

Configuração do Switch

Criação de VLANs

As VLANs (Virtual Local área networks) são redes locais virtuais criadas para separar áreas de operação ou domínio de uma determinada organização.

Criando VLAN podemos separar LANs ligadas a um mesmo switch. Cada Vlan tem o seu domínio de Broadcast. As VLANs são associadas em conexões lógicas.

Tipos de VLAN:

- VLAN de dados
- VLAN padrão (VLAN 1)
- VLAN nativa
- VLAN de gerenciamento

Para encaminhamento de de tráfego das VLANs deve-se utilizar portas de tronco (Trunk).

O protocolo de tronco utilizado pela cisco é o IEEE 802.1q.

O critério para selecção de uma VLAN é através do seu ID, ou seja VLAN 20, 20 é o seu ID e deve ser configurado em todos os switch que têm equipamento que fazem parte dessa VLAN.

a) Criar Vlan e Configurar endereço ip na Vlan:

```
S1(config)# vlan 99
```

```
S1(config-vlan)# exit
```

```
S1(config)# interface vlan99
```

```
S1(config-if)# ip address 192.168.1.2
```

```
255.255.255.0
```

```
S1(config-if)# no shutdown
```

O tráfego enviado numa VLAN nativa não deve ser marcado.

Comando Para habilitar uma porta a VLAN:

```
S1(config)# interface fa0/1(Abrir a interface)
```

```
S1(config-if)# Switchport mode access (Para acesso de uma VLAN)
```

```
S1(config-if)# Switchport access vlan 2 (habilitar na Vlan 2)
```

Comando para habilitar manualmente uma interface como tronco para passar dados das VLANs:

```
S1(config)# interface f0/1
```

```
S1(config-if)# switchport mode trunk
```

Direccionar Vlans para uma interface:

```
S1(config)# interface f0/1
```

```
S1(config-if)# switchport mode trunk
```

```
S1(config-if)# switchport trunk allowed vlan 10,99
```

Comando para verificar trafego de VLAN:

```
S1#show interfaces fa0/8 switchport
```

Propagação de VLANs usando VTP e DTP

VTP (VLAN Trunking Protocol) é um protocolo usado para distribuir informações sobre VLANs nos switches. Dessa forma apenas configuramos ou criamos as VLANs num switch e fizemos a distribuição delas utilizando o VTP. Para tal terá um switch como servidor de VLANs e os outros serão clientes.

Para Servidor vtp:

```
S1(config)#vtp mode server
```

```
S1(config)#vtp domain itls.com
```

```
S1(config)#vtp password 1234
```

Para Cliente vtp:

```
S1(config)#vtp mode client
```

```
S1(config)#vtp domain itls.com
```

```
S1(config)#vtp password 1234
```

DTP (Dynamic Trunking Protocol) usamos esse protocolo para negociação de links de troncos entre os switches. Essa negociação é feita apenas se a porta de switch vizinho estiver configurado em modo de tronco suporte para DTP.

Comandos:

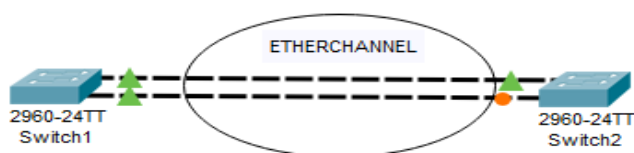
S1(config-if)# Switchport mode access (Para acesso de uma VLAN)

S1(config-if)# Switchport mode dynamic auto (Para negociação automática)

S1(config-if)# Switchport mode dynamic desirable (Para enviar configurações de tronco).

EtherChannel e Port-Channel

Os dois métodos permitem agrupar interfaces de modos a trabalhar como apenas uma, aumentando desse modo a largura de Banda da ligação entre dois switches.



Para Switch 1:

S1(config)#interface port-channel 1

S1(config)#interface range fa0/1-2

S1(config-if-range)#speed 100

S1(config-if-range)#duplex full

S1(config-if-range)#channel-group 1 mode active

Para Switch 2:

S2(config)#interface port-channel 1

S2(config)#interface range fa0/1-2

S2(config-if-range)#speed 100

S2(config-if-range)#duplex full

S2(config-if-range)#channel-group 1 mode active

Configuração no Roteador

Roteamento é o processo da escolha do melhor caminho para envio de pacotes de uma rede para a outra.

Os roteadores são computadores, porque têm as mesmas características de um computador, ou seja, eles têm: CPU, sistema operacional, memória e armazenamento.

Podemos transformar um computador para se comportar como um roteador, bastando instalar um S.O com essa função, como o: PF Sense.

Gateway padrão: é o dispositivo de rede capaz de rotear o tráfego para outras redes.

Apresenta as seguintes características:

- Encaminhar tráfego para outras redes;
- Deve ter um endereço local no mesmo intervalo de endereço que outros hosts da rede;
- Cada Interface do roteador se conecta a um domínio de broadcast.

Comandos para verificar a rota de um pacote:

- PC# Tracert 192.168.2.1
- Roteador# Traceroute 192.168.2.1

Comando para verificar conectividade:

- PC# ping 192.168.2.10

Tabela de Roteamento: são usadas para determinar o melhor caminho para envio de pacotes. Podem ser rotas apreendidas de forma estáticas ou dinâmicas.

- De forma estática as rotas são inseridas manualmente na tabela de rota.
- De forma dinâmica as redes remotas são assimiladas automaticamente por meio de um protocolo de roteamento.

Roteamento Estático

Quando usar roteamento estático:

- Manutenção simples em redes menores;
- Roteamento para as redes Stub (é uma rede que tem apenas 1 único caminho para enviar informações para outras redes);
- Usar uma rota padrão para representar um caminho que não tem correspondência.

Vantagens:

- As rotas estáticas não são anunciadas na rede, resultando em maior segurança;
- As rotas estáticas usam menor largura de banda do que os protocolos de roteamento;
- O caminho que uma rota estática usa para enviar dados é conhecido.

Configurar rota estática:

```
Router(config)# ip route endereço da rede Máscara de sub-rede interface de saída/endereço do próximo salto Distância administrativa (Opcional)
```

```
Router(config)# ip route 172.16.1.0 255.255.255.0 192.168.1.2
```

Rota estática padrão:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2 2
```

OBS: Por padrão as rotas estáticas têm o valor 1 como valor da distância administrativa, mas ela podem variar de 0 à 255. Quanto menor maior prioridade.

Rota estática Sumarizada:

O endereço sumarizado de partilhar aspectos relacionados aos endereços de sub-redes (VLSM). Ele pode ser calculado através da igualdade que eles têm convertendo em binário.

Sub-rede: 172.20.0.0/16; 172.21.0.0/16; 172.22.0.0/16 e 172.23.0.0/16.

A rede sumarizada será: 172.20.0.0/14.

Verificar rota estática: Router# Show route static

OBS: Para verificar as rotas estáticas depois do comando show, verificamos todas as rotas com a marcação *S.

Roteamento Dinâmico

O roteamento dinâmico permite descobrir redes remotas de forma automática. Alguns protocolos de roteamentos dinâmicos são: RIP, OSPF e IGRP.

Vantagens do roteamento Dinâmico:

- Não depende do tamanho da rede;
- Adequado em todas as topologias nas quais são necessários vários roteadores;
- Adapta-se rapidamente a topologia.

No roteamento dinâmico devem ser informados as rotas directamente conectadas. Para ver as redes conectadas usa-se o comando: **Router# Show ip route connected**

ROTEAMENTO COM RIP	
R1(config)# router rip R1(config-router)# version 2 R1(config-router)# passive-interface g0/1 R1(config-router)# network 172.30.0.0 R1(config-router)# network 10.0.0.0 R1(config-router)# no auto-summary R2(config-router)# default-information originate	Entrar nas configurações RIP. Activar a versão 2. Evita que actualizações RIP se enviem por essa interface Declarar as redes directamente conectada. Desactivar a sumarização automática Redistribuir as Rotas padrão
ROTEAMENTO COM OSPF	
R1(config)# router ospf 1 R1(config-router)# network 192.168.1.0 0.0.0.255 area 0 R1(config-router)# network 192.168.12.0 0.0.0.3 area 0 R1(config-router)# network 192.168.13.0 0.0.0.3 area 0	Entrar no modo de configuração de OSPF e definir a área para troca de dados sobre roteamento. Declaração das redes com seus correspondentes wildcard (máscara coringa).

Para verificar os roteamentos dinâmicos usamos os comandos:

- R1# Show ip route ospf, para o OSPF
- R1# Show ip route rip, para o RIP

Listas de Controle de Acesso

Os roteadores modernos oferecem serviços que anteriormente eram exclusivos para outros dispositivos de rede. As listas de acesso (Access-List) é um dos serviços mais utilizados durante a configuração de segurança nos roteadores, eles são usados para permitir ou bloqueiar o acesso de acordo ao endereço ip, protocolos e muito mais. Funções também realizadas por um firewall.

Por padrão os roteadores não têm as listas de acesso (ACL) configuradas, portanto por padrão um roteador não filtra tráfego.

As listas de acesso pode ser de entrada ou de saída, a de entrada filtra o pacote na entrada do roteador e a de saída filtra de acordo a saída do mesmo. Elas são colocadas nas interfaces dos roteadores, desde modo uma interface pode ter duas ACL desde que estejam nas posições diferentes, mas não é o aconselhável.

As ACL podem ser padrão de 1 até 99, ou Estendida acima de 99. Elas também podem ser nomeadas, quando substituídos o número da ACL com o termo Standard (para padrão) ou Extended (para ACL estendida).

LISTAS DE ACESSO (ACL)	
R3(config)# access-list 1 R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255 R3(config)# access-list 1 deny any	Criar uma lista de acesso Permitir uma rede completa Negar todo o resto
R3(config)# interface g0/1 R3(config-if)# ip access-group 1 out/in	Aplica a uma interface de entrada ou de saída
R3# show access-lists 1 R3# show access-lists	Verificar a configuração das ACL.
R3# show ip interface g0/1 R3# show ip interface	Para ver onde se aplicou uma ACL
R1(config)# ip access-list standard BALCAO1 R1(config-std-nacl)# permit host 192.168.30.3 R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255	Criar uma ACL Padrão nomeada Permite um único host. Permite uma rede completa

R1(config)# interface g0/1 R1(config-if)# ip access-group BALCAO1 in	Se aplica a uma interface de entrada.
R1(config)# int s0/0/0 R1(config-if)# ip access-group 100 out	Aplicar ACL na saída de uma interface.
R3(config)# ip access-list extended WEB-POLICY R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80 R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80	Criar uma ACL estendida nomeada. Permite a uma rede ir a um host com porta de destino TCP 80.

Servidor DHCP

O DHCP (Dynamic Host configuration protocol), ou seja o protocolo de configuração dinâmica de host, é protocolo que permite oferecer endereços Ip e outras configurações de rede de modo dinâmico. Ele permite criar um pool de endereços válidos de rede que serão atribuídos para os host clientes DHCP.

O protocolo DHCP opera de acordo a quatro funções principais: Discover, offer, request e ACK (Acknowledge).

Os hosts ao enviar mensagem para pedido DHCP usam o endereço 0.0.0.0 e envia uma mensagem as solicitação de broadcast que não faz parte de rede alguma, mas envia para todas as redes.

Para receber e enviar informações DHCP usa-se o protocolo UDP para a transmissão de dados:

- Request: UDP porta 67
- Offer: UDP Porta 68

DHCP (DYNAMIC HOST CONFIGUTION PROTOCOL)

R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9	Excluir uma range de IP associado a uma rede.
R2(config)# ip dhcp pool itslab R2(dhcp-config)# network 192.168.1.0 255.255.255.0 R2(dhcp-config)# default-router 192.168.1.1 R2(dhcp-config)# dns-server 209.165.200.225 R2(dhcp-config)# domain-name ccna-lab.com R2(dhcp-config)# lease 2	Criar um pool DHCP. Definir a rede e o gateway da rede. Definir um DNS de uma rede. Definir um servidor de domínio de uma rede. Definir o tempo de reserva de uma IP
R1(config)# interface g0/0 R1(config-if)# ip helper-address 192.168.2.254	Se o servidor DHCP está em outra rede, se torna broadcast a interface da rede que se pretende atribuir endereço

NAT para IPV4

O NAT (Name address Translator) é um protocolo que faz a tradução de endereços privados em endereços públicos e vice-versa de modo a redes privadas poderem rotear pacotes pela internet. O nat é configurado no rotear de borda na ligação com um ISP.

Existem três formas de configurar o NAT: Estático, Dinâmico e conversão de endereço de porta (PAT- Port Address Translation).

Estático:

- Configuração estática pelo administrador de rede e permanece constante.

Dinâmico:

- Usa um Pool de endereço público e atribui os endereços em ordem de chegada;
- Requer número total de endereços públicos para número total de sessões simultâneas de usuários.

PAT:

- Mapeia vários IP privados para único público;

- Usa o número de portas para encaminhar pacotes de respostas ao dispositivo interno.

NAT ESTÁTICO	
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225	Configurar um NAT estático.
Gateway(config)# interface g0/1 Gateway(config-if)# ip nat inside Gateway(config-if)# interface s0/0/1 Gateway(config-if)# ip nat outside	Definir a interface que vai a rede interna. Definir a interface que vai a rede externa.
Gateway# show ip nat translations	Verificar a tradução
Gateway# show ip nat statistics	Verificar estatísticas de NAT
Gateway# clear ip nat translation * Gateway# clear ip nat statistics	Limpar a tabela e estatísticas
NAT DINÂMICO	
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255	Permite que se traduza a rede especificada.
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224	Definir um conjunto de endereços públicos utilizados para traduzir.
Gateway(config)# ip nat inside source list 1 pool public_access	Definir a lista origem interna que se vai traduzir um conjunto externo.
NAT COM SOBRECARGA	
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255	Definir a rede que será traduzida.
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248	Definir um conjunto de IP públicas utilizados para tradução.
Gateway(config)# ip nat inside source list 1 pool public_access overload	Definir um NAT de uma lista origem de conjunto de IPs externas sobrecarregado.
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload	NAT com sobrecarga sem definir um pool externo, apenas uma interface de saída.
Gateway(config)# interface g0/1 Gateway(config-if)# ip nat inside Gateway(config-if)# interface s0/0/1 Gateway(config-if)# ip nat outside	Identificar as interfaces inside (entrada) e outside (saída).

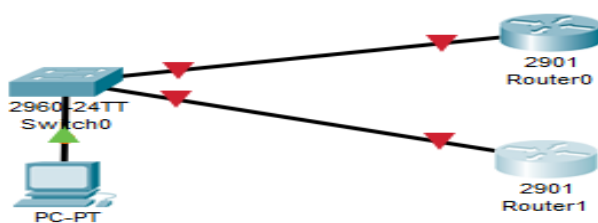
HSRP

O protocolo HSRP oferece redundância da roteadores em uma rede sem dificultar o funcionamento da mesma. Atribuindo um endereço ip virtual aos roteadores da topologia.

Esse protocolo permite que um roteador no caso de falha os outros configurados no modo standby (espera), possam criar caminho para a rede continuar a rotear pacotes para outras redes. Para tal basta ambos partilharem de endereços standby que será usado como gateway para as rede e para prioridade entre os roteadores mudamos a prioridade em que as interfaces possam receber esse endereço.

Rede: 172.16.0.0/24

Gateway : 172.16.0.1/24



```
R1(config)# interface g0/0
R1(config-if)# ip add 172.16.0.2 255.255.255.0
R1(config-if)#standby ip 172.16.0.1
R1(config-if)#standby priority 200
R1(config-if)# standby preempt
```

```
R1(config)# interface g0/0
R1(config-if)# ip add 172.16.0.3
255.255.255.0
R1(config-if)#standby ip 172.16.0.1
R1(config-if)#standby priority 199
```