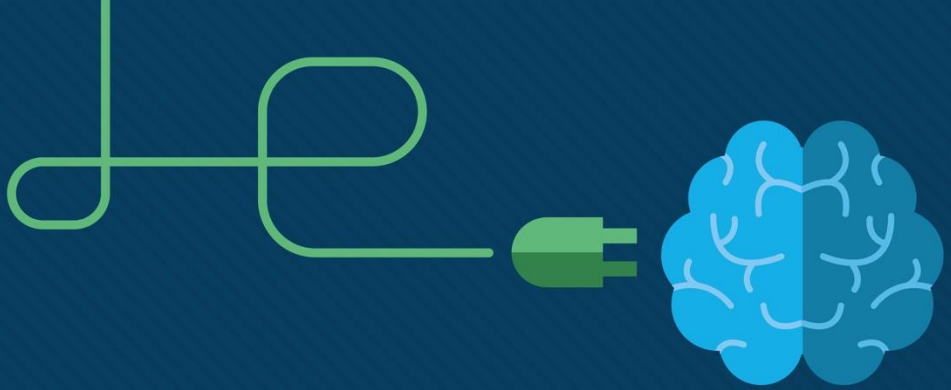


Módulo 17: Construa uma rede pequena

CCNA_M1-Introdução às redes v7.0 (ITN)

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br

Objetivos do módulo

Título do módulo: Criar uma rede pequena

Objetivo do módulo: Implementar um design de rede para uma pequena rede para incluir um roteador, um switch e dispositivos finais.

Título do Tópico	Objetivo do Tópico
Dispositivos em uma rede pequena	Identificar os dispositivos usados em uma rede pequena.
Aplicações e protocolos de redes pequenas	Identificar os protocolos e aplicações usadas em uma rede pequena.
Escalar para redes maiores	Explicar como uma rede pequena serve de base para redes maiores.
Verificar a conectividade	Usar a saída dos comandos ping e tracert para verificar a conectividade e determinar o desempenho da rede relacionada.
Host e comandos IOS	Usar o host e os comandos IOS para adquirir informações sobre os dispositivos em uma rede.
Metodologias de solução de problemas	Descrever as metodologias de solução de problemas de rede comuns.
Cenários de solução de problemas	Solucionar problemas com dispositivos na rede.

17.1 – Dispositivos em uma Rede Pequena

Dispositivos em uma Rede Pequena Topologias de uma Rede Pequena

- A maioria das empresas são pequenas, a maioria das redes de negócios também são pequenas.
- Um pequeno design de rede geralmente é simples.
- Redes pequenas geralmente têm uma única conexão WAN fornecida por DSL, cabo ou conexão Ethernet.
- As redes grandes exigem que um departamento de TI mantenha, proteja e solucione problemas de dispositivos de rede e proteja dados organizacionais. Pequenas redes são gerenciadas por um técnico de TI local ou por um profissional contratado.

Seleção de Dispositivo de uma Rede Pequena

Como redes grandes, redes pequenas exigem planejamento e design para atender aos requisitos do usuário. O planejamento assegura que todos os requisitos, fatores de custo e opções de implantação recebam a devida consideração. Uma das primeiras considerações de design é o tipo de dispositivos intermediários a serem usados para oferecer suporte à rede.

Os fatores que devem ser considerados ao selecionar dispositivos de rede incluem:

- Custo
- Velocidade e Tipos de Portas/Interfaces
- Capacidade de expansão
- Serviços e Recursos do Sistema Operacional

Endereçamento de uma Rede Pequena

Ao implementar uma rede, crie um esquema de endereçamento IP e use-o. Todos os hosts e dispositivos em uma internetwork devem ter um endereço exclusivo. Os dispositivos que serão fatoriais no esquema de endereçamento IP incluem o seguinte:

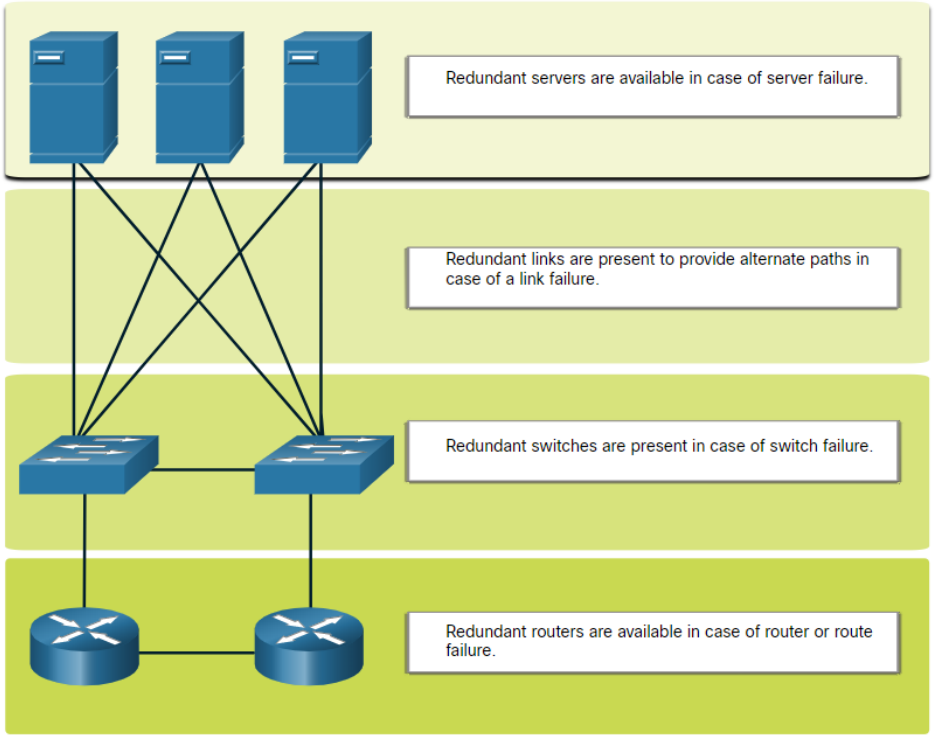
- Dispositivos do usuário final - O número e o tipo de conexões (ou seja, com fio, sem fio, acesso remoto)
- Servidores e dispositivos periféricos (por exemplo, impressoras e câmeras de segurança)
- Dispositivos intermediários, incluindo comutadores e pontos de acesso

É recomendável planejar, documentar e manter um esquema de endereçamento IP baseado no tipo de dispositivo. O uso de um esquema de endereçamento IP planejado facilita a identificação de um tipo de dispositivo e a solução de problemas.

Redundância de uma Rede Pequena

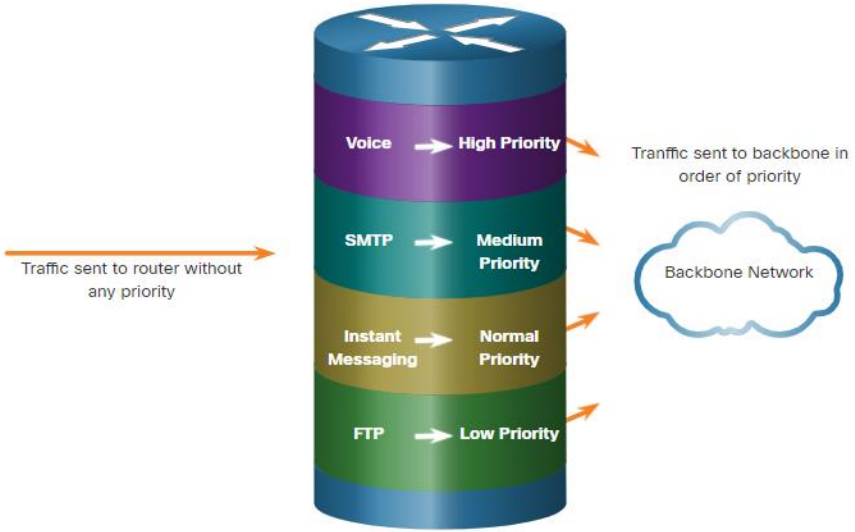
Para manter um alto grau de confiabilidade, *redundância* é necessária no design da rede. A redundância ajuda a eliminar os pontos únicos de falha.

A redundância pode ser realizada instalando equipamentos duplicados. Isso também pode ser realizado fornecendo links de rede duplicados para áreas críticas.



Gerenciamento de Tráfego

- O objetivo de um bom design de rede é aumentar a produtividade dos funcionários e minimizar o tempo de inatividade da rede.
- Os roteadores e comutadores em uma rede pequena devem ser configurados para rastrear o tráfego em tempo real, como voz e vídeo, de maneira possível em relação a outro tráfego de dados. Um bom design de rede implementará a qualidade de serviço (QoS).
- O enfileiramento com prioridade tem quatro filas. A fila de prioridade alta é sempre esvaziada primeiro.



17.2 – Aplicações e Protocolos de Redes Pequenas

Aplicações Comuns

Depois de configurá-lo, sua rede ainda precisa de certos tipos de aplicativos e protocolos para funcionar. A rede é tão útil quanto as aplicações que estão nela.

Há duas formas de programa de software ou processos que fornecem acesso à rede:

- **Aplicativos de Rede**: aplicativos que implementam protocolos da camada de aplicativos e podem se comunicar diretamente com as camadas inferiores da pilha de protocolos.
- **Serviços de Camada de Aplicativo**: para aplicativos que não são compatíveis com a rede, os programas que fazem interface com a rede e preparam os dados para transferência.

Protocolos Comuns

Protocolos de rede dão suporte às aplicações e serviços usados por funcionários em uma rede pequena.

- Normalmente, os administradores de rede exigem acesso a dispositivos e servidores de rede. As duas soluções de acesso remoto mais comuns são Telnet e Secure Shell (SSH).
- HTTP (Hypertext Transfer Protocol) e HTTP (Hypertext Transfer Protocol Secure) são usados entre clientes Web e servidores Web.
- O SMTP (Simple Mail Transfer Protocol) é usado para enviar email, o POP3 (Internet Post Protocol) ou o IMAP (Internet Mail Access Protocol) são usados pelos clientes para recuperar o email.
- File Transfer Protocol (FTP) e Security File Transfer Protocol (SFTP) são usados para baixar e carregar arquivos entre um cliente e um servidor FTP.
- O DHCP (Dynamic Host Configuration Protocol) é usado pelos clientes para adquirir uma configuração IP de um servidor DHCP.
- O Serviço de Nomes de Domínio (DNS) resolve nomes de domínio para endereços IP.

Observação: um servidor pode fornecer vários serviços de rede. Por exemplo, um servidor pode ser um servidor de e-mail, FTP e SSH.

Protocolos Comuns (Cont.)

Esses protocolos de rede compreendem o conjunto de ferramentas fundamentais de um profissional de rede, definindo:

- Processos em cada extremidade de uma sessão de comunicação.
- Tipos de mensagens
- Sintaxe das mensagens
- Significado dos campos informativos
- Como as mensagens são enviadas e a resposta esperada
- Interação com a camada inferior seguinte

Muitas empresas estabeleceram uma política de uso de versões seguras (por exemplo, SSH, SFTP e HTTPS) desses protocolos sempre que possível.

Aplicações de Voz e Vídeo

- Hoje, as empresas estão cada vez mais usando telefonia IP e mídia de streaming para se comunicar com clientes e parceiros de negócios, além de permitir que seus funcionários trabalhem remotamente.
- O administrador de redes deve assegurar que o equipamento adequado foi instalado na rede e que os dispositivos de rede foram configurados para garantir entrega prioritária.
- Os fatores que um pequeno administrador de rede deve considerar ao oferecer suporte a aplicativos em tempo real:
  - **Infraestrutura -** Tem capacidade e capacidade para suportar aplicações em tempo real?
  - **VoIP -** VoIP geralmente é menos caro do que a telefonia IP, mas ao custo de qualidade e recursos.
  - **Telefonia IP -** Isso emprega servidores dedicados forma controle de chamada e sinalização.
  - **Aplicações em Tempo Real -**A rede deve suportar mecanismos de Qualidade de Serviço (QoS) para minimizar problemas de latência. Protocolo de transporte em tempo real (RTP) e Protocolo de controle de transporte em tempo real (RTCP) e dois protocolos que oferecem suporte a aplicativos em tempo real.

17.3 – Escalar para Redes Maiores

Crescimento de Redes Pequenas

O crescimento é um processo natural para muitas empresas de pequeno porte, e suas redes devem acompanhá-lo. Idealmente, o administrador da rede tem tempo de entrega suficiente para tomar decisões inteligentes sobre o crescimento da rede alinhado com o crescimento da empresa.

Para escalonar uma rede, vários elementos são necessários:

- **Documentação de Rede -** Topologia Física e Lógica
- **Inventário de Dispositivos –** Lista de dispositivos que usam ou compõem a rede
- **Orçamento -** orçamento de TI detalhado, incluindo orçamento de compra de equipamentos para o ano fiscal
- **Análise de Tráfego -** Protocolos, aplicativos e serviços e seus respectivos requisitos de tráfego devem ser documentados

Esses elementos são usados para subsidiar a tomada de decisão que acompanha o crescimento de uma rede pequena.

Análise de Protocolo

É importante entender o tipo de tráfego que está atravessando a rede, bem como o fluxo de tráfego atual. Existem várias ferramentas de gerenciamento de rede que podem ser usadas para esse fim.

Para determinar os padrões de fluxo de tráfego, é importante fazer o seguinte:

- Capturar o tráfego durante as horas de pico de utilização para obter uma boa ideia dos diferentes tipos de tráfego.
- Realize a captura em diferentes segmentos e dispositivos de rede, pois algum tráfego será local para um segmento específico.
- As informações reunidas pelo analisador de protocolos são avaliadas com base na origem e destino do tráfego, bem como no tipo de tráfego que é enviado.
- Essa análise pode ser usada para tomar uma decisão sobre como gerenciar o tráfego com mais eficiência.

Utilização da Rede pelos Funcionários

Muitos sistemas operacionais fornecem ferramentas integradas para exibir essas informações de utilização de rede. Essas ferramentas podem ser usadas para capturar um “instantâneo” de informações, como as seguintes:

- Sistema Operacional e a versão desse sistema
- Utilização da CPU
- Utilização da memória RAM
- Utilização das unidades de disco
- Aplicações que não são de rede
- Aplicações de rede

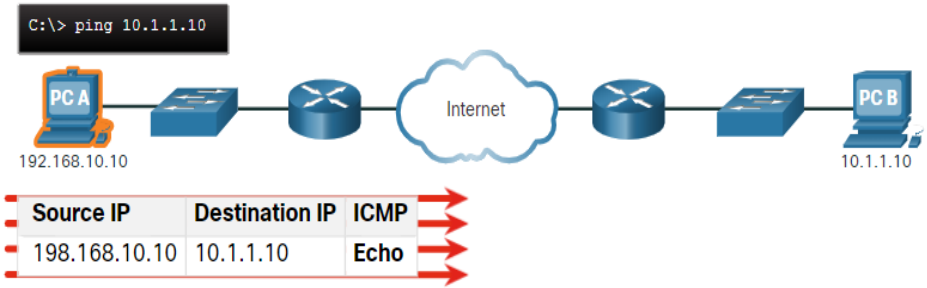
Documentar snapshots para funcionários em uma pequena rede por um período de tempo é muito útil para identificar requisitos de protocolo em evolução e fluxos de tráfego associados.

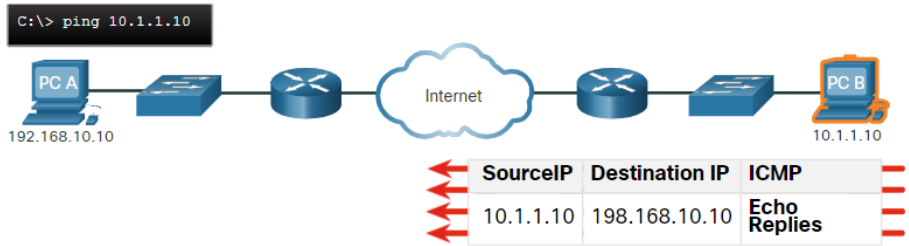
17.4 - Verificar a Conectividade.

Verificar Conectividade com Ping

Independentemente de sua rede ser pequena e nova, ou se você está dimensionando uma rede existente, você sempre vai querer ser capaz de verificar se seus componentes estão corretamente conectados uns aos outros e à internet.

- O comando ping, disponível na maioria dos sistemas operacionais, é a maneira mais eficaz de testar rapidamente a conectividade da Camada 3 entre um endereço IP de origem e de destino.
- O comando ping usa as mensagens ICMP echo (ICMP Type 8) e echo reply (ICMP Type 8).





Verificar Conectividade com Ping (Cont.)

Em um host Windows 10, o comando ping envia quatro mensagens de eco ICMP consecutivas e espera quatro respostas de eco ICMP consecutivas do destino. O ping IOS envia cinco mensagens de eco ICMP e exibe um indicador para cada resposta de eco ICMP recebida.

C

Elemento	Descrição
!	•O ponto de exclamação indica o recebimento bem-sucedido de uma mensagem de resposta de eco. •Ele valida uma conexão de Camada 3 entre origem e destino.
.	•Um período significa que o tempo expirou esperando por uma mensagem de resposta de eco. •Isso indica que ocorreu um problema de conectividade em algum lugar no caminho.
U	•O "**U**" indica que um roteador no caminho respondeu com uma mensagem ICMP de destino inalcançável. •Possíveis motivos incluem que o roteador não sabe a direção para a rede de destino ou não conseguiu localizar o host na rede de destino.

Nota: Outras possíveis respostas de ping incluem Q, M,? , ou &. No entanto, o significado destes estão fora do escopo para est

Ping Estendido

O Cisco IOS oferece um modo "estendido" do comando **ping**.

O ping estendido é inserido no modo EXEC privilegiado, digitando **ping** sem um endereço IP de destino. Em seguida, você receberá vários prompts para personalizar o **ping**estendido.

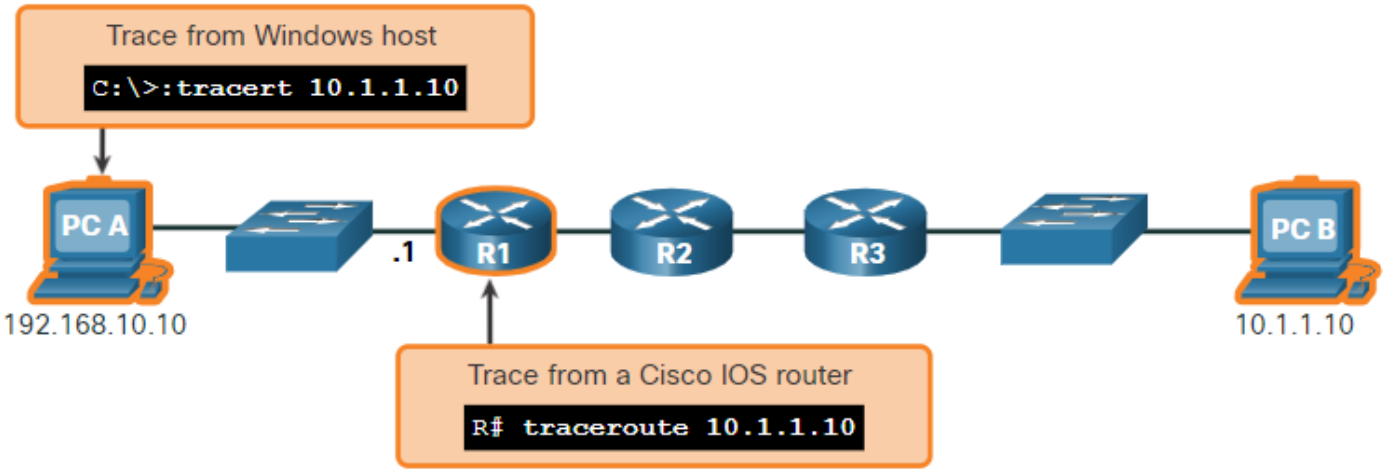
Nota: Pressionar **Enter** aceita os valores padrão indicados. O comando **ping ipv6** é usado para pings estendidos do IPv6.

```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

Verificar Conectividade com Traceroute

O comando ping é útil para determinar rapidamente se há um problema de conectividade da Camada 3. No entanto, ele não identifica onde o problema está localizado ao longo do caminho.

- Traceroute pode ajudar a localizar áreas problemáticas da Camada 3 em uma rede. O comando trace retorna uma lista dos saltos no roteamento de um pacote pela rede.
- A sintaxe do comando trace varia entre os sistemas operacionais.



Verificar Conectividade com Traceroute (Cont.)

- Segue-se uma saída de exemplo do comando **tracert** num anfitrião Windows 10.

  Observação: Use **Ctrl-C** para interromper um **tracert** no Windows.

- A única resposta bem-sucedida foi do gateway no R1. Solicitações de rastreamento para o próximo salto expirado conforme indicado pelo asterisco (*), o que significa que o próximo roteador de salto não respondeu ou há uma falha no caminho de rede. Neste exemplo, parece haver um problema entre R1 e R2.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1     2 ms     2 ms     2 ms  192.168.10.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
^C
C:\Users\PC-A>
```

Verificar Conectividade com Ping (Cont.)

Seguem-se as saídas de exemplo do comando traceroute de R1:

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 10.1.1.10 1 msec 0 msec
R1#
```

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3  *  *  *
  4  *  *  *
  5  *
```

- À esquerda, o rastreamento validou que poderia atingir o PC B.
- À direita, o host 10.1.1.10 não estava disponível e a saída mostra asteriscos onde as respostas expiraram. Os tempos limite indicam um potencial problema de rede.
- Use **Ctrl-Shift-6** para interromper um **traceroute** no Cisco IOS.

Nota: A implementação do Windows do traceroute (tracert) envia solicitações de eco do ICMP. Cisco IOS e Linux usam UDP com um número de porta inválido. O destino final retornará uma mensagem de porta ICMP inacessível.

Traceroute Estendido

Como o comando **ping** estendido, há também um comando **traceroute** estendido. Ele permite que o administrador ajuste parâmetros relacionados à operação de comando.

O comando **tracert** do Windows permite a entrada de vários parâmetros por meio de opções na linha de comando. No entanto, ele não é guiado como o comando estendido traceroute IOS. A saída a seguir exibe as opções disponíveis para o comando **tracert** do Windows:

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name
Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
C:\Users\PC-A>
```

Verificar aConectividade Traceroute Estendido (Cont.)

- A opção **traceroute** estendido do Cisco IOS permite que o usuário crie um tipo especial de rastreamento ajustando parâmetros relacionados à operação do comando.
- O traceroute estendido é inserido no modo EXEC privilegiado digitando **traceroute**sem um endereço IP de destino. O IOS orientará você pelas opções de comando apresentando diversos prompts relacionados à configuração de todos os parâmetros diferentes.

- **Observação**:Ao pressionar **Enter**, você aceita os valores padrão indicados.

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3  *
    10.1.1.10 2 msec 2 msec
R1#
```

Linha de Base de Rede

- Uma das ferramentas mais eficazes para o monitoramento e a solução de problemas de desempenho de rede é estabelecer uma linha de base da rede.
- Um método para iniciar uma linha de base é copiar e colar os resultados de um ping, trace, ou outro comando relevante executado em um arquivo texto. Esses arquivos de texto podem ser marcados com a data e salvos em um arquivo para posterior recuperação e comparação.
- Entre os itens a serem considerados estão as mensagens de erro e os tempos de resposta de cada host.
- Redes corporativas devem possuir linhas de base extensas, mais extensas do que podemos descrever neste curso. Ferramentas profissionais de software estão disponíveis para armazenamento e manutenção das informações de linha de base.

Laboratório - Teste de Latência da Rede com Ping e Traceroute

Nesse laboratório, você completará os seguintes objetivos:

- Parte 1: Usar Ping para Documentar a Latência da Rede
- Parte 2: Usar Traceroute para Documentar a Latência de Rede

17.5 - Host e Comandos IOS

Configuração de IP em um Host do Windows

No Windows 10, você pode acessar os detalhes do endereço IP do **Centro de Rede e Compartilhamento** para exibir rapidamente as quatro configurações importantes: endereço, máscara, roteador e DNS. Ou você pode emitir o comando **ipconfig** na linha de comando de um computador Windows.

- Use o comando **ipconfig /all** para visualizar o endereço MAC, bem como vários detalhes sobre o endereçamento da camada 3 do dispositivo.
- Se um host estiver configurado como um cliente DHCP, a configuração do endereço IP poderá ser renovada usando os comandos **ipconfig /release** e **ipconfig /renew** .
- O serviço Cliente DNS nos computadores com Windows também otimiza o desempenho da decisão do nome DNS ao armazenar nomes previamente definidos na memória. O comando **ipconfig /displaydns** exibe todas as inserções do DNS em cache em um sistema de computador Windows

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

Configuração IP em um Host Linux

- A verificação das configurações de IP usando a GUI em uma máquina Linux será diferente dependendo da distribuição Linux e da interface de desktop.
- Na linha de comando, use o comando **ifconfig** para exibir o status das interfaces ativas no momento e sua configuração IP.
- O comando **IP address do** Linux é usado para exibir endereços e suas propriedades. Ele também pode ser usado para adicionar ou excluir endereços IP.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Observação: A saída exibida pode variar dependendo da distribuição Linux.

Configuração IP em um Host de MacOS

- Na GUI de um host Mac, abra **Preferências de Rede > Avançadas** para obter as informações de endereçamento IP.
- O comando **ifconfig** também pode ser usado para verificar a configuração IP da interface na linha de comando.
- Outros comandos úteis do macOS para verificar as configurações de IP do host incluem **networksetup -listallnetworkservices** e **networksetup -getinfo < serviço de rede >** .

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```

O Comando arp.

O comando **arp** é executado a partir do prompt de comando do Windows, Linux ou Mac. O comando lista todos os dispositivos atualmente no cache ARP do host.

- O comando **arp -a** exibe o endereço IP conhecido e a vinculação de endereço MAC. O cache do ARP exibe apenas informações de dispositivos que foram acessados recentemente.
- Para assegurar que a cache ARP esteja preenchida, faça **ping** em um dispositivo para que ele tenha uma entrada na tabela ARP.
- O cache pode ser limpo usando o comando **netsh interface ip delete arpcache** e depois no caso em que o administrador da rede queira repovoar o cache com informações atualizadas.

Observação: Você pode precisar de acesso de administrador no host para poder usar o comando netsh interface ip delete arpcache.

Comandos Comuns Revisitados: show

Comando	Descrição
show running-config	Verifica a configuração e as configurações atuais
show interfaces	Verifica o status da interface e exibe quaisquer mensagens de erro
show ip interface	Verifica as informações da Camada 3 de uma interface
show arp	Verifica a lista de hosts conhecidos nas LANs Ethernet locais
show ip route	Verifica as informações de roteamento da Camada 3
show protocols	Verifica quais protocolos estão operacionais
show version	Verifica a memória, as interfaces e as licenças do dispositivo

O Comando show cdp neighbors

O CDP fornece as seguintes informações sobre cada dispositivo CDP vizinho:

- **Identificadores** de dispositivo- O nome do host configurado de um switch, roteador ou outro dispositivo
- Lista de endereços **- pelo menos um endereço de camada de rede para cada protocolo compatível**
- Identificador de porta **- o nome de uma porta local e remota na forma de uma string de caracteres ASCII, como FastEthernet 0/0**
- **Lista de capacidades** - Se um dispositivo específico é um switch de Camada 2 ou um switch de Camada 3
- Plataforma **-**

O comando **sho** dispositivo vizinho.

```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122              S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

O Comando show ip interface brief

Um dos comandos mais usados é o comando **show ip interface brief**. Ele exibe um resultado mais abreviado do que o comando **show ip interface**. Ele exibe um resumo das principais informações para todas as interfaces de rede em um roteador.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.254.250 YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
```

Vídeo – O Comando show version

Este vídeo demonstrará o uso do comando show version para visualizar informações sobre o roteador.

Packet Tracer – Interpretar a Saída do Comando show

Esta atividade foi planejada como complemento sobre o uso dos comandos **show** do roteador. Você não precisa configurar, mas sim analisar a saída de vários comandos show.

17.6 – Metodologias de Solução de Problemas

Abordagens Básicas de Solução de Problemas

Etapa	Descrição
Etapa 1. Identificar o Problema	•A primeira etapa no processo de solução de problemas. •Embora ferramentas possam ser usadas nesta etapa, uma conversa com o usuário geralmente é muito útil.
Etapa 2. Estabelecer uma teoria de causas prováveis	•Depois que o problema é identificado, tente estabelecer uma teoria de causas prováveis. •Esta etapa renderá algumas causas prováveis do problema.
Etapa 3. Testar a Teoria para Determinar a Causa	•De acordo com as causas prováveis, teste suas teorias para determinar qual delas é a causa do problema. •Um técnico pode aplicar uma solução rápida para testar e verificar se resolve o problema. •Se uma solução rápida não corrigir o problema, talvez seja necessário pesquisar mais sobre o problema para estabelecer a causa exata.
Etapa 4. Estabelecer um plano de ação e implementar a solução	Depois de determinar a causa exata do problema, estabeleça um plano de ação para resolvê-lo e implementar a solução.
Etapa 5. Verifique a solução e implemente medidas preventivas	•Depois de corrigir o problema, verifique a funcionalidade completa. •Se aplicável, implemente medidas preventivas.
Etapa 6. Documentar Descobertas, Ações e Resultados	•Na etapa final do processo de solução de problemas, documente as descobertas, as ações e os resultados. •Essa documentação será muito importante para referência futura.

Resolver ou Escalonar?

- Em algumas situações, talvez não seja possível resolver o problema imediatamente. Um problema deve ser escalado quando requer uma decisão do gerente, algum conhecimento específico ou nível de acesso à rede indisponível para o técnico de solução de problemas.
- Uma política da empresa deve indicar claramente quando e como um técnico deve escalar um problema.

O Comando debug

- O comando IOS **debug** permite ao administrador exibir mensagens de processo, protocolo, mecanismo e evento do SO em tempo real para análise.
- Todos os comandos de **debug** são inseridos no modo EXEC privilegiado. O Cisco IOS permite restringir a saída de **debug** para incluir somente o recurso ou sub-recurso relevante. Use comandos de **debug** apenas para solucionar problemas específicos.
  - Para listar uma breve descrição das opções do comando de debug, use o comando **debug?** no modo EXEC privilegiado na linha de comando.
  - Para desativar um determinado recurso de depuração, adicione a palavra-chave **na** frente do comando de **debug**:
  - Outra opção é inserir o formulário **undebug** do comando no modo EXEC privilegiado:
  - Para desativar de uma vez todos os comandos de debug, use o comando **undebug all**:
- Seja cauteloso ao usar alguns comandos de **debug**, pois eles podem gerar uma quantidade substancial de saída e usar uma grande parte dos recursos do sistema. O roteador pode ficar tão ocupado exibindo mensagens **debug** que não teria capacidade de processamento suficiente para executar suas funções de rede ou até ouvir comandos para desativar a depuração.

O Comando terminal monitor

- Para direcionar a exibição das mensagens de registro do sistema em um terminal (console virtual), use o comando **terminal monitor** no modo EXEC privilegiado. Para interromper o registro de mensagens em um terminal, use o comando EXEC privilegiado do **terminal no monitor**.

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
 Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

```
R1#  terminal monitor
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

17.7 – Cenários de Solução de Problemas

Operação Duplex e Problemas de Incompatibilidade

- As interfaces Ethernet de interconexão devem operar no mesmo modo duplex para obter melhor desempenho de comunicação e evitar ineficiência e latência no link.
- O recurso de negociação automática Ethernet facilita a configuração, minimiza problemas e maximiza o desempenho do link entre dois links Ethernet interconectados. Primeiramente, os dispositivos conectados anunciam seus recursos de compatibilidade e, depois, escolhem o modo de desempenho mais alto, compatível com as duas extremidades.
- Se um dos dois dispositivos conectados estiverem operando no modo full-duplex e o outro no modo half-duplex, ocorrerá uma incompatibilidade de duplex. Já que a comunicação de dados ocorre por meio de um link físico, no caso de uma incompatibilidade de duplex o desempenho do link físico seria muito ruim.
- As incompatibilidades duplex são normalmente causadas por uma interface mal configurada ou, em casos raros, por uma negociação automática com falha. As incompatibilidades de duplex podem ser difíceis de resolver, visto que a comunicação entre os dispositivos continua ocorrendo.

Problemas de Endereçamento IP em Dispositivos IOS

- Duas causas comuns de atribuição de IPv4 incorreta são os erros de atribuição manual ou problemas relacionados a DHCP.
- Os administradores de rede normalmente precisam atribuir de forma manual os endereços IP aos dispositivos, como servidores e roteadores. Se for cometido um erro durante a atribuição, provavelmente ocorrerão problemas de comunicação com o dispositivo.
- Em um dispositivo IOS, use os comandos **show ip interface** ou **show ip interface brief** para verificar quais endereços IPv4 foram atribuídos às interfaces de rede. Por exemplo, emitir o comando **show ip interfacebrief** conforme mostrado validaria o status da interface em R1.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

Problemas de Endereçamento IP em Dispositivos Finais

- Em máquinas com Windows, quando o dispositivo não consegue entrar em contato com um servidor DHCP, o Windows atribui automaticamente um endereço que pertence ao intervalo 169.254.0.0/16. Esse recurso é chamado de endereçamento IP privado automático (APIPA).
- Freqüentemente, um computador com um endereço APIPA não poderá se comunicar com outros dispositivos na rede, porque esses dispositivos provavelmente não pertencerão à rede 169.254.0.0/16.
  - **Nota**: Outros sistemas operacionais, como Linux e OS X, não usam APIPA.
- Se o dispositivo não puder se comunicar com o servidor DHCP, o servidor não conseguirá atribuir um endereço IPv4 para a rede específica e o dispositivo não será capaz de se comunicar.
- Para verificar os endereços IP atribuídos a um computador com Windows, use o comando **ipconfig**.

Problemas de Gateway Padrão

- O gateway padrão para um dispositivo final é o dispositivo de rede mais próximo, pertencente à mesma rede que o dispositivo final, que pode encaminhar tráfego para outras redes. Se um dispositivo tiver um endereço de gateway padrão errado ou inexistente, ele não conseguirá se comunicar com os dispositivos em redes remotas.
- Semelhantes aos problemas de endereçamento IPv4, os problemas de gateway padrão podem estar relacionados à configuração errada (no caso de atribuição manual) ou a problemas de DHCP (se a atribuição manual estiver em uso).
- Para verificar o gateway padrão em computadores baseados no Windows, use o comando **ipconfig**.
- Em um roteador, use o comando **show ip route** para listar a tabela de roteamento e verificar se o gateway padrão, conhecido como uma rota padrão, foi definido. Essa rota é usada quando o endereço de destino do pacote não corresponde a nenhuma outra rota na tabela de roteamento.

Resolução de Problemas de DNS.

- É comum que os usuários relacionem por engano a operação de um link da Internet com a disponibilidade do DNS.
- Os endereços do servidor DNS podem ser atribuídos manualmente ou automaticamente via DHCP.
- Embora seja comum para as empresas gerenciarem seus próprios servidores DNS, qualquer servidor DNS alcançável pode ser usado para resolver nomes.
- A Cisco oferece OpenDNS que fornece serviço DNS seguro filtrando phishing e alguns sites de malware. Os endereços OpenDNS são 208.67.222.222 e 208.67.220.220. Recursos avançados, como filtragem de conteúdo da Web e segurança, estão disponíveis para famílias e empresas.
- Use o **ipconfig /all** como mostrado para verificar qual servidor DNS está sendo usado pelo computador Windows.
- O comando **nslookup** é outra ferramenta útil para solucionar problemas de DNS em PCs. Com o **nslookup**, um usuário pode fazer manualmente consultas de DNS e analisar a resposta de DNS.

Packet Tracer – Solucione Problemas de Conectividade

O objetivo desta atividade do Packet Tracer é solucionar problemas de conectividade, se possível. Caso contrário, os problemas deverão ser documentados de forma clara para que possam ser encaminhados.

Packet Tracer – Solucione Problemas de Conectividade– Modo Físico
Laboratório - Solucione Problemas de Conectividade

Nesta atividade do modo físico do Packet Tracer e no laboratório, você completará os seguintes objetivos:

- Identificar o problema
- Implementar alterações de rede
- Verificar a funcionalidade completa
- Documentar descobertas e alterações de configuração

17.8 - Módulo Prática e Quiz

Packet Tracer – Projeto e Desenvolvimento de uma Pequena Rede de Negócios – Modo Físico

Laboratório – Projeto e Desenvolvimento de uma Pequena Rede de Negócios

Nesta atividade do modo físico do Packet Tracer e no laboratório, você completará os seguintes objetivos:

- Projeto e Desenvolvimento de uma Rede
- Explicar como é criada uma pequena rede de segmentos diretamente conectados, configurados e verificados

Packet Tracer - Desafio de integração de habilidades

Nesta atividade de Tracer de Pacotes, você usará todas as habilidades adquiridas ao longo deste curso.

Cenário:

Os roteadores Central, do cluster do ISP e o servidor Web estão completamente configurados. Você deve criar um novo esquema de endereçamento IPv4 que acomode 4 sub-redes usando a rede 192.168.0.0/24. O maior departamento de TI precisa de 25 hosts. O maior departamento de vendas (Sales) precisa de 50 hosts. A sub-rede para o restante da equipe (staff) precisa de 100 hosts. Uma sub-rede para convidados (guest) será futuramente adicionada para acomodar 25 hosts. Você também deve concluir as configurações básicas de segurança e as configurações de interface no R1. Em seguida, você definirá a interface SVI e as configurações básicas de segurança nos comutadores S1, S2 e S3.

Packet Tracer – Desafio de Solução de Problemas

Nesta atividade de rastreador de pacotes, você solucionará e resolverá vários problemas em uma LAN existente.

O Que eu Aprendi Neste Módulo?

- Os fatores a serem considerados ao selecionar dispositivos de rede para uma rede pequena são custo, velocidade e tipos de portas/interfaces, capacidade de expansão e recursos e serviços do SO.
- Ao implementar uma rede, crie um esquema de endereçamento IP e use-o em dispositivos finais, servidores e periféricos e dispositivos intermediários.
- A redundância pode ser conseguida instalando equipamentos duplicados, mas também pode ser fornecida fornecendo links de rede duplicados para áreas críticas.
- Os roteadores e comutadores em uma rede pequena devem ser configurados para rastrear o tráfego em tempo real, como voz e vídeo, de maneira possível em relação a outro tráfego de dados.
- Há duas formas de programas de software ou processos que fornecem acesso à rede: aplicações de rede e serviços da camada de aplicação.
- Para dimensionar uma rede, vários elementos são necessários: documentação de rede, inventário de dispositivos, orçamento e análise de tráfego.
- O comando ping é a maneira mais eficaz de testar rapidamente a conectividade da Camada 3 entre um endereço IP de origem e de destino.
- O Cisco IOS oferece um modo “estendido” do comando ping que permite ao usuário criar tipos especiais de pings ajustando parâmetros relacionados à operação do comando.

O Que eu Aprendi Neste Módulo (Cont.)?

- O comando trace retorna uma lista dos saltos no roteamento de um pacote pela rede.
- Há também um comando traceroute estendido. Ele permite que o administrador ajuste parâmetros relacionados à operação de comando.
- Os administradores de rede exibem as informações de endereçamento IP (endereço, máscara, roteador e DNS) em um host Windows emitindo o comando ipconfig. Outros comandos necessários são **ipconfig /all**, **ipconfig /release**e **ipconfig /renew**e **ipconfig /displaydns**.
- A verificação das configurações de IP usando a GUI em uma máquina Linux será diferente dependendo da distribuição Linux (distro) e da interface de desktop. Os comandos necessários são ifconfig e ip address.
- Na GUI de um host Mac, abra Preferências de Rede > Avançadas para obter as informações de endereçamento IP. Outros comandos de endereçamento IP para Mac são ifconfig e networksetup -listallnetworkservices e networksetup -getinfo <network service>.
- O comando **arp** é executado a partir do prompt de comando do Windows, Linux ou Mac. O comando lista todos os dispositivos atualmente no cache ARP do host, que inclui o endereço IPv4, endereço físico e o tipo de endereçamento (estático / dinâmico) para cada dispositivo.
- O comando **arp -a** exibe o endereço IP conhecido e a vinculação de endereço MAC.

O Que eu Aprendi Neste Módulo? (Cont.)?

- Os comandos show comuns são **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**e **show version**. O comando **show cdp neighbor** fornece as seguintes informações sobre cada dispositivo vizinho do CDP: identificadores, lista de endereços, identificador de porta, lista de recursos e plataforma.
- O comando **show cdp neighbors detail** ajudará a determinar se um dos vizinhos CDP apresenta um erro de configuração IP.
- A saída de **show ip interface brief** exibe todas as interfaces no roteador, o endereço IP atribuído a cada interface, se houver, e o status operacional da interface.
- As seis etapas básicas para a solução de problemas da Etapa 1. Identificar o problema 2. Estabeleça uma teoria das causas prováveis. Etapa 3. Teste da teoria para determinar a causa. Etapa 4. Estabeleça um plano de ação e implemente a solução. Etapa 5. Verificar a solução e implementar medidas preventivas. Etapa 6. Documentar as descobertas, as ações e os resultados.
- Um problema deve ser escalado quando requerer a decisão de um gerente, algum conhecimento específico ou nível de acesso à rede indisponível para o técnico de solução de problemas.
- Os processos, protocolos, mecanismos e eventos do IOS geram mensagens para comunicar seus status. O comando de debug do IOS permite que o administrador exiba essas mensagens em tempo real para análise.
- Para direcionar a exibição das mensagens de registro do sistema em um terminal (console virtual), use o comando terminal monitor no modo EXEC privilegiado.

Novos Termos e Comandos

- Aplicações de rede
- serviços da camada de aplicação
- Ping Estendido
- Traceroute estendido
- linha de base de rede
- **ifconfig**
- **netsh interface ip delete arpcache**
- método científico
- **depurar**
- **terminal monitor**


CISCO