RD Press

Guia Básico para Configuração de Switches Cisco

Diego Dias

RD PRESS

Guia Básico para Configuração de Switches Cisco

© 2014 RD Press
Rotadefault.com.br
Comutadores.com.br

Autor: Diego Dias
Revisão: Roger Sales
Millena Mota

Índice

Quem deve ler esse livro?

Esse livro pode ser utilizado por técnicos ou administradores de Switches Ethernet Cisco, familiarizados ou não com a configuração de VLANs e a comunicação entre as redes.

O ebook também servirá para administradores com formação CCNA ou equivalente que desejam por necessidade profissional gerenciar um ambiente com diversos Switches Cisco com o conteúdo focado nas melhores práticas, não focado em certificações.

Apesar do Título do livro ser **Guia Básico para Configuração de Switches Cisco** o material te dará uma base para administrar Switches de uma rede local existente e adicionar novas máquinas e usuários na rede da sua empresa, com comandos e cenários do dia-a-dia de um administrador de Redes para configuração de VLANs, administração básica de um Switch, configurar portas access, trunk e Roteamento entre VLANs.

Apesar de haver inúmeros outros assuntos relevantes para Switches em uma rede local como os protocolos STP, LACP, FHRP, features de segurança, etc; deixo esses tópicos para um próximo volume.

Agrego nesse material as experiencias como adminsitrador de redes de pequeno e médio porte até a administração de Data Centers.

O Livro inclui estudos de caso para refletirmos em topologias similares a cenários reais, trabalhando de forma progressiva desde a criação de VLANs, interfaces de Acesso, Trunk até o Roteamento entre VLANs e rotas para o Roteador de Internet.

Agradecimentos

A atividade de escrever novamente um ebook foi muito prazerosa, assim como administrar semanalmente os blogs. Apesar de não conseguir exemplificar nesse material tudo o que gostaria, sinto-me novamente feliz por tê-lo concluído.

Gostaria de agradecer mais uma vez aos meus amigos do Rota Default: Roger Sales e Ricardo Amaral, pela amizade e companherismo.

Para finalizar, quero agradecer a minha esposa pelo incentivo e louvar a Deus pela possibilidade de ler, estudar, escrever e descansar.

"*O Senhor é misericordioso e compassivo, paciente e transbordante de amor*."
Salmos 145:8

Capítulo

1

Introdução aos Switches Ethernet

Este capítulo é uma breve introdução ao processo de evolução dos hubs para os switches ethernet.

Uma rede de computadores consiste em dois ou mais dispositivos interligados entre si de modo a compartilhar recursos físicos e lógicos por um padrão de endereçamento lógico para comunicação das máquinas. Para ocorrer a comunicação dos computadores em uma rede, utilizamos equipamentos que disponibilizam uma quantidade de portas para acesso aos hosts, servidores e etc.

No inicio do padrão Ethernet para comunicação das redes locais, adotou-se a utilização de HUBs para a conexão de diversos equipamentos - como computadores e impressoras.

A função de um HUB é repetir o sinal recebido por uma porta para todas as outras portas com dispositivos conectados, não utilizando nenhum filtro ou inteligência no encaminhamento de informações.

Conforme o crescimento de uma rede local, a arquitetura do HUB ocasiona colisões de quadros, resultando em uma comunicação lenta entre os equipamentos de rede. Na terminologia da Ethernet, uma **colisão** ocorre quando dois dispositivos tentam "falar" ao mesmo tempo.

O protocolo **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*) permite que os dispositivos comuniquem-se, sem perda de informações, possibilitando que as máquinas escutem o meio físico antes de iniciar a comunicação, coordenando assim o controle do tráfego para evitar colisões. Se houver colisão, é encaminhado um sinal de alerta para os dispositivos esperarem um tempo aleatório antes de iniciar a comunicação

novamente. Colisões serão consideradas um problema ou erro de transmissão, após ocorrerem 16 vezes consecutivas, resultando em um timeout.

A comunicação entre os dispositivos proporcionada por HUBs é denominada como **um domínio de colisão** pois permitem em toda a sua extensão a colisão de "pacotes" na comunicação entre os computadores, limitando a escalabilidade de equipamentos na LAN e possibilitando assim apenas um único dispositivo comunicar em determinado momento em toda a rede.

Os HUBs também não possuem inteligência para identificação de loops físicos na rede dificultando a detecção de problemas, impossibilitando também a utilização de métodos de alta disponibilidade, como a redundância de cabos, etc.

Uma das coisas mais interessantes para administradores de rede é a detecção de tempestades de broadcast ocasionada por HUB's inseridos sem o consentimento da equipe de TI. Em varias situações só conseguimos descobrir o problema após desconectarmos os UpLinks (conexão com outros Switches) um a um.

Switches

O desenvolvimento de novos dispositivos tornou-se necessário para melhora de desempenho desse ambiente, como por exemplo: equipamentos como MAU's, Bridges e Switches.

Os Switches Ethernet trouxeram a capacidade de encaminhamento de pacotes (entenda-se quadros/frames) baseado no endereço MAC de cada dispositivo; ao invés de encaminhar o sinal para todas as portas, a informação é encaminhada somente para o dispositivo correto.

Os Comutadores, nome também dado aos Switches, possuem um grande numero de portas que possibilitam criar dominios de colisão separados para cada interface em full-duplex, deixando de lado a preocupação com conceito para dominios de colisão.

O aprendizado de endereços MAC nos Switches é feito de maneira dinâmica otimizando o consumo do link e tornando cada porta como um domínio de colisão.

Exemplo 1-1 *Visualizando a tabela MAC de um Switch Cisco 3560*

```
Switch# show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0002.16db.7b69    DYNAMIC     Fa0/3
   1    00d0.9725.4a8e    DYNAMIC     Fa0/2
   1    00d0.9725.4aee    DYNAMIC     Fa0/1
```

Um Switch possui grande vantagem pela utilização de processadores, RAM e ASICS para rápido encaminhamento dos quadros.

Exemplo 1-2 *Posição de um Switch no modelo de referência OSI*

Conforme **Exemplo 1-2**, o termo Switch L2, Layer 2 ou de Camada 2, atribui a função do Switch que consiste em apenas utilizar o endereço MAC para encaminhamento de quadros.

Protocolo ARP

Mas o leitor pode questionar: Se os Switches efetuam a leitura de endereços

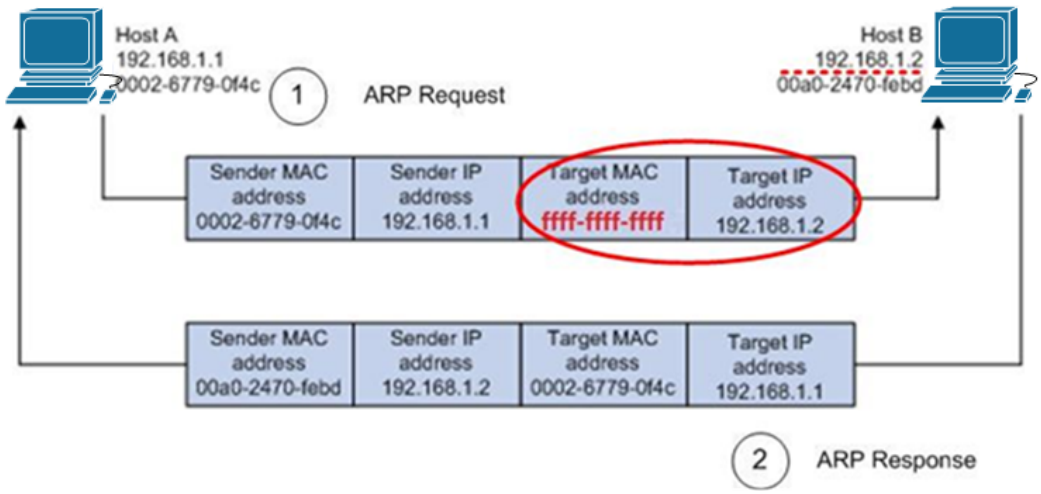
MAC para encaminhamento de quadros, como é feita a leitura da comunicação entre máquinas que utilizam o endereço IP?

Com a utilização do protocolo IP para conexão entre hosts em uma LAN, o Switch fará a leitura do protocolo ARP trocado entre as máquinas para armazenamento e encaminhamento de pacotes baseado no endereço MAC de cada equipamento ao invés do endereço lógico de rede (endereço IP).

O Protocolo ARP é utilizado na comunicação entre dispositivos em uma Rede Ethernet da mesma subrede IPv4. A principal função do ARP é a tradução de endereço IP em endereço MAC:

1. O emissor encaminha em broadcast no cabeçalho Ethernet (ffff-ffff-ffff) um pacote ARP contendo o próprio endereço MAC, e o IP nos campos de endereço de origem do cabeçalho ARP, além do endereço IP de destino do outro host, esperando assim uma resposta com um endereço MAC respectivo não-conhecido.

Exemplo 1-3 *Solicitação de requisição ARP(1) e resposta ARP(2)*



2. Após a resposta da requisição ARP, o mapeamento do endereço IP pertencente ao endereço MAC é armazenado em cache por alguns minutos pelas máquinas e pelo Switch. Se houver uma nova comunicação com o IP mapeado na tabela ARP, o dispositivo deverá consultar o mapeamento em cache; e não encaminhará uma mensagem em Broadcast solicitando novamente o endereço MAC. Após o timeout do endereço, uma nova consulta é encaminhada à rede.

Para a próxima comunicação entre as máquinas, enquanto o cache estiver valido, o endereço do host com o MAC e o IP já será conhecido.

Exemplo 1-4 *Visualizando a tabela ARP no Switch*

```
Switch# show ip arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   0001.C7AC.67B8  ARPA   Vlan1
Internet  192.168.1.10           0   00D0.9725.4A8E  ARPA   Vlan1
Internet  192.168.1.11           0   0030.F246.0BC4  ARPA   Vlan1
Internet  192.168.1.30           0   0002.16DB.7B69  ARPA   Vlan1
```

Exemplo 1-5 *Visualizando a tabela ARP em uma máquina com Windows7*

```
C:\Users\comutadores>arp -a

interface: 192.168.1.100 --- 0x13
  Internet Address      Physical Address      Type
  192.168.1.1           00-01-c7-ac-67-b8     dynamic
  192.168.1.20          00-21-6a-99-dc-22     dynamic
  192.168.1.23          00-21-6a-99-dc-01     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

A principal vantagem do ARP é a facilidade do mapeamento dinâmico de endereços de hardware (MAC) para endereços de rede (IP).

Os dispositivos só exibirão a tabela ARP da sub-rede que pertence!

O processo de Switching (comutação) na camada de enlace do modelo OSI é capaz de encaminhar "pacotes" baseado apenas no endereço MAC, incrementando largura de banda e densidade de portas para a rede.

A tabela MAC e a tabela ARP podem ser consultadas na necessidade de identificar em qual Switch e/ou porta está conectado cada equipamento. *Em diversos cenários já utilizei a consulta ARP para identificar o endereço MAC de um Servidor problemático forçando o Switch a pingar o endereço IP para rastrear a*

porta que o equipamento está conectado, corrigindo assim um problema de negociação de Velocidade e Duplex.

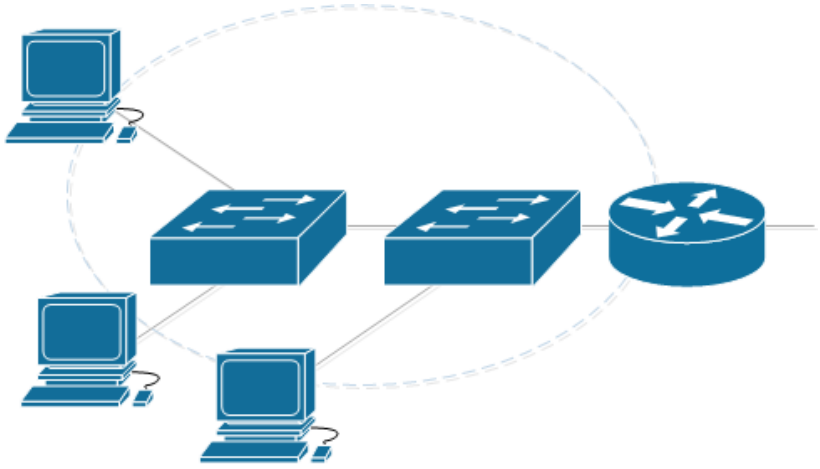
Domínio de Broadcast

Para comunicação simples entre computadores, as máquinas devem ter a configuração de endereço IP na mesma subrede para troca de mensagens unicast e broadcast como fim à resolução de endereços.

Os dispositivos agrupados nessa subrede e conectados ao Switch farão parte do mesmo **domínio de Broadcast**, incluindo cenários com diversos Switches conectados a rede. Esse cenário é necessário para a comunicação de diversos protocolos em redes com endereçamento IPv4.

O conceito de domínios de broadcast ajuda a compreender os limites em que uma máquina pode conversar com os outros dispositivos da rede sem a necessidade de um roteador.

Exemplo 1-6 *Domínio de Broadcast*



Lembrando que para descoberta de hosts em uma rede IPv4 pode utiliza-se de mensagens ARP em broadcast. O termo dominio de broadcast relaciona-se ao limite em que as mensagens broadcast podem ser encaminhadas (geralmente até o roteador). Com a monitoração das mensagens ARP, dos endereços unicast desconhecidos e mensagens em broadcast durante troca de mensagens entre as máquinas é que o Switch monta a sua tabela com endereços MAC para encaminhamento dos “pacotes”.

Conforme ocorre o crescimento da rede, é possível filtrar as mensagens trocadas entre os dispositivos com a criação de **VLANs**, que assim permitem a divisão dos domínios de Broadcast em um mesmo Switch e a comunicação unicast entre os equipamentos. No capítulo 3 abordaremos a utilização de VLANs em uma rede.

Se houver algum problema de comunicação entre equipamentos dispersos na Rede da empresa dentro da mesma VLAN, verifique se a conexão entre os Switches está permitindo a passagem das mensagens dessa VLAN - fazendo a extensão do domínio de Broadcast.

As melhores práticas sugerem a criação de uma subrede para cada VLAN.

Para a comunicação entre as VLANs será necessário a utilização de um Roteador ou um Switch escolhido como Core com capacidade "L3" para Roteamento dessas redes.No capitulo 6 abordaremos o Roteamento entre VLANs em uma rede.

Switching

Em sua função básica, um Switch deverá apenas ler e armazenar as informações de Camada Enlace para encaminhar os "pacotes" em baixa latência, separar cada porta em um único domínio de colisão e cada VLAN em um domino de Broadcast; mas em sua evolução lhe foram atribuídas diversas funções como encaminhamento baseado em informações da camada de Rede, Transporte e Aplicação.

A utilização de features como Spanning-Tree (802.1d, 802.1w e 802.1s) e Link-Aggregation (802.3ad) permitiram a construção de topologias com alta-disponibilidade contra queda de enlaces com a utilização de caminhos redundantes e o empilhamento dos Switches com as features VSS, StackWise e outras acrescentando maior inteligência aos dispositivos.

Nesse volume focaremos nas funções principais de Comutação da Camada 2 e 3.

Espero que apreciem o material... Uma boa leitura a todos!

Capítulo 2

Administração do IOS

A Administração do IOS torna-se bastante simples após o aprendizado de algumas dicas que facilitam o trabalho e a configuração dos Switches.

O Sistema Operacional IOS tem em sua interface de linha de comando (CLI) três principais modos de comando. Cada modo tem acesso a diferentes opções:

User Mode (User EXEC mode)

O user mode é o primeiro modo que um usuário tem acesso ao logar em um Switch. O user mode pode ser identificado pelo nome do Switch seguido pelo caracter "**>**". O user mode permite apenas executar básicos comandos básicos do sistema.

Exemplo 2-1 *User Mode*

```
Switch>
```

Privileged mode (Privileged EXEC Mode)

O modo privileged permite ao usuário visualizar a configuração, reiniciar e acessar o modo de configuração, além dos comandos disponíveis no modo user mode. O privileged mode pode ser identificado pelo nome do Roteador seguido pelo caracter "**#**". Para acessar o modo previlegiado, basta digitar o comando enable.É também possivel configurar autenticação para restringir o acesso ao privileged mode.

Exemplo 2-2 *Privileged Mode*

```
Switch> enable
Switch#
```

Global Configuration mode

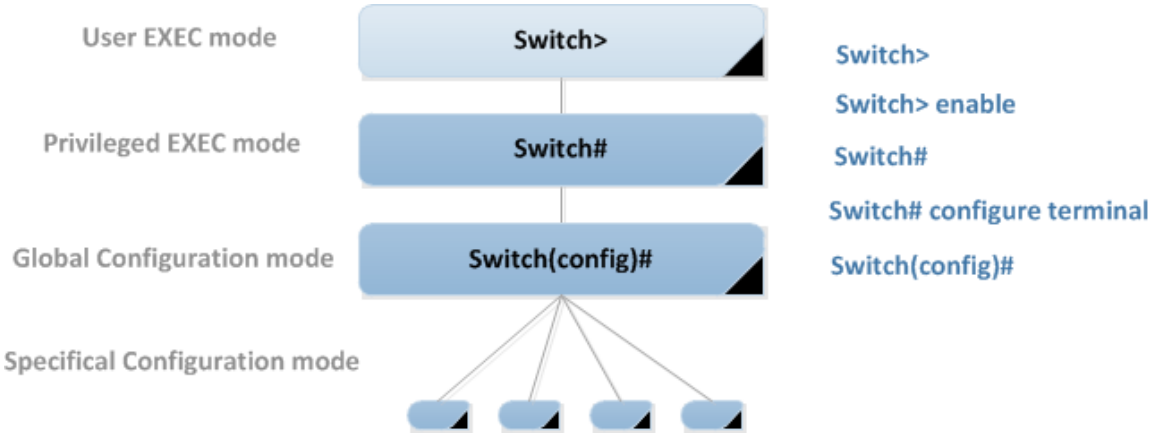
O modo de configuração global permite ao usuário modificar a configuração corrente do Switch. Para isso basta digitar o comando "configure terminal" do modo previlegiado. Para sair do modo de configuração, o usuário pode digitar o comando "end" ou pressionar Ctrl+Z.

Exemplo 2-3 *Global Configuration Mode*

```
Switch# configure terminal
Switch(config)#
```

O modo global de configuração tem alguns submodulos e pode variar da configuração global identificado inicialmente por "(config)#" precedido pelo nome do equipamento.

Exemplo 2-4 Resumo dos m*odos de configuração*



Ao efetuarmos o acesso ao Switch via Telnet ou console no Switch e após passar pelo processo de autenticação cairemos por padrão no "**user mode**" que é o primeiro nível de acesso no Switch, permitindo a execução de comandos "show" que permitem a visualização básica de monitoração do equipamento. Para acessar o modo privilegiado e ter acesso a todos os comandos para visualização da configuração e do sistema digite, **enable**. Já para iniciar uma configuração digite "**configure terminal**" e acesse o modo global de configuração.

Configurando a autenticação para conexão ao Switch

Os métodos comuns para acesso aos Switches Cisco IOS são atráves da porta console ou através das linhas de terminal virtual(vty). O uso de um cliente Telnet ou de um cliente Secure Shell (SSH) são os dois métodos para conectar uma linha terminal virtual.

Senhas deverão ser configuradas para acesso vty (telnet) e console, inclusive para controle de acesso ao modo privilegiado. Segue abaixo a configuração de autenticação para acesso Telnet e SSH.

Exemplo 2-5 *Configurando a autenticação na console e VTY*

```
Switch>enable
! Digite enable para mudar do user mode para o privileged mode
Switch# configure terminal
Switch(config)# line console 0
! acesso para a interface console
Switch(config-line)# login local
! habilitando a autenticação local
Switch(config-line)# password d13go
! configurando a senha d13go
Switch(config-line)# exit
#
Switch(config)#line vty 0 15
! acesso a interface vty, responsável pela autenticação Telnet
Switch(config-line)#login local
Switch(config-line)#password d13go
Switch(config-line)# exit
#
```

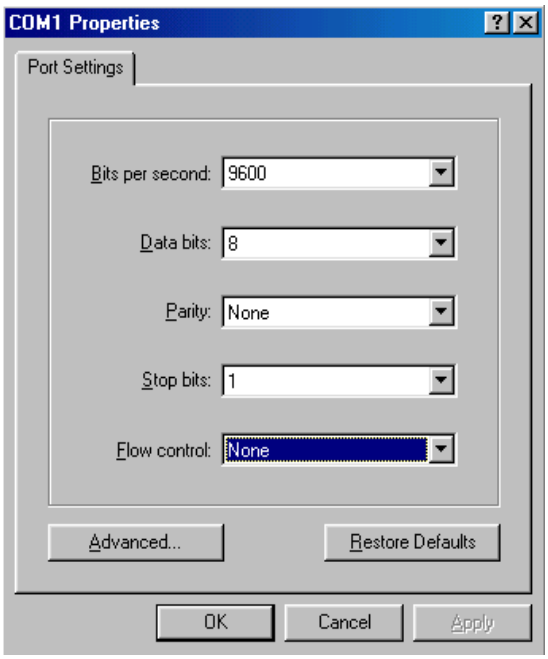
Como dito anteriormente a interface vty refere-se ao acesso virtual (Telnet [habilitado por default] e SSH). Para esse tipo de acesso é necessário a configuração de endereço IP no Switch e a utilização de algum emulador de terminal para acesso ao Switch como o putty ou SecureCRT para windows, etc.

Já a interface AUX refere-se ao acesso via cabo Console. A diferença do acesso via Console para o Telnet ou SSH é que o acesso via console é um acesso "físico" ao equipamento, sendo necessário conectar um cabo diretamente do Switch na porta console para um PC utilizando um emulador de terminal.

Depois de estabelecer a conexão física de seu terminal ou PC com o dispositivo, devemos configurar o terminal para que se comunique com o dispositivo devidamente. Você deverá definir o seu terminal para suportar as seguintes definições:

- Emulação VT100
- Transmissão 9600
- Sem paridade
- 8 bits de dados
- 1 bit de fim

Exemplo 2-6 *Exemplo dos parâmetros no software cliente para conexão via Console*



Um pouco mais sobre o SSH

O SSH é um protocolo que fornece uma conexão segura e criptografada entre um cliente SSH e o servidor , executando uma linha terminal virtual semelhante ao Telnet.

Os clientes SSH e os servidores podem fornecer autenticação do usuário usando o sistema de chaves publicas RSA utilizando uma combinação do ID do usuário e senha apenas. O servidor SSH no IOS usa o RSA para

gerar o par de chaves, utilizado como fim, para configurar uma sessão criptografada para o cliente.

Uma vez que o usuário esteja configurado no dispositivo e o terminal vty habilitado com senha, para ativar o SSH seu Switch IOS devemos ter um nome de host devidamente configurado anteriormente e o nome do dominio. As chaves RSA são geradas com o comando **crypto key generate rsa** para zerar as chaves e desativar o servidor SSH utilize o comando **crypto key zeroize rsa**.

Exemplo 2-7 *Configurando a autenticação na console e VTY*

```
Switch#
Switch# configure terminal
Switch(config)# hostname SwitchRD
!Configurando o hostname
SwitchRD(config)# ip domain-name rotadefault.com.br
!Configurando o domínio
SwitchRD(config)# crypto key generate rsa
!Gerando as chaves RSA
SwitchRD(config)# ip ssh
!Ativando o SSH
#
```

Para exibir a chave RSA pública utilizada pelo SSH digite o comando **show crypto key mypublickey rsa**.

Gerência de usuários

Para visualizar todos os usuários conectados ao dispositivo e identificar o acesso, digite o comando **display users**.

Exemplo 2-8 *Visualizando os usuários conectados com o comando display users.*

```
SwitchRD#show users
    Line       User       Host(s)          Idle       Location
*  1 vty 0     fulano     idle             00:00:00   192.168.1.39

```

Ajuda nos comandos CLI

Para obter ajuda durante a visualização é possível utilizar as dicas abaixo:

- Para obter ajuda online, utilize o caracter ***?*** para obter a lista de todos os comandos possíveis para a view onde se encontra.

- Para obter os parâmetros possíveis em um comando, utilize o caractere ***?*** a frente do comando. Por exemplo:

  Switch#show ?

- Para obter a lista de possíveis comandos iniciados por uma sequência de caracteres, tecle **?** logo após o mesmo. Por exemplo:

  Switch#p?

- É possível completar um comando ou parâmetro automaticamente, utilize a tecla ***<tab>***

- Caso não tenha outro comando ou parâmetro com a mesma identificação inicial, o mesmo será completado.

- Durante a apresentação de múltiplas telas, use:

  <barra de espaço> para apresentar a próxima pagina

  <ENTER> para apresentar a próxima linha

Comandos show "chave"

O comando **show running-config** exibe a configuração atual que está na memória volátil do dispositivo e em execução.

O comando **show startup-config** exibe a configuração salva na memória NVRAM e que será solicitada quando o dispositivo for iniciado.

O comando **show mac address-table** mostra a tabela com o mapeamento de endereços MAC e portas do switch.

O comando **show ip arp** exibe a tabela contendo o mapeamento de endereço IP, MAC, porta e VLAN do dispositivo.

Os dispositivos Cisco IOS incluem filtros para comandos display com a inclusão de pipes "**|**" seguindos pela sintaxe **begin** ou **include**, etc, como por exemplo:

show running-config | begin vlan

O comando **show interface** exibe o status das portas, contadores de tráfego, erros e etc.

Interfaces

As portas Ethernet 10/100BASE-T suportam MDI/MDI-X auto-sensing. Elas podem operar em half-duplex, full-duplex e auto-negotiation e negociar com outros dispositivos para determinar velocidade e modo de operação.

As portas GigabitEthernet 10/100/1000BASE-T suportam MDI/MDI-X auto-sensing, e operam em 1000 Mbps full duplex, 100 Mbps half/full duplex e 10 Mbps half/full duplex, além de trabalharem com auto-negociação.

As portas Gigabit GBIC & SFP operam em 1000Mbps full duplex mode que pode ser configurado como **full** (full-duplex) e **auto** (auto-negotiation) e a velocidade pode ser configurada como **1000** (1000Mbps) e **auto** (auto-negotiation).

As portas 10Gigabit Ethernet operam em 10000Mbps full-duplex. O modo duplex pode ser configurado como **full** (full-duplex) e **auto** (auto-negotiation)e a velocidade pode ser configurada como **10000** (10000Mbps) e **auto** (auto-negotiation).

Como funciona a auto-negociação?

A auto-negociação é um protocolo da Camada Física do modelo de referência OSI, que permite que dois equipamentos de rede (Switches, Roteadores e Servidores) negociem *velocidade* e *duplex* para escolha dinâmica do melhor cenário para a comunicação de dados.

O padrão é bastante útil no dimensionamento de redes para a compatibilidade entre as versões 10/100/1000Mb das interfaces.

Apesar da instabilidade inicial do padrão (devido à incompatibilidade dos fabricantes na adoção do modelo), as discussões da especificação da auto-negociação foram eliminados pela versão de 1998 do IEEE 802.3. Em 1999, o protocolo de negociação foi significativamente ampliado por IEEE 802.3ab, que especificava o protocolo de GigabitEthernet, tornando obrigatória a auto-negociação para 1000BASE-T.

A auto-negociação é utilizada por dispositivos com diferentes *velocidades* de operação (como 10Mb e 1Gb) e diferentes modos de operação *duplex* (*Half-duplex e Full-duplex*).

A incompatibilidade de duplex (***duplex mismatch***) ocorre quando um dispositivo está em *full-duplex* e o outro está funcionando em *half-duplex*. Por causa desse cenário um grande número de colisões irá ocorrer no lado *half-duplex*. Uma segunda ressalva é que interfaces configuradas manualmente não funcionam adequadamente com interfaces configuradas como auto-negociação.

Problemas de ***duplex mismatch*** são comuns e difíceis de diagnosticar, pois a rede continua a funcionar; e em testes básicos de troubleshooting, reportam uma conexão ativa, mas a rede funciona com lentidão.

Zerar contadores

Durante problemas de rede é possível visualizarmos os contadores de erros nas interfaces com o comando ***show interfaces.*** Nos casos em que há a necessidade de zerarmos os contadores para eliminarmos falsos positivos podemos utilizar o comando ***clear counters*** .

Memória RAM, ROM, Flash e NVRAM

Para salvar a configuração utilize os comando **write memory** ou **copy running-config startup-config**.

Para visualizarmos o arquivo atual, o arquivo do próximo boot e o arquivo de backup digite: **show boot.**