

Tecnologias de Redes



Cruzeiro do Sul Virtual
Educação a distância

Material Teórico



Tipos de Redes e Sistema Operacional de Rede

Responsável pelo Conteúdo:

Prof. Esp. Antonio Eduardo Marques da Silva

Revisão Textual:

Prof. Esp. Claudio Pereira do Nascimento

UNIDADE

Tipos de Redes e Sistema Operacional de Rede



- Componentes de Rede;
- Dispositivos Finais de Rede;
- Dispositivos Intermediários de Rede;
- Meios Físicos de Rede;
- Formas de Representação de Rede;
- Tipos de Redes de Comunicação;
- Sistema Operacional de Rede (SOR).



OBJETIVO DE APRENDIZADO

- Compreender e abordar os tipos de redes existentes, tais como LANs, MANs e WANs;
- Ter conhecimentos básicos do sistema operacional de rede da Cisco IOS.



Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:

Determine um horário fixo para estudar.

Mantenha o foco! Evite se distrair com as redes sociais.

Procure manter contato com seus colegas e tutores para trocar ideias! Isso amplia a aprendizagem.

Seja original! Nunca plágie trabalhos.

Aproveite as indicações de Material Complementar.

Conserve seu material e local de estudos sempre organizados.

Não se esqueça de se alimentar e de se manter hidratado.

Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu “momento do estudo”;
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

Componentes de Rede

O caminho que uma mensagem enviada em uma rede percorre da máquina origem a máquina destino podendo ser tão simples quanto um único cabo conectando ponto a ponto ou tão complexo quanto uma rede de abrangência geográfica global. Essa infraestrutura de rede é o alicerce que dá suporte à rede. Ela tem o intuito de fornecer um canal estável e confiável sobre o qual nossas comunicações podem ocorrer.

Uma infraestrutura de rede contém três categorias básicas de componentes de rede, que seriam:

- Dispositivos de Rede (Hosts);
- Meio Físico (Cabo Coaxial, Cabo de Par trançado, Fibra Óptica);
- Serviços de Rede.

Dispositivos de rede e meio físico de rede são os elementos físicos (hardware da rede). O hardware de rede geralmente define os componentes visíveis da plataforma de rede, tais como um Servidor, um PC, um Switch, um Roteador, um Ponto de Acesso sem Fio ou os cabos de conexão utilizados para conectar os dispositivos. No caso de meio físico sem fio, as mensagens são transmitidas pelo próprio ar através da utilização de frequência de rádio invisível ou de ondas infravermelhas.

Tais componentes de rede são utilizados para fornecer serviços e processos, que são os programas de comunicação, chamados de software, executados nos dispositivos conectados à uma rede. Um serviço de rede fornece informações em resposta a uma solicitação cliente. Os serviços incluem muitos dos aplicativos de rede mais comuns que os usuários utilizam todos os dias, como serviços de hospedagem de e-mail, serviços de hospedagem de arquivos e serviços de hospedagem de páginas na Web. Os processos fornecem a funcionalidade com o intuito de direcionar e mover as mensagens através rede. (TANENBAUM, A. S., 2011)

Dispositivos Finais de Rede

Os dispositivos de rede que os usuários estão mais familiarizados são conhecidos de dispositivos finais de rede ou hosts. Esses hosts formam a interface entre os clientes e a rede de comunicação.

Alguns exemplos de dispositivos finais de rede (hosts), seriam:

- Computadores (estações de trabalho, laptops e servidores);
- Impressoras de Rede;
- Telefones VoIP;

- Terminal de Telepresença;
- Câmeras de Vídeo e Segurança;
- Dispositivos Móveis (smartphones, tablets, PDAs e scanners).

Um host pode ser a origem ou o destino de uma mensagem transmitida através da rede. Para distinguir um host de outro, cada host em uma rede é identificado utilizando um endereço. Quando um host inicia a comunicação da informação, ele utiliza o endereço do host de destino para especificar para onde a mensagem deveria ser transmitida (STALLINGS, W. e ROSS K., 2010).

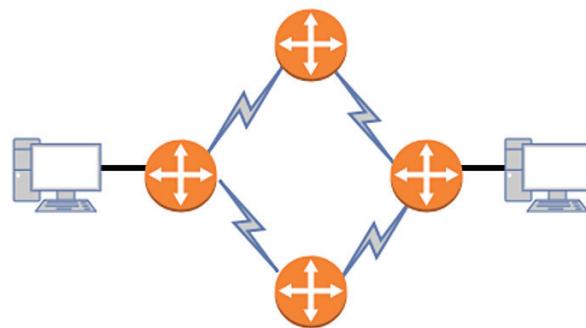


Figura 1 – Dispositivos finais de rede

Fonte: Acervo do Conteudista

Dispositivos Intermediários de Rede

Os dispositivos intermediários de rede se interconectam a dispositivos finais e possuem o objetivo de definir os limites da rede. Esses dispositivos fornecem conectividade e funcionam em segundo plano para garantir que os dados sejam transmitidos através da rede. Esses dispositivos se conectam aos hosts individuais à rede e podem se conectar em várias redes individuais para formar uma rede interconectada.

Exemplos de alguns dispositivos intermediários de rede seriam:

- Acesso à Rede (switches e pontos de acesso sem fio);
- Interconexão (roteadores);
- Segurança (firewalls).

O gerenciamento dos dados é feito a medida em que eles fluem pela rede que é uma das funções dos dispositivos intermediários. Eles utilizam o endereço do host destino, em conjunto com as informações sobre as interconexões de rede, afim de determinar o caminho que as mensagens devem percorrer na rede em questão.

Os processos em execução dos dispositivos de rede intermediários desempenham as seguintes funções:

- Regenerar e retransmitir sinais de dados;
- Manter informações sobre quais caminhos existem na rede;
- Notificar outros dispositivos de erros e falhas de comunicação;
- Direcionar dados por caminhos alternativos quando houver uma falha de conexão;
- Classificar e direcionar mensagens de acordo com prioridades de Qualidade de Serviços (QoS) aplicada na rede;
- Permitir ou negar o fluxo de dados, com base em configurações de segurança limítrofe.

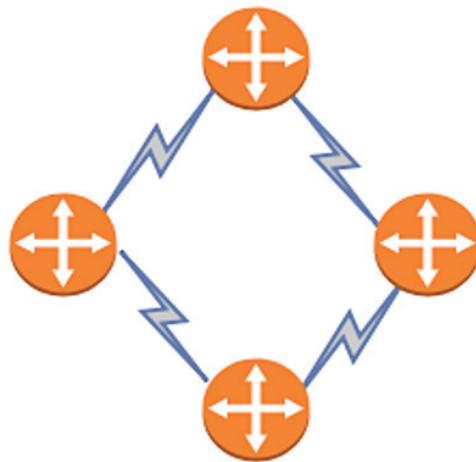


Figura 2 – Dispositivos intermediários de rede

Fonte: Acervo do Conteudista

Meios Físicos de Rede

A comunicação de rede é transmitida por um meio físico, que fornece o canal sobre o qual a mensagem é transmitida da origem ao destino.

As redes modernas utilizam basicamente três tipos de meios físicos para possibilitar a interconexão dos dispositivos e fornecer o caminho por onde os dados podem ser transmitidos. Esses meios físicos são:

- Fios metálicos (cabô de par trançado “UTP e ScTP” e cabo coaxial);
- Fibras de vidro ou polímero / plástico (cabô de fibra óptica);
- Transmissão sem fio através do ar.

A codificação do sinal que deve ocorrer na mensagem a ser transmitida é diferente para cada tipo de meio físico utilizado. Nos fios metálicos, os dados são codificados em impulsos elétricos que correspondem a padrões específicos e que representam letras e números. Nas transmissões de fibra óptica são enviados pulsos

de luz, dentro de cadeias de luz infravermelha ou visível. Em transmissão sem fio, padrões de ondas eletromagnéticas representam os vários valores de bit que são trafegados pelo ar. (TANENBAUM, A. 2011)

Diferentes tipos de meios físicos de rede possuem diferentes características mecânicas, elétricas e benefícios sendo adequados para o mesmo propósito que é a transmissão dos dados na rede. Os critérios para a escolha de um meio físico de rede seriam:

- A distância que o meio físico consegue carregar um sinal com êxito;
- O ambiente no qual o meio físico deve ser instalado;
- A quantidade de dados que devem ser transmitidos;
- A velocidade que tais dados devem ser transmitidos;
- O custo do meio físico e instalação de infraestrutura utilizada.

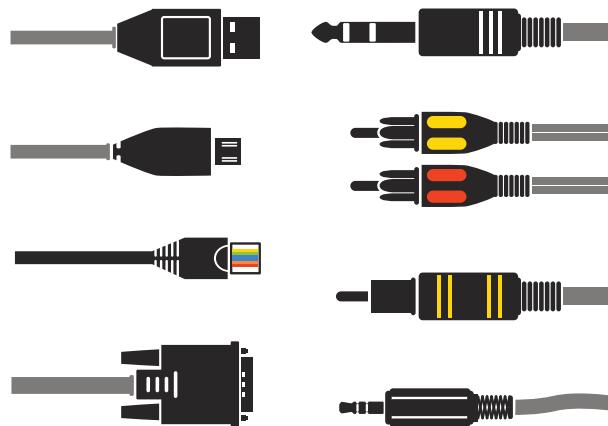


Figura 3 – Meios físicos de rede

Fonte: iStock/Getty Images

Formas de Representação de Rede

Um diagrama de rede fornece uma maneira fácil de entender o formato como os dispositivos em uma rede estão conectados. Esse diagrama usa uma simbologia específica para representar os diferentes dispositivos e formas conexões que uma rede utiliza. Esse tipo de “imagem” de uma rede é conhecido como um diagrama de topologia de rede.

Consideramos um protocolo como uma forma de linguagem e como qualquer linguagem é representada através de símbolos para representar os diferentes dispositivos finais, dispositivos de rede e meios físicos. A capacidade de reconhecer essas representações lógicas dos componentes físicos de rede é crucial para poder visualizar a organização e a operação de uma rede. (TANENBAUM, A. S., 2011)

Além dessas representações, uma terminologia especializada é usada para se discutir como cada um desses dispositivos e meios físicos se conectam aos outros. Alguns exemplos desses dispositivos:

- **Placa de Interface de Rede (NIC)** – o Network Interface Card, placa de rede, ou um adaptador de LAN, fornece a conexão física à rede em um host a um outro dispositivo. O meio físico, tais como cabos metálicos que conectam o host através de uma placa de rede as portas de conexão dispositivos de rede intermediários;
- **Porta de Conexão Física** – um conector em um dispositivo de rede permite que o meio físico seja conectado a um host ou a outro dispositivo de rede intermediário;
- **Interface** – as portas especializadas em um dispositivo de rede que se conectam a redes individuais. Os roteadores por exemplo são utilizados para interconectar redes diferentes, as portas em um roteador são chamadas de interfaces de rede, como uma interface serial ou interface ethernet.

Diagramas de Topologia

Os diagramas de topologia de rede são obrigatórios para qualquer profissional que trabalha com uma rede de dados. Eles fornecem um mapa visual dos dispositivos que fazem parte dessa rede e como a mesma está conectada.

Existem dois tipos de diagramas de topologia, incluindo:

- **Diagramas de Topologia Física** – identificam a localização física de dispositivos intermediários, portas configuradas e instalação dos cabos em uma rede;
- **Diagramas de Topologia Lógica** – identificam logicamente dispositivos, portas e esquema de endereçamento IP utilizados nos hosts que fazem parte de uma rede.

Tipos de Redes de Comunicação

Uma Infraestrutura de rede pode variar muito em relação dos seguintes itens, por exemplo:

- Tamanho da área de cobertura da rede;
- Número de usuários conectados à rede;
- Número e tipos de serviços disponíveis aos usuários.

Os dois tipos mais comuns de infraestruturas de rede:

- **Rede de Área Local (LAN)** – uma infraestrutura de rede que fornece acesso a usuários e dispositivos finais em uma área geograficamente limitada, como por exemplo um andar de um edifício ou uma sala;
- **Rede de Longa Distância (WAN)** – uma infraestrutura de rede que fornece acesso a outras redes dentro de uma grande área geograficamente ilimitada. A Internet seria o melhor exemplo de uma rede desse tipo;

- **Rede Metropolitana (MAN)** – uma infraestrutura de rede que abrange uma área física geograficamente maior que uma LAN, porém menor que uma WAN de uma abrangência de uma cidade por exemplo. As MANs são operadas normalmente por uma entidade publica, ou uma grande organização privada;
- **Rede de Área Local sem Fio (WLAN)** – semelhante a uma LAN cabeada, mas interconecta sem fio hosts dentro de uma área geográfica pequena e limitada;
- **Rede de Armazenamento (SAN)** – uma infraestrutura de rede projetada para suportar servidores de rede e fornecer armazenamento, recuperação e replicação de dados. Envolve servidores de alto desempenho, vários conjuntos de discos (chamadas blocos) e tecnologia de interconexão Fibre Channel (FC).

Redes de Área Local (LAN)

As redes de área local ou LANs são uma infraestrutura de rede que abrange uma área geográfica limitada. Os principais recursos das LANs podem ser:

- Dispositivos finais de interconexão de LANs em uma área limitada, como uma residência, uma sala de aula, um edifício de escritórios ou um campus acadêmico;
- Uma LAN é geralmente administrada por uma organização privada ou por um administrador de rede. O controle administrativo que rege as políticas de segurança e controle de acesso é executado no nível de rede;
- As LANs fornecem largura de banda e vazão em alta velocidade para os dispositivos finais e aos dispositivos intermediários de rede.

Redes de Longa Distância (WAN)

As redes de longa distância (WANs) são uma infraestrutura de rede que abrange uma grande área geográfica, como por exemplo a ligação entre estados ou até mesmo a ligação entre países no globo terrestre. As WANs são geralmente gerenciadas por provedores de serviços (SP) ou por provedores de serviços de Internet (ISP). A Internet (Redes das Redes) é classificada como uma rede WAN.

Os principais recursos das WANs incluem:

- As WANS têm como objetivo interconectar as LANs em grandes áreas geográficas, como entre cidades, estados, províncias, países ou continentes;
- As WANs são geralmente administradas por vários prestadores de serviço de internet e conectividade;
- As WANs geralmente fornecem links de velocidade mais lenta se comparada com as LANs.

Sistema Operacional de Rede (SOR)

Todos os dispositivos finais e os dispositivos de rede conectados à Internet exigem um sistema operacional de rede (SOR) para auxiliar na execução de uma função. Quando um computador é ligado e conectado em uma rede, ele carrega o sistema operacional que está normalmente instalado em uma memória ROM, unidade de disco HDD, SSD ou flash na memória de trabalho (também conhecida como RAM) para que a CPU possa do dispositivo possa executar suas aplicações. A parte do código do sistema operacional que interage diretamente com o hardware é conhecida como kernel e a parte que faz a interface com os aplicativos e o usuário final é conhecida como shell. O usuário pode interagir com o uso do shell na interface de linha de comando (CLI) ou na interface gráfica de usuário (GUI), muito utilizada em ambientes gráficos como o sistema operacional Windows. (CISCO NETACAD, 2017)

Ao usar a CLI, o usuário interage diretamente com o sistema operacional em um ambiente baseado em texto ao inserir comandos no teclado digitados a frente de um prompt de comando. O sistema executa o comando, geralmente fornecendo uma saída textual. Já a interface GUI permite que o usuário interaja com o sistema operacional em um ambiente que utiliza imagens gráficas, multimídia e texto. As ações são realizadas pela interação com as imagens na tela graficamente. A GUI é mais fácil de usar e requer menos conhecimento do operador na estrutura do comando para se utilizar o sistema. Por esse motivo, muitas pessoas confiam em ambientes de GUI. A maioria dos sistemas operacionais do dispositivo final é acessada usando a GUI, incluindo o MS Windows, MAC OS X, Linux, Apple iOS, Android e muito mais.

O método mais comum para configurar um roteador residencial é utilizar um navegador Web para acessar uma GUI fácil de usar. A maioria dos roteadores residenciais permite a atualização da estrutura de um sistema operacional conhecida como firmware, caso novos recursos ou vulnerabilidades de segurança sejam descobertos. (STALLINGS, W. e ROSS K., 2010)



Figura 4 – SOR Cisco IOS

Os dispositivos de rede de infraestrutura também utilizam um sistema operacional de rede. O sistema operacional de rede utilizado em dispositivos da Cisco é chamado de Internetwork Operating System (IOS). O Cisco IOS é um termo genérico dos sistemas operacionais de **rede** usados em dispositivos de rede da Cisco,

como por exemplo switches e roteadores que independem do tamanho ou do tipo do dispositivo. O método mais comum de acessar esses dispositivos através do IOS é usando uma CLI.

Finalidade do Sistema Operacional

Sistemas operacionais de rede são de várias formas semelhantes aos sistemas operacionais de computadores pessoais. Um sistema operacional executa várias funções técnicas internas que permite que um usuário:

- Possa usar um mouse;
- Exiba a saída de informações em um monitor;
- Insira comandos de texto na prompt de comando;
- Selecione opções dentro de uma janela da caixa de diálogo.

As funções internas de switches e roteadores são muito parecidas, pois, fornecem uma interface ao administrador de rede. O administrador de rede pode inserir comandos para configurar, ou programar, o dispositivo para realizar várias funções de rede. Os detalhes operacionais do IOS variam de dispositivos de redes interconectadas, dependendo do propósito do dispositivo e dos recursos por ele suportados.

O Cisco IOS é um termo que abrange diversos sistemas operacionais diferentes em execução para vários dispositivos de rede. Existem muitas variações distintas do Cisco IOS:

- O IOS para switches, roteadores e outros dispositivos de rede da Cisco;
- Versões numeradas de IOS para um determinado dispositivo da rede da Cisco;
- O recurso IOS define o fornecimento de pacotes diferentes de recursos e serviços.

Assim como um computador pode executar o Microsoft Windows 8 ou 10 e o MacBook pode executar o OS X, o dispositivo de rede da Cisco executa uma versão específica do Cisco IOS. A versão do IOS depende do tipo de dispositivo que está sendo utilizado e dos recursos necessários para tal. É possível atualizar a versão ou o conjunto de recursos do IOS para obter recursos adicionais.

Localização do IOS nos Equipamentos

Em muitos dispositivos Cisco, o IOS é armazenado na memória flash e depois carregado na memória de acesso aleatório (RAM) ou também conhecida como memória de trabalho, para depois ser executado em CPU. Quando o dispositivo é inicializado, essa atividade possui muitas funções que incluem armazenar dados que são utilizados pelo dispositivo para dar suporte a operações de rede. O IOS é carregado na RAM por causa do desempenho dessa memória, que é muito mais rápida do que as outras memórias, no entanto, a RAM é considerada uma memória volátil porque os dados são perdidos caso o dispositivo deixe de ser alimentado pela

energia elétrica (ciclo de energia). Um ciclo de energia ocorre quando um dispositivo é desligado propositalmente ou por acidente e então religado novamente.

A quantidade de memória flash e de memória RAM necessárias para um o armazenamento a operação de um determinado IOS varia muito, pois depende da arquitetura do equipamento utilizado. Para fins de manutenção de rede e de planejamento, é importante determinar os requisitos de flash e de RAM para cada dispositivo a ser utilizado. É possível que os requisitos das versões mais recentes do IOS possam exigir mais memória RAM e memória flash do que em alguns dispositivos mais básicos e que podem oferecer menos recursos.

Funções do IOS

Os roteadores, switches e pontos de acesso da Cisco que utilizam o IOS executam funções esperadas pelos administradores de rede, depois de corretamente configuradas e devem funcionar conforme o esperado. As principais funções executadas ou habilitadas pelos roteadores, switches e pontos de acesso da Cisco incluem:

- Oferecer segurança de rede limítrofe e dos dispositivos;
- Endereçamento IP de interfaces físicas e virtuais;
- Permitir configurações específicas à interface com o objetivo de otimizar a conectividade do respectivo meio físico;
- Fazer corretamente o roteamento (Encaminhamento de pacotes através do melhor caminho) dos dados de rede;
- Habilitar tecnologias de Qualidade de serviço (QoS);
- Suportar tecnologias de gerenciamento de rede.

Cada recurso ou serviço de rede possui uma coleção de comandos de configuração associadas, que permitem que um administrador de rede possa implementá-las.

Os serviços fornecidos pelo sistema operacional Cisco IOS são geralmente acessados usando uma CLI – Interface de Linha de Comando através de comandos aplicados em uma prompt de execução.

Métodos de Acesso do IOS

Existem várias maneiras de poder acessar o ambiente de CLI do Cisco IOS. Os métodos mais comuns seriam:

- Porta Console (A primeira forma de acesso);
- Porta AUX (porta auxiliar se pode conectar um modem);
- Conexão Telnet ou SSH.

Porta de Console

A porta do console ou apenas porta console é uma porta física de gerenciamento de rede que fornece acesso out-of-band (OOB) em um dispositivo da Cisco. O acesso OOB ou fora da banda em português refere-se ao acesso por meio de um canal dedicado de gerenciamento que é usado somente para fins de manutenção e acesso ao dispositivo. A vantagem de usar uma porta de console é que o dispositivo estará acessível mesmo se nenhum serviço de rede estiver sido configurado e inicializado. Ao executar uma configuração inicial, um computador que executa o software de emulação do terminal é conectado à uma porta de console do dispositivo usando um cabo especial conhecido como cabo console, cabo rollover ou cabo de gerência. Comandos de configuração utilizados para configurar o switch, o roteador ou um ponto de acesso podem ser inseridos no computador conectado em sua porta de comunicação (COM1, COM2, etc.).



Figura 5 – Porta console

A porta do console também pode ser usada quando os serviços de rede falharem e quando o acesso remoto ao dispositivo Cisco IOS não for possível. Se isso ocorrer, uma conexão ao console pode permitir que um computador determine o status do dispositivo. (CISCO NETACAD, 2017). Por padrão, a console transmite a inicialização do dispositivo, a depuração e as mensagens de erro realizadas através do processo de boot do dispositivo. Depois que o técnico de rede estiver conectado ao dispositivo através do cabo de console, ele poderá executar qualquer comando de configuração necessário a realização de suas atividades.

Para muitos dispositivos da Cisco que utilizam o sistema operacional IOS, o acesso do console não exige qualquer forma de segurança, por padrão. Ou seja, por padrão nenhuma senha de acesso é definida. No entanto, o console deve ser configurado pelo administrador com senhas para impedir acesso não autorizado ao dispositivo a ser acessado. Caso uma senha seja perdida, existe um conjunto de procedimentos especiais para contornar a senha e acessar o dispositivo, tal processo é conhecido como “password recover”. O dispositivo de rede deve estar localizado dentro de uma sala trancada, um ambiente apropriado e refrigerado ou em um rack de equipamentos, afim de impedir o acesso físico e indevido de pessoas não autorizadas.

Porta Auxiliar (AUX)

Uma maneira mais antiga de estabelecer uma sessão de CLI remotamente é via uma conexão dial-up de telefone com um modem conectado à porta auxiliar (AUX) de um roteador. Esse procedimento é semelhante à uma conexão de console, esse método de conexão AUX é também uma conexão out-of-band e não exige que serviços de rede sejam configurados ou estejam disponíveis no dispositivo. Caso os serviços de rede falharem, será possível que o administrador possa acessar remotamente o switch ou o roteador através de uma linha telefônica.



Figura 6 – Porta console

A porta AUX também pode ser usada localmente, como a porta do console, com uma conexão direta a um computador executando um programa de emulação de terminal. A porta do console também é preferencial sobre a porta auxiliar para correção de erros, pois ela exibe mensagens de inicialização, de depuração e de erros por padrão.

Coneção Telnet

A sessão Telnet é um método usado para estabelecer de forma remota uma sessão de CLI de um dispositivo, por meio de uma interface virtual, através da conexão de rede. Diferente da conexão do console, as sessões Telnet exigem serviços de rede ativos no dispositivo, ou seja, precisam de propriedades de configuração anteriormente realizadas para que o equipamento seja acessado. O dispositivo de rede deve ter pelo menos uma interface ativada e configurada com um endereço de rede, como por exemplo um endereço IPv4. Os dispositivos Cisco IOS incluem um processo de servidor Telnet que permite os usuários poderem inserir comandos de configuração a partir de um determinado cliente Telnet. Além de suportar o processo de servidor Telnet, o dispositivo Cisco IOS também contém um cliente Telnet. Isso pode permitir que um administrador de rede use a sessão telnet do dispositivo através do CLI da Cisco para qualquer outro dispositivo que ofereça suporte a este processo.

Coneção SSH

O Protocolo Secure Shell (SSH) pode fornecer um login remoto semelhante ao Telnet, porém muito mais seguro que seu antecessor. Por esse motivo o SSH fornece o processo de autenticação de senha mais forte do que o Telnet e utiliza um sistema de criptografia para transportar dados desta sessão. Isso mantém o ID de usuário, a senha e os detalhes da sessão de gerenciamento em privacidade. Como prática é recomendada que se utilize a sessão SSH ao invés da sessão Telnet por motivos de segurança óbvios.

A maioria das versões do sistema operacional da Cisco IOS inclui um servidor SSH, e esse serviço é habilitado por padrão (default). Outros dispositivos exigem

que o servidor SSH seja habilitado manualmente. Esses dispositivos Cisco incluem também um cliente SSH que pode ser utilizado para estabelecer sessões de SSH com outros dispositivos de uma forma segura.

Programas de Emulação de Terminal

Há vários programas de emulação de terminal excelentes disponíveis para conectar a um dispositivo de rede por meio de uma conexão serial de comunicação sobre uma porta de console ou de uma conexão Telnet/SSH. Podemos incluir as seguintes aplicações:

- PuTTY;
- Tera Term;
- SecureCRT;
- HyperTerminal.

Essas aplicações de emulação de terminal permitem que o administrador de rede aumente sua produtividade ajustando tamanhos de janela, alterando tamanhos de fontes e alterando esquemas de cores.

Navegação no Sistema Operacional Cisco IOS

Depois que um administrador de rede estiver conectado a um dispositivo de rede, será possível configurá-lo, através da navegação de vários modos de configuração do IOS. Esses modos são muito semelhantes em switches, roteadores e pontos de acesso. O CLI utiliza uma estrutura hierárquica para que esses modos possam ser acessados.

Utilizando essa hierarquia dos modos do Cisco IOS, podemos definir os seguintes modos mais clássicos e utilizados:

- Modo de execução do usuário (EXEC usuário);
- Modo de execução privilegiado (EXEC privilegiado);
- Modo de configuração global;
- Outros modos de configuração específicos, tais como o modo de configuração da interface, o modo de line, o modo de roteamento, o modo de protocolo e muitos outros.

Cada modo possui um prompt específico que é utilizado para realizar determinadas tarefas através de um conjunto de comandos disponíveis somente para aquele modo de configuração. Por exemplo, o modo de configuração global permite que um administrador defina as configurações no dispositivo que afeta o dispositivo como um todo, como configurar um nome para tal dispositivo (comando hostname). No entanto, um modo diferente é necessário se o administrador de rede desejar definir configurações de segurança em uma porta específica em um switch. Nesse caso, o administrador de rede deve acessar o modo de configuração de interface (config-if) dessa porta específica. Todas as configurações inseridas no modo de configuração de interface se aplicam somente a essa porta.

```
Comando User EXEC - Router>
ping
show (limitado)
enable
etcetera
```

Comandos Privileged EXEC - Router#

Todas as User EXEC comandos

debug comandos
reload
configure
etcetera

Comandos de configuração global - Router(config)#

hostname
enable secret
ip route
interface ethernet
serial
dsl
etcetera

router rip
ospf
eigrp
etcetera

line vty
console
etcetera

Comandos de interface -
Router(config-if)#
ip address
ipv6 address
encapsulation
shutdown/no shutdown
etcetera

Comandos Routing Engine -
Router(config-router)#
network
version
auto summary
etcetera

Comandos de linha -
Router(config-line)#
password
login
modem comandos
etcetera

Figura 7 – Estrutura hierárquica do IOS

A estrutura hierárquica pode ser configurada para fornecer segurança. Uma autenticação diferente pode ser necessária para cada modo hierárquico. Isso controla o nível de acesso que o pessoal de rede pode receber.

Modos Primários de Configuração

Os dois modos primários de operação são o modo EXEC usuário e o modo EXEC privilegiado. Como um recurso de segurança, o software Cisco IOS separa as sessões EXEC em dois níveis de acesso. Como mostrado na próxima figura. O modo EXEC privilegiado possui um nível superior de autoridade e privilégio no qual permite que o usuário possa fazer um todo no equipamento.

Modo EXEC Usuário

O modo EXEC usuário tem recursos limitados e com poucos privilégios, mas é útil para algumas operações básicas no equipamento. O modo EXEC usuário está no nível mais básico da estrutura hierárquica dos modos de configuração. Tal modo é o primeiro modo executado na entrada no CLI de um dispositivo IOS, logo que tal equipamento é inicializado.

O modo EXEC usuário permite somente uma quantidade limitada de comandos básicos de monitoramento, como por exemplo comando de verificação, como alguns

comandos show, o ping e tracert. O nível EXEC usuário não permite a execução de quaisquer comandos que poderiam alterar a configuração do dispositivo como um todo, muito menos comandos que possam apagar arquivos de configuração e resetar o respectivo dispositivo.

Por padrão, não há autenticação exigida para acessar o modo EXEC usuário através da conexão console. Contudo, essa é uma boa prática para garantir que a autenticação seja configurada durante a configuração inicial. (CISCO NETACAD, 2017)

O modo EXEC usuário é identificado pelo prompt do CLI que termina com o símbolo >. Esse é um exemplo que mostra o símbolo > no prompt:

Switch>

Modo EXEC privilegiado

A execução de comandos de configuração e gerenciamento exige que o administrador de rede use o modo EXEC privilegiado ou um modo mais específico na hierarquia. Isso significa que um usuário deve entrar no modo EXEC usuário primeiro e, de lá, acessar o modo EXEC privilegiado. (CISCO NETACAD, 2017)

O modo EXEC privilegiado pode ser identificado pelo prompt terminando com o símbolo #.

Switch#

Por padrão, o modo EXEC privilegiado não requer autenticação. É uma boa prática garantir que a autenticação seja configurada.

O modo de configuração global e outros modos de configuração como por exemplo o de configuração de interface, só podem ser alcançados a partir do modo EXEC privilegiado.

Modo de Configuração Global

O modo de configuração global ou config. Global, afeta a operação no dispositivo como um todo, por esse motivo esse nome. Tal modo de configuração é acessado antes dos modos de configuração específicos, como os modos de interface e o modo de roteamento.

O comando CLI a seguir é usado para tirar o dispositivo do modo EXEC privilegiado e acessar o modo de configuração global, afim de permitir a entrada de comandos de configuração desse modo, através de uma conexão de terminal.

Switch# configure terminal

Depois que tal comando for executado, o prompt é alterado para mostrar que o switch está no modo de configuração global, como mostrado:

Switch(config)#

Modos Específicos de Configuração

No modo de configuração global, o usuário pode inserir diferentes modos de subconfiguração. Cada um desses modos permite a configuração de uma parte específica ou função do dispositivo de IOS. A lista abaixo mostra alguns deles:

- **Modo de Interface** - para configurar uma das interfaces de rede (Fa0/0, S0/0/0);
- **Modo de Linha** - para configurar uma das linhas físicas ou virtuais (console, AUX, VTY).

Para sair de um modo específico de configuração e voltar ao modo de configuração global, insira o comando `exit` em um prompt do sistema operacional. Para deixar o modo de configuração por completo e voltar ao modo EXEC privilegiado, insira o comando `end` ou use a sequência de teclas `<Ctrl-Z>`.

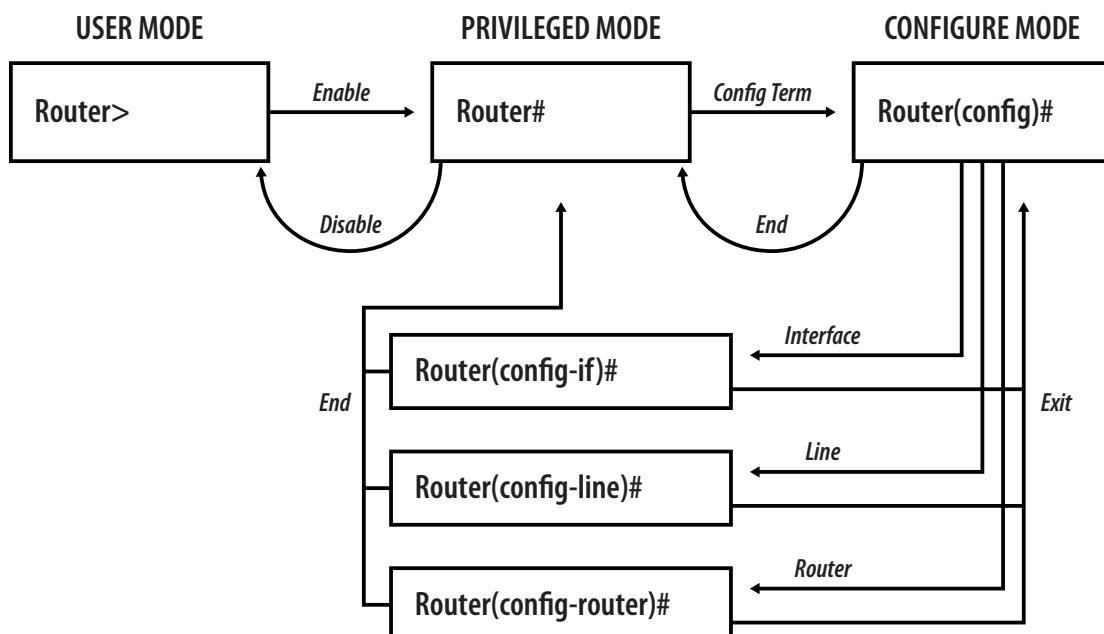


Figura 8 – Modos de configuração

Prompts de Comando

Ao usar a CLI, o modo é identificado pelo prompt da linha de comando que é único para aquele respectivo modo. Por padrão, todo prompt começa com o nome do dispositivo, como por exemplo `router` ou `switch`. Após o nome, o restante do prompt indica o modo que ele está. Por exemplo, o prompt padrão do modo de configuração global em um `switch` seria:

`Switch(config)#`

Navegar Entre os Modos do IOS

Os comandos `enable` e `disable` são usados para alterar a CLI entre o modo EXEC usuário e o modo EXEC privilegiado, respectivamente.

Do modo usuário para acessar o modo EXEC privilegiado, use o comando enable. O modo EXEC privilegiado é algumas vezes chamado de modo habilitar. E o comando disable é usado para retornar do modo privilegiado para o modo usuário. O comando exit no modo privilegiado termina toda a sessão com o dispositivo.

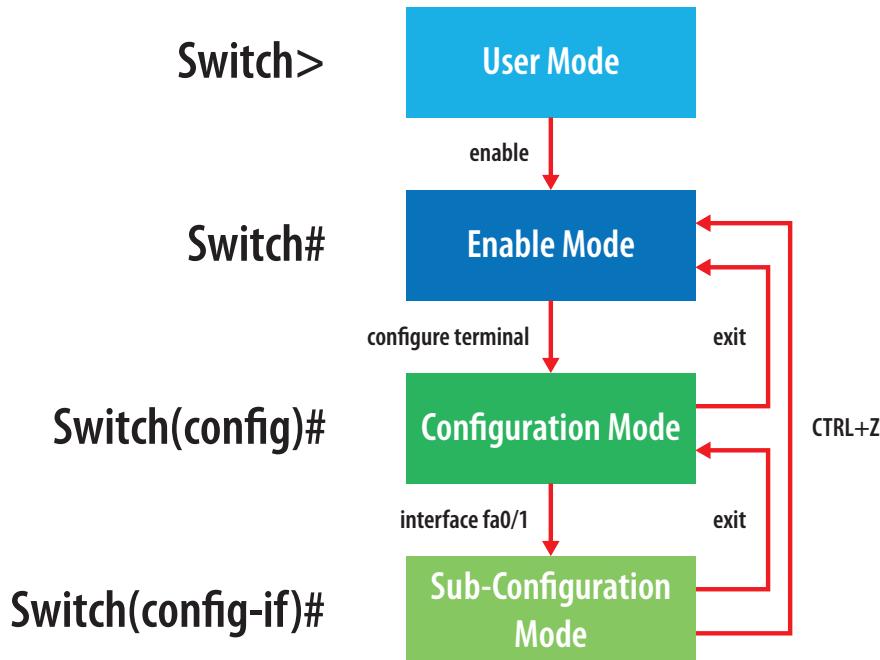


Figura 9 – Navegando entre modos do IOS

Ajuda Contextual ou Help

O Cisco IOS possui várias formas de ajuda (help) disponíveis:

- Ajuda Contextual;
- Verificação de Sintaxe de Comando;
- Teclas de Acesso e Atalhos.

A ajuda contextual fornece uma lista de comandos e os argumentos associados a esses comandos dentro do contexto do modo atual. Para acessar a ajuda contextual, insira uma interrogação, ?, em qualquer prompt. Há uma resposta imediata, sem a necessidade de usar a tecla <Enter> para executá-lo.

Um uso da ajuda contextual existe para se obter uma lista de comandos disponíveis. Ela pode ser usada quando você não tiver certeza do nome ou sintaxe para um determinado comando ou se você quiser ver se o IOS suporta um comando específico em um modo específico.

Comandos de Monitoramento

Com o intuito de verificar e solucionar eventuais problemas na operação da rede, devemos checar a operação dos dispositivos de rede. O comando básico de monitoramento é o comando show ou o comando debug.

Existem muitas variações e qualificadores diferentes para o comando show ou debug. À medida que você desenvolve mais habilidade com o Cisco IOS, aprenderá a usar e interpretar melhor os resultados desses comandos. Teste o comando show? para obter uma lista de sub-comandos disponíveis em um determinado contexto ou modo a ser aplicado.

Um comando show pode fornecer várias informações sobre a configuração, a operação e o status de partes de um switch ou roteador da Cisco. Podemos verificar alguns dos comandos mais comuns do Cisco IOS.

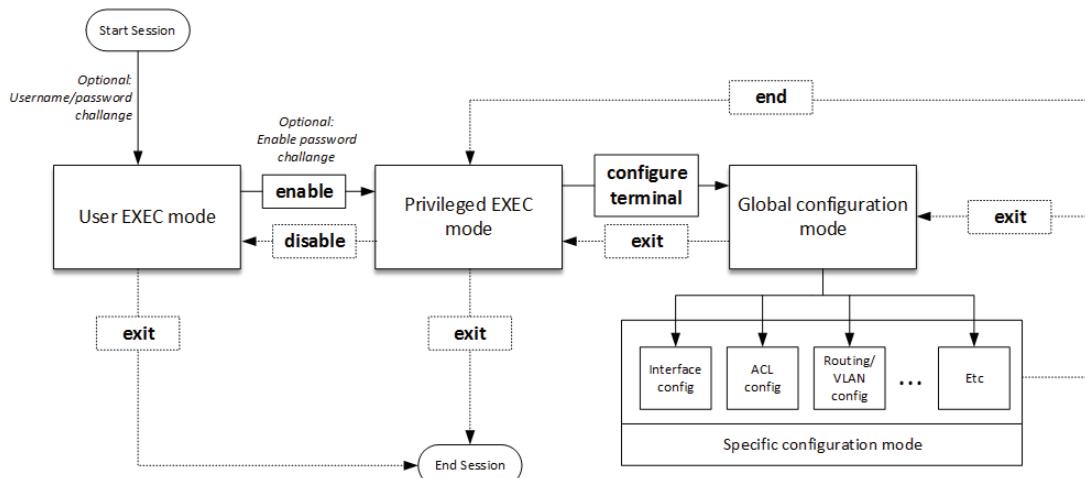


Figura 10 – Entendendo comandos do IOS

Proteção ao Dispositivo

Limitar fisicamente o acesso a dispositivos de rede colocando-os em racks fechados ou abertos seria uma boa prática de segurança física; no entanto, senhas são a principal defesa contra o acesso não autorizado a estes dispositivos de rede. Cada dispositivo, até mesmo roteadores domésticos, deve ter senhas configuradas localmente para limitar o acesso (CISCO NETACAD, 2017).

O Cisco IOS utiliza modos de configuração hierárquicos para auxiliar na segurança do dispositivo em questão, fazendo parte desse reforço de segurança lógica do equipamento. O sistema operacional pode aceitar várias senhas para determinar e permitir diferentes privilégios de acesso ao equipamento.

As senhas apresentadas aqui são:

- **Habilitar Senha** – limita o acesso ao modo EXEC privilegiado, com senha em texto claro;
- **Habilitar Senha Secreta** – limita o acesso ao modo EXEC privilegiado, com senha criptografada em MD5;

- **Senha do Console** – limita o acesso via conexão console ao dispositivo a ser utilizado;
- **Senha VTY** – limita o acesso ao dispositivo com conexão de sessão Telnet.

```
UNICSUL#enable
UNICSUL#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UNICSUL(config)#enable password cruzeirodosul
UNICSUL(config)#enable secret cisco
```

Figura 11 – Comandos de proteção de senha

```
UNICSUL(config)#line console 0
UNICSUL(config-line)#password cisco
UNICSUL(config-line)#login
UNICSUL(config-line)#
UNICSUL(config-line)#line vty 0 4
UNICSUL(config-line)#password cisco
UNICSUL(config-line)#login
```

Figura 12 – Comandos de proteção de console e VTY

Arquivo de Configuração

O arquivo de configuração em execução na memória RAM reflete a configuração atual aplicada a um dispositivo Cisco. Ele contém comandos usados para determinar como o dispositivo deve operar na rede. Modificar uma configuração em execução afeta imediatamente a operação de um dispositivo Cisco. (CISCO NETACAD, 2017)

O arquivo de configuração de execução (running-configuration) é armazenado na memória de operação / trabalho do dispositivo ou na memória de acesso aleatório (RAM). Isso significa que o arquivo de configuração de execução está temporariamente ativo enquanto o dispositivo Cisco está sendo executando (ligado) e energizado. Entretanto, se a energia do dispositivo for perdida ou se o equipamento for reiniciado, todas as mudanças na configuração serão perdidas a menos que elas tenham sido salvas, pois a memória RAM é uma memória volátil.

Depois de fazer alterações em um arquivo de configuração em execução, considere estas opções distintas:

- Retorne o dispositivo à sua configuração original;
- Remova todas as configurações do dispositivo;
- Torne a configuração alterada a nova configuração de inicialização.

```
UNICSUL#show running-config
Building configuration...

Current configuration : 726 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname UNICSUL
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cruzeirodosul
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524V3D0
!
```

Figura 13 – Arquivo de Configuração em RAM

O arquivo de configuração de inicialização (startup-configuration) reflete a configuração que será usada pelo dispositivo na reinicialização, este arquivo está armazenado na NVRAM, que uma memória rápida e não volátil. Quando um dispositivo de rede tiver sido configurado e a configuração em execução tiver sido modificada, será importante salvar essas alterações no arquivo de configuração de inicialização. Isso impede que as alterações sejam perdidas devido a uma falha de energia ou uma reinicialização intencional. (CISCO NETACAD, 2017)

Antes de se comprometer com as alterações, use os comandos show adequados para verificar a operação do dispositivo. O comando show running-config pode ser usado para verificar um arquivo de configuração em execução. Quando as alterações forem certificadas de estarem corretas, use o comando copy running-config startup-config no prompt do modo EXEC privilegiado. O comando para salvar a configuração em execução para o arquivo de configuração de inicialização é:

Switch# copy running-config startup-config

Depois de ser executado, o arquivo de configuração em execução atualiza o arquivo de configuração de inicialização copiando em memória NVRAM.

Se as alterações feitas à configuração de execução não tiverem o efeito desejado, pode ser necessário restaurar o dispositivo à sua configuração anterior. Considerando que não sobrescrevemos a configuração de inicialização com as alterações, podemos substituir a configuração em execução pela configuração de inicialização. Isso é feito melhor ao reiniciar o dispositivo usando o comando reload no prompt do modo EXEC privilegiado (CISCO NETACAD, 2017).

Ao iniciar uma recarga, o IOS detectará que o running config tem alterações que não foram salvas na configuração de inicialização. Um prompt aparecerá para perguntar se precisa salvar as alterações feitas. Para descartar as alterações, insira n ou no (CISCO NETACAD, 2017). Outro prompt aparecerá para confirmar a recarga. Para confirmar, pressione Enter. Pressionar qualquer outra tecla irá abortar o processo.

Material Complementar

Indicações para saber mais sobre os assuntos abordados nesta Unidade:



Sites

Curso WEB: CISCO NETACAD

Curso WEB: CISCO NETACAD – Módulo de Introdução a Redes – Capítulo 1: Explorando a Rede.

<https://goo.gl/kSQz1K>

Curso WEB: CISCO NETACAD

Curso WEB: CISCO NETACAD – Módulo de Introdução a Redes – Capítulo 2: Configuração de um Sistema Operacional de Rede.

<https://goo.gl/kSQz1K>



Livros

Redes de Computadores e a Internet

STALLINGS, W. e ROSS K. – Redes de Computadores e a Internet - 5^a Ed., Pearson, 2010.

Redes de Computadores

TANENBAUM, A. S. – Redes de Computadores – 5^a Ed., Pearson, 2011.

Referências

CISCO NETACAD – **Módulo de Introdução a Redes (CCNA1)** – 6^a Versão, Cisco Systems, 2017. (material on-line). Disponível em: <<https://www.netacad.com/pt-br>>

STALLINGS, W. e ROSS K. – **Redes de Computadores e a Internet** - 5^a Ed., Pearson, 2010.

TANENBAUM, A. S. – **Redes de Computadores** – 5^a Ed., Pearson, 2011.



Cruzeiro do Sul
Educacional