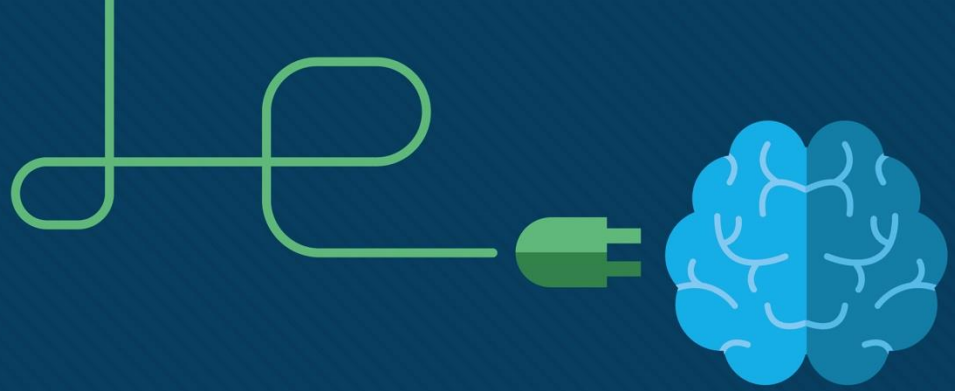


Módulo 17: Construa uma rede pequena

Versão original: Cisco Network Academy
Versão modificada: Eduardo Costa

Introdução às redes v7.0 (ITN)

Objetivos do módulo

Título do módulo: Construir uma rede pequena

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

Título do Tópico	Objetivo do Tópico
Dispositivos numa rede pequena	Identificar os dispositivos usados numa rede pequena.
Aplicações e protocolos de redes pequenas	Identificar os protocolos e aplicações usadas numa 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 relativo da rede.
Comandos de host e IOS	Usar comandos nos hosts e no IOS para adquirir informações sobre os dispositivos numa rede.
Metodologias de resolução de problemas	Descrever as metodologias comuns de resolução de problemas de rede.
Cenários de resolução de problemas	Resolver problemas com dispositivos na rede.

17.1 – Dispositivos numa rede pequena

Topologias de redes pequenas

- A maioria das empresas são pequenas. A maioria das redes das empresas também são pequenas.
- Um projeto de uma rede pequena é geralmente simples.
- Redes pequenas geralmente têm uma única ligação à WAN fornecida por DSL, cabo ou ligação Ethernet.
- Redes grandes requerem um departamento de TI para manter, proteger e resolver problemas de dispositivos de rede e proteger dados organizacionais. Redes pequenas são geridas por um técnico de TI local ou por um profissional contratado.

Seleção de dispositivos para uma rede pequena

Tal como as redes grandes, as redes pequenas também requerem planeamento e projeto para atender aos requisitos dos utilizadores. O planeamento garante que todos os requisitos, fatores de custo e opções de implantação sejam devidamente considerados. Uma das primeiras considerações de projeto é o tipo de dispositivos intermediários a serem usados para oferecer suporte à rede.

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 operativo

Endereçamento IP para 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 incluídos no esquema de endereçamento IP são os seguintes:

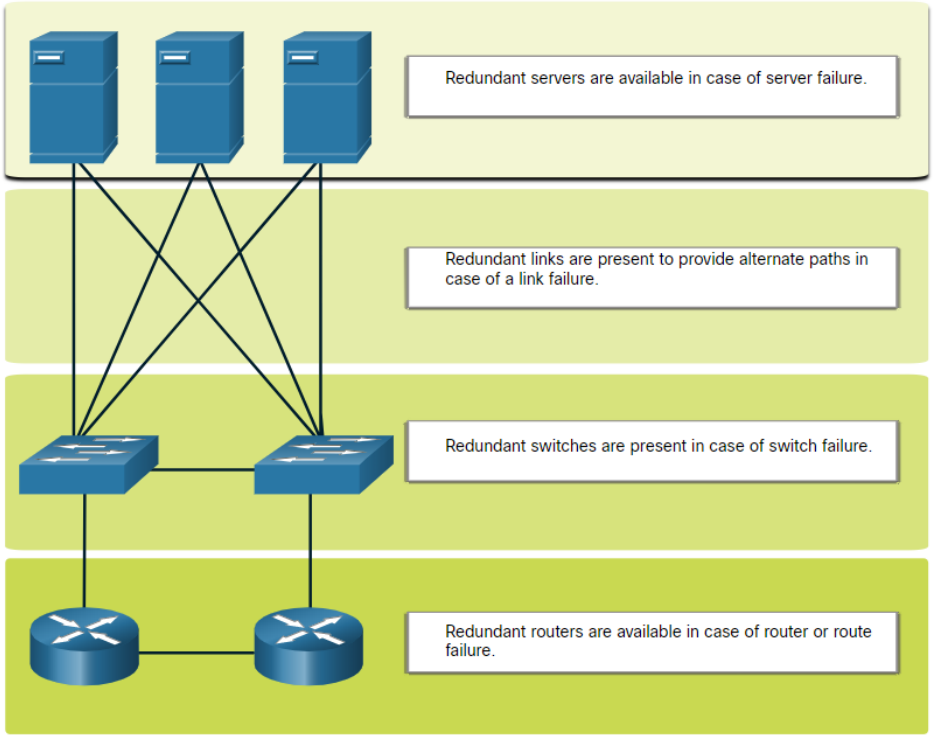
- Dispositivos do utilizador final - O número e o tipo de conexões (ou seja, com cabo, sem fios, acesso remoto)
- Servidores e dispositivos periféricos (por exemplo, impressoras e cameras de segurança)
- Dispositivos intermediários, incluindo switches e pontos de acesso

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

Redundância numa rede pequena

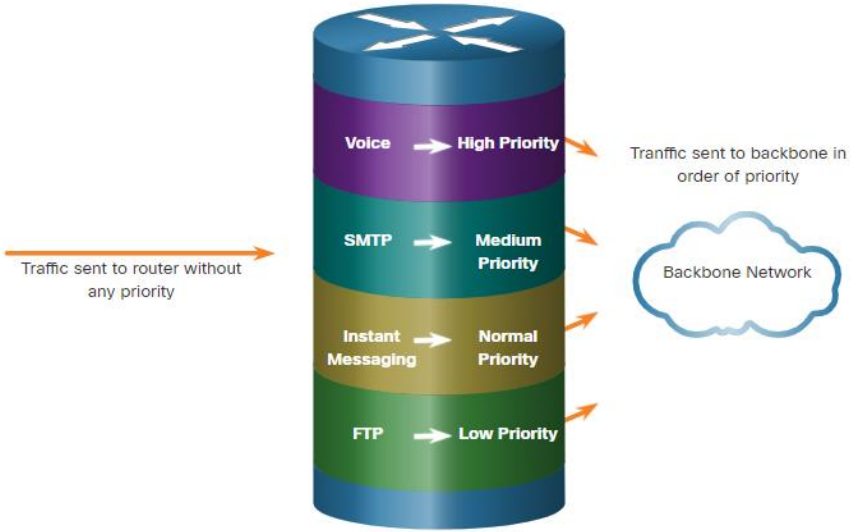
Para manter um alto grau de fiabilidade, é necessário *redundância* no projeto da rede. A redundância ajuda a eliminar os pontos únicos de falha.

A redundância pode ser conseguida instalando equipamentos duplicados. Também pode ser conseguida fornecendo ligações de rede duplicadas nas áreas críticas.



Gestão de Tráfego

- O objetivo de um bom projeto de rede é aumentar a produtividade dos funcionários e minimizar o tempo de inatividade da rede.
- Os routers e switches numa rede pequena devem ser configurados para suportar tráfego em tempo real, como voz e vídeo, de modo adequado relativamente ao tráfego de dados. Um bom projeto de rede implementará a qualidade de serviço (QoS).
- O enfileiramento por prioridade tem quatro filas com diferentes prioridades. A fila de alta prioridade é sempre esvaziada primeiro.



17.2 – Aplicações e protocolos de redes pequenas

Aplicações Comuns

Depois de configurada, a rede ainda precisa de certos tipos de aplicações e protocolos para funcionar. A rede é tão útil quanto as aplicações que estão nela.

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

- **Aplicações de rede**: aplicações que implementam protocolos da camada de aplicação e podem comunicar diretamente com as camadas inferiores da pilha protocolar.
- **Serviços da camada de aplicação**: são programas que fazem interface com a rede e preparam os dados para transferência, e são usados pelas aplicações que precisam de assistência para usar os recursos da rede.

Protocolos Comuns

Os protocolos de rede oferecem suporte às aplicações e serviços usados pelos funcionários numa rede pequena.

- Os administradores de rede geralmente necessitam de aceder a dispositivos e servidores de rede. As duas soluções de acesso remoto mais comuns são Telnet e Secure Shell (SSH).
- O 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 os emails.
- File Transfer Protocol (FTP) e Security File Transfer Protocol (SFTP) são usados para descarregar e carregar ficheiros 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 constituem um conjunto de ferramentas fundamentais de um profissional de rede, definindo:

- Processos em qualquer 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 em dia, as empresas estão usando cada vez mais a voz sobre IP e streaming de multimédia para comunicar com clientes e parceiros de negócios, além de permitir que os seus funcionários trabalhem remotamente.
- O administrador de redes deve garantir que o equipamento adequado foi instalado na rede e que os dispositivos de rede estejam configurados para garantir entrega com diferentes prioridades.
- Fatores que um administrador de rede deve considerar ao oferecer suporte a aplicações em tempo real:
  - **A Infraestrutura -** tem capacidade e recursos para suportar aplicações em tempo real?
  - **VoIP -** VoIP geralmente é mais barato do que a telefonia IP, mas à custa da qualidade e das características.
  - **Telefonia IP –** Utiliza servidores dedicados para controlo de chamadas e sinalização.
  - **Aplicações em Tempo Real -**A rede deve suportar mecanismos de Qualidade de Serviço (QoS) para minimizar problemas de latência. O protocolo de transporte em tempo real (RTP) e o protocolo de controlo de transporte em tempo real (RTCP) são dois protocolos que oferecem suporte a aplicações em tempo real.

17.3 – Escalar para redes maiores

Crescimento das redes pequenas

O crescimento é um processo natural para muitas empresas pequenas e suas redes devem acompanhar esse crescimento. Idealmente, o administrador de rede deve ter tempo de execução suficiente para tomar decisões inteligentes sobre o crescimento da rede alinhado com o crescimento da empresa.

Para dimensionar 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 –** Devem ser documentados os protocolos, aplicações e serviços e os respectivos requisitos de tráfego

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

Análise de Protocolo

É importante entender o tipo de tráfego que usa rede, bem como o fluxo de tráfego atual. Existem várias ferramentas de gestão 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.
- Executar 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 o tipo de tráfego que é enviado.
- Essa análise pode ser usada para tomar decisões sobre como gerir o tráfego eficientemente.

Utilização da rede pelos funcionários

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

- SO e versão do SO
- Utilização da CPU
- Utilização da RAM
- Utilização das Drives
- Aplicações que não são de rede
- Aplicações de rede

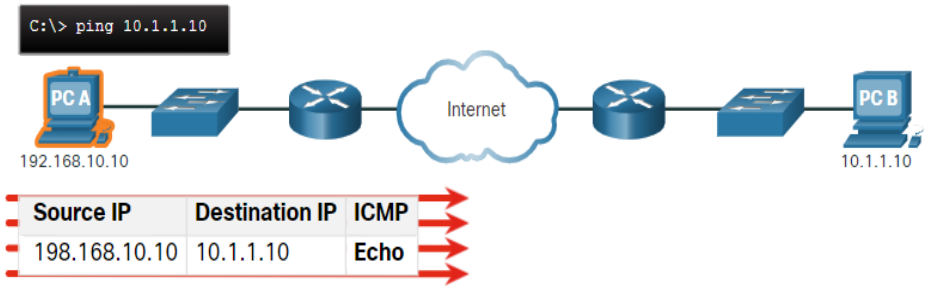
Documentar snapshots para funcionários numa rede pequena por um período de tempo é muito útil para identificar requisitos na evolução de protocolo e fluxos de tráfego associados.

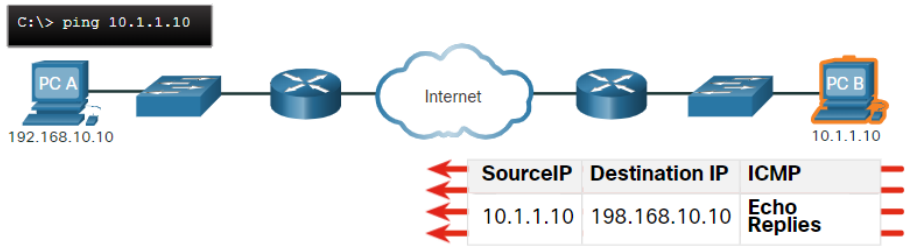
17.4 - Verificar a conectividade.

Verificar conectividade com Ping

Quer a rede ser pequena e nova, ou uma rede existente esteja a ser redimensionada, é sempre desejado ser capaz de verificar se os componentes estão corretamente conectados entre si e à internet.

- O comando ping, está disponível na maioria dos sistemas operativos, e 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 de pedido de eco (ICMP Type 8 – echo request) e de resposta de eco (ICMP Type 0 - echo reply) do protocolo ICMP.





Verificar conectividade com Ping (Cont.)

Nm host Windows 10, o comando ping envia quatro mensagens de pedido eco ICMP consecutivas e espera quatro respostas de eco ICMP consecutivas do destino. O ping no IOS envia cinco mensagens de pedido de eco ICMP e apresenta um indicador para cada resposta de eco ICMP recebida.

Os indicadores de ping do IOS são os seguintes:

Elemento	Descrição
!	•O ponto de exclamação indica a receção bem-sucedids de uma mensagem de resposta de eco. •Valida uma conexão de Camada 3 entre origem e destino.
.	•Um ponto significa que o tempo expirou esperando por uma mensagem de resposta de eco. •Isso indica que ocorreu um problema de conectividade em algum lugar ao longo do caminho.
U	•O "**U**" indica que um router no caminho respondeu com uma mensagem ICMP de destino inalcançável. •Os motivos possíveis incluem o router não saber a direção da rede de destino ou não conseguiu localizar o host na rede de destino.

Nota: Outras respostas possíveis de ping incluem Q, M,? , ou &. No entanto, o significado delas está fora do âmbito deste módulo.

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, são apresentados várias prompts para personalizar o **ping**.

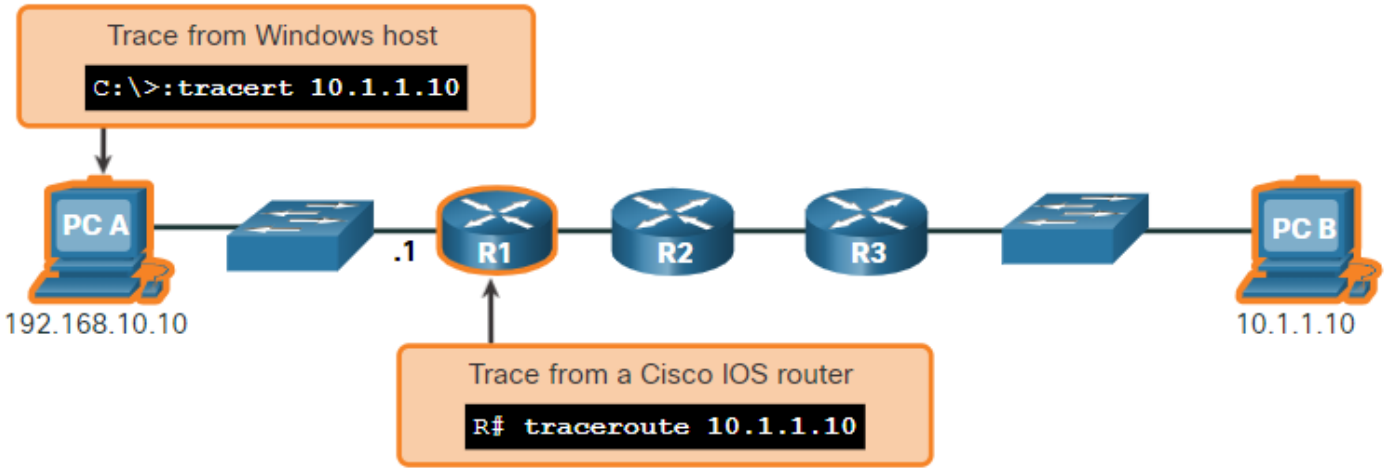
Nota: Pressionar "**Enter**" aceita os valores por omissão indicados. O comando **ping ipv6** é usado para pings estendidos em IPv6.

```
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 o Traceroute

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

- O Traceroute pode ajudar a localizar áreas problemáticas da Camada 3 numa rede. O comando trace retorna uma lista de saltos à medida que um pacote é encaminhado pela rede.
- A sintaxe do comando trace varia entre os sistemas operativos.



Verificar conectividade com o Traceroute (Cont.)

- A figura apresenta a saída de exemplo do comando **tracert** num host Windows 10.

  Nota: Usar **Ctrl-C** interrompe um **tracert** no Windows.

- A única resposta bem-sucedida foi do gateway R1. As solicitações de rastreamento para o próximo salto expiraram conforme indicado pelo asterisco (*), significando que o router de próximo 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 o Traceroute (Cont.)

As figuras seguintes apresentam as saídas do comando traceroute no 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  *
```

- Na figura à esquerda, o rastreamento validou que pode chegar ao PC B.
- Na figura à direita, o host 10.1.1.10 não estava disponível e a saída mostra asteriscos onde as respostas expiraram. Timeouts indicam um potencial problema de rede.
- Usar **Ctrl-Shift-6** interrompe 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

Tal como existe o comando **ping** estendido, há também existe um comando **traceroute** estendido. Permite que o administrador ajuste parâmetros relacionados ao funcionamento do comando.

O comando **tracert** do Windows permite a entrada de vários parâmetros através de opções na linha de comando. No entanto, ele não é guiado como o comando estendido traceroute no 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>
```

Traceroute Estendido (Cont.)

- A opção **traceroute** estendido no Cisco IOS permite que o utilizador crie um tipo especial de rastreamento ajustado aos parâmetros relacionados com o funcionamento do comando.
- O **traceroute** estendido é inserido no modo EXEC privilegiado digitando **traceroute** sem um endereço IP de destino. O IOS guia o utilizador pelas opções do comando apresentando uma série de prompts relacionados com a configuração dos vários parâmetros.

- **Nota**: Ao pressionar **Enter**, você aceita os valores por omissão 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 da rede (Baseline)

- Uma das ferramentas mais eficazes para o monitorizar e solucionar 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 da execução de um ping, traceroute, ou outros comandos relevantes num ficheiro de texto. Esses ficheiros de texto podem ficar marcados com a data em que foram registados e guardados num ficheiro para recuperação e comparação posterior.
- Entre os itens a serem considerados estão as mensagens de erro e os tempos de resposta de host para host.
- As redes empresariais devem ter linhas de base extensivas, mais extensivas do que o descrito neste curso. Ferramentas de software a nível profissional estão disponíveis para armazenar e manter das informações de linha de base.

17.5 – Comandos de Host e IOS

Configuração de IP em um Host do Windows

No Windows 10, pode aceder-se aos detalhes do endereço IP no **Centro de Rede e Partilha** para visualizar rapidamente as quatro configurações importantes: endereço, máscara, router e DNS. Alternativamente pode ser usado o comando **ipconfig** na linha de comando de um computador Windows.

- O comando **ipconfig /all** permite visualizar o endereço MAC, bem como vários detalhes sobre o endereçamento da camada 3 do dispositivo.
- Se um host for 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 PCs com Windows também otimiza o desempenho da resolução de nomes DNS ao armazenar nomes previamente resolvidos na memória. O comando **ipconfig /displaydns** exibe todas as entradas DNS em cache num 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 num Host Linux

- A verificação das configurações de IP usando a GUI numa máquina Linux será diferente dependendo da distribuição Linux e da interface da área de trabalho.
- Na linha de comando, use o comando **ifconfig** para exibir o estado das interfaces atualmente ativas e sua configuração IP.
- O comando Linux **ip address** é usado para exibir endereços e suas propriedades. 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
```

Nota: A saída apresentada pode variar dependendo da distribuição Linux.

Configuração IP num Host de MacOS

- Na GUI de um host Mac, abrir **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 da prompt de comando do Windows, Linux ou Mac. O comando lista todos os dispositivos atualmente na cache ARP do host.

- O comando **arp -a** exibe o endereço IP conhecido e o endereço MAC associado. A cache do ARP exibe apenas informações de dispositivos que foram acedidos recentemente.
- Para garantir que a cache ARP seja preenchida, execute um **ping** para um dispositivo para que ele tenha uma entrada na tabela ARP.
- A cache pode ser limpa usando o comando **netsh interface ip delete arpcache** no caso em que o administrador da rede desejar preencher novamente a cache com informações atualizadas.

Nota: Poderá ser preciso ter acesso de administrador no host para poder usar o comando **netsh interface ip delete arpcache**.

Comandos **show** comuns revisitados

Comando	Descrição
show running-config	Mostra a configuração e as definições atuais
show interfaces	Mostra o estado da interface e exibe mensagens de erro
show ip interface	Mostra a informação da camada 3 de uma interface
show arp	Mostra a lista de hosts conhecidos nas LANs Ethernet locais
show ip route	Mostra as informações de encaminhamento da camada 3
show protocols	Mostra que protocolos estão em funcionamento
show version	Mostra a memória, as interfaces e licenças do dispositivo

O comando show cdp neighbors

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

- **Identificadores dos dispositivos** - O nome do host configurado de um switch, router ou outro dispositivo
- **Lista de endereços** - pelo menos um endereço de camada de rede para cada protocolo suportado
- **Identificador de porta** - O nome da 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** - A plataforma de hardware do dispo**sitivo**

O comando **show cdp neighbors detail** mostra o endereço IP de um 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**. Este comando fornece uma saída mais abreviada do que o comando **show ip interface**. Ele fornece um resumo das principais informações para todas as interfaces de rede num router.

```
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
```

17.6 – Metodologias de resolução de problemas

Abordagens Básicas de Resolução de Problemas

Etapa	Descrição
Etapa 1. Identificar o Problema	•Esta é a primeira etapa no processo de resolução de problemas. •Embora possam ser usadas ferramentas nesta etapa, uma conversa com o utilizador geralmente é muito útil.
Etapa 2. Estabelecer uma teoria das causas prováveis	•Depois de identificado o problema, tente estabelecer uma teoria das causas prováveis. •Esta etapa geralmente produz mais do que uma causa provável para o problema.
Etapa 3. Testar a Teoria para determinar a causa	•Com base nas causas prováveis, testar as 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. Verificar a solução e implementar medidas preventivas	•Depois de corrigir o problema, verifique a funcionalidade total. •Se aplicável, implemente medidas preventivas.
Etapa 6. Documentar descobertas, ações e resultados	•Na etapa final do processo de resolução de problemas, documente as descobertas, as ações e os resultados. •Essa documentação será muito importante para referência futura.

Resolver ou escalar?

- Em algumas situações, pode não ser possível resolver o problema imediatamente. O problema deve ser escalado quando requer uma decisão do gestor, algum conhecimento específico ou nível de acesso à rede indisponível para o técnico de resolução de problemas.
- A política da empresa deve estabelecer claramente quando e como um técnico deve escalar um problema.

O comando debug

- O comando IOS **debug** permite que o administrador visualizar mensagens de processos, protocolos, mecanismos e eventos 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 uma característica de depuração específica, adicione a palavra-chave **no** na frente do comando de **debug**:
  - Em alternativa, pode inserir-se a forma do comando **undebug** do comando no modo EXEC privilegiado:
  - Para desligar 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 router pode ficar muito ocupado exibindo mensagens **debug** que não terá capacidade de processamento suficiente para executar as suas funções de rede ou até ouvir comandos para desativar a depuração.

O comando terminal monitor

- **debug** e algumas outras mensagens de saída do IOS não são exibidas automaticamente em conexões remotas. Isso ocorre porque as mensagens de log são impedidas de serem exibidas nas linhas vty.
- Para exibir mensagens de log num terminal (consola virtual), use o comando **terminal monitor** no modo EXEC privilegiado. Para parar de registrar mensagens num terminal, use o comando **terminal no monitor** no modo EXEC privilegiado.

```
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 Resolução de Problemas

Funcionamento duplex e problemas de incompatibilidade

- A interligação de interfaces Ethernet devem funcionar no mesmo modo duplex para obter melhor desempenho de comunicação e evitar ineficiência e latência na ligação.
- As características de autonegociação nas interfaces Ethernet facilitam a configuração, minimizam problemas e maximizam o desempenho da ligação entre dois links Ethernet. Os dispositivos conectados primeiro anunciam as características suportadas e, em seguida, escolhem o modo de desempenho mais alto compatível com ambas as extremidades.
- Se um dos dois dispositivos conectados estiver a funcionar no modo full-duplex e o outro no modo half-duplex, ocorrerá uma incompatibilidade de duplex. Embora a comunicação de dados ocorra através de um link com incompatibilidade de duplex, o desempenho do link será muito mau.
- As incompatibilidades duplex são normalmente causadas por uma interface mal configurada ou, em casos raros, por uma falha na negociação automática. As incompatibilidades de duplex podem ser difíceis de resolver, pois a comunicação entre os dispositivos continua existindo.

Problemas de Endereçamento IP em Dispositivos IOS

- Duas causas comuns de atribuição de IPv4 incorreta são os erros de atribuição manual ou problemas relacionados com o DHCP.
- Os administradores de rede normalmente precisam atribuir endereços IP de forma manual a dispositivos, como servidores e routers. Se for cometido um erro durante a atribuição, provavelmente ocorrerão problemas de comunicação com o dispositivo.
- Num dispositivo IOS, use os comandos **show ip interface** ou **show ip interface brief** para verificar quais os endereços IPv4 atribuídos às interfaces de rede. Por exemplo, executar o comando **show ip interfacebrief** conforme mostrado validaria o estado das interfaces 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 em 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 - Automatic Private IP Addressing).
- Um computador com um endereço APIPA não será capaz de comunicar com outros dispositivos na rede, porque esses dispositivos provavelmente não pertencerão à rede 169.254.0.0/16.
- **Nota**: Outros sistemas operativos, 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 comunicar.
- Para verificar os endereços IP atribuídos a um computador com Windows, use o comando **ipconfig**.

Problemas de Gateway por Omissão

- O gateway por omissão 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 por omissão errado ou inexistente, ele não será capaz de comunicar com os dispositivos em redes remotas.
- Semelhantes aos problemas de endereçamento IPv4, os problemas de gateway por omissão podem estar relacionados com a configuração incorreta (no caso de atribuição manual) ou a problemas de DHCP (se a atribuição automática estiver em uso).
- Para verificar o gateway por omissão em computadores baseados no Windows, use o comando **ipconfig**.
- Num router, use o comando **show ip route** para listar a tabela de encaminhamento e verificar se o gateway por omissão, conhecido como uma rota por omissão, foi definida. Esta rota é usada quando o endereço de destino do pacote não corresponde a nenhuma outra rota na tabela de encaminhamento.

Resolução de Problemas de DNS.

- É comum que os utilizadores relacionem erradamente 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 gerirem os 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** para verificar qual o servidor DNS que está a ser usado pelo computador Windows.
- O comando **nslookup** é outra ferramenta útil para solucionar problemas de DNS em PCs. Com o **nslookup**, um utilizador pode fazer manualmente consultas de DNS e analisar a resposta de DNS.

17.8 - Sumário

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 conseguida fornecendo links de rede duplicados para áreas críticas.
- Os routers e switches numa 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 utilizador criar tipos especiais de pings ajustando parâmetros relacionados à operação do comando.

O Que eu Aprendi Neste Módulo (Cont.)?

- O comando traceroute retorna uma lista dos saltos no encaminhamento 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, router 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 numa 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** apresenta o endereço IP conhecido e a associação do 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 router, o endereço IP atribuído a cada interface, se houver, e o estado 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 o seu estado. O comando de debug do IOS permite que o administrador exiba essas mensagens em tempo real para análise.
- Para direcionar a apresentação das mensagens de registo do sistema para um terminal (console virtual), use o comando terminal monitor no modo EXEC privilegiado.