Prime

CCS-A

Dispositivos de Rede

Noções Básicas Sobre Dispositivos de Rede

- Para desempenhar qualquer função de trabalho como profissional de segurança, você precisa estar familiarizado com vários dispositivos de rede.

Por que?

Realizar uma auditoria de segurança dentro de uma organização, que envolve:

- Identificar os dispositivos usados na empresa;

- Fazer recomendações sobre dispositivos mais seguros a serem usados.

Hub

- Dispositivo de rede mais antigo usado para conectar todos os sistemas em um ambiente de rede.
- O hub é um dispositivo de camada 1 do modelo OSI (Open Systems Interconnection) que simplesmente recebe um sinal de um sistema e envia o sinal para todas as outras portas do hub.

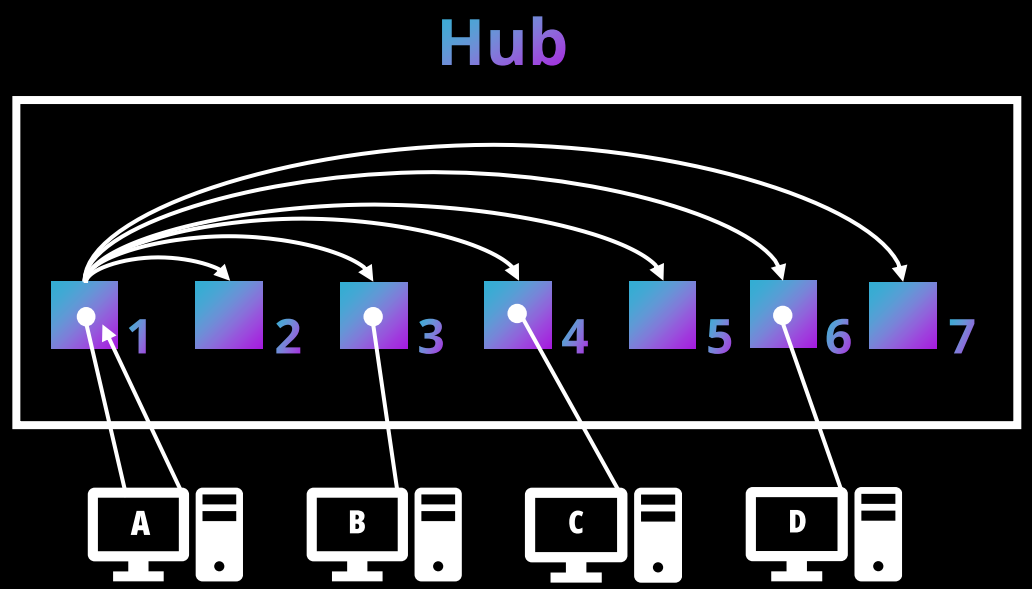


Figura 1

Sobre o Funcionamento de um Hub

DESVANTAGENS:

- Largura de banda é consumida ao enviar dados para todas as portas do hub;
- Problema de segurança caso os sistemas de rede recebam os dados.

Outros computadores podem receber uma cópia do tráfego.

Switch

É semelhante a um hub de rede, pois é usado para conectar todos os sistemas em um ambiente de rede. A diferença é que um switch é um dispositivo de camada 2 que filtra o tráfego pelo endereço de camada 2.

Figura 2 Switch

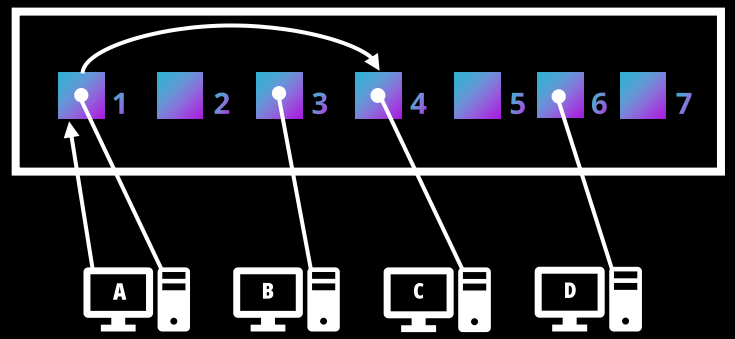


Figura 3

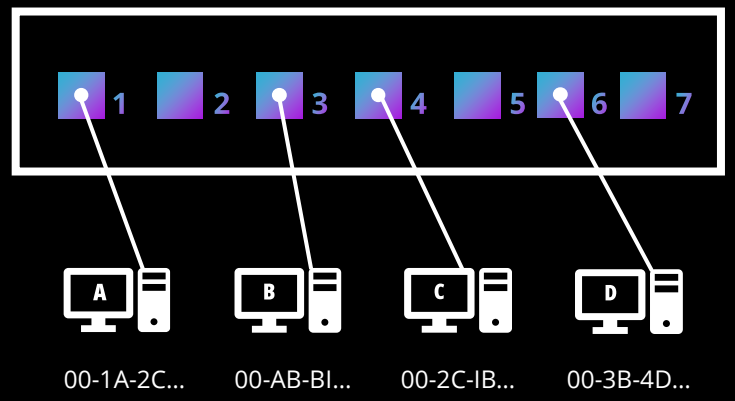
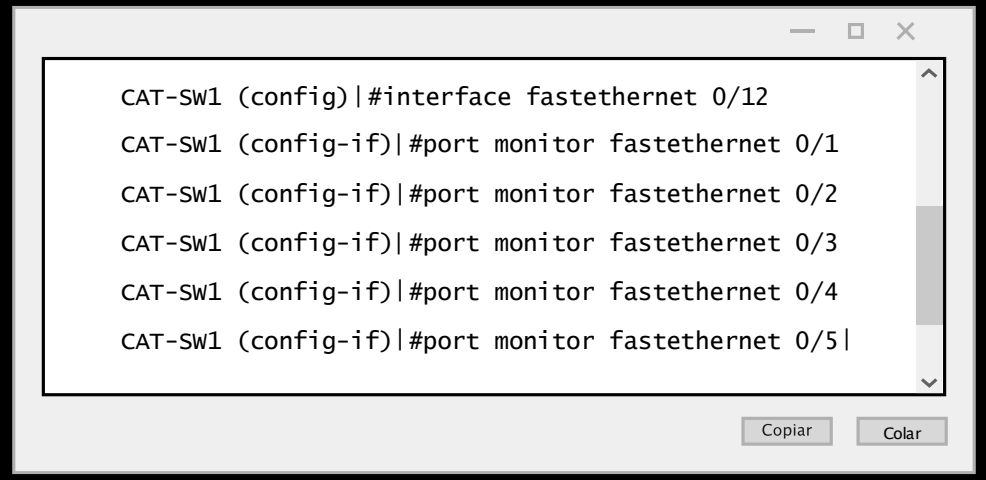


Tabela de endereços MAC	
MAC	**Port**
00-1A-2C...	1
00-AB-BI...	3
00-2C-IB...	4
00-3B-4D...	6

Sobre o Funcionamento de um Switch

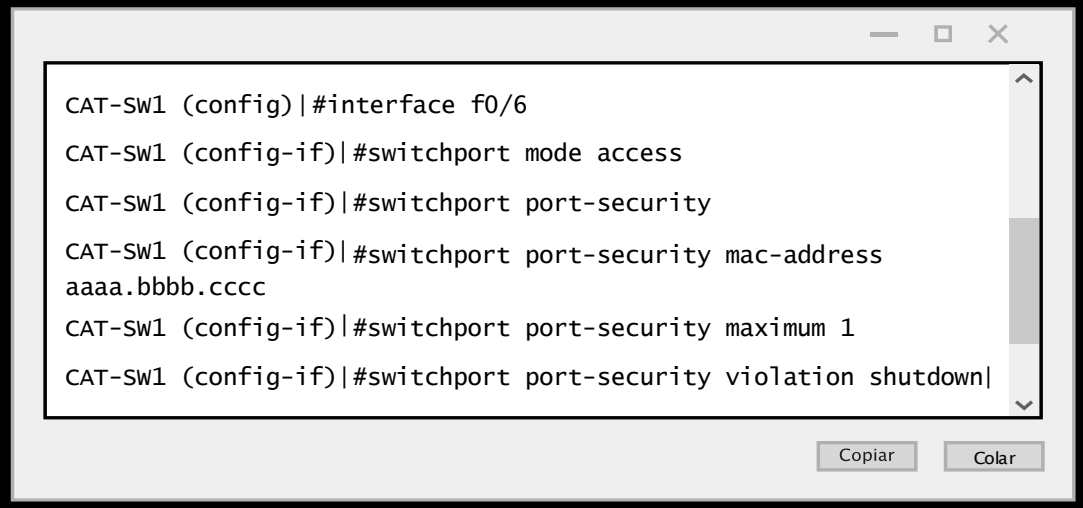
- Filtragem: um switch filtra o tráfego, o que impede que outros capturem e visualizem informações potencialmente confidenciais.
- Espelhamento de porta: recurso de alguns switches que permite ao administrador copiar o tráfego de outras portas para uma única porta de destino (conhecida como porta de monitoramento).
- Os comandos a seguir são usados para configurar a porta 12 (conhecida como interface) no switch para monitorar o tráfego enviado ou recebido nas portas 1 a 5:



Segurança da Porta

- A **segurança da porta** é um recurso de um switch de rede que permite configurar uma porta para um endereço MAC específico.

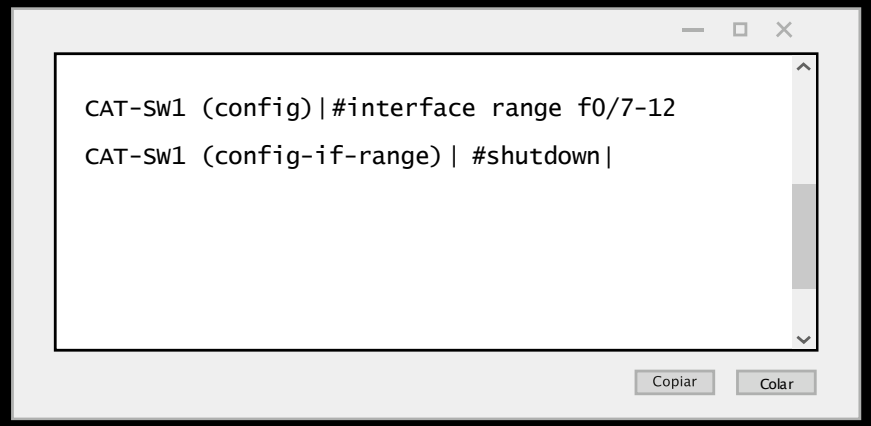
- Quando um sistema não autorizado se conecta à porta do switch, o switch pode desabilitar temporariamente a porta até que o sistema correto seja conectado ao switch ou desabilitar a porta até que um administrador reative a porta.



Capacidade de Desabilitar Portas

- Se você tiver portas no switch que não estão sendo usadas, é uma prática recomendada de segurança desativá-las.

- Os comandos a seguir são usados para desabilitar as portas 7 a 12 em um switch Cisco com o comando shutdown:



Domínios de Colisão

DEFINIÇÃO:

Grupo de sistemas que compartilham o mesmo segmento de rede e, portanto, podem ter seus dados colidindo entre si.

- Com um switch, cada porta no switch cria um domínio de colisão separado que é seu próprio segmento de rede.

VLAN

OBJETIVO:

O objetivo de uma VLAN é criar várias redes dentro de um switch de rede.

Coloca-se as portas do switch em agrupamentos de VLAN. Quando um sistema é conectado a uma porta no switch, ele se torna um membro da VLAN à qual a porta está associada.

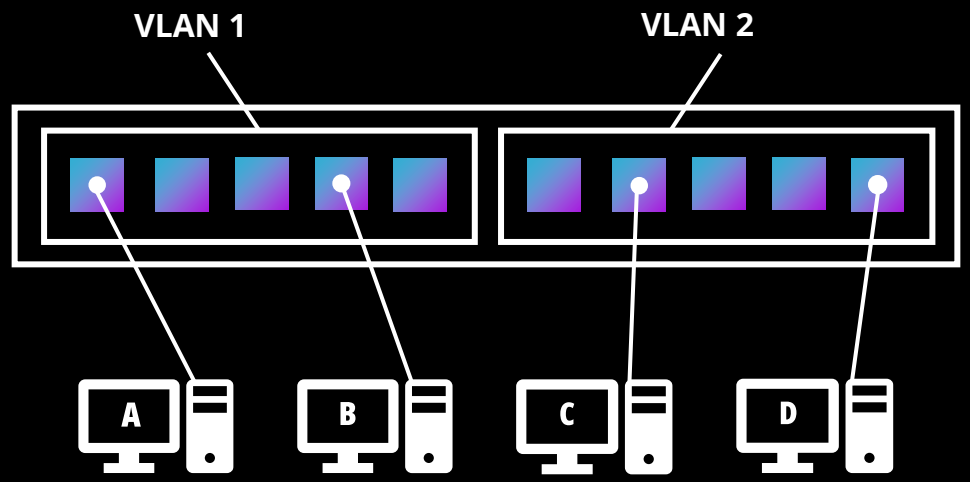


Figura 4

Olhando para VLANs em um switch

O código a seguir mostra como configurar VLANs em um switch Cisco Catalyst.

```
CAT-SW1|enable
CAT-SW1|#config term
CAT-SW1 (config)| #vlan 1
CAT-SW1 (config-vlan)|#name PrivateLAN
CAT-SW1 (config-vlan)|#exit
CAT-SW1 (config)| #vlan 2
CAT-SW1 (config-vlan)| ##name WebServers
CAT-SW1 (config-vlan)|#exit |
```

Copiar Colar

Olhando para VLANs em um switch

- Uma vez que as VLANs foram criadas, você coloca portas diferentes em VLANs específicas. Por exemplo, os comandos a seguir colocam as portas 18 a 24 na VLAN dos WebServers:

```
CAT-SW1 (config)|#interface range f0/0/18 - 24
CAT-SW1 (config-if-range)|#switchport access vlan 2|
```

Copiar Colar

Roteador

Um roteador é um dispositivo de camada 3 responsável pelo roteamento ou envio de dados de uma rede para outra rede.

Ele usa uma tabela de roteamento que reside em sua memória para determinar as redes para as quais ele sabe como enviar dados.

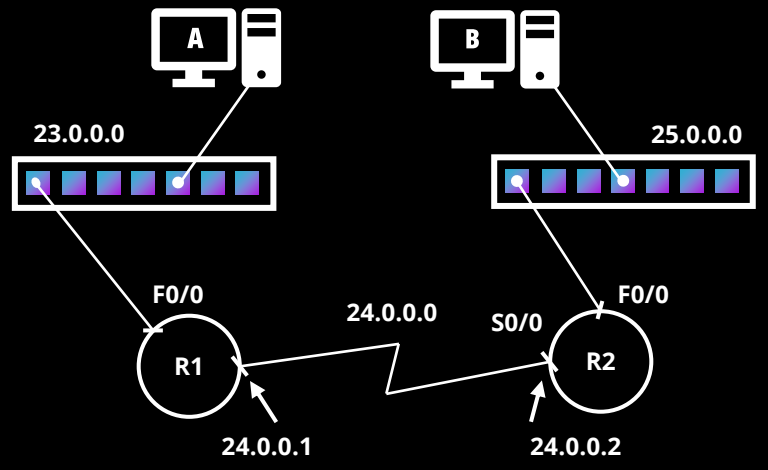
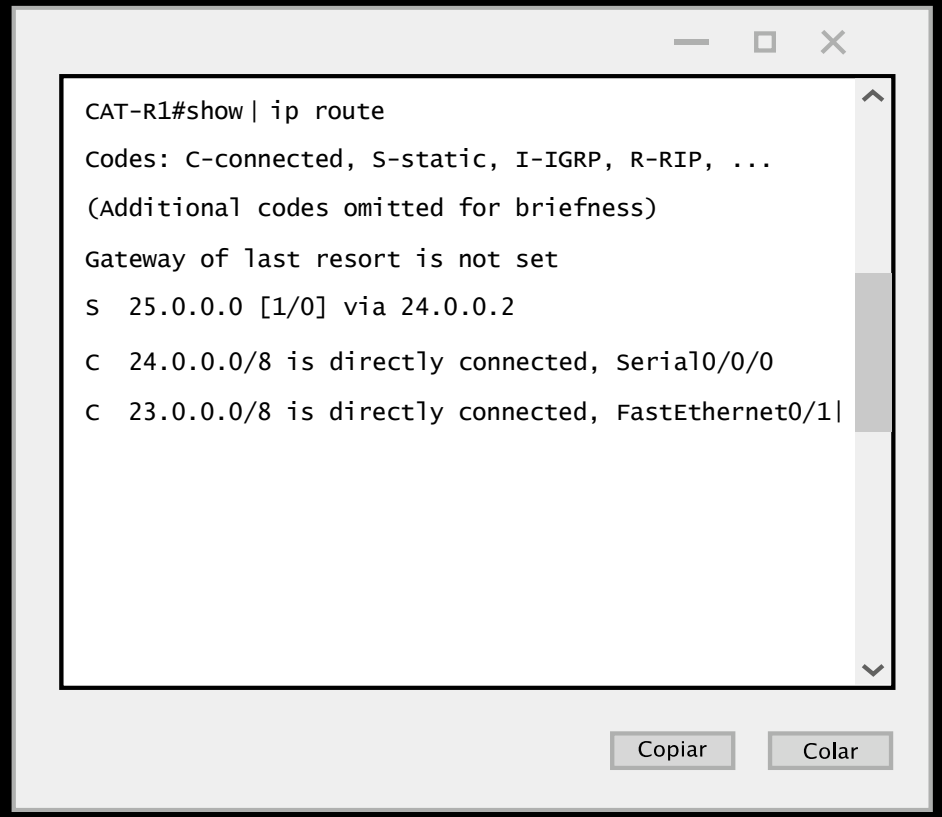


Figura 5

Tabela de Roteamento	
Network	**Path**
23.0.0.0	F0/0
24.0.0.0	S0/0
25.0.0.0	24.0.0.2

Roteador

Os roteadores são ótimos dispositivos de rede porque definem os limites da rede criando o que é chamado de domínio de *broadcast* (transmissão), que é um grupo de sistemas que podem receber as mensagens de transmissão uns dos outros.



Balanceador de carga

- Dispositivo projetado para dividir a carga entre componentes como servidores ou roteadores.
- Balanceamento de carga significa tentar melhorar o desempenho. Vários servidores ou dispositivos entre os quais a carga de trabalho é dividida.
- Os balanceadores de carga têm várias configurações que permitem definir como o balanceador de carga funciona:
  - Round-robin;
  - Afinidade;
  - Persistência;
  - Agendamento.

Ativo/Passivo vs. Ativo/Ativo

- Configuração **ativa/passiva**, um sistema, chamado de node, lida com todo o trabalho (o node ativo), enquanto o outro node (o node passivo) fica em espera, pronto para assumir se o node ativo falhar.

- Configuração **ativa/ativa**, ambos os nodes estão online e são capazes de lidar com solicitações, basicamente dividindo a carga de trabalho. Se um node falhar, o outro node lidará com toda a carga de trabalho até que o node com falha seja recuperado.

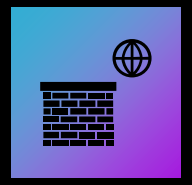
- Pode ser incluído mais nodes, como redundância, para ambas as configurações com um IP Virtual.

DNS Round-Robin

Com o **round-robin**, a solução de balanceamento de carga simplesmente envia a solicitação para o próximo servidor da lista.

- Um exemplo de balanceamento de carga round-robin é o uso do **Domain Name System (DNS);**
- Não verifica se o sistema está funcionando.

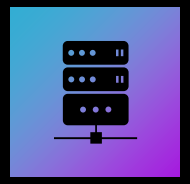
Firewalls



Um **firewall** é um dispositivo de rede que controla qual tráfego tem permissão para entrar ou sair da rede.

- Filtra o tráfego com base nas regras;
- Indica qual tráfego é permitido.

Servidores Proxy



Um **servidor proxy** é um dispositivo para o qual todos os clientes enviam seu tráfego da Internet e, em seguida, o servidor proxy envia as solicitações à Internet em nome dos usuários.

- Usa o NAT (tabela de endereço da rede);
- Alguns são transparentes (sem autenticação);
- Existem os proxies reversos que recebem o tráfego de entrada (para um servidor web).

OBRIGADO !

DISPOSITIVOS DE REDE