



# Módulo 7: Verificação de Conectividade



CyberOps Associate v1.0

Prof. Clemilson Oliveira

[clemilson.oliveira@edu.sc.senai.br](mailto:clemilson.oliveira@edu.sc.senai.br)



# Objetivos do módulo

**Título do Módulo:** Verificação de Conectividade

**Objetivo do módulo:** Usar ferramentas de verificação de conectividade ICMP

Título do Tópico	Objetivo do Tópico
ICMP	Explicar como o protocolo ICMP é usado para testar a conectividade da rede.
Utilitários Ping e Traceroute	Usar ferramentas do Windows, ping e traceroute para verificar a conectividade de rede.

# 7.1 ICMP

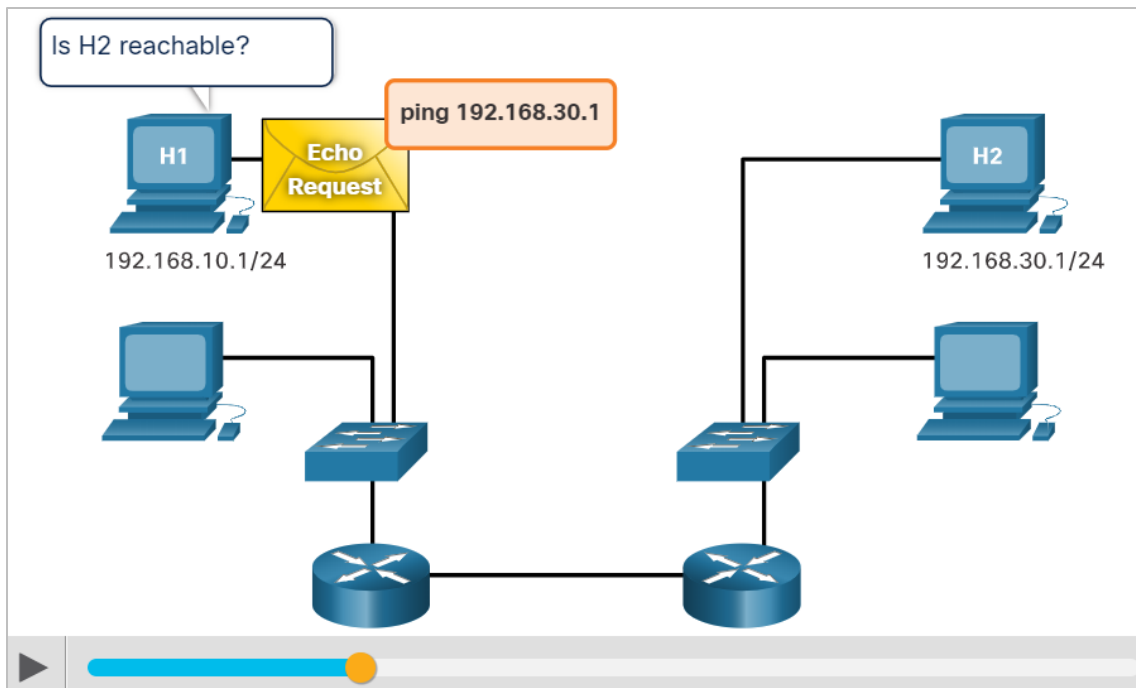
## Mensagens ICMPv4

- O conjunto TCP / IP fornece mensagens a serem enviadas no caso de certos erros. Essas mensagens são enviadas com os serviços do ICMP.
- O objetivo dessas mensagens é fornecer feedback sobre problemas relacionados ao processamento de pacotes IP sob certas condições.
- As mensagens ICMP não são necessárias e muitas vezes não são permitidas por questões de segurança.
- O ICMP está disponível tanto para IPv4 como para IPv6. ICMPv4 é o protocolo de mensagens para IPv4. O ICMPv6 fornece os mesmos serviços para IPv6, mas inclui funcionalidades adicionais.
- As mensagens ICMP comuns a ICMPv4 e ICMPv6 incluem confirmação de host, destino ou serviço inacessível, tempo excedido e redirecionamento de rota.

# Mensagens ICMPv4 (Cont.)

## Confirmação de host

- Uma mensagem de eco ICMP pode ser usada para determinar se um host está operacional.
- O host local envia uma solicitação de eco ICMP (ICMP Echo Request) para um host. Se o host estiver disponível, o host de destino enviará uma resposta de eco (Echo Reply).
- Esse uso das mensagens de eco ICMP é a base do utilitário ping.



## Mensagens ICMPv4 (Cont.)

### Destino ou Serviço Inalcançável

- Quando um host ou um gateway recebe um pacote que não pode entregar, ele pode usar uma mensagem ICMP de destino inalcançável para notificar à origem que o destino ou o serviço está inalcançável.
- A mensagem conterá um código que indica por que não foi possível entregar o pacote. Os códigos de destino inacessível para ICMPv4 incluem o seguinte:
  - **0** - Net unreachable (Rede inacessível)
  - **1** - Host unreachable (Host inacessível)
  - **2** - Protocol unreachable (Protocolo inacessível)
  - **3** - Port unreachable (Porta inacessível)

**Nota:** *ICMPv6 tem códigos ligeiramente diferentes para mensagens de destino inacessível.*

## Mensagens ICMPv4 (Cont.)

### **Tempo Excedido**

- Uma mensagem ICMPv4 de tempo excedido é usada por um roteador para indicar que um pacote não pode ser encaminhado porque o campo Vida Útil (TTL) do pacote foi reduzido a 0.
- Se um roteador recebe um pacote e o campo TTL do pacote IPv4 diminui para zero, ele descarta o pacote e envia uma mensagem de tempo excedido para o host de origem.
- O ICMPv6 também enviará uma mensagem de tempo excedido se o roteador não conseguir encaminhar um pacote IPv6 porque o pacote expirou.
- O IPv6 não tem um campo TTL. Ele usa o campo de limite de salto para determinar se o pacote expirou.

# Mensagens ICMPv6 RS e RA

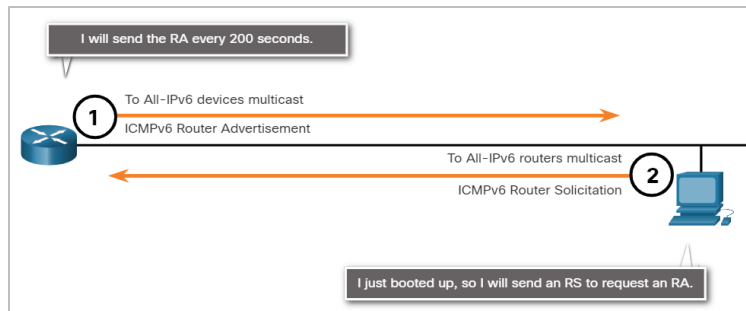
- ICMPv6 tem novos recursos e funcionalidades aprimoradas não encontradas no ICMPv4. As mensagens ICMPv6 são encapsuladas no IPv6.
- Ele tem quatro novos protocolos como parte do Neighbour Discovery Protocol (ND ou NDP).
- Mensagens entre um roteador IPv6 e um dispositivo IPv6:
  - Mensagem de Solicitação de Roteador (RS)
  - Mensagem de Anúncio de Roteador (RA)
- Mensagens entre dispositivos IPv6:
  - Mensagem de solicitação de vizinhos (NS)
  - Mensagem de anúncio de vizinhos (NA)



## Mensagens ICMPv6 RS e RA (Cont.)

### Solicitação de roteador: mensagens entre um roteador IPv6 e um dispositivo IPv6

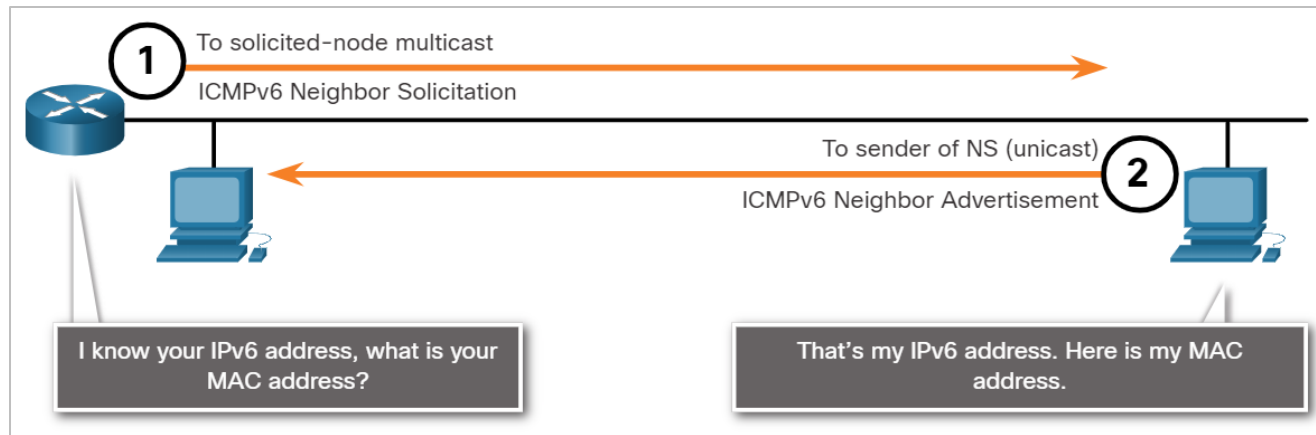
- As mensagens de RA são enviadas por roteadores para fornecer informações de endereçamento aos hosts usando Stateless Address Auto Configuration (SLAAC).
- Um roteador enviará uma mensagem de RA periodicamente ou em resposta a uma mensagem de RS. Um host que use SLAAC configurará o gateway padrão como o endereço de link local do roteador que enviou o RA.
- Quando um host é configurado para obter suas informações de endereçamento automaticamente usando SLAAC, o host enviará uma mensagem RS ao roteador solicitando uma mensagem RA.



## Mensagens ICMPv6 RS e RA (Cont.)

### Resolução de endereço: mensagens entre dispositivos IPv6

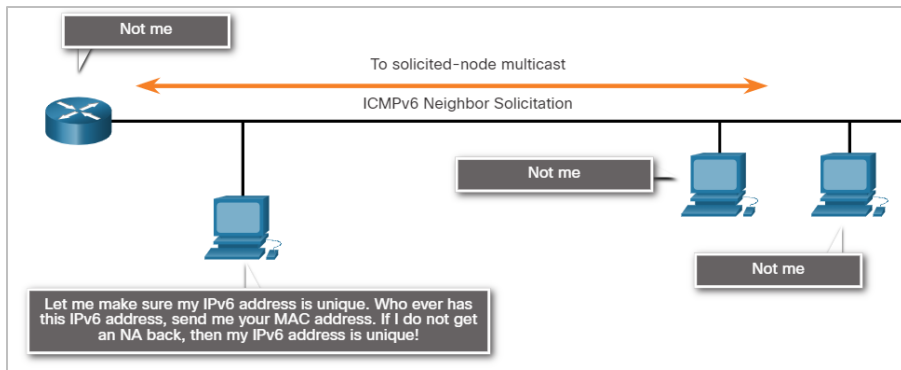
- As mensagens de NA são enviadas quando um dispositivo conhece o endereço IPv6 de um dispositivo, mas não conhece seu endereço MAC. Isso equivale a uma requisição ARP no IPv4.
- As mensagens NA são enviadas em resposta a uma mensagem NS e correspondem ao endereço IPv6 de destino no NS. A mensagem de NA inclui o endereço MAC Ethernet do dispositivo. Isso é equivalente a uma resposta ARP em IPv4.



## Mensagens ICMPv6 RS e RA (Cont.)

### Detecção de Endereço Duplicado (DAD)

- Quando um dispositivo é atribuído a um endereço unicast global ou unicast local de link, o DAD é executado no endereço para garantir que ele seja exclusivo.
- Para verificar a exclusividade de um endereço, o dispositivo enviará uma mensagem NS com seu próprio endereço IPv6.
- Se outro dispositivo na rede tiver esse endereço, ele responderá com uma mensagem NA que notificará o dispositivo de envio de que o endereço está em uso. Se uma mensagem de NA correspondente não for devolvida em um determinado período, o endereço unicast será único e aceitável para uso.



## 7.2 Utilitários Ping e Traceroute

## - Teste e Verificação de Rede com Comandos CLI do Windows

Este vídeo demonstrará o teste e verificação de rede com comandos CLI do Windows.



# Ping – Teste de Conectividade

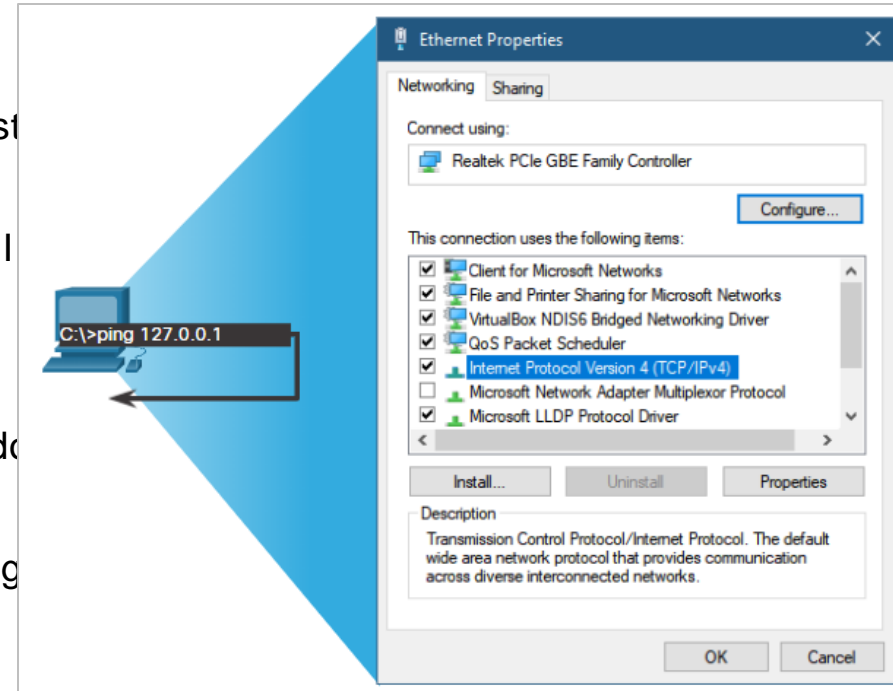
- O Ping é um utilitário de teste IPv4 e IPv6 que usa a solicitação de eco ICMP e as mensagens de resposta de eco para testar a conectividade entre hosts.
- Para testar a conectividade com outro host em uma rede, uma solicitação de eco é enviada ao endereço do host usando o comando **ping**. Se o host no endereço especificado receber a requisição de eco, ele enviará uma resposta de eco.
- À medida que cada resposta de eco é recebida, o **ping** fornece feedback sobre o tempo entre o envio da solicitação e o recebimento da resposta. Esta pode ser uma medida do desempenho da rede.
- O ping tem um valor de tempo limite para a resposta. Se a resposta não é recebida dentro do tempo de espera, o ping mostra uma mensagem informando que a resposta não foi recebida.

# Ping – Teste de Conectividade (Cont.)

- Depois que todas as solicitações são enviadas, o utilitário **ping** fornece um resumo que inclui a taxa de sucesso e o tempo médio de ida e volta até o destino.
- Os tipos de testes de conectividade realizados com **ping** incluem o seguinte:
  - Fazendo ping no loopback local
  - Fazendo ping no gateway padrão
  - Fazendo ping no host remoto

# Faça o ping do Loopback

- O ping pode ser usado para testar a configuração interna do IPv4 ou IPv6 no host local.
- Para realizar este teste, execute **ping** no endereço de loopback local de 127.0.0.1 para IPv4 (:::1 for IPv6).
- Uma resposta vinda de 127.0.0.1 para IPv4 (ou :::1 para IPv6) indica que o IP está instalado corretamente no host. Essa resposta vem da camada de rede.
- Essa resposta testa o IP através da camada de rede do I
- Uma mensagem de erro indica que o TCP/IP não está operacional no host.
- O ping no host local confirma que o TCP/IP está instalado e funcionando no host local.
- O ping 127.0.0.1 faz com que o dispositivo envie um ping para si mesmo.



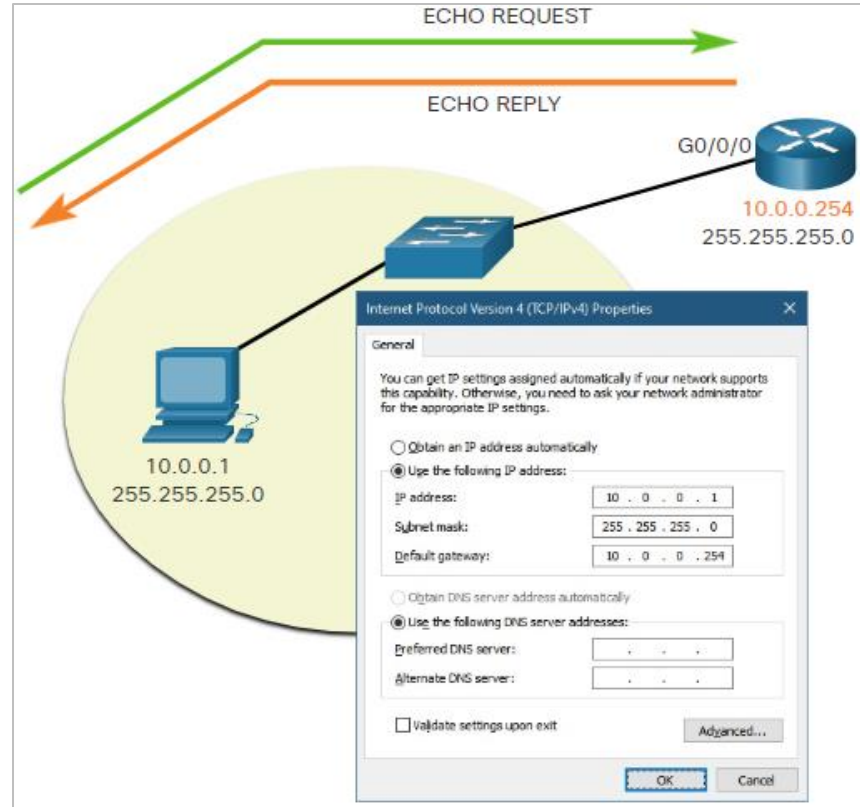


## Faça Ping no Gateway Padrão

- O **ping** pode ser usado para testar a capacidade de um host de se comunicar na rede local. Isso é feito executando o ping do endereço IP do gateway padrão do host.
- Um **ping** bem-sucedido no gateway padrão indica que o host e a interface do roteador que atua como gateway padrão estão operacionais na rede local.
- Para este teste, o endereço do gateway padrão é usado principalmente porque o roteador está sempre operacional. Se o endereço do gateway padrão não responder, um **ping** pode ser enviado ao endereço IP de outro host na rede local que está operacional.
- Se o gateway padrão ou outro host responder, o host local poderá se comunicar com êxito pela rede local.
- Se o gateway padrão não responder, mas outro host, isso pode indicar um problema com a interface do roteador servindo como gateway padrão.
- Uma possibilidade é que o endereço do gateway padrão incorreto tenha sido configurado no host ou a interface do roteador possa estar totalmente operacional, mas com segurança aplicada a ela.

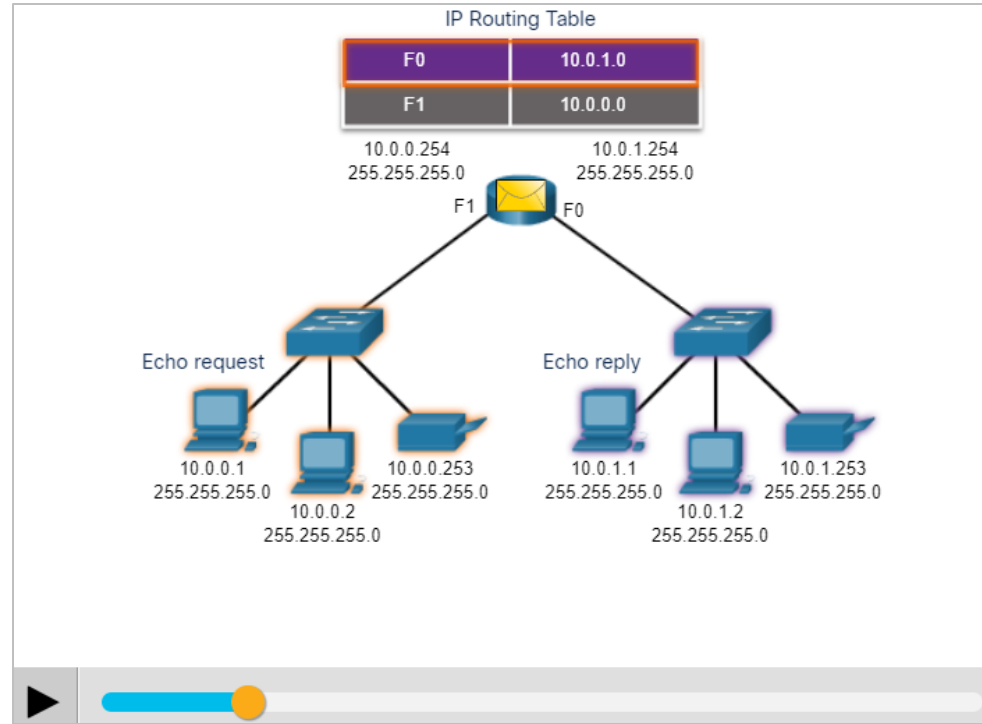
## Faça Ping no Gateway Padrão (Cont.)

O host envia um ping ao gateway padrão, enviando uma solicitação de eco ICMP. O gateway padrão envia uma resposta de eco confirmando a conectividade.



# Fazer Ping em um Host Remoto

- O ping também pode ser usado para testar a capacidade de um host local de se comunicar por uma rede interconectada. O host local pode executar ping em um host IPv4 operacional de uma rede remota.
- O roteador usa sua tabela de roteamento IP para encaminhar os pacotes.
- Se esse ping for bem-sucedido, a operação de uma grande parte da internet e a funcionalidade do host remoto podem ser verificadas.
- Um **ping** bem-sucedido na rede confirma a comunicação na rede local, a operação do roteador como o gateway padrão e a operação de todos os outros roteadores no caminho entre a rede local e a rede do host remoto.



# Traceroute - Teste o Caminho

- O ping é usado para testar a conectividade entre dois hosts, mas não fornece informações sobre detalhes de dispositivos entre os hosts.
- Traceroute (**tracert**) é um utilitário que gera uma lista de saltos que foram alcançados com sucesso ao longo do caminho. Essa lista pode dar informações importantes para a verificação e a solução de erros.
- Se os dados atingirem o destino, o rastreamento listará a interface de cada roteador no caminho entre os hosts.
- Caso ocorra falha nos dados em algum salto ao longo do caminho, o endereço do último roteador que respondeu ao rastreamento poderá fornecer uma indicação de onde está o problema ou das restrições de segurança que foram encontradas.

## Traceroute - Teste o Caminho (Cont.)

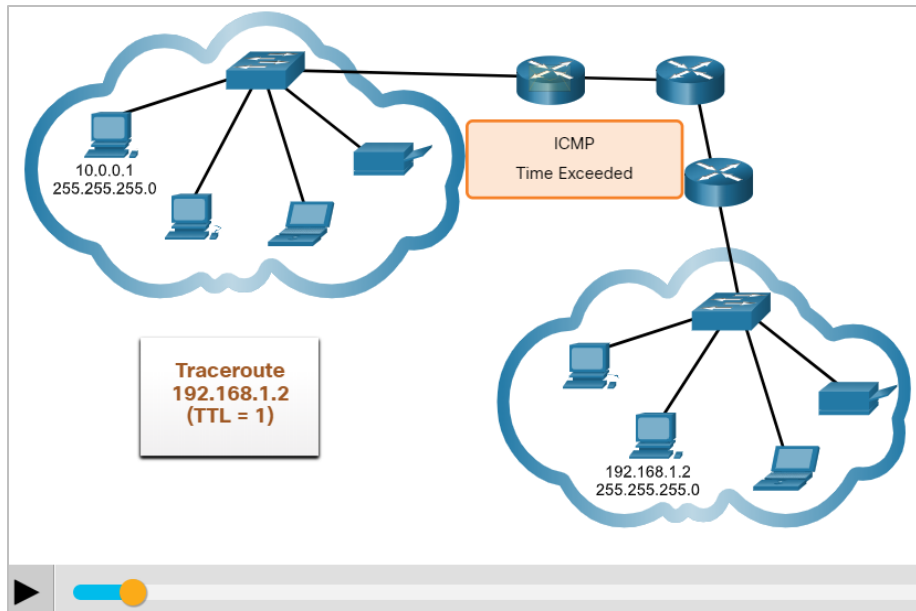
### Tempo de Ida e Volta (RTT)

- O traceroute fornece um tempo de ida e volta para cada salto ao longo do caminho e indica se um salto falha em responder.
- O tempo de ida e volta é o tempo que um pacote leva para alcançar o host remoto e retornar a resposta do host.
- Um asterisco (\*) é usado para indicar um pacote perdido ou não respondido.
- Essas informações podem ser usadas para localizar um roteador problemático no caminho ou podem indicar que o roteador está configurado para não responder.
- Se a tela mostrar tempos de resposta altos ou perdas de dados de um salto específico, isso é uma indicação de que os recursos do roteador ou de suas conexões podem ser usados em excesso.

# Traceroute - Teste o Caminho (Cont.)

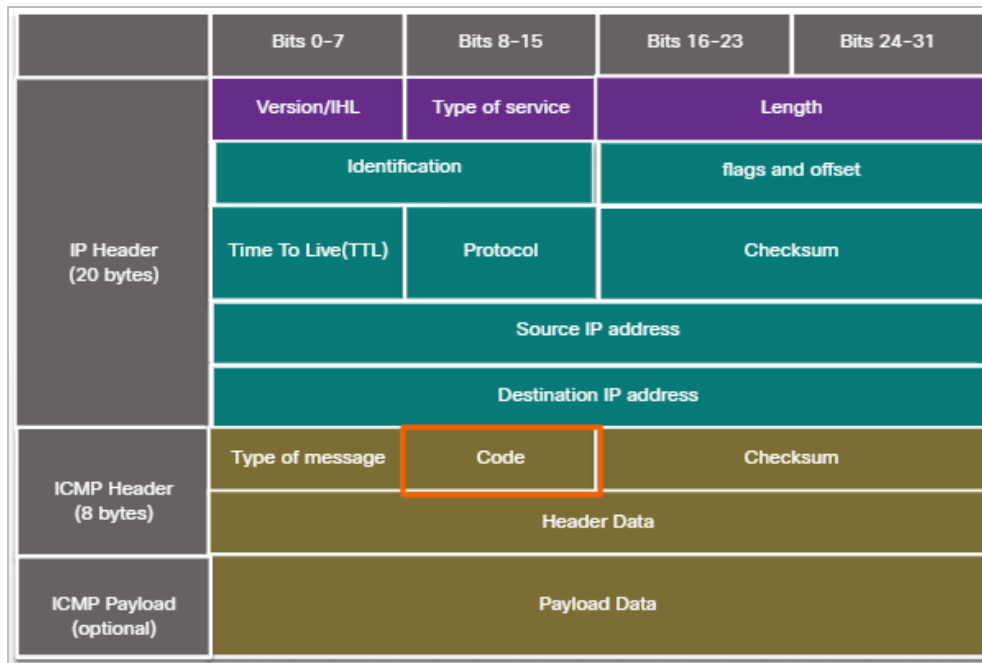
**Limite de salto IPv4 TTL e IPv6:** O Traceroute usa a função do campo TTL no IPv4 e o campo Hop Limit no IPv6 nos cabeçalhos da Camada 3, junto com a mensagem ICMP Time Exceeded.

- A primeira sequência de mensagens enviada do traceroute tem um valor de campo TTL de 1 que faz com que o TTL atinja o tempo limite do pacote IPv4 no primeiro roteador. Este roteador responde com uma mensagem ICMPv4 com tempo excedido. Agora o Traceroute tem o endereço do primeiro salto.
- O Traceroute aumenta progressivamente o campo TTL (2, 3, 4...) para cada sequência de mensagens. Isso fornece ao rastreamento o endereço de cada salto à medida que os pacotes expiram mais adiante no caminho. O campo TTL continua a aumentar até que o destino seja alcançado.
- Depois que o destino final é alcançado, o host responde com uma mensagem de Porta inacessível do ICMP ou uma mensagem de resposta de eco do ICMP, em vez da mensagem Tempo excedido do ICMP.



# Formato de Pacote ICMP de Utilitários Ping e Traceroute

- O ICMP é encapsulado diretamente em pacotes IP.
- O ICMP atua como uma carga útil de dados dentro do pacote IP. Ele tem um campo de dados de cabeçalho especial.
- Possui um campo de dados de cabeçalho especial. Estes são alguns códigos de mensagem comuns:
  - **0** – Echo reply (resposta a um ping)
  - **3** – Destino Inalcançável
  - **5** – Redirect (use outra rota para o destino)
  - **8** – Echo request (para ping)
  - **11** – Time Exceeded (TTL tornou-se 0)



## Packet Tracer – Verifique o Endereçamento IPv4 e IPv6

Neste Packet Tracer, você fará o seguinte:

- Verifique a configuração de endereçamento IPv4 e IPv6.
- Teste a conectividade com Ping e Tracert.



# 7.3 Resumo de Verificação de Conectividade

# O que aprendi neste módulo?

- O conjunto TCP / IP envia mensagens ICMP quando os pacotes IP encontram problemas de encaminhamento.
- ICMPv4 é o protocolo de mensagens para IPv4, enquanto ICMPv6 fornece esses mesmos serviços para IPv6 e inclui funcionalidades adicionais.
- As mensagens ICMP comuns a ICMPv4 e ICMPv6 incluem confirmação de host, destino ou serviço inacessível, tempo excedido e redirecionamento de rota.
- ICMPv6 inclui as quatro mensagens ICMPv6 adicionais para o Neighbour Discovery Protocol (NDP).
- Essas mensagens são mensagens de solicitação de roteador (RS) e anúncios de roteador (RA) enviadas entre roteadores IPv6 e hosts IPv6 e mensagens de solicitação de vizinho (NS) e anúncio de vizinho (NA) enviadas entre dispositivos IPv6.

## O que aprendi neste módulo? (Continuação)

- O Ping é um utilitário de teste IPv4 e IPv6 que usa a solicitação de eco ICMP e as mensagens de resposta de eco para testar a conectividade entre hosts.
- Alguns dos tipos de testes de conectividade executados com ping incluem ping no loopback local, ping no gateway padrão e ping em um host remoto.
- Traceroute (tracert) é um utilitário que gera uma lista dos saltos do roteador que foram alcançados com sucesso ao longo de um caminho.
- O Traceroute usa uma função do campo TTL no IPv4 e o campo Hop Limit nos cabeçalhos IPv6 Layer 3, junto com a mensagem ICMP Time Exceeded.
- O ICMP é encapsulado diretamente em pacotes IP como a carga de dados. A carga de dados ICMP contém campos de dados de cabeçalho especiais.

