando o software VirtualBox. Nesta aula você aprenderá um pouco mais sobre os *switches*, seus detalhes e modos de operação, além de como o *switch* armazena o MAC de cada computador ligado a ele. Iniciará também o estudo sobre Redes Locais Virtuais, conhecidas como VLAN (*Virtual Local Area Network*).

Objetivos

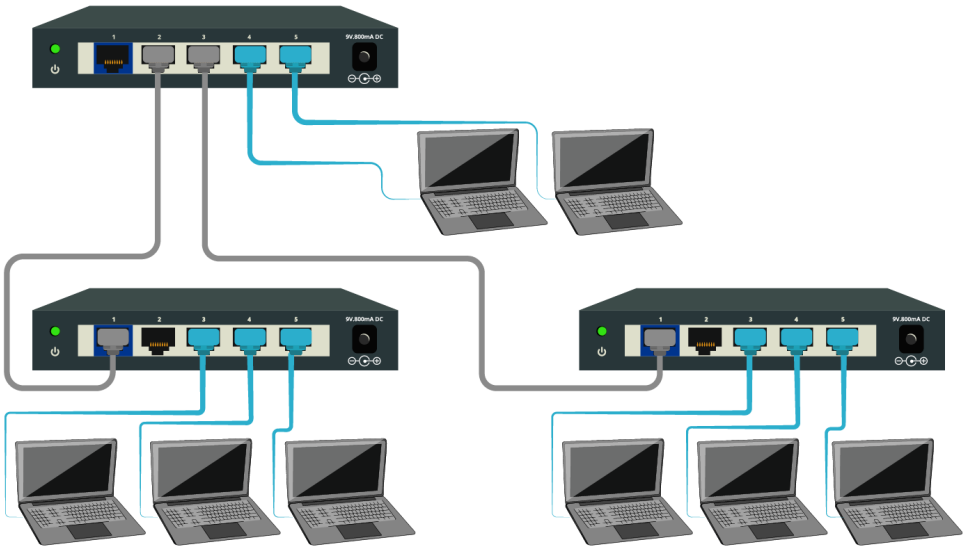
- Definir o funcionamento dos *switches* e seus modos de operação;
- Estudar a capacidade de aprendizagem de endereços MAC pelos *switches*;
- Conhecer o protocolo STP que evita loops em redes Ethernet;
- Definir o conceito de VLAN e suas formas de uso.

Aprendendo um pouco mais sobre os Switches

Nós já falamos sobre *switches* na aula 3, na qual mostramos a sua função, a diferença entre ele e um hub, e a sua relação com as pontes (bridges), lembram? Agora, nos aprofundaremos um pouco mais nesse equipamento de camada dois (enlace) que é de vital importância nas redes de computadores.

Sabemos que os switches podem ter diversos números de portas a depender do modelo, sendo os mais comuns os de 4, 8, 16 e 24 portas, e, em geral, eles apresentam uma, duas ou quatro portas com velocidades maiores que as demais, as quais são usadas para fazer as interligações entre os *switches*. E que interligação é essa? Como dissemos, a quantidade de portas dos *switches* mais comuns é de até 24 portas, e muitas vezes em nossas redes o número de computadores é bem superior ao número de portas dos *switches*. Surge, então, a dúvida: o que fazer para ligar todos os computadores na mesma rede se um único *switch* não comporta todas as máquinas? É necessário interligar os *switches*, conforme mostra a **Figura 1**. Esse tipo de interligação também pode ser chamado de cascateamento de *switches*.

Figura 01 - Cascateamento de *switches.*



Fonte: http://www-personal.umich.edu/~csev/hng/book/06wiring/ Acesso em: 20 ago. 2016.

Podemos interligá-los de algumas formas. Se ligarmos um cabo de rede de uma porta qualquer de um *switch* a outra porta qualquer do outro *switch*, eles já estarão interligados e poderemos adicionar máquinas em ambos, que elas terão capacidade de se comunicar, fazendo parte da mesma rede.

Como dito antes, existem portas no *switch* com velocidades maiores e é bastante comum utilizarmos essas portas para fazer essa ligação entre eles, o que permitirá maior velocidade de transferência de dados entre os *switches*. Isso é necessário, pois todo o tráfego gerado pelas máquinas de cada *switch* fluirá apenas por essa porta. Vale salientar que essa interligação de switches usando cabo de rede só permite a interligação de até cinco *switches*.

Já vimos que podemos interligar *switches* usando um cabo normal ligando uma ponta em cada *switch* e que, em geral, são usadas as portas mais rápidas. Mas, se quisermos que a velocidade de transmissão dos dados entre os *switches* seja ainda maior, podemos fazer essa ligação usando mais de um cabo para formar esse link entre os *switches*. Esse processo é denominado **Link Aggregation** (enlace agregado). Para isso funcionar é necessário configurar as portas de cada *switch* que participarão dessa ligação com a opção de enlace agregado. No final, a velocidade final do link agregado será a soma das velocidades das portas que participam da agregação.

Por exemplo, se foram usados três cabos ligando portas de 100 Mbps para essa interligação, a velocidade de transmissão entre os *switches* será de 300 Mbps (soma das velocidades das três portas), além disso, essa ligação servirá de redundância, pois se uma das portas apresentar algum problema e parar de funcionar, o tráfego entre os *switches* ficará dividido entre as outras duas portas que permanecerem funcionando, agora a 200Mbps (soma das velocidades das duas portas que restaram funcionando).

Alguns tipos de *switches*, os melhores e mais caros, têm portas feitas especialmente para interligar *switches* que usam cabos específicos para isso e têm uma velocidade muito superior à das portas normais.

Você acha que os quadros com endereços *multicast* e *broadcast* são repassados de modo diferente pelos *swicthes*? Se você respondeu sim, acertou. Enquanto quadros com endereços *unicast* são encaminhados apenas na porta onde a estação de destino está conectada, quadros *multicast* e *broadcast* são encaminhados por

todas as portas do *switch*. Portanto, mesmo que sua rede utilize apenas *switches*, lembre-se, um quadro enviado para um endereço de *broadcast* ocupará toda a rede, pois será retransmitido por todas as portas de todos os *switches*. Desse modo, embora os endereços *broadcast* sejam importantes para diversas aplicações, se utilizados em excesso, eles podem comprometer o desempenho da rede. Esse é um dos fatores que fazem com que as pessoas evitem criar redes com um número muito alto de máquinas, preferindo dividir a rede em várias redes menores.

Modos de Operação dos *Switches*

Você já sabe que a função do *switch* é interligar as máquinas da rede, permitindo que todas se comuniquem entre si. Veremos agora que eles podem trabalhar em quatro diferentes modos de operação: *cut-through, store-and-forward, adaptative cut-through* e ainda o *fragment-free*. No entanto, abordaremos somente os dois primeiros modos, pois eles é que são usados na prática.

No modo **cut-through**, o *switch* já começa a retransmitir os quadros para o endereço de destino assim que recebe a informação no quadro onde esse endereço está. Perceba que aqui o *switch* não faz análise alguma no quadro, repassando-o para a porta onde está a estação de destino, da mesma forma que recebeu. Uma vantagem desse modo de operação é que o quadro fica pouco tempo dentro do *switch*, pois é repassado assim que chega, e isso reduz a latência (Período de inatividade entre um estímulo e a resposta por ele provocada.), diminuindo o trabalho executado pelo *switch*.

Já no modo **store-and-forward**, o *switch* recebe o quadro da porta de origem, armazena-o na memória, faz alguns tipos de checagens e depois o encaminha para a porta de destino. Isso lhe dá a possibilidade de descartar os quadros inválidos e de solicitar a retransmissão dos quadros defeituosos. Quais as vantagens que esse modo oferece em relação ao outro? Bem, ele oferece mais estabilidade e um uso mais eficaz da rede, além de permitir que os *switches* trabalhem com as portas em diferentes velocidades, sem precisar diminuir a velocidade da porta de maior velocidade para ficar compatível com a de menor.

Capacidade do *Backplane*

O circuito interno do barramento de comunicação do *switch*, chamado de *backplane*, é responsável por fazer a movimentação dos pacotes entre as portas. Esse barramento deverá ter uma capacidade de transferir dados muito superior à velocidade das portas do *switch*, pois ele precisa encaminhar ao mesmo tempo todos os dados que estão chegando ou saindo do *switch* de cada porta. Assim, a relação existente entre a velocidade do *backplane* com a de um *switch* é de que a do *backplane* seja pelo menos a metade da soma das taxas máximas de transmissão de todas as portas do *switch*, para o caso de elas serem *half duplex*. Quando as portas estiverem operando no modo *full duplex*, a capacidade de repasse dos pacotes deverá ser igual ou maior à soma das taxas máximas de transmissão das portas do *switch.*

Atividade 01

---

1. Quais são as vantagens e desvantagens dos modos de operação *cut-through* e *store-and-forward?*

Para checar sua resposta clique aqui.

Resposta

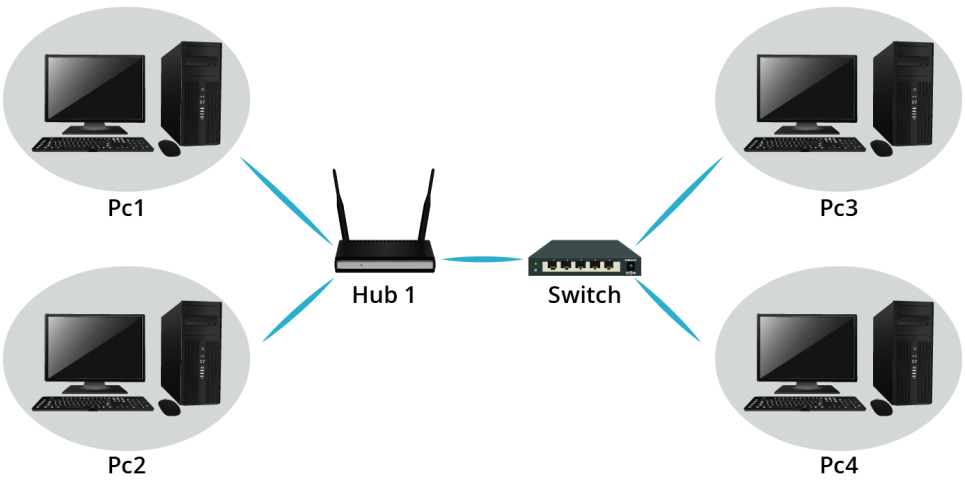
1. O modo de operação cut-though tem a vantagem de tornar a entrega dos quadros pelo switch mais veloz, já que o switch não analisa se o quadro está íntegro (foi transmitido sem erros). No entanto, justamente por não fazer essa análise, o cut-though fica em desvantagem em relação ao modo de operação store-and-forward, o qual realiza essa checagem, fazendo com que somente os quadros íntegros sejam encaminhados para a porta de destino. Outra vantagem do store-and-forward é permitir que o switch trabalhe com portas em diferentes velocidades sem ter de diminuir a velocidade da porta de maior velocidade para ficar com a de menor velocidade, como acontece no modo cut-though.

Capacidade de Aprendizagem de Endereços MAC

Como já vimos, os *switches* são equipamentos “inteligentes”, pois eles possuem a capacidade de aprender os endereços MAC e as portas de origem dos computadores que estão ligados a ele. Essa aprendizagem é feita por meio de uma tabela, na qual o *switch* armazena todos os endereços MAC “vistos” em cada porta. Assim, os *switches* implementam o repasse dos quadros baseados nas informações contidas nessa tabela, checando o endereço de origem e o de destino de cada quadro. Toda vez que um quadro chega ao *switch*, este checa se o endereço de destino já está na tabela, a fim de enviar somente para a porta associada àquele endereço. Caso não esteja, esse quadro é enviado para todas as portas. Perceba que nesse segundo caso, o envio do *switch* é similar ao de um *broadcast*, e aumenta o tráfego na rede. Por fim, quando o destino receber esse quadro e o responder, será armazenado seu endereço MAC na tabela SAT (*Source Address Table*) do *switch*.

Essa aprendizagem automática realizada pelos *switches* pode ser dividida em 5 partes. Para apresentá-las, usaremos o cenário apresentado na **Figura 2**, em que os computadores pc1 e pc2 estão ligados a um *hub* que, por sua vez, está ligado a um *switch*; enquanto os computadores pc3 e pc4 estão ligados diretamente ao *switch*.

Figura 02 - Cenário com quatro computadores, um *hub* e um *switch*.



Fonte: Elaborado pelo Autor.

1. **Aprendizado**: sempre que o computador pc1 enviar um pacote para o computador pc3, o qual está conectado em uma porta diferente, o *switch* automaticamente aprende em que porta está conectado o computador pc1 e salva essa informação em sua tabela.

2. **Flooding (inundação)**: como o *switch* não sabe em que porta o computador pc3 está conectado, ele envia o pacote para todas as portas, exceto à porta na qual o pacote chegou. Como o pacote está endereçado ao computador pc3, somente este recebe o pacote e envia uma resposta ao computador pc1, para que o computador pc1 saiba que o pacote chegou ao destino. Com isso, o *switch* fica sabendo qual porta está conectada ao computador pc3 e salva essa informação em sua tabela SAT.

3. **Encaminhamento:** agora o *switch* sabe quais portas estão conectadas aos computadores pc1 e pc3 e simplesmente encaminha o pacote do computador pc3 para o computador pc1. Então, todos os pacotes subsequentes que forem trocados entre esses dois computadores são encaminhados diretamente para as suas portas destinos.

4. **Filtragem:** quando o computador pc2 envia um pacote para o computador pc1, esse pacote chega até o *switch*, o qual checa o pacote e adiciona uma entrada referente ao computador pc2 em sua tabela SAT. Uma vez que o computador pc1 já está na tabela, o *switch* sabe que ambos os computadores estão conectados à mesma porta e, portanto, não precisa reenviar o pacote para estabelecer a comunicação. Com isso, o *switch* filtrará os pacotes entre computadores pc1 e pc2.

5. **Envelhecimento:** como os *switches* possuem uma quantidade limitada de memória para armazenamento da tabela SAT, a técnica de envelhecimento é utilizada para liberar espaço nessa tabela quando uma determinada entrada não é utilizada por algum tempo. Com isso, computadores que foram desligados ou desconectados da rede não ficam ocupando espaço na tabela SAT do *switch*, o que resulta na liberação do espaço para o registro de outros computadores.

Protocolo IEEE 802.1D Spanning Tree

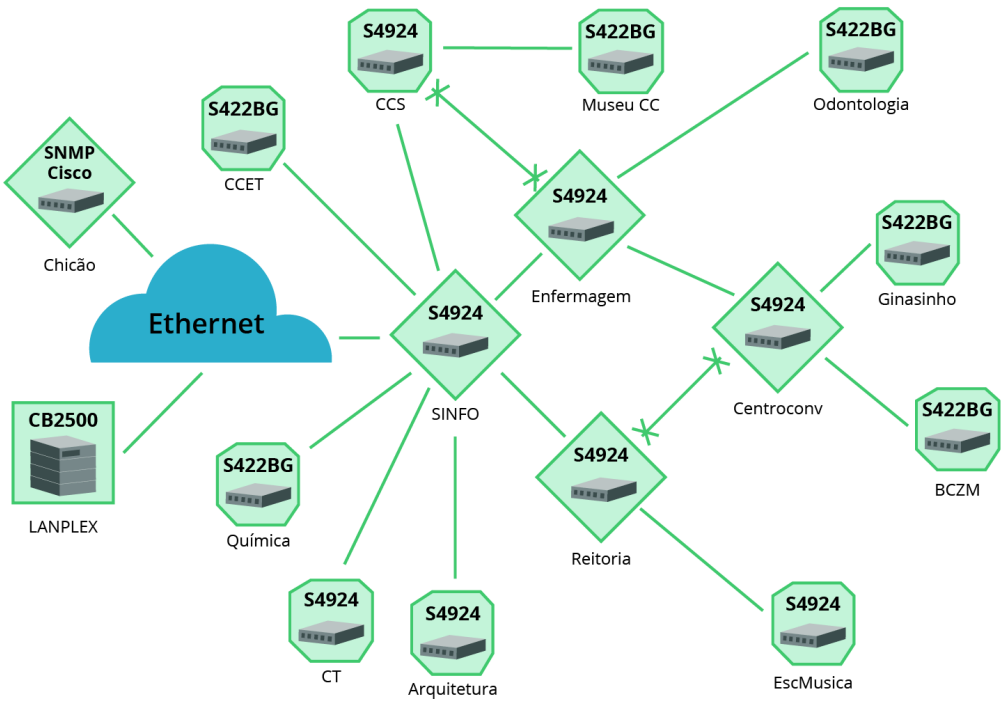
Você já viu nesta aula que diversos *switches* podem ser interligados de diversas maneiras. Entretanto, isso gera um problema, pois, durante a fase de *flooding*, um pacote *broadcast* é enviado a todas as portas do *switch*, as quais podem estar

ligadas a outros *switches*, fazendo com que o processo se repita. Por causa disso, é necessário ter bastante cuidado, quando interligamos vários *switches*, para não criarmos *loops* entre eles, o que pode gerar um congestionamento de *broadcast* na rede.

Para tentar evitar a ocorrência desses congestionamentos e *loops*, foi criado o protocolo *spanning tree* (STP), padronizado pela IEEE com a especificação 802.1D. Esse protocolo permite detectar se um *switch* tem mais de uma maneira de se comunicar com um computador, sendo capaz de determinar o melhor caminho para um determinado *host* e de desativar os caminhos menos eficientes ou que apresentam uma largura de banda menor. Além disso, esse protocolo também guarda os outros caminhos, sendo capaz de habilitar um dos caminhos menos eficientes caso o mais eficiente venha a falhar.

A **Figura 3** mostra um exemplo da antiga topologia da Rede UFRN, em que aparecem switches instalados em algumas unidades da universidade, sendo possível perceber dois loops entre os switches do backbone – um entre o switch do CCS (Centro de Ciências da Saúde), Enfermagem e SINFO (Superintendência de Informática) e o outro entre Enfermagem, Centro de Convivência, Reitoria e SINFO.

Figura 03 - Antiga Rede UFRN mostrando loops desativados pelo STP.



Fonte: Elaborado pelo Autor.

Observe que, para cada loop, é mostrado enlaces com um “X” nas portas dos switches, indicando que o link estará inativo até que uma nova topologia seja montada evitando o loop. Por exemplo, se o enlace entre a SINFO e o CCS falhar, o enlace entre o CCS e a Enfermagem é reativado, garantindo a conectividade entre todos os switches.

Atividade 02

---

1. Como funciona o processo de aprendizagem de endereço MAC nos *switches?*
2. Já que *loop* em uma rede Ethernet é um problema, por que alguns backbones de rede ainda possuem loops? Qual o benefício de se ter um *loop*?

Para checar sua resposta clique aqui.

Respostas

1. O processo de aprendizagem de endereço MAC por porta no switch acontece da seguinte forma: toda vez que chega um quadro no switch, este observa o endereço MAC de origem do quadro e a porta por onde aquele quadro chegou, assumindo que o computador com esse endereço MAC está ligado a essa porta. Assim, os quadros com destino a esse endereço MAC serão encaminhados apenas a essa porta.
2. Um loop em um backbone de rede significa que temos uma espécie de anel de conectividade entre todos os pontos que formam o backbone. Essa topologia é especialmente interessante quando se quer garantir a conectividade mesmo na falha de um enlace qualquer entre os pontos. Por exemplo, imagine um anel com três pontos: A, B e C, interligados via enlaces de A com B, B com C e C com A. Caso o enlace de B com C falhe, por exemplo, B ainda pode falar com C por intermédio de A.

Dividindo a Rede Física em Redes Virtuais: VLAN

Estudaremos agora um pouco mais sobre o conceito de VLAN (*Virtual LAN – Local Area Network*), que é o artifício usado para melhorar a forma de gerenciar as redes. O padrão que descreve essa tecnologia é o **IEEE 802.1Q**, e ele será mais detalhado na próxima aula

Antes de estudarmos VLAN, é importante mencionar que nem todos os *switches* a suportam. Com isso, podemos dividir os *switches* em duas categorias, com base na possibilidade de configuração. O ***switch* gerenciável** é aquele que pode ser configurado, permitindo a alteração de diversos parâmetros de funcionamento do *switch*, tais como desativar uma determinada porta ou um conjunto de portas, determinar a prioridade de portas e permitir a criação de VLAN. O ***switch* não gerenciável** já vem pronto para o uso e não permite que você faça alterações. Geralmente um *switch* não gerenciável é utilizado apenas em redes residenciais.

Criar VLAN em um switch é dividi-lo logicamente (não fisicamente), de forma que ele "pareça" ser dois ou mais equipamentos distintos. As portas de cada parte dessa divisão lógica não podem se comunicar diretamente, visto que estarão isoladas pela configuração empregada nas portas do *switch*. Para cada VLAN que eu crio, posso associar algumas portas, e apenas as portas que estiverem associadas a essa VLAN conseguirão se comunicar. Contudo, vale frisar que, embora seja como se dividíssemos o *switch* fisicamente, tudo é feito logicamente por *software*. Vamos exemplificar isso para simplificar e facilitar o entendimento. Suponha que criamos uma VLAN e atribuímos o número 10 a ela (pois as VLAN's têm números de 0 a 4096 como identificadores) e associamos a essa VLAN as portas 1,2,3,4 e 5 e às portas restantes associamos a VLAN 11. Dessa forma, nenhum equipamento que esteja nas portas da VLAN 10 poderão se comunicar (enviar pacotes) diretamente para a VLAN 11 e vice-versa.

Assim, perceba que a função de uma VLAN é isolar grupos de computadores na rede. Elas permitem que computadores conectados em vários *switches* diferentes façam parte da mesma rede (VLAN). Além disso, cada par de *switches* pode estar conectado por um único cabo, ou seja, não é necessário um cabo para cada VLAN. Dentre algumas razões para a adoção de VLAN, podemos citar as questões de segurança, separando computadores que contêm dados sigilosos do resto da rede,

reduzindo, assim, a possibilidade de acesso não autorizado; ou a divisão em departamentos, em que uma empresa poderia configurar VLAN para os departamentos, os quais utilizam muito a Internet, ou para conectar categorias específicas de empregados em departamentos diferentes (como gerentes).

Tipos de VLAN

Existem algumas formas de se criar VLAN, mas abordaremos apenas as mais usadas.

- **VLAN por porta:** o administrador da rede especifica a qual VLAN cada porta irá pertencer. Os equipamentos que forem ligados nessas portas farão parte daquela VLAN especificada. Esse é o tipo mais utilizado de VLAN.

- **VLAN por MAC *address:*** essa forma oferece algumas vantagens, mas é muito trabalhosa, pois o administrador tem de pegar os MAC's de cada equipamento e cadastrar no *switch* como fazendo parte de uma determinada VLAN. Assim, mesmo que o equipamento mude de porta, ele continuará na mesma VLAN, pois não estará atrelada à porta e sim ao MAC.

- **VLAN por autenticação 802.1X:** nesse método, só após ser autenticado na rede, o usuário poderá fazer alguma coisa. E podem ser criados vários tipos de configuração para os usuários, e assim, mesmo que pessoas diferentes se autentiquem na mesma máquina, cada pessoa obterá recursos diferentes. É importante entendermos o seguinte: a fim de os equipamentos que fazem parte de VLAN's diferentes poderem se comunicar, é necessário o uso de um roteador (conectado às várias VLAN's), o qual roteará os pacotes entre as redes, assim como acontece com as redes separadas fisicamente.

Na próxima aula, abordaremos detalhadamente o primeiro tipo de configuração de VLAN, o que é feito por porta do switch. Até lá!

Atividade 03

1. O que são redes virtuais (VLAN)?
2. Quais os tipos de VLAN? O que as diferenciam?

Para checar sua resposta clique aqui.

Respostas

1. São segmentações da rede física criadas a partir dos switches para isolar grupos de computadores por um determinado contexto ou objetivo comum.
2. Existem a VLAN por porta, por MAC address e por autenticação 802.1x. A VLAN por porta separa as redes através da conectividade com cada porta do switch. A por MAC address cria a VLAN a partir dos endereços MAC dos computadores. Já a por autenticação 802.1x usa esse protocolo de autenticação para identificar o usuário e definir a qual VLAN cada usuário pertence.

Leitura Complementar

1. 802.1Q-2014 - Bridges and Bridged Networks http://www.ieee802.org/1/pages/802.1Q-2014.html.
2. Wiring Your Home http://www-personal.umich.edu/~csev/hng/book/06wiring/.

Resumo

Nesta aula, você aprendeu mais detalhes sobre o funcionamento dos switches, seus modos de operação e como eles “aprendem” os endereços MAC ligados a cada porta. Além disso, iniciou o estudo sobre as redes locais virtuais (VLAN), vendo que é possível criar, de maneira lógica, redes virtuais a partir de uma rede física real. Na próxima aula você estudará detalhadamente o protocolo de VLAN, iniciando a partir da motivação para se criar VLAN’s e, em seguida, aprendendo como elas são configuradas nos *switches*.

Autoavaliação

1. Descreva quais as principais diferenças entre um hub e um switch.
2. Como se chama o protocolo da camada de enlace que é manipulado pelos switches?
3. Cite uma situação em que seria interessante o uso de VLAN.
4. Para um sistema de rede sem fio de um campus universitário, onde centenas ou até mesmo milhares de alunos precisam ter acesso a uma rede sem fio, qual o melhor tipo de VLAN a utilizar? Justifique.

Para checar sua resposta clique aqui.

Respostas

1. Um hub implementa a comunicação em barra repetindo o sinal que chega em uma porta em todas as outras, não havendo qualquer processamento do que é enviado pelos computadores ligados a ele. Já o switch implementa uma comunicação em estrela, analisando o destino de cada quadro e se o quadro foi transmitido sem erros.

2. O protocolo da camada de enlace manipulado pelos switches é o Ethernet.

3. Uma situação que demanda o uso de VLAN é separar o tráfego das diversas redes pertencentes a uma organização pelo tipo de uso dos computadores nessas redes, tendo cada departamento, por exemplo, sua VLAN. Esse esquema de segmentação da rede possibilita o compartilhamento de recursos na rede apenas para os computadores que fazem parte da VLAN onde o recurso se encontra.

4. Em uma rede Wi-Fi de um campus, onde temos diversos tipos de usuários (alunos, professores, visitantes, etc.), o melhor tipo de VLAN a se utilizar é o de autenticação 802.1x, o qual permite identificar o usuário do Wi-Fi e encaminhá-lo para a VLAN (rede) ao seu perfil de acesso aos recursos da rede.

Referências

FOROUZAN, B. **Comunicação de dados e redes de computadores.** 3. ed. Bookman, 2006.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet.** 3. ed. São Paulo: Addison Wesley, 2006.

TANENBAUM, A. S. **Redes de computadores.** 4. ed. Editora Campus, 2003.