Redes Locais Virtuais (VLAN) e Equipamentos

Neste capítulo serão abordados os principais equipamentos utilizados em uma rede local (LAN), e como implantar redes locais virtuais (VLAN).

Objetivos

Ao final deste capítulo, você saberá:

- Distinguir os diferentes equipamentos de uma rede local
- Escolher quais equipamentos são necessários para cada estrutura de rede
- Como configurar e planejar redes virtuais

Introdução

Todas as redes locais necessitam de concentradores para interligar computadores e outros equipamentos, como impressoras e *Access Points*. Inicialmente em uma rede de pequeno porte é possível utilizar equipamentos como *Hubs*. Na medida em que esta rede assume maiores proporções, são necessários novos investimentos, como a inclusão de *Switches*, posteriormente roteadores e a divisão do tráfego em redes virtuais.

Contudo, a definição do porte de uma rede não depende apenas da quantidade de computadores e equipamentos que ela interliga, a equação é bem mais complexa. Pois depende principalmente das necessidades dos usuários dessa rede, como por exemplo: interligação entre diferentes localidades, distância entre os equipamentos e do tráfego gerado e recebido.

Nesse sentido, neste capítulo serão descritos os diferentes equipamentos utilizados em uma rede local e quais suas principais características que devem ser observadas durante a escolha desses equipamentos, bem como, o funcionamento e a configuração de redes virtuais.

Hubs

Os *hubs*, ou concentradores (Figura 3.1), foram os primeiros equipamentos utilizados em redes locais com topologia em estrela (protocolo de enlace *Ethernet*), onde todos os equipamentos de rede são conectados através de um cabo UTP até as portas do equipamento.

Figura 3.1: Ilustração de um HUB (Figura 467593871)

Os *hubs* funcionam por *broadcast*, isso é, quando qualquer equipamento da rede realiza uma transmissão, todos os outros equipamentos recebem esta transmissão e cada um decide se aquela informação deve ser encaminhada da camada de enlace para a camada de rede do seu equipamento, ou descartada. Observe que dessa maneira, apenas um computador pode transmitir por vez, limitando o uso de *hubs* para redes que possuem poucos computadores, ou baixo tráfego da rede. Em redes domésticas, onde o objetivo é a conexão com a Internet, esse equipamento atende perfeitamente a necessidade, pois com uma conexão de 30 Mbps (Megabits por segundo) para a Internet, possuindo 5 computadores conectados a uma velocidade de 1 Gbps (Gigabits por segundo) até o *hub*, não haverá gargalo de tráfego no HUB, e sim no roteador conectado na Internet.

Como os *hubs* estão a bastante tempo no mercado, sua velocidade pode variar: 10 Mbps, 100 Mbps e 1Gbps. A sua quantidade de portas também é bastante variável, de 4 até 48 portas. Contudo, para redes maiores que 8 computadores, atualmente é indicado o uso de *switches*.

Switches

Os *switches* (Figura 3.2) são os principais equipamentos concentradores de redes utilizados atualmente, ele difere do *Hub* por saber identificar quais são os equipamentos que estão conectados em suas portas. Para realizar isso, o *switch* armazena em sua memória, um mapeamento que identifica quais endereços MACs (*Media Access Control*) estão conectados em cada uma de suas portas, quando um equipamento realiza uma transmissão para outro equipamento, o *switch*, ao invés de realizar um *broadcast*, encaminha a informação apenas para o destino correto. Essa característica permite que ocorra mais de uma transmissão ao mesmo tempo, aumentando a velocidade da rede local.

Figura 3.2: Ilustração de um Switch. (Figura 181110319)

Os *switches* possuem velocidades de 100 Mbps, 1 Gbps e 10 Gbps, podem funcionar tanto com cabos de pares trançados (UTP), quanto com fibras óticas no mesmo equipamento. Importante ressaltar que o *switch* possui muitas características e recursos além da velocidade e da quantidade de portas, que devem ser observadas antes da escolha do equipamento, entre elas:

Quantidade de endereços MAC

Como informado, o *switch* armazena em memória os endereços MACs. Em uma rede que interliga vários *switches*, todos eles devem conhecer os MACs dos equipamentos que estão conectados nos outros *switches*. Caso os *switches* da rede tenham pouca memória, a tabela de endereços MACs será sempre alterada, incluindo os equipamentos que estão transmitindo e retirando os equipamentos que estão a mais tempo sem transmitir, gerando um pequeno atraso no inicio da conexão.

SNMP (*Simple Network Management Protocol*)

Esse protocolo é utilizado para gerência do equipamento. Através dele é possível coletar informações como: tráfego por porta, utilização de CPU, temperatura, e outras. Essas informações são muito importantes para soluções de problemas. Por exemplo, uma rede de 5 *switches* e 300 computadores está lenta. Será que tem um computador transmitindo um número muito elevado de dados? Como descobrir? Centralizando as informações coletadas por SNMP de todos os *switches* em uma gerência é possível verificar essas informações em minutos.

Agregação de portas (*Link Aggregation*)

Com essa funcionalidade é possível conectar mais de uma porta entre dois *switches*. Isso é necessário quando o tráfego entre dois *switches* está muito elevado, assim podemos aumentar a velocidade entre eles agregando varias portas físicas como uma única porta lógica.

Importante!

O *Link Aggregation* é definido pela norma IEEE 802.3ad, importante verificar se o *switch* realiza a agregação de portas seguindo esse padrão. Caso contrário, a agregação de portas só funcionará com equipamentos do mesmo fabricante.

Velocidade total (*Aggregate Bandwidth*)

Em muitos switches, a velocidade total suportada pelo equipamento não condiz com o número de portas. Isso é, você tem um *switch* de 24 portas de 1 Gbps, teoricamente esse equipamento teria uma velocidade total de 24 Gbps. Contudo, nem todos os equipamentos funcionam assim, alguns possuem uma velocidade agregada menor, então é importante observar essa característica.

STP (*Spanning Tree Protocol*)

Esse protocolo permite resolver dois problemas: *loop* e redundância. Em uma rede complexa com muitos *switches* interconectados, é possível que acidentalmente alguém realize uma segunda conexão entre os *switches*, isso gera um loop, onde os dados são encaminhados entre os *switches* de forma eterna, fazendo com que todos os equipamentos da rede parem de funcionar por causa do elevado trafego entre eles. Com o STP habilitado, automaticamente, quando um *switch* percebe que possui dois caminhos diferentes para chegar ao mesmo endereço MAC, bloqueia uma das portas, evitando que a rede pare.

Devido a capacidade de bloquear portas de forma automática, o STP permite também que se conecte mais de uma porta entre *switches* para obter-se redundância. Assim, o protocolo sempre deixará uma das portas bloqueada, caso ocorra um problema de cabeamento na porta em uso, ativará a porta bloqueada.

VLAN (Virtual LAN)

Como o próprio nome já diz, o recurso de Virtual LAN permite ao switch possuir diferentes redes dentro do mesmo equipamento que não se conectam entre si. Isso é interessante, por exemplo, para separar a rede administrativa da rede educacional de uma escola, ou separar os diferentes departamentos de uma empresa, de modo que um computador não consiga conexão com outro, mesmo estando fisicamente no mesmo *switch* (Figura 3.3).

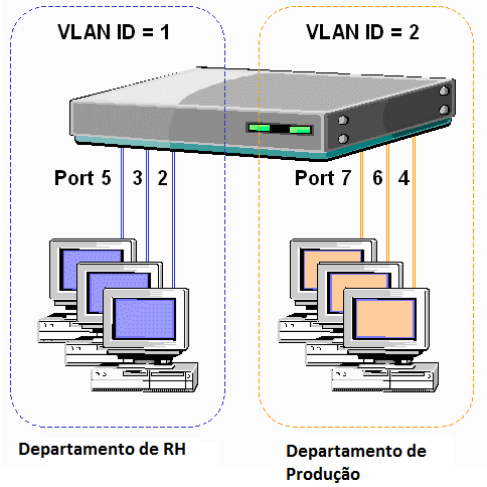

Figura 3.3: Exemplo de uso de VLAN em um switch

http://www.corecom.com/external/livesecurity/vlan-fig1.gif (redesenhar)

Outra possibilidade do uso de VLANs é transportar varias redes virtuais de um *switch* a outro por um único cabo de rede. Assim, podemos ter redes virtuais que se estendem por diferentes *switches*. Conforma ilustrado na Figura 3.4

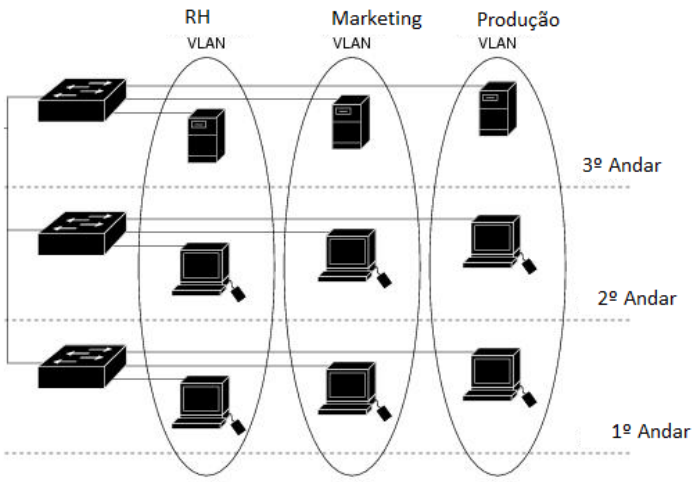

Figura 3.4: Exemplo de uso de VLAN em vários switches

http://www.cisco.com/c/dam/en/us/td/i/000001-100000/15001-20000/16501-17000/16751.ps/_jcr_content/renditions/16751.jpg (redesenhar)

No final deste capítulo será abordado novamente o funcionamento de VLANs com maiores detalhes de como implantar VLAN em uma rede local.

Access Point

São equipamentos que funcionam de forma análoga aos *hubs*, porém, ao invés de utilizar cabos de par transado, utilizam ondas de radiofrequência, também conhecidas por *wireless* ou WI-FI.

Os *Access Points* são os equipamentos responsáveis pela distribuição do sinal WI-FI, sendo de sua responsabilidade a disponibilização de diferentes velocidades, sistemas de segurança e faixas de frequências. Obviamente, os equipamentos que recebem o sinal de WI-FI, como *notebooks*, *tablets*, e outros, também devem ser compatíveis com a mesma tecnologia disponibilizada pelo Access Point, pois também são equipamentos transmissores. Entre os padrões para redes WI-FI abordados no capítulo 2, os três mais utilizados são:

IEEE 802.11b: opera na frequência de 2,4 GHz, possui velocidade máxima de 11 Mbps.

IEEE 802.11g: também opera na frequência de 2,4 GHz, mas possui uma velocidade de 54 Mpbs. Vale ressaltar que a velocidade degrada de acordo com a distância e na medida em que mais computadores se conectam no mesmo *Access Point*.

IEEE 802.11n: padrão desenvolvido em 2007 que permite que a velocidade chegue até 600 Mbps, pode operar nas frequências de 2,4 GHz e/ou 5GHz.

Curiosidade: A frequência de 2,4 GHz é a mesma utilizada por telefones sem fio e fornos de micro-ondas, o que

pode interferir na qualidade de seu sinal wireless.

Existem *Access Points* que funcionam concomitante com os três padrões, permitindo que diferentes dispositivos se conectem a rede WI-FI. Com relação ao alcance do sinal WI-FI, vai depender da potência em que o sinal é transmitido, medido em mW (miliwatts).

Curiosidade:
1 mW corresponde á 10^{-3} W

Referente às diferentes formas de segurança para as redes Wi-FI, destam-se:

WEP: *Wired Equivalent Privacy*, padrão criado em 1999, onde sua senha de proteção pode ser facilmente descoberta, devido ao pequeno tamanho de 40 bits de sua chave de criptográfica.

WPA: O padrão de segurança WPA *(Wi-Fi Protected Access*) funciona com chaves temporais (que se modificam de tempos em tempos), possuindo tamanho de 128 bits, o que garante uma maior proteção quando a invasão da rede sem fio. Com o WPA também foi disponibilizada a autenticação por usuário, através do EAP (*Extensible Authentication Protocol*) o qual permite que o *Access Point* consulte uma base de usuários/senhas na rede, antes de fornecer acesso ao dispositivo que pretende entrar na rede wireless.

WPA2: Uma evolução do padrão WPA, com chave criptográfica de 256 bits e algoritmo de criptografia AES (*Advanced Encryption System*), que agrega uma maior segurança contra possíveis invasões.

Router

Diferentemente dos hubs, switches e *access points* que atuam na camada de enlace, os *routers* (roteadores) atuam sobre a camada de rede, isso é, sobre a camada IP. Outra característica importante dos roteadores é a possibilidade de trabalhar com diferentes protocolos de camada de enlace. Isto é, transformar um quadro do padrão *Frame Relay* para *Ethernet*, ou do ATM para o MPLS (abordados no capítulo 5), entre outros.

Assim, em um ambiente doméstico, quando necessitamos disponibilizar o acesso a internet, necessitamos de um roteador, que disponibiliza além de endereços IP para nossa rede local, a transformação do quadro do padrão ADSL para o Ethernet. Esse mesmo princípio é utilizado em maior escala em redes corporativas, onde há a necessidade de interligar diferentes locais que utilizam em suas LAN o padrão *ethernet*, e necessitam de comunicar utilizando os canais de comunicação das operadoras de telefonia/internet que utilizam os mais diversos protocolos de redes WAN.

Referente às características físicas, com exceção dos roteadores domésticos, a sua grande maioria é modular, permitindo incluir módulos de interfaces físicas de acordo com a necessidade e o crescimento da rede. Assim como num *switch*, no roteador é necessário observar a capacidade e as funcionalidades antes de escolher um, principalmente:

- Os protocolos suportados e necessários para a estrutura da rede: OSPF, BGP, IPv4, IPv6, etc.

- A quantidade de memória, pois cada protocolo habilitado no roteador consome mais memória de acordo com o tamanho das informações armazenadas, como rotas e regras de encaminhamento.

- As funcionalidades como NAT, *Link Aggregation*, VLAN, DHCP, etc.

Funcionamento de VLANs

Como explicado anteriormente nesse capítulo, o conceito de Virtual LAN permite possuirmos redes virtuais distintas em um único switch ou roteador, ou até mesmo transportar essas redes virtuais por toda a rede local, passando por diferentes equipamentos.

Para que isso seja possível, o quadro ethernet (abordado do capítulo 2), foi acrescido de 4 bytes, seguindo a especificação IEEE 802.1Q, onde nesses 4 bytes foi inserido o TAG de VLAN, que possui o identificador da VLAN, chamado de VLAN ID, que refere-se ao número da VLAN que o quadro Ethernet pertence.

Na especificação 802.1Q, a VLAN ID pode variar entre 1 e 4094, sendo que todo o switch que tem o suporte à VLAN habilitado, coloca suas portas físicas na VLAN 1, assim todos os equipamentos conectados nesse switch por padrão estão na mesma rede. No momento que se altera a VLAN ID de uma porta do switch, ela passa a se conectar apenas com as portas possuem o mesmo VLAN ID. Para entender melhor as possibilidades de uso das VLANs, vamos utilizar o estudo de caso representado na Figura 3.5.

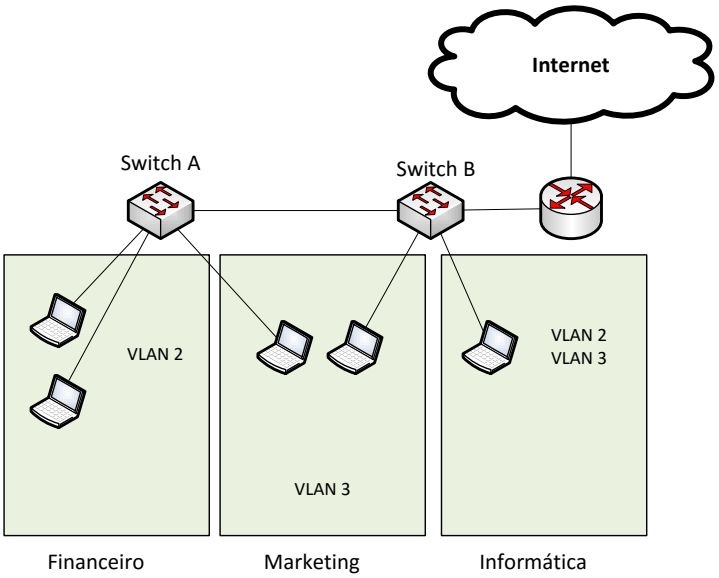

Figura 3.5: Estudo de caso de uso de VLANs

A referida estrutura possui três departamentos, onde por questão de segurança, os computadores do departamento de Marketing não devem estar na mesma rede que os computadores do Financeiro. Sendo assim, foi criada duas VLANs distintas, a VLAN de número 2 para o Financeiro e a VLAN 3 para o Marketing. Entretanto, o departamento de Informática da empresa possui um computador para realizar suporte remoto aos dois departamentos, o qual necessita ter acesso as duas VLANs concomitantemente.

Para implementar a referia estrutura, necessitamos configurar duas portas do Switch A na VLAN 2 para o Financeiro e uma porta na VLAN3 para o Marketing (Quadro 3.1). Contudo, a porta que interliga o Switch A ao Switch B necessita transportar as duas VLANs pelo mesmo cabo, nessa situação devemos configurar as portas que interligam os dois Switches em modo TRUNK (tronco), onde os quadros ethernet utilizam o padrão IEEE 802.1Q. Na Interligação das estações de trabalho do Financeiro e do Marketing as portas do *switch* são configuradas em modo ACCESS (acesso), com isso os computadores não necessitam saber que estão trabalhando com VLAN, pois o quadro *ethernet* não é alterado.

```
interface FastEthernet 1
  description PC1-Financeiro
  switchport mode access
  switchport access vlan 2

interface FastEthernet 2
  description PC2-Financeiro
  switchport mode access
  switchport access vlan 2
```

```
interface FastEthernet 3
  description PC1-Marketing
  switchport mode access
  switchport access vlan 3

interface FastEthernet 24
  description Conexao Switch A – B
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 2,3
```

Quadro 3.1: Exemplo de configuração do Switch A (sintaxe dos equipamentos cisco)

No Switch B existe uma porta configurada na VLAN 3 em modo ACCESS, uma porta configurada em modo TRUNK até o roteador e mais uma porta configurada em modo TRUNK para o departamento de Informática (Quadro 3.2).

```
interface FastEthernet 1
  description PC2-Marketing
  switchport mode access
  switchport access vlan 3

interface FastEthernet 2
  description Conexao PC1-Informatica
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 2,3
```

```
interface FastEthernet 23
  description Conexao Switch B - A
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 2,3

interface FastEthernet 24
  description Conexao Switch B - Router
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlan 2,3
```

Quadro 3.2: Exemplo de configuração do Switch B (sintaxe dos equipamentos cisco)

A estação de trabalho do Departamento de Informática receberá os quadros Ethernet contendo o TAG de VLAN e para acessar a rede deverá configurar duas interfaces de redes virtuais para que possa se comunicar com os computadores do Marketing e do Financeiro. No quadro 3.3 está um exemplo de configuração do arquivo /etc/network/interfaces do Ubuntu (Debian), onde na placa de rede eth0 estão configuradas as VLANs 2 e 3.

Dica: antes de alterar o arquivo, execute:

```
apt-get install vlan
```

```
auto vlan2
iface vlan2 inet static
  address xxx.xxx.xxx.xxx
  netmask xxx.xxx.xxx.xxx
  mtu 1500
  vlan_raw_device eth0

auto vlan3
iface vlan3 inet static
  address xxx.xxx.xxx.xxx
  netmask xxx.xxx.xxx.xxx
  mtu 1500
  vlan_raw_device eth0
```

Quadro 3.3: Exemplo de uso de VLANs no Linux Ubuntu (Debian)

Curiosidade

No sistema operacional Windows, o recurso de criação de VLAN é fornecido pelo fabricante da placa de rede e não pelo sistema operacional, como no Linux. Dessa forma, nem todas as placas de rede tem suporte a trabalhar com VLAN no Windows, esse recurso acaba sendo limitado a placas de redes utilizadas em servidores de rede.