

2023

Redes de Computadores

Módulo 07 – Camada de
rede

Índice

8 - Camada de rede

8.0 - Introdução

8.0.1 - Por que devo cursar este módulo?

8.0.2 - O que vou aprender neste módulo?

8.1 - Características de camada de rede

8.1.1 - A camada de Rede

8.1.2 - Encapsulamento IP

8.1.3 - Características do IP

8.1.4 - Sem Conexão

8.1.5 - Melhor esforço

8.1.6 - Independente de Mídia

8.1.7 - Verifique sua compreensão - Características de IP

8.2 - Pacote IPv4

8.2.1 - Cabeçalho do Pacote IPv4

8.2.2 - Campos do cabeçalho de pacote IPv4

8.2.3 - Vídeo - Exemplo de cabeçalhos IPv4 no Wireshark

8.2.4 - Verifique sua compreensão - Pacote IPv4

8.3 - Pacote IPv6

8.3.1 - Limitações do IPv4

8.3.2 - Visão geral do IPv6

8.3.3 - Campos do cabeçalho de pacote IPv4 no cabeçalho de pacote IPv6

8.3.4 - Cabeçalho do Pacote IPv6

8.3.5 - Vídeo - Exemplo de cabeçalhos IPv6 no Wireshark

8.3.6 - Verifique sua compreensão - Pacote IPv6

8.4 - Como um Host Roteia

8.4.1 - Decisão de Encaminhamento do Host

8.4.2 - Gateway Padrão

8.4.3 - Um host direciona para o gateway padrão

8.4.4 - Tabelas de Roteamento dos Hosts

8.4.5 - Verifique seu entendimento - Como um host roteia

8.5 - Introdução ao Roteamento

8.5.1 - Decisão de Encaminhamento de Pacotes do Roteador

8.5.2 - Tabela de Roteamento do Roteador IP

8.5.3 - Roteamento estático

8.5.4 - Roteamento dinâmico

8.5.5 - Tabelas de roteamento de roteador de vídeo- IPv4

8.5.6 - Introdução a uma tabela de roteamento IPv4

8.5.7 - Verifique sua compreensão - Introdução ao roteamento

8.6 - Módulo Prática e Quiz

8.6.1 - O que eu aprendi neste módulo?

8.6.2 - Teste de Módulo - Camada de Rede

8.0 Introdução

8.0.1 Por que devo cursar este módulo?

Bem-vindo a Camada de Rede!

Até agora você deve ter notado que os módulos neste curso estão progredindo de baixo para cima através das camadas de modelo OSI. Na camada de rede do modelo OSI, apresentamos protocolos de comunicação e protocolos de roteamento. Digamos que você deseja enviar um e-mail para um amigo que mora em outra cidade, ou mesmo em outro país. Essa pessoa não está na mesma rede que você. Uma rede comutada simples não consegue obter a sua mensagem mais longe do que o fim da sua própria rede. Você precisa de alguma ajuda para manter esta mensagem movendo-se ao longo do caminho para o dispositivo final do seu amigo. Para enviar um e-mail (um vídeo, um arquivo, etc.) para qualquer pessoa que não esteja em sua rede local, você deve ter acesso a roteadores. Para acessar roteadores, você deve usar protocolos de camada de rede. Para ajudá-lo a visualizar esses processos, este módulo contém duas atividades Wireshark. Aproveite!

8.0.2 O que vou aprender neste módulo?

Título do módulo: Camada de rede

Objetivo do módulo: Explicar como os roteadores usam protocolos e serviços de camada de rede para viabilizar a conectividade de ponta a ponta.

Título do Tópico	Objetivo do Tópico
Características de camada de rede	Explicar como a camada de rede usa protocolos IP para obter informações confiáveis. comunicações.
Pacote IPv4	Explicar a função dos principais campos do cabeçalho no pacote IPv4.
Pacote IPv6	Explicar a função dos principais campos do cabeçalho no pacote IPv6.
Como um host roteia	Explicar como os dispositivos de rede usam tabelas de roteamento para direcionar pacotes a um Rede de destino.
Tabelas de roteamento do roteador	Explicar a função dos campos na tabela de roteamento de um roteador.

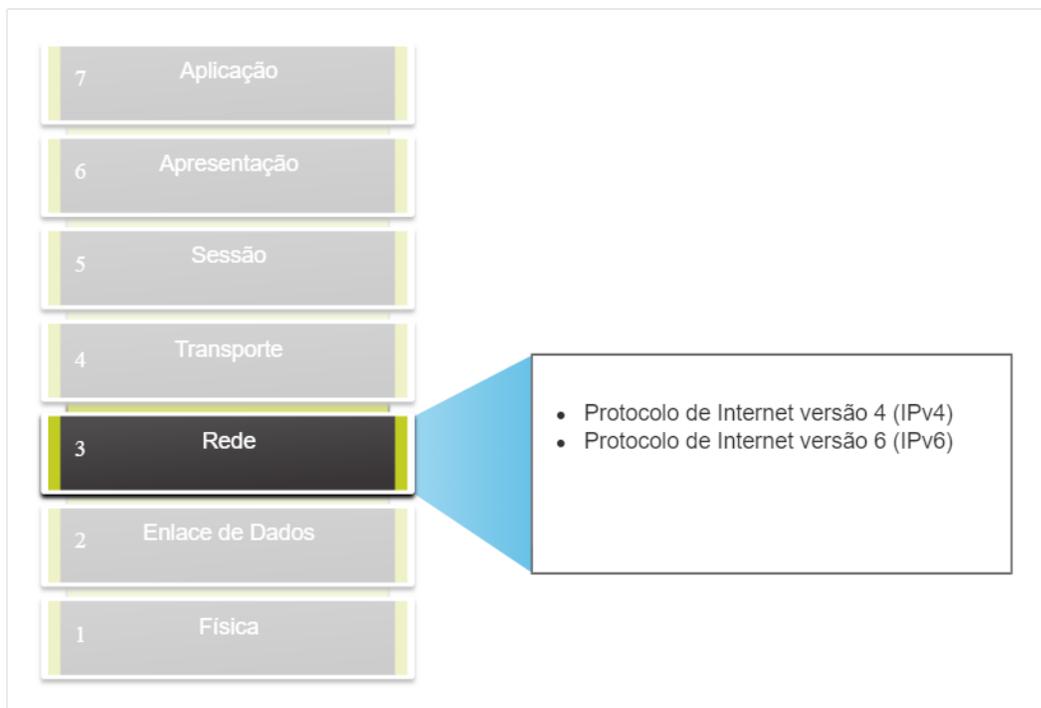
8.1 Características de camada de rede

8.1.1 A camada de Rede

A camada de rede, ou Camada OSI 3, fornece serviços para permitir que dispositivos finais troquem dados entre redes. Como mostrado na figura, IP versão 4 (IPv4) e IP versão 6 (IPv6) são os principais protocolos de comunicação de camada de rede. Outros protocolos de camada de rede incluem protocolos de roteamento, como OSPF (Open Shortest Path First) e protocolos de mensagens, como ICMP (Internet Control Message Protocol).

Protocolos da Camada de Rede

- Protocolo de Internet versão 4 (IPv4)
- Protocolo de Internet versão 6 (IPv6)

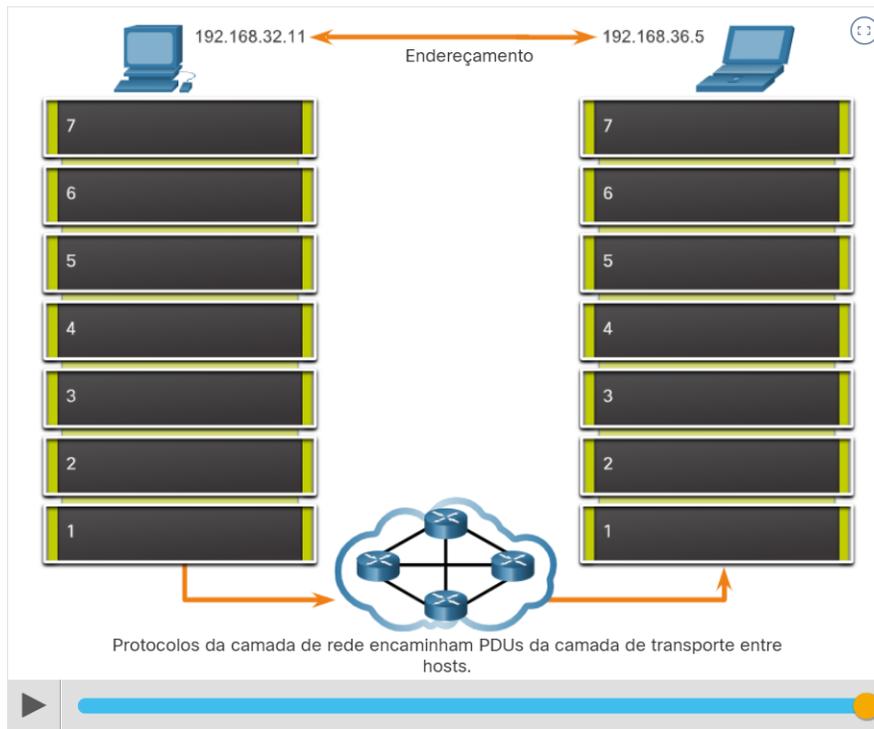


Para realizar comunicações de ponta a ponta através dos limites da rede, os protocolos de camada de rede executam quatro operações básicas:

- **Endereçamento de dispositivos finais** - Os dispositivos finais devem ser configurados com um endereço IP exclusivo para identificação na rede.
- **Encapsulamento** - A camada de rede encapsula a unidade de dados de protocolo (PDU) da camada de transporte em um pacote. O processo de encapsulamento adiciona informações de cabeçalho IP, como os endereços IP dos hosts origem (emissor) e destino (receptor). O processo de encapsulamento é executado pela origem do pacote IP.
- **Roteamento** - A camada de rede fornece serviços para direcionar os pacotes para um host de destino em outra rede. Para trafegar para outras redes, o pacote deve ser processado por um roteador. A função do roteador é escolher o melhor caminho e direcionar os pacotes para o host de destino em um processo conhecido como roteamento. Um pacote pode atravessar muitos roteadores antes de chegar ao host de destino. Cada roteador que um pacote atravessa para chegar ao host de destino é chamado de salto.
- **Desencapsulamento** - Quando o pacote chega na camada de rede do host de destino, o host verifica o cabeçalho IP do pacote. Se o endereço IP de destino no cabeçalho corresponder ao seu próprio endereço IP, o cabeçalho IP será removido do pacote. Depois que o pacote é desencapsulado pela camada de rede, a PDU resultante da Camada 4 é transferida para o serviço apropriado na camada de transporte. O processo de desencapsulamento é executado pelo host de destino do pacote IP.

Diferentemente da camada de transporte (OSI Layer 4), que gerencia o transporte de dados entre os processos em execução em cada host, os protocolos de comunicação da camada de rede (ou seja, IPv4 e IPv6) especificam a estrutura de pacotes e o processamento usado para transportar os dados de um host para outro hospedeiro. A operação sem levar em consideração os dados contidos em cada pacote permite que a camada de rede transporte pacotes para diversos tipos de comunicações entre vários hosts.

Clique em Reproduzir na figura para ver uma animação que demonstra a troca de dados.

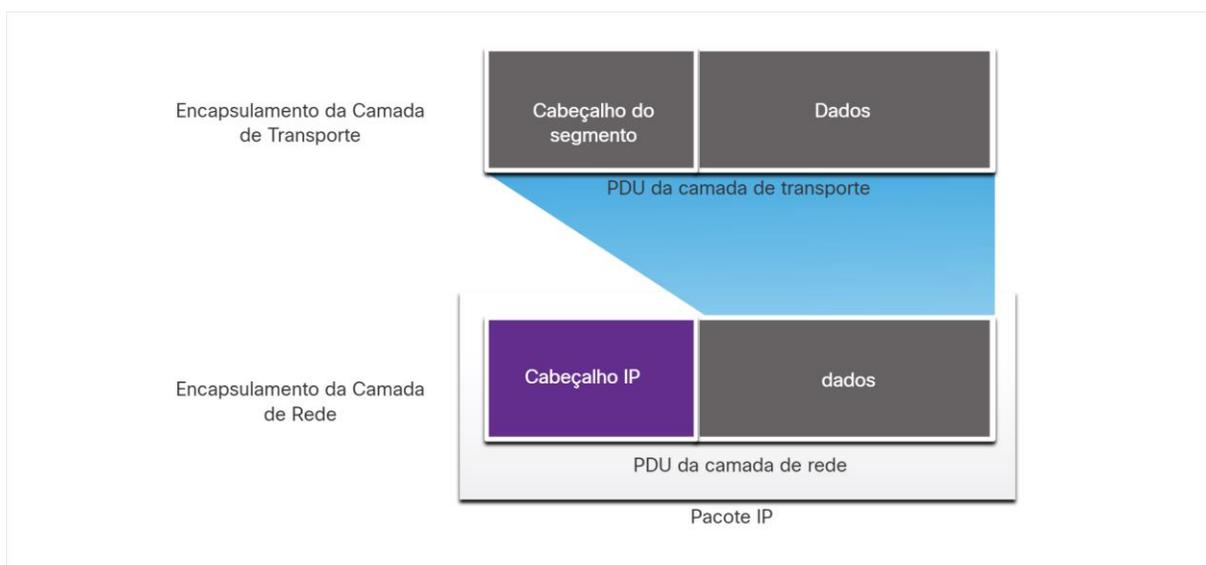


8.1.2 Encapsulamento IP

O IP encapsula o segmento da camada de transporte (a camada logo acima da camada de rede) ou outros dados adicionando um cabeçalho IP. O cabeçalho IP é usado para entregar o pacote ao host de destino.

A figura ilustra como a PDU da camada de transporte é encapsulada pela PDU da camada de rede para criar um pacote IP.

A ilustração mostra a PDU da camada de transporte sendo encapsulada em um pacote IP. Na parte superior do gráfico está o encapsulamento da camada de transporte. Ele mostra o cabeçalho do segmento seguido por dados. Isso inclui a PDU da camada de transporte. Isso é transmitido para a camada de rede para encapsulamento adicional e se torna a parte de dados da PDU da camada de rede. Um cabeçalho IP é adicionado na frente dos dados para criar o pacote IP.



O processo de encapsulamento camada por camada possibilita o desenvolvimento e a expansão dos serviços nas diferentes camadas sem afetar outras camadas. Isso significa que os segmentos da camada de transporte podem ser imediatamente empacotados por IPv4, IPv6 ou qualquer protocolo que venha a ser desenvolvido no futuro.

O cabeçalho IP é examinado por dispositivos de Camada 3 (ou seja, roteadores e switches de Camada 3) à medida que viaja através de uma rede até seu destino. É importante notar que as informações de endereçamento IP permanecem as mesmas desde o momento em que o pacote sai do host de origem até chegar ao host de destino, exceto quando traduzidas pelo dispositivo que executa a Tradução de Endereços de Rede (NAT) para IPv4.

Observação: O NAT é discutido em módulos posteriores.

Os roteadores implementam protocolos de roteamento para rotear pacotes entre redes. O roteamento realizado por esses dispositivos intermediários examina o endereçamento da camada de rede no cabeçalho do pacote. Em todos os casos, a parte de dados do pacote, ou seja, a PDU da camada de transporte encapsulada ou outros dados, permanece inalterada durante os processos da camada de rede.

8.1.3 Características do IP

O IP foi desenvolvido como um protocolo com baixa sobrecarga. Ele fornece apenas as funções necessárias para enviar um pacote de uma origem a um destino por um sistema interconectado de redes. O protocolo não foi projetado para rastrear e gerenciar o fluxo de pacotes. Essas funções, se exigido, são realizadas por outros protocolos em outras camadas, principalmente TCP na Camada 4.

Estas são as características básicas da IP:

- **Sem conexão** - Não há conexão com o destino estabelecido antes do envio de pacotes de dados.
- **Melhor esforço** - o IP é inerentemente não confiável, porque a entrega de pacotes não é garantida.
- **Independente da mídia** - A operação é independente do meio (ou seja, cobre, fibra ótica ou sem fio) que carrega os dados.

8.1.4 Sem Conexão

O IP não tem conexão, o que significa que nenhuma conexão ponta a ponta dedicada é criada pelo IP antes que os dados sejam enviados. A comunicação sem conexão é conceitualmente semelhante a enviar uma carta a alguém sem notificar o destinatário com antecedência. A figura resume esse ponto-chave.

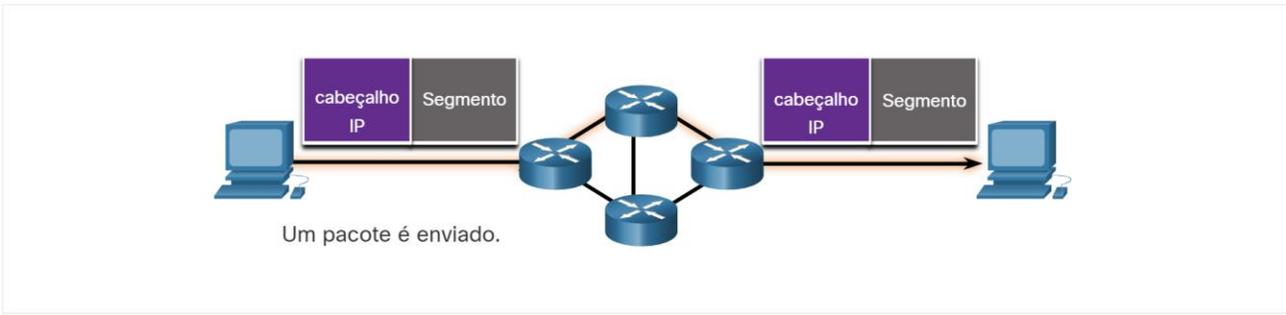
um pacote, que consiste em um cabeçalho e segmento IP, é enviado de uma origem em uma rede para um destino em outra rede

Sem conexão - Analogia



As comunicações de dados sem conexão funcionam com o mesmo princípio. Como mostra a figura, o IP não requer troca inicial de informações de controle para estabelecer uma conexão ponto a ponto antes do encaminhamento dos pacotes.

Sem conexão - Rede

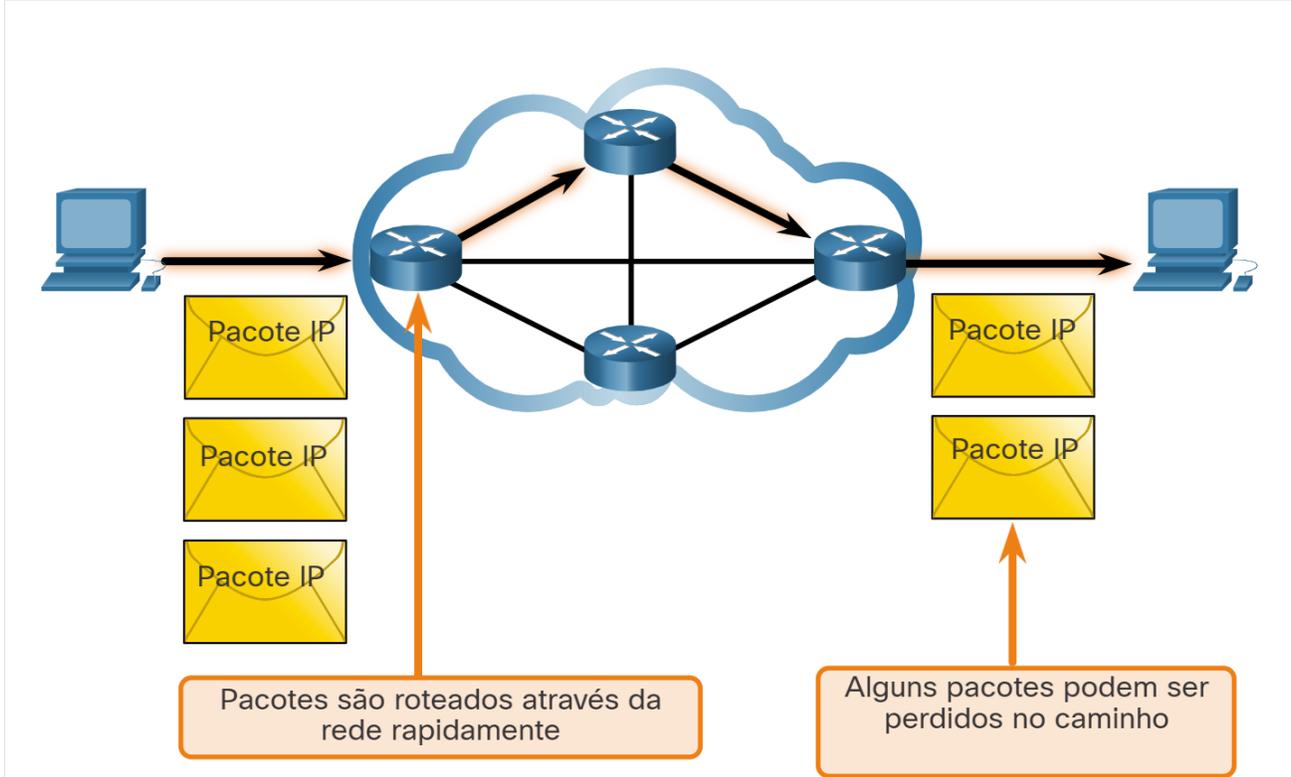


8.1.5 Melhor esforço

O IP também não requer campos adicionais no cabeçalho para manter uma conexão estabelecida. Esse processo reduz bastante a sobrecarga do IP. No entanto, sem conexão de ponta a ponta pré-estabelecida, os remetentes não sabem se os dispositivos de destino estão presentes e funcionais ao enviar pacotes, nem sabem se o destino recebe o pacote ou se o dispositivo de destino pode acessar e ler o pacote.

O protocolo IP não garante que o pacote enviado seja, de fato, recebido. A figura ilustra a característica de entrega não confiável ou de melhor esforço do protocolo IP.

O diagrama mostra uma origem em uma rede e um destino em outra rede. Entre os dois hosts é uma nuvem que consiste em quatro roteadores em uma topologia de malha. Três pacotes IP deixam o host de origem, mas apenas dois chegam ao host de destino. O texto no gráfico diz: Os pacotes são roteados pela rede rapidamente; Alguns pacotes podem ser perdidos no caminho. Pacotes são roteados através da rede rapidamente Alguns pacotes podem ser perdidos no caminho Pacote IPPacote IPPacote IPPacote IPPacote IP



Por ser um protocolo de camada de rede não confiável, o IP não garante que todos os pacotes enviados serão recebidos. Outros protocolos gerenciam o processo de rastreamento de pacotes e garantem sua entrega.

8.1.6 Independente de Mídia

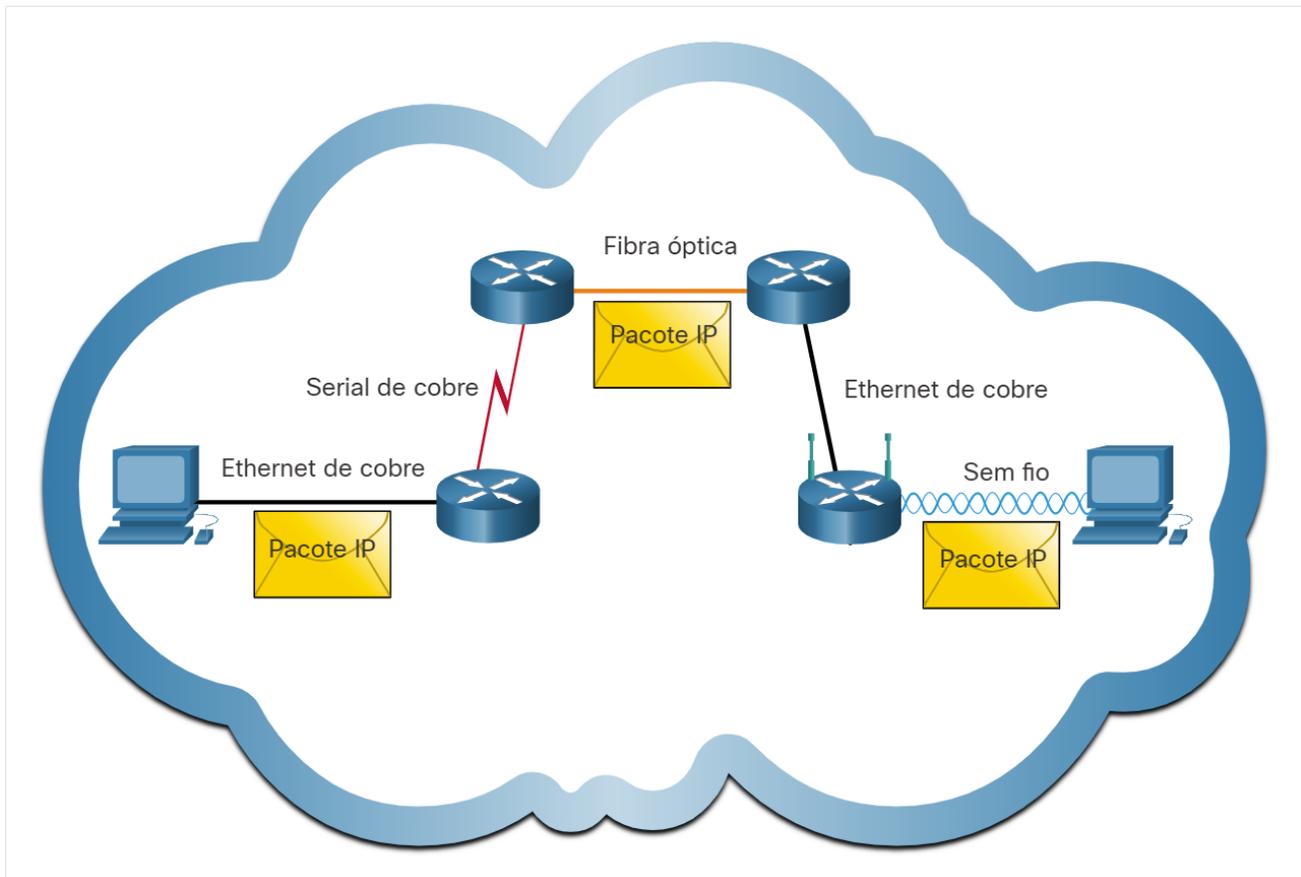
Não confiável significa que o IP não tem a capacidade de gerenciar e recuperar pacotes não entregues ou corrompidos. Isso ocorre porque, embora os pacotes IP sejam enviados com informações sobre o local da entrega, eles

não contêm informações que podem ser processadas para informar ao remetente se a entrega foi bem-sucedida. Os pacotes podem chegar ao destino corrompidos, fora de sequência ou simplesmente não chegar. O IP não tem capacidade de retransmitir os pacotes em caso de erros.

Se os pacotes forem entregues fora de ordem ou estiver faltando algum pacote, as aplicações que usam os dados, ou serviços de camada superior, deverão resolver esses problemas. Isso permite que o IP funcione de forma bem eficiente. No conjunto de protocolos TCP / IP, a confiabilidade é o papel do protocolo TCP na camada de transporte.

O IP opera independentemente da mídia que transporta os dados nas camadas inferiores da pilha de protocolos. Conforme mostra a figura, os pacotes IP podem ser comunicados como sinais elétricos por cabo de cobre, sinais ópticos nas fibras ou sinais de rádio em redes sem fio.

O diagrama mostra uma topologia de rede dentro de uma nuvem com um pacote viajando por vários tipos de mídia entre dois hosts. Um pacote IP é mostrado movendo-se entre um host e um roteador através de uma conexão Ethernet de cobre. O primeiro roteador é conectado ao segundo roteador através de uma conexão serial de cobre. Um pacote IP é mostrado movendo-se entre o segundo roteador e um terceiro roteador através de uma conexão de fibra óptica. O terceiro roteador está conectado a um quarto roteador, que é um roteador sem fio. Um pacote IP é mostrado movendo-se entre o quarto roteador e um host através de uma conexão sem fio.



Os pacotes IP podem trafegar por diferentes meios físicos.

A camada de enlace de dados OSI é responsável por pegar um pacote IP e prepará-lo para transmissão pelo meio de comunicação. Isso significa que a entrega de pacotes IP não se limita a nenhum meio específico.

Há, no entanto, uma característica muito importante dos meios físicos que a camada de rede considera: o tamanho máximo da PDU que cada meio consegue transportar. Essa característica é chamada de unidade máxima de transmissão (maximum transmission unit - MTU). Parte das comunicações de controle entre a camada de enlace de dados e a camada de rede é a definição de um tamanho máximo para o pacote. A camada de enlace de dados passa o valor da MTU para a camada de rede. A camada de rede então determina o tamanho que os pacotes podem ter.

Em alguns casos, um dispositivo intermediário, geralmente um roteador, deve dividir um pacote IPv4 ao encaminhá-lo de um meio para outro com uma MTU menor. Esse processo é chamado fragmentação do pacote ou fragmentação. A fragmentação causa latência. Os pacotes IPv6 não podem ser fragmentados pelo roteador.

8.1.7 Verifique sua compreensão - Características de IP

Verifique sua compreensão das características da camada de rede escolhendo a melhor resposta para as seguintes perguntas.

1. Qual camada OSI envia segmentos para serem encapsulados em um pacote IPv4 ou IPv6?
 - Camada de enlace de dados
 - Camada de rede
 - camada de transporte
 - camada de sessão
2. Qual camada é responsável por pegar um pacote IP e prepará-lo para transmissão pelo meio de comunicação?
 - Camada física
 - Camada de rede
 - Camada de enlace de dados
 - camada de transporte
3. Qual é o termo para dividir um pacote IP ao encaminhá-lo de uma mídia para outra mídia com uma MTU menor?
 - encapsulamento
 - fragmentação
 - segmentação
 - serialização
4. Qual método de entrega não garante que o pacote seja entregue totalmente sem erros?
 - sem conexão
 - melhor esforço
 - Independe de meios físicos

1. Qual camada OSI envia segmentos para serem encapsulados em um pacote IPv4 ou IPv6?

Você entendeu!

- Camada de enlace de dados
- Camada de rede
- camada de transporte
- camada de sessão

2. Qual camada é responsável por pegar um pacote IP e prepará-lo para transmissão pelo meio de comunicação?

Você entendeu!

- Camada física
- Camada de rede
- Camada de enlace de dados
- camada de transporte

3. Qual é o termo para dividir um pacote IP ao encaminhá-lo de uma mídia para outra mídia com uma MTU menor?

Você entendeu!

- encapsulamento
- fragmentação
- segmentação
- serialização

4. Qual método de entrega não garante que o pacote seja entregue totalmente sem erros?

Você entendeu!

- sem conexão
- melhor esforço
- independe de meios físicos

Bom trabalho!

Você identificou com sucesso as respostas corretas.

1. **Camada de Transporte** PDUs, chamados de segmentos, são encapsulados na camada de rede por IPv4 e IPv6 em pacotes.
2. A **camada de enlace de dados** recebe pacotes IP da camada de rede e os encapsula para transmissão pelo meio.
3. **Fragmentação** é o processo de divisão de pacotes IP para trafegar em um meio com um MTU menor.
4. A **entrega de melhor** esforço não garante que os pacotes serão entregues ao destino.

Você respondeu 4 das 4 perguntas corretamente.

8.2 Pacote IPv4

8.2.1 Cabeçalho do Pacote IPv4

O IPv4 é um dos principais protocolos de comunicação de camada de rede. O cabeçalho do pacote IPv4 é usado para garantir que esse pacote seja entregue para sua próxima parada no caminho para seu dispositivo final de destino.

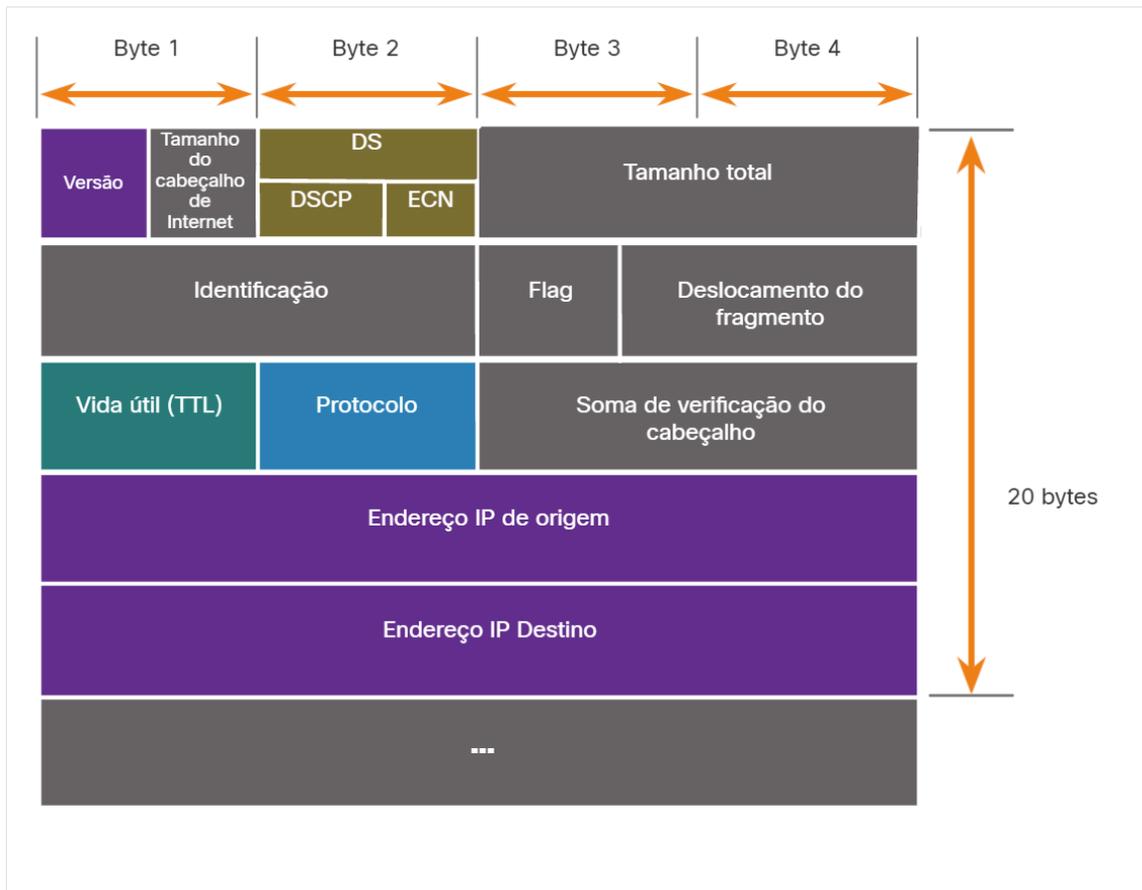
O cabeçalho de um pacote IPv4 consiste em campos com informações importantes sobre o pacote. Esses campos contêm números binários que são examinados pelo processo da Camada 3.

8.2.2 Campos do cabeçalho de pacote IPv4

Os valores binários de cada campo identificam várias configurações do pacote IP. Os diagramas de cabeçalho de protocolo, cuja leitura é feita da esquerda para a direita, de cima para baixo, disponibilizam uma visualização para consultar ao discutir os campos de protocolo. O diagrama de cabeçalho de protocolo IP na figura identifica os campos de um pacote IPv4.

nomes e comprimento de bits de campos em um cabeçalho de pacote IPv4

Campos no cabeçalho do pacote IPv4



Campos significativos no cabeçalho IPv4 incluem o seguinte:

- **Versão** – Contém um valor binário de 4 bits definido como 0100 que identifica que este é um pacote IP versão 4.
- **Serviços diferenciados ou DiffServ (DS)** - Anteriormente chamado de Tipo de Serviço (ToS), o campo DS é um campo de 8 bits usado para determinar a prioridade de cada pacote. Os seis bits mais significativos do campo DiffServ são os bits do ponto de código de serviços diferenciados (DSCP) e os dois últimos são os bits de notificação de congestionamento explícita (ECN).
- **Checksum de cabeçalho** — Isso é usado para detectar corrupção no cabeçalho IPv4.
- **Tempo de vida (TTL)** – TTL contém um valor binário de 8 bits que é usado para limitar a vida útil de um pacote. O dispositivo de origem do pacote IPv4 define o valor TTL inicial. É diminuído em um cada vez que o pacote é processado por um roteador. Se o campo TTL for decrementado até zero, o roteador descartará o pacote e enviará uma mensagem ICMP de tempo excedido para o endereço IP de origem. Como o roteador decrementa o TTL de cada pacote, o roteador também deve recalcular a soma de verificação do cabeçalho.
- **Protocolo** - Este campo é usado para identificar o protocolo de próximo nível. O valor binário de 8 bits indica o tipo de carga de dados que o pacote está carregando, o que permite que a camada de rede transfira os dados para o protocolo apropriado das camadas superiores. Valores comuns incluem ICMP (1), TCP (6) e UDP (17).
- **Endereço IP Origem** – Contém um valor binário de 32 bits que representa o endereço IP origem do pacote. O endereço de origem IPv4 é sempre um endereço unicast.
- **Endereço IP Destino** – Contém um valor binário de 32 bits que representa o endereço IP destino do pacote. O endereço IPv4 destino é um endereço unicast, multicast, ou broadcast.

Os dois campos mais referenciados são os endereços IP de origem e destino. Esses campos identificam a procedência do pacote e para onde ele vai. Normalmente, esses endereços não mudam durante a viagem da origem ao destino.

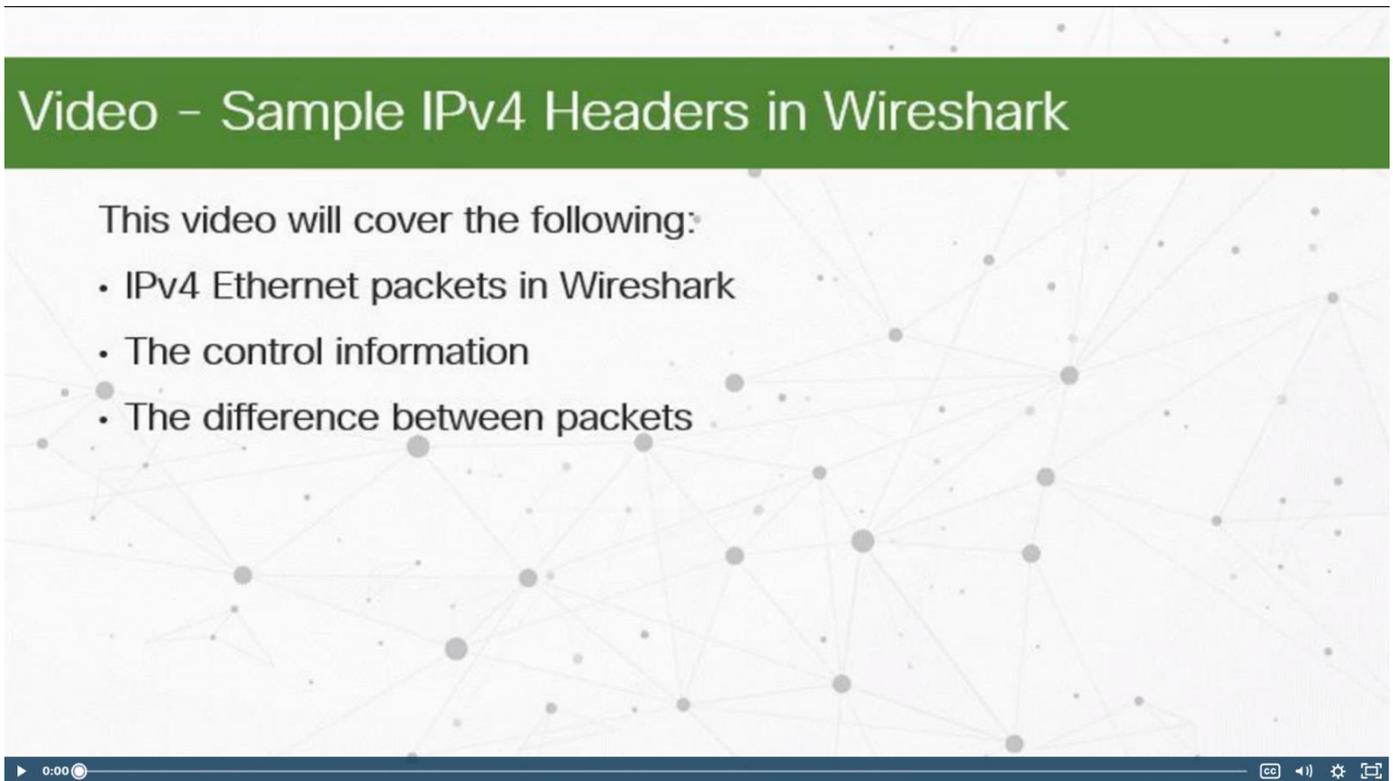
Os campos Tamanho do Cabeçalho de Internet (IHL), Tamanho Total e Soma de Verificação do Cabeçalho servem para identificar e validar o pacote.

Outros campos são usados para reorganizar um pacote fragmentado. O pacote IPv4 usa especificamente os campos Identificação, Flags e Deslocamento do Fragmento para organizar os fragmentos. Um roteador pode precisar fragmentar um pacote IPv4 ao encaminhá-lo de um meio para outro com uma MTU menor.

Os campos Opções e Preenchimento raramente são usados e estão além do escopo deste módulo.

8.2.3 Vídeo - Exemplo de cabeçalhos IPv4 no Wireshark

Clique em Reproduzir na figura para ver uma demonstração do exame de cabeçalhos IPv4 em uma captura do Wireshark.



Duração: 5:21

8.2.4 Verifique sua compreensão - Pacote IPv4

Verifique sua compreensão do pacote IPv4 escolhendo a melhor resposta para as seguintes perguntas.

1. Quais são os dois campos mais comumente referenciados em um cabeçalho de pacote IPv4 que indicam de onde o pacote está vindo e para onde ele está indo? (Escolha duas.)

- endereço IP de destino
- protocolo
- Tempo de Vida
- Endereço IP origem
- Serviços diferenciados (DS)

2. Qual instrução está correta sobre campos de cabeçalho de pacote IPv4?

- Os endereços IPv4 de origem e destino permanecem os mesmos durante a viagem da origem para o destino.
- O campo Time to Live é usado para determinar a prioridade de cada pacote.
- Os campos Comprimento total e soma de verificação de cabeçalho são usados para reordenar um pacote fragmentado.
- O campo Versão identifica o protocolo de nível seguinte.

3. Qual campo é usado para detectar corrupção no cabeçalho IPv4?

- Soma de verificação do cabeçalho
- Tempo de Vida
- Protocolos
- Serviços diferenciados (DS)

4. Qual campo inclui valores comuns como ICMP (1), TCP (6) e UDP (17)?

- Soma de verificação do cabeçalho
- Tempo de Vida
- Protocolos
- Serviços diferenciados (DS)

1. Quais são os dois campos mais comumente referenciados em um cabeçalho de pacote IPv4 que indicam de onde o pacote está vindo e para onde ele está indo? (Escolha duas.)

Você entendeu!

endereço IP de destino

protocolo

Tempo de Vida

Endereço IP origem

Serviços diferenciados (DS)

2. Qual instrução está correta sobre campos de cabeçalho de pacote IPv4?

Você entendeu!

Os endereços IPv4 de origem e destino permanecem os mesmos durante viagem da origem para o destino.

O campo Time to Live é usado para determinar a prioridade de cada pacote.

Os campos Comprimento total e soma de verificação de cabeçalho são usados para reordenar um pacote fragmentado.

O campo Versão identifica o protocolo de nível seguinte.

3. Qual campo é usado para detectar corrupção no cabeçalho IPv4?

Você entendeu!

Soma de verificação do cabeçalho

Tempo de Vida

Protocolos

Serviços diferenciados (DS)

4. Qual campo inclui valores comuns como ICMP (1), TCP (6) e UDP (17)?

Você entendeu!

Soma de verificação do cabeçalho

Tempo de Vida

Protocolos

Serviços diferenciados (DS)

Bom trabalho!

Você identificou com sucesso as respostas corretas.

- Os campos de cabeçalho IP que identificam a origem do pacote e para onde ele está indo são **Endereço IP de Origem** e **Endereço IP de Destino**.
- Os endereços IP de origem e de destino no pacote IP não são alterados na rota da origem para o destino.
- O campo **Checksum de cabeçalho** em um cabeçalho IPv4 é usado para detectar pacotes corrompidos.
- O campo **protocolo** identifica o protocolo da camada superior que é transportado dentro do pacote IP. Protocolos comuns são TCP, UDP e ICMP.

Você respondeu 4 das 4 perguntas corretamente.

8.3 Pacote IPv6

8.3.1 Limitações do IPv4

O IPv4 ainda está em uso hoje. Este tópico é sobre IPv6, que eventualmente substituirá o IPv4. Para entender melhor por que você precisa conhecer o protocolo IPv6, ele ajuda a conhecer as limitações do IPv4 e as vantagens do IPv6.

Ao longo dos anos, protocolos e processos adicionais foram desenvolvidos para enfrentar novos desafios. No entanto, mesmo com alterações, ele ainda enfrenta três grandes problemas:

- **Esgotamento do endereço IPv4** - O IPv4 tem um número limitado de endereços públicos exclusivos disponíveis. Embora haja aproximadamente 4 bilhões de endereços IPv4, o número crescente de novos dispositivos

Legenda Há 4 bilhões de endereços IPv4 Há 340 undecilhões de endereços IPv6

Nome do Número	Notação Científica	Número de Zeros
1 mil	10 ³	1.000
1 milhão	10 ⁶	1.000.000
1 bilhão	10 ⁹	1.000.000.000
1 trilhão	10 ¹²	1.000.000.000.000
1 quadrilhão	10 ¹⁵	1.000.000.000.000.000
1 quintilhão	10 ¹⁸	1.000.000.000.000.000.000
1 sextilhão	10 ²¹	1.000.000.000.000.000.000.000
1 setilhão	10 ²⁴	1.000.000.000.000.000.000.000.000
1 octilhão	10 ²⁷	1.000.000.000.000.000.000.000.000.000
1 nonilhão	10 ³⁰	1.000.000.000.000.000.000.000.000.000.000
1 decilhão	10 ³³	1.000.000.000.000.000.000.000.000.000.000.000
1 undecilhão	10 ³⁶	1.000.000.000.000.000.000.000.000.000.000.000.000

Legenda

- Há 4 bilhões de endereços IPv4
- Há 340 undecilhões de endereços IPv6

8.3.3 Campos do cabeçalho de pacote IPv4 no cabeçalho de pacote IPv6

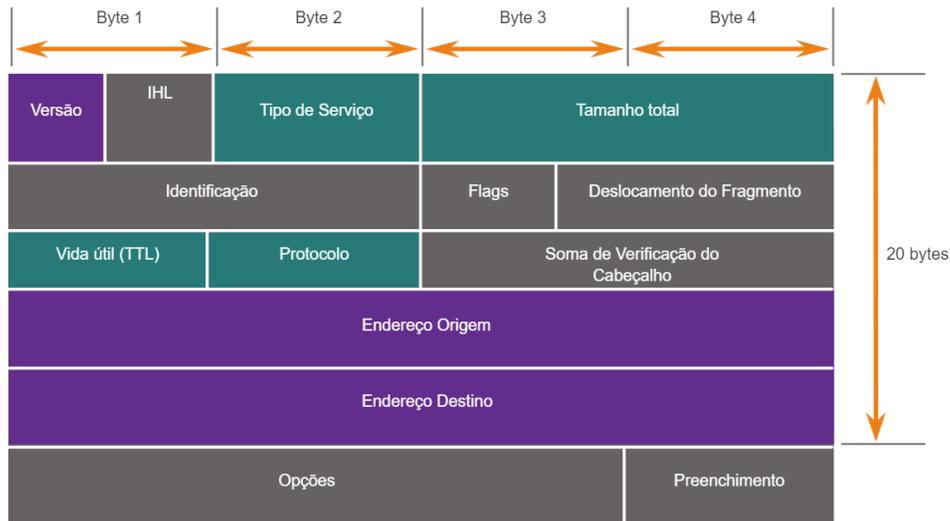
Uma das principais melhorias de design do IPv6 em relação ao IPv4 é o cabeçalho IPv6 simplificado.

Por exemplo, o cabeçalho IPv4 consiste em um cabeçalho de comprimento variável de 20 octetos (até 60 bytes se o campo Opções for usado) e 12 campos de cabeçalho básicos, sem incluir o campo Opções e o campo Preenchimento.

Para o IPv6, alguns campos permaneceram os mesmos, alguns campos mudaram de nome e posição e alguns campos do IPv4 não são mais necessários, conforme destacado na figura.

O diagrama mostra um cabeçalho de pacote IPv4 e indica quais campos mantiveram o mesmo nome, quais campos alteraram nomes e posição e quais campos não foram mantidos no IPv6. Os campos que mantiveram o mesmo nome são: versão, endereço de origem e endereço de destino. Os campos que alteraram nomes e posição são: tipo de serviço, duração total, tempo de vida e protocolo. Os campos que não foram mantidos no IPv6 são: DIH, identificação, sinalizadores, deslocamento de fragmento, soma de verificação de cabeçalho, opções e preenchimento.

Cabeçalho do Pacote IPv4



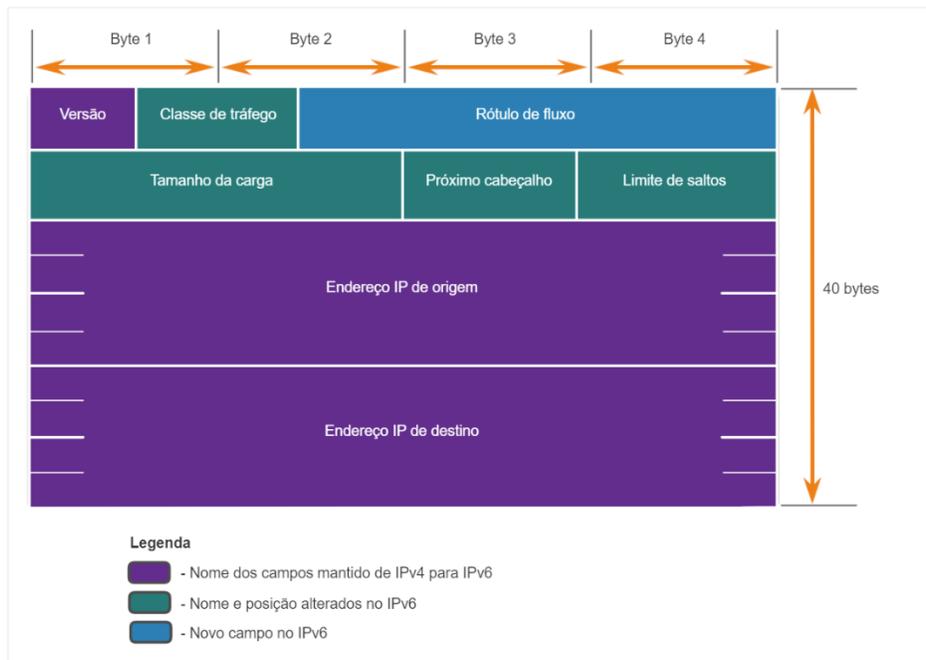
- Legenda**
- Nome dos campos mantido de IPv4 para IPv6
 - Nome e posição alterados no IPv6
 - Novo campo no IPv6

A figura mostra campos de cabeçalho de pacote IPv4 que foram mantidos, movidos, alterados, bem como aqueles que não foram mantidos no cabeçalho do pacote IPv6.

Por outro lado, o cabeçalho simplificado do IPv6 mostrado na figura a seguir consiste em um cabeçalho de comprimento fixo de 40 octetos (em grande parte devido ao comprimento dos endereços IPv6 de origem e de destino).

O cabeçalho simplificado IPv6 permite um processamento mais eficiente de cabeçalhos IPv6.

Cabeçalho do Pacote IPv6



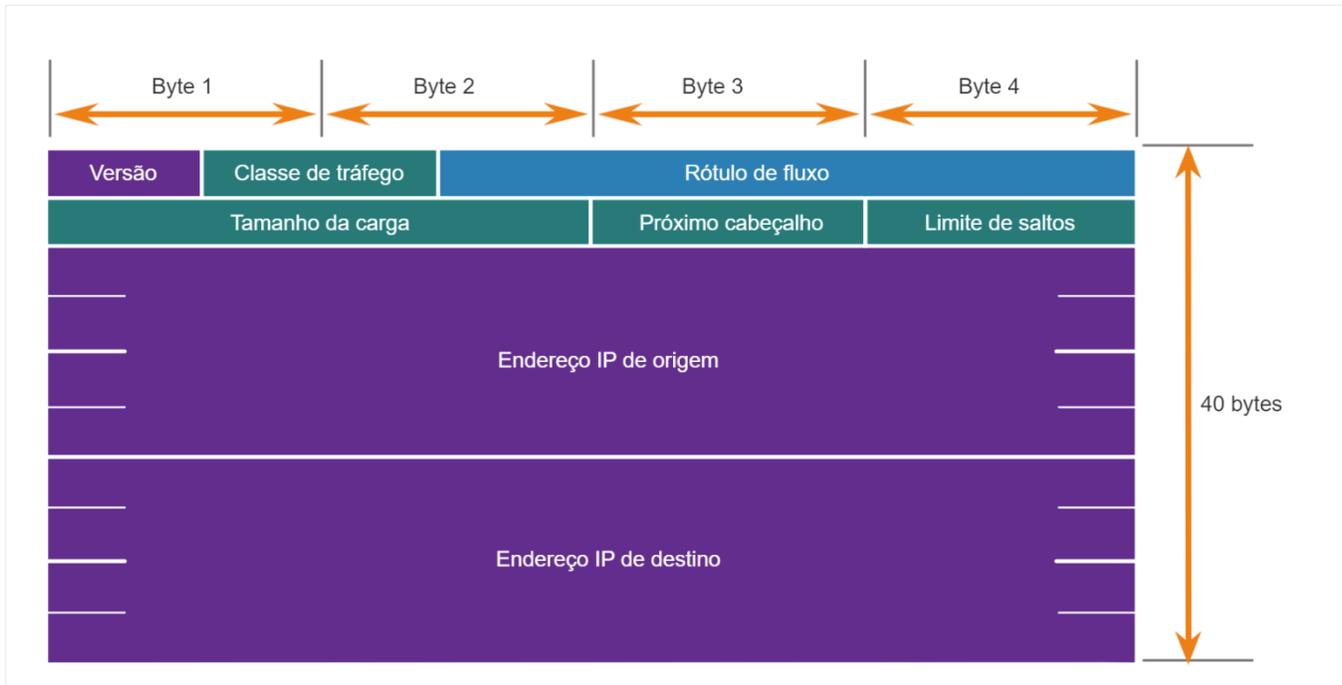
- Legenda**
- Nome dos campos mantido de IPv4 para IPv6
 - Nome e posição alterados no IPv6
 - Novo campo no IPv6

O diagrama mostra um cabeçalho de pacote IPv6 e indica quais campos mantiveram o mesmo nome de IPv4 para IPv6, quais campos alteraram nomes e posição no IPv6, quais campos não foram mantidos no IPv6 e novos campos no IPv6. Os nomes de campo que foram mantidos da mesma forma são: versão, endereço IP de origem e endereço IP de destino. Os campos que alteraram nomes e posição no IPv6 são: classe de tráfego, comprimento da carga útil, próximo cabeçalho e limite de salto. O campo que é NOVO para IPv6 é rótulo de fluxo.

A figura mostra os campos de cabeçalho de pacote IPv4 que foram mantidos ou movidos junto com os novos campos de cabeçalho de pacote IPv6.

8.3.4 Cabeçalho do Pacote IPv6

O diagrama de cabeçalho de protocolo IP na figura identifica os campos de um pacote IPv6.



Campos no cabeçalho do pacote IPv6

Os campos no cabeçalho do pacote IPv6 incluem o seguinte:

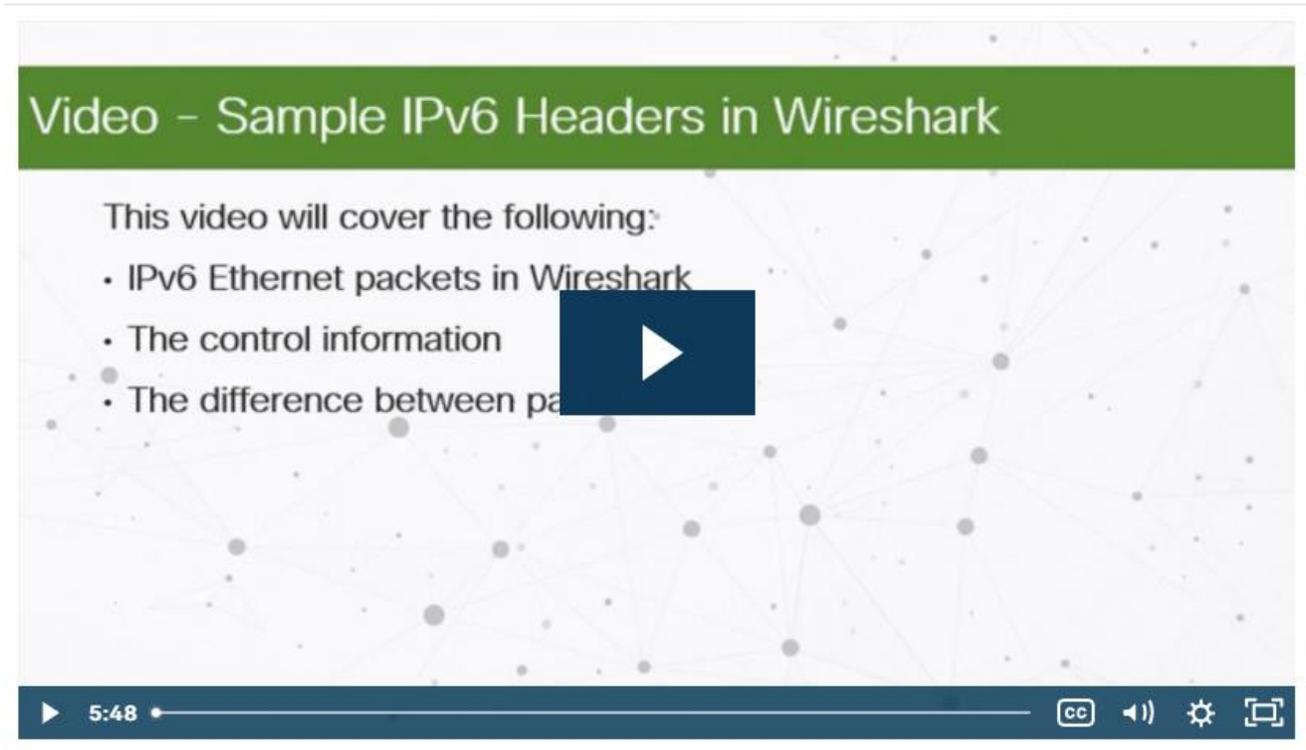
- **Versão** - Este campo contém um valor binário de 4 bits definido como 0110 que identifica isso como um pacote IP versão 6.
- **Classe de tráfego** - Este campo de 8 bits é equivalente ao campo DSc (Serviços diferenciados de IPv4).
- **Etiqueta de fluxo** - Este campo de 20 bits sugere que todos os pacotes com a mesma etiqueta de fluxo recebam o mesmo tipo de manipulação pelos roteadores.
- **Comprimento da carga útil** - Este campo de 16 bits indica o comprimento da parte dos dados ou da carga útil do pacote IPv6. Isso não inclui o comprimento do cabeçalho IPv6, que é um cabeçalho fixo de 40 bytes.
- **Próximo cabeçalho** - Este campo de 8 bits é equivalente ao campo Protocolo IPv4. Ele exibe o tipo de carga de dados que o pacote está carregando, permitindo que a camada de rede transfira os dados para o protocolo apropriado das camadas superiores.
- **Limite de salto** - Este campo de 8 bits substitui o campo TTL IPv4. Esse valor é subtraído de um por cada roteador que encaminha o pacote. Quando o contador atinge 0, o pacote é descartado e uma mensagem de ICMPv6 com tempo excedido é encaminhada para o host de envio. Isso indica que o pacote não atingiu seu destino porque o limite de salto foi excedido. Ao contrário do IPv4, o IPv6 não inclui uma soma de verificação do cabeçalho IPv6, porque esta função é executada nas camadas inferior e superior. Isso significa que a soma de verificação não precisa ser recalculada por cada roteador quando diminui o campo Limite de Hop, o que também melhora o desempenho da rede.
- **Endereço IPv6 de origem** - Este campo de 128 bits identifica o endereço IPv6 do host de envio.
- **Endereço IPv6 de destino** - Este campo de 128 bits identifica o endereço IPv6 do host de recebimento.

Um pacote IPv6 pode conter também cabeçalhos de extensão (EH), que fornecem informações de camada de rede. Opcionais, os cabeçalhos de extensão ficam posicionados entre o cabeçalho IPv6 e a carga. Eles são usados para fragmentação, segurança, suporte à mobilidade e muito mais.

Ao contrário de IPv4, os roteadores não fragmentam os pacotes IPv6 roteados.

8.3.5 Vídeo - Exemplo de cabeçalhos IPv6 no Wireshark

Clique em Reproduzir na figura para ver uma demonstração do exame de cabeçalhos IPv6 em uma captura do Wireshark.



Duração: 5:48

8.3.6 Verifique sua compreensão - Pacote IPv6

Verifique sua compreensão do pacote IPv6, selecione a melhor resposta para as seguintes perguntas.

1. Quais três opções são os principais problemas associados ao IPv4? (Escolha três.)
 - Redução do número de endereços IP disponíveis
 - maior complexidade da rede e expansão da tabela de roteamento da Internet
 - sempre em conexões
 - falta de conectividade de ponta a ponta
 - fronteiras globais e políticas
 - muitos endereços IPv4 disponíveis
2. Quais duas opções são as melhorias fornecidas pelo IPv6 em comparação com o IPv4? (Escolha duas.)
 - suporta campos adicionais para pacotes complexos
 - aumentou o espaço de endereço IP
 - padroniza o uso de NAT
 - suporta redes baseadas em classe
 - usa um cabeçalho mais simples para fornecer melhor manipulação de pacotes
3. Qual é o verdadeiro do cabeçalho IPv6?
 - consiste em 20 octetos.
 - consiste em 40 octetos.

- contém 8 campos de cabeçalho.
- contém 12 campos de cabeçalho.

4. Qual é o verdadeiro do cabeçalho do pacote IPv6?

- O campo Limite de salto substitui o campo Tempo de vida do IPv4.
- Os endereços IPv6 de origem e destino mudam durante a viagem da origem para o destino.
- O campo Tempo de vida substitui o campo DiffServ.
- O campo Versão identifica o próximo cabeçalho.

1. Quais três opções são os principais problemas associados ao IPv4? (Escolha três.)

Você entendeu!

- Redução do número de endereços IP disponíveis
- maior complexidade da rede e expansão da tabela de roteamento da Internet
- sempre em conexões
- falta de conectividade de ponta a ponta
- fronteiras globais e políticas
- muitos endereços IPv4 disponíveis

2. Quais duas opções são as melhorias fornecidas pelo IPv6 em comparação com o IPv4? (Escolha duas.)

Você entendeu!

- suporta campos adicionais para pacotes complexos
- aumentou o espaço de endereço IP
- padroniza o uso de NAT
- suporta redes baseadas em classe
- usa um cabeçalho mais simples para fornecer melhor manipulação de pacotes

3. Qual é o verdadeiro do cabeçalho IPv6?

Você entendeu!

- consiste em 20 octetos.
- consiste em 40 octetos.
- contém 8 campos de cabeçalho.
- contém 12 campos de cabeçalho.

4. Qual é o verdadeiro do cabeçalho do pacote IPv6?

Você entendeu!

- O campo Limite de salto substitui o campo Tempo de vida do IPv4.
- Os endereços IPv6 de origem e destino mudam durante a viagem da origem para o destino.
- O campo Tempo de vida substitui o campo DiffServ.
- O campo Versão identifica o próximo cabeçalho.

Bom trabalho!

Você identificou com sucesso as respostas corretas.

1. O IPv4 foi padronizado na década de 1980 e tem várias limitações tecnológicas, como a falta de conectividade de ponta a ponta e um espaço de endereços esgotado.
2. Existem várias melhorias técnicas feitas no IPv6, duas das quais são um pool de endereços IP muito maior e um cabeçalho de protocolo simplificado.
3. O cabeçalho IPv6 é um comprimento fixo de 40 octetos e contém 8 campos de cabeçalho.
4. Vários campos no cabeçalho IPv6 substituíram campos no cabeçalho IPv4. Por exemplo, o campo Limite de salto substituiu o campo Time to Live do cabeçalho IPv4.

Você respondeu 4 das 4 perguntas corretamente.

8.4 Como um Host Roteia

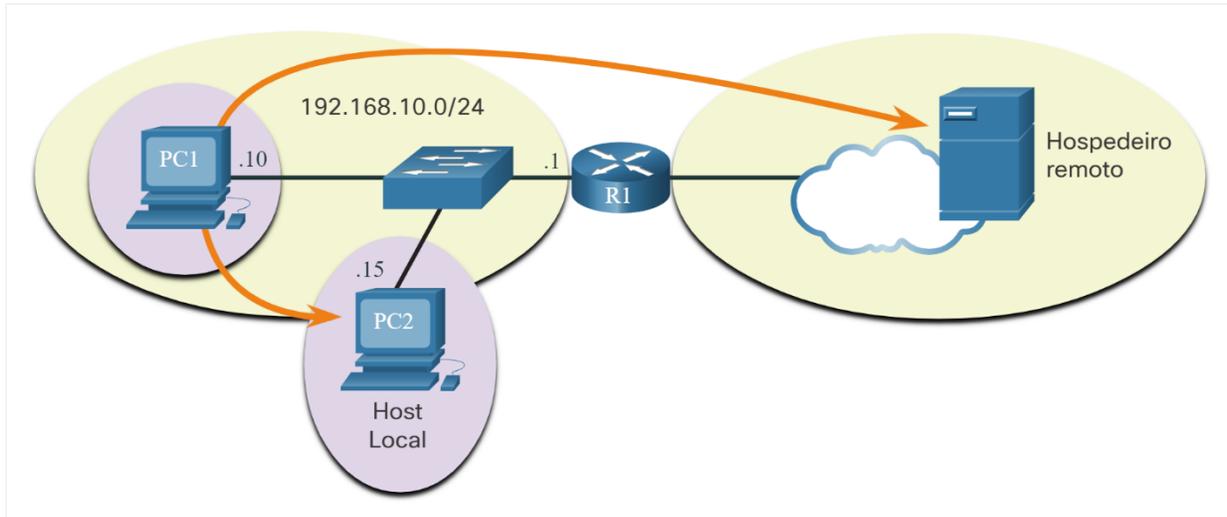
8.4.1 Decisão de Encaminhamento do Host

Com IPv4 e IPv6, os pacotes são sempre criados no host de origem. O host de origem deve ser capaz de direcionar o pacote para o host de destino. Para fazer isso, os dispositivos finais do host criam sua própria tabela de roteamento. Este tópico discute como os dispositivos finais usam tabelas de roteamento.

Outra função da camada de rede é direcionar pacotes entre hosts. Um host pode enviar um pacote para o seguinte:

- **Itself** - Um host pode fazer um ping a si mesmo, enviando um pacote para um endereço IPv4 especial de 127.0.0.1 ou um IPv6 address ::1, que é referido como a interface de loopback. O ping na interface de loopback testa a pilha de protocolos do TCP/IP no host.
- **Host local** - Este é um host de destino que está na mesma rede local que o host de envio. Os hosts de origem e destino compartilham o mesmo endereço de rede.
- **Host remoto** - Este é um host de destino em uma rede remota. Os hosts de origem e destino não compartilham o mesmo endereço de rede.

A figura ilustra a conexão PC1 a um host local na mesma rede e a um host remoto localizado em outra rede.



O diagrama mostra um host, PC1, conectando-se a um host local, PC2, na mesma rede e a um host remoto, um servidor, em outra rede. PC1 e PC2 estão conectados a um switch na rede 192.168.10.0/24. PC1 tem um endereço de .10 e PC2 tem um endereço de .15. O switch está conectado a um roteador, R1, no endereço .1. Do outro lado do R1 há uma conexão com a nuvem onde o host remoto reside. PC1R1.10.1PC2.15

Se um pacote é destinado a um host local ou a um host remoto é determinado pelo dispositivo final de origem. O dispositivo final de origem determina se o endereço IP de destino está na mesma rede em que o próprio dispositivo de origem está. O método de determinação varia de acordo com a versão IP:

- **Em IPv4** - O dispositivo de origem usa sua própria máscara de sub-rede juntamente com seu próprio endereço IPv4 e o endereço IPv4 de destino para fazer essa determinação.
- **Em IPv6** - O roteador local anuncia o endereço de rede local (prefixo) para todos os dispositivos na rede.

Em uma rede doméstica ou comercial, você pode ter vários dispositivos com e sem fio interconectados usando um dispositivo intermediário, como um switch LAN ou um ponto de acesso sem fio (WAP). Este dispositivo intermediário fornece interconexões entre hosts locais na rede local. Os hosts locais podem interagir entre si e compartilhar informações sem a necessidade de dispositivos adicionais. Se um host estiver enviando um pacote para um dispositivo configurado com a mesma rede IP que o dispositivo host, o pacote será simplesmente encaminhado para fora da interface do host, através do dispositivo intermediário e diretamente ao dispositivo de destino.

Obviamente, na maioria das situações, queremos que nossos dispositivos possam se conectar além do segmento de rede local, como em outras residências, empresas e na Internet. Os dispositivos que estão além do segmento de rede local são conhecidos como hosts remotos. Quando um dispositivo de origem envia um pacote a um dispositivo de destino remoto, é necessária a ajuda de roteadores e do roteamento. O roteamento é o processo de identificação do melhor caminho até um destino. O roteador conectado ao segmento de rede local é conhecido como gateway padrão (default gateway).

8.4.2 Gateway Padrão

O gateway padrão é o dispositivo de rede (ou seja, roteador ou switch da Camada 3) que pode rotear o tráfego para outras redes. Comparando a rede com uma sala, o gateway padrão é a porta. Se você quiser ir para outra sala (rede), vai precisar encontrar essa porta.

Em uma rede, um gateway padrão geralmente é um roteador com esses recursos:

- Ele possui um endereço IP local no mesmo intervalo de endereços que outros hosts na rede local.
- Ele pode aceitar dados na rede local e encaminhar dados para fora da rede local.
- Ele direciona o tráfego para outras redes.

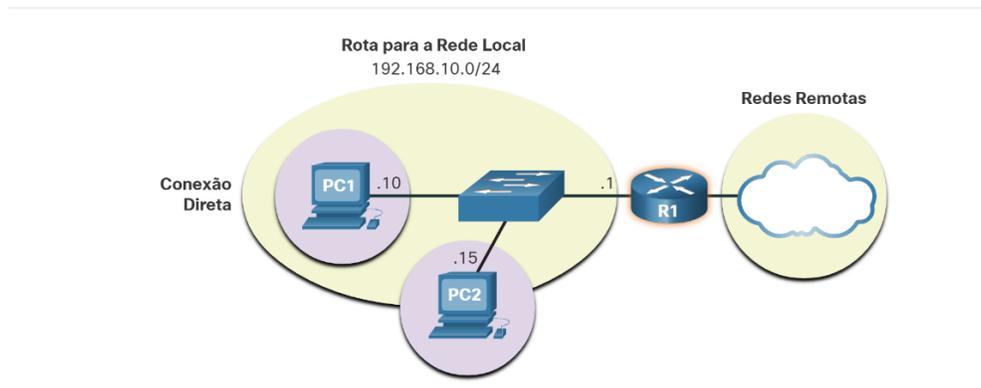
Um gateway padrão é necessário para enviar tráfego fora da rede local. O tráfego não pode ser encaminhado para fora da rede local se não houver gateway padrão, o endereço de gateway padrão não estiver configurado ou o gateway padrão estiver inativo.

8.4.3 Um host direciona para o gateway padrão

Uma tabela de roteamento de host normalmente inclui um gateway padrão. No IPv4, o host recebe o endereço IPv4 do gateway padrão dinamicamente do DHCP (Dynamic Host Configuration Protocol) ou configurado manualmente. No IPv6, o roteador anuncia o endereço de gateway padrão ou o host pode ser configurado manualmente.

Na figura, PC1 e PC2 são configurados com o endereço IPv4 de 192.168.10.1 como o gateway padrão.

O diagrama mostra dois hosts, PC1 e PC2, conectados a um switch na rede 192.168.10.0/24, a rota de rede local. O switch é conectado a um roteador, R1, que é conectado à nuvem que representa redes remotas. PC1 tem um endereço de .10, PC2 tem um endereço de .15 e a interface do roteador à qual o switch está conectado tem um endereço de .1. Os PCs, o switch e a interface do roteador têm uma conexão direta.



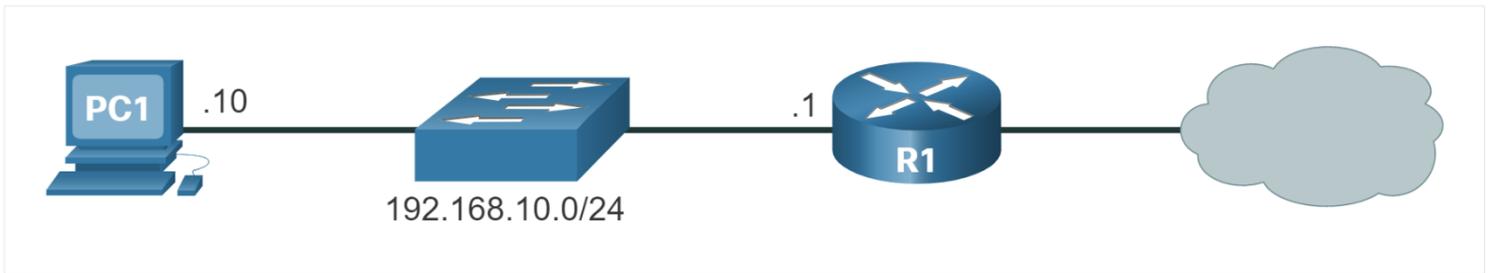
A configuração do gateway padrão cria uma rota padrão na tabela de roteamento do computador. Uma rota padrão é a rota ou o caminho que o computador usa quando tenta entrar em contato com uma rede remota.

Tanto PC1 quanto PC2 terão uma rota padrão para enviar todo o tráfego destinado a redes remotas para R1.

8.4.4 Tabelas de Roteamento dos Hosts

Em um host do Windows, o comando **route print** ou **netstat -r** pode ser usado para exibir a tabela de roteamento do host. Ambos os comandos geram a mesma saída. O resultado pode parecer confuso no começo, mas é bastante simples de entender.

A figura exibe uma topologia de exemplo e a saída gerada pelo **netstat -r** comando.



O diagrama mostra uma topologia de rede que consiste em um host, PC1, conectado a um switch na rede 192.168.10.0/24. O switch está conectado a um roteador, R1, que é então conectado à nuvem. O PC1 tem um endereço de 0,10 e a interface do roteador à qual o switch está conectado tem um endereço de .1.

Tabela de Roteamento IPv4 de PC1

```
C:\Users\PC1 > netstat -r
IPv4 Route Table
=====
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0 192.168.10.1 192.168.10.10 25
127.0.0.0 255.0.0.0 No link 127.0.0.1 306
127.0.0.1 255.255.255.255 On-Link 127.0.0.1 306
127.255.255.255 255.255.255.255 On-Link 127.0.0.1 306
192.168.10.0 255.255.255.0 No link 192.168.10.10 281
192.168.10.10 255.255.255.255 On-Link 192.168.10.10 281
192.168.10.255 255.255.255.255 On-Link 192.168.10.10 281
224.0.0.0 240.0.0.0 No link 127.0.0.1 306
224.0.0.0 240.0.0.0 No link 192.168.10.10 281
255.255.255.255 255.255.255.255 On-link 127.0.0.1 306
255.255.255.255 255.255.255.255 On-Link 192.168.10.10 281
```

Observação: A saída exibe apenas a tabela de rotas IPv4.

A inserção do comando **netstat -r** ou o comando equivalente **route print** exibe três seções relacionadas às conexões de rede TCP / IP atuais:

- **Lista de interfaces** - lista o endereço MAC (Media Access Control) e o número de interface atribuído de todas as interfaces com capacidade de rede no host, incluindo adaptadores Ethernet, Wi-Fi e Bluetooth.
- **Tabela de rotas IPv4** - lista todas as rotas IPv4 conhecidas, incluindo conexões diretas, rede local e rotas padrão locais.
- **Tabela de rotas IPv6** - lista todas as rotas IPv6 conhecidas, incluindo conexões diretas, rede local e rotas padrão locais.

8.4.5 Verifique seu entendimento - Como um host roteia

Verifique sua compreensão de como um host é roteado escolhendo a melhor resposta para as seguintes perguntas.

1. Qual declaração sobre decisões de encaminhamento de host é verdadeira?
 - Um host não pode fazer ping em si mesmo.
 - Um host de destino remoto está na mesma rede local que o host de envio.
 - Os hosts locais podem se alcançar sem a necessidade de um roteador.
 - O roteamento é habilitado em switches para descobrir o melhor caminho para um destino.
2. Qual instrução de gateway padrão é verdadeira?
 - Um gateway padrão é necessário para enviar pacotes para outros hosts na rede local.
 - O endereço de gateway padrão é o endereço IP de um switch em uma rede remota.

- O endereço de gateway padrão é o endereço IP do roteador na rede local.
- O tráfego só pode ser encaminhado para fora da rede local se não houver gateway padrão.

3. Quais dois comandos podem ser inseridos em um host Windows para exibir sua tabela de roteamento IPv4 e IPv6? (Escolha duas.)

- netroute -l
- netstat -r
- print route
- route print
- print net

1. Qual declaração sobre decisões de encaminhamento de host é verdadeira?

Você entendeu!

- Um host não pode fazer ping em si mesmo.
- Um host de destino remoto está na mesma rede local que o host de envio.
- Os hosts locais podem se alcançar sem a necessidade de um roteador.
- O roteamento é habilitado em switches para descobrir o melhor caminho para um destino.

2. Qual instrução de gateway padrão é verdadeira?

Você entendeu!

- Um gateway padrão é necessário para enviar pacotes para outros hosts na rede local.
- O endereço de gateway padrão é o endereço IP de um switch em uma rede remota.
- O endereço de gateway padrão é o endereço IP do roteador na rede local.
- O tráfego só pode ser encaminhado para fora da rede local se não houver gateway padrão.

3. Quais dois comandos podem ser inseridos em um host Windows para exibir sua tabela de roteamento IPv4 e IPv6? (Escolha duas.)

Você entendeu!

- netroute -l
- netstat -r
- print route
- route print
- print net

Bom trabalho!

Você identificou com sucesso as respostas corretas.

1. Não é necessário um roteador para encaminhar pacotes entre hosts locais na rede.
2. O gateway padrão é o endereço IP de um roteador na rede local.
3. Os comandos **netstat -r** e **route print** exibirá a tabela de roteamento de um host do Windows.

Você respondeu 3 das 3 perguntas corretamente.

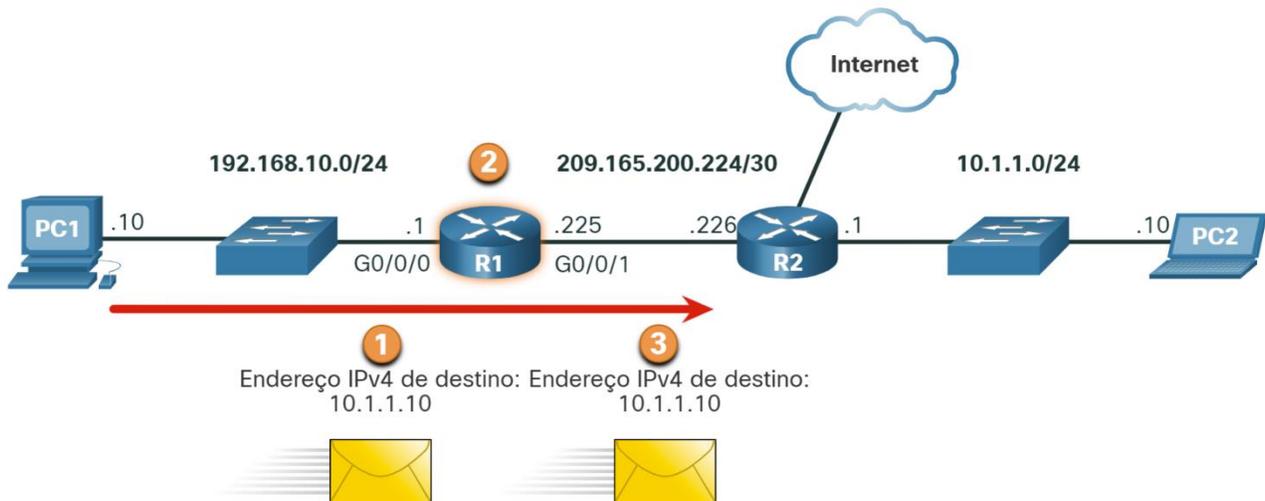
8.5.1 Decisão de Encaminhamento de Pacotes do Roteador

O tópico anterior discutiu tabelas de roteamento de host. A maioria das redes também contém roteadores, que são dispositivos intermediários. Os roteadores também contêm tabelas de roteamento. Este tópico aborda as operações do roteador na camada de rede. Quando um host envia um pacote para outro host, ele consulta sua tabela de roteamento para determinar para onde enviar o pacote. Se o host de destino estiver em uma rede remota, o pacote será encaminhado para o gateway padrão, que geralmente é o roteador local.

O que acontece quando um pacote chega na interface do roteador?

O roteador examina o endereço IP de destino do pacote e pesquisa sua tabela de roteamento para determinar para onde encaminhar o pacote. A tabela de roteamento contém uma lista de todos os endereços de rede conhecidos (prefixos) e para onde encaminhar o pacote. Essas entradas são conhecidas como entradas de rota ou rotas. O roteador encaminhará o pacote usando a melhor (mais longa) entrada de rota correspondente.

O diagrama é uma topologia de rede que mostra o que acontece com um pacote IPv4 à medida que é roteado entre redes. O host PC1, com um endereço de .10, está conectado a um switch na rede 192.168.10.0/24 que está conectado à interface G0/0/0 do roteador R1 com um endereço de .1. Rede 209.165.200.224/30 conecta a interface G0/0/1 em R1, endereço .225, a outro roteador, R2 no endereço .226. R2 está conectado a um switch na rede 10.1.1.0/24 ao qual o host PC2, endereço .10, está conectado. O R2 também possui uma conexão com a nuvem da Internet. Um pacote com o endereço IPv4 de destino 10.1.1.10 é enviado de PC1 para R1. Em seguida, o R1 envia o pacote com o endereço IPv4 de destino 10.1.1.10 para R2.



1. O pacote chega na interface Gigabit Ethernet 0/0/0 do roteador R1. R1 desencapsula o cabeçalho Ethernet da camada 2 e o trailer.
2. O roteador R1 examina o endereço IPv4 de destino do pacote e procura a melhor correspondência em sua tabela de roteamento IPv4. A entrada de rota indica que esse pacote deve ser encaminhado para o roteador R2.
3. O roteador R1 encapsula o pacote em um novo cabeçalho e trailer Ethernet e encaminha o pacote para o próximo roteador R2 de salto.

A tabela a seguir mostra as informações pertinentes da tabela de roteamento R1.

Tabela de Roteamento de R1

Rota	Próximo salto ou interface de saída
192.168.10.0 /24	G0/0/0
S209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2
Rota padrão 0.0.0.0/0	via R2

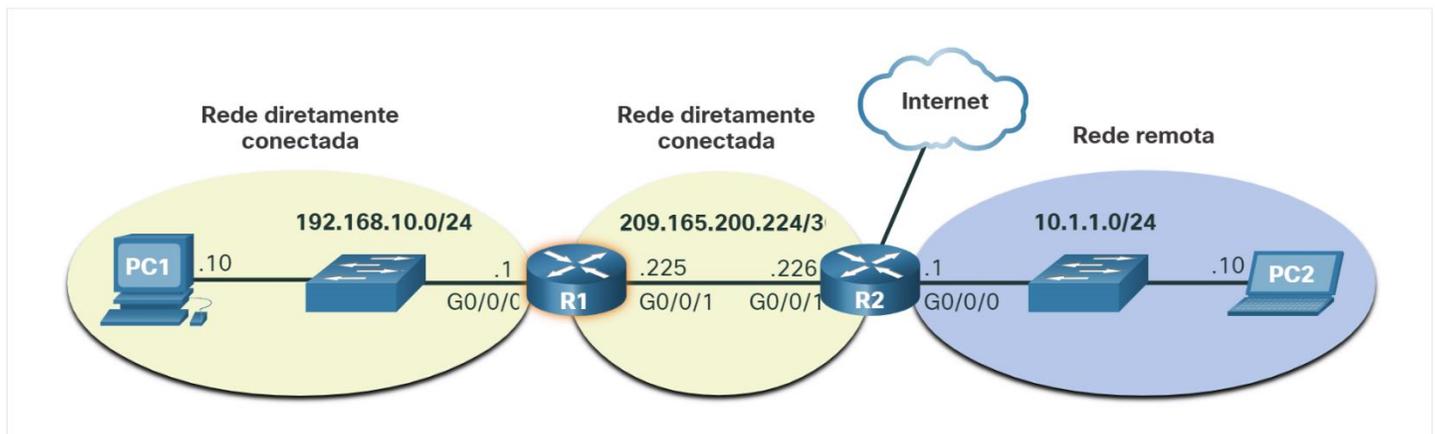
8.5.2 Tabela de Roteamento do Roteador IP

A tabela de roteamento do roteador contém entradas de rota de rede listando todos os possíveis destinos de rede conhecidos.

A tabela de roteamento armazena três tipos de entradas de rota:

- **Redes conectadas diretamente** - Essas entradas de rota de rede são interfaces de roteador ativas. Os roteadores adicionam uma rota diretamente conectada quando uma interface está configurada com um endereço IP e está ativada. Cada interface do roteador está conectada a um segmento de rede diferente. Na figura, as redes diretamente conectadas na tabela de roteamento IPv4 R1 seriam 192.168.10.0/24 e 209.165.200.224/30.
- **Redes remotas** - Essas entradas de rotas de rede são conectadas a outros roteadores. Os roteadores aprendem sobre redes remotas sendo explicitamente configurados por um administrador ou trocando informações de rota usando um protocolo de roteamento dinâmico. Na figura, a rede remota na tabela de roteamento IPv4 R1 seria 10.1.1.0/24.
- **Rota padrão** — Como um host, a maioria dos roteadores também inclui uma entrada de rota padrão, um gateway de último recurso. A rota padrão é usada quando não há correspondência melhor (mais) na tabela de roteamento IP. Na figura, a tabela de roteamento IPv4 R1 provavelmente incluiria uma rota padrão para encaminhar todos os pacotes para o roteador R2.

A figura identifica as redes remotas e diretamente conectadas ao roteador R1.



O R1 tem duas redes de conexão direta:

- 192.168.10.0/24
- 209.165.200.224/30

R1 também tem redes remotas (ou seja, 10.1.1.0/24 e internet) que ele pode aprender sobre.

O diagrama é uma topologia de rede que identifica redes diretamente conectadas e redes remotas de um roteador. O host PC1, com um endereço de .10, está conectado a um switch na rede 192.168.10.0/24 que está conectado à interface G0/0/0 do roteador R1 com um endereço de .1. Rede 209.165.200.224/30 conecta a interface G0/0/1 em R1, endereço .225, a outro roteador, R2 no endereço .226 em G0/0/1. R2 está conectado a um switch na rede 10.1.1.0/24 ao qual o host PC2, endereço .10, está conectado. O R2 também possui uma conexão com uma nuvem da Internet. As redes 192.168.10.0/24 e 209.165.200.224/30 são mostradas como redes conectadas diretamente à R1 e à rede 10.1.1.0/24 (deve ser 10.1.1.0/24?) é mostrado como uma rede remota para R2.

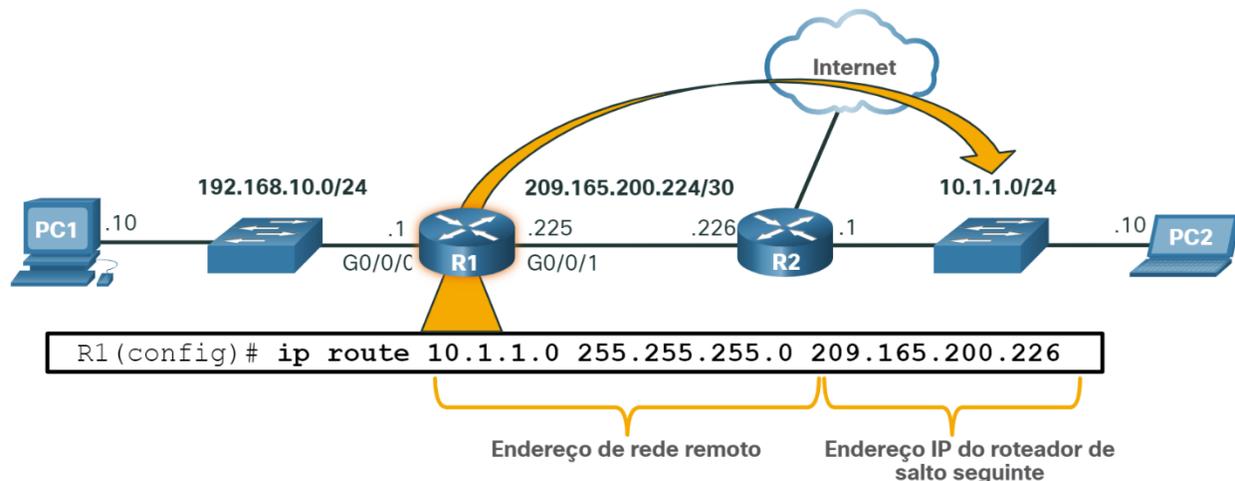
Um roteador pode aprender sobre redes remotas de duas maneiras:

- **Manualmente** - As redes remotas são inseridas manualmente na tabela de rotas usando rotas estáticas.
- **Dinamicamente** - As rotas remotas são aprendidas automaticamente usando um protocolo de roteamento dinâmico.

8.5.3 Roteamento estático

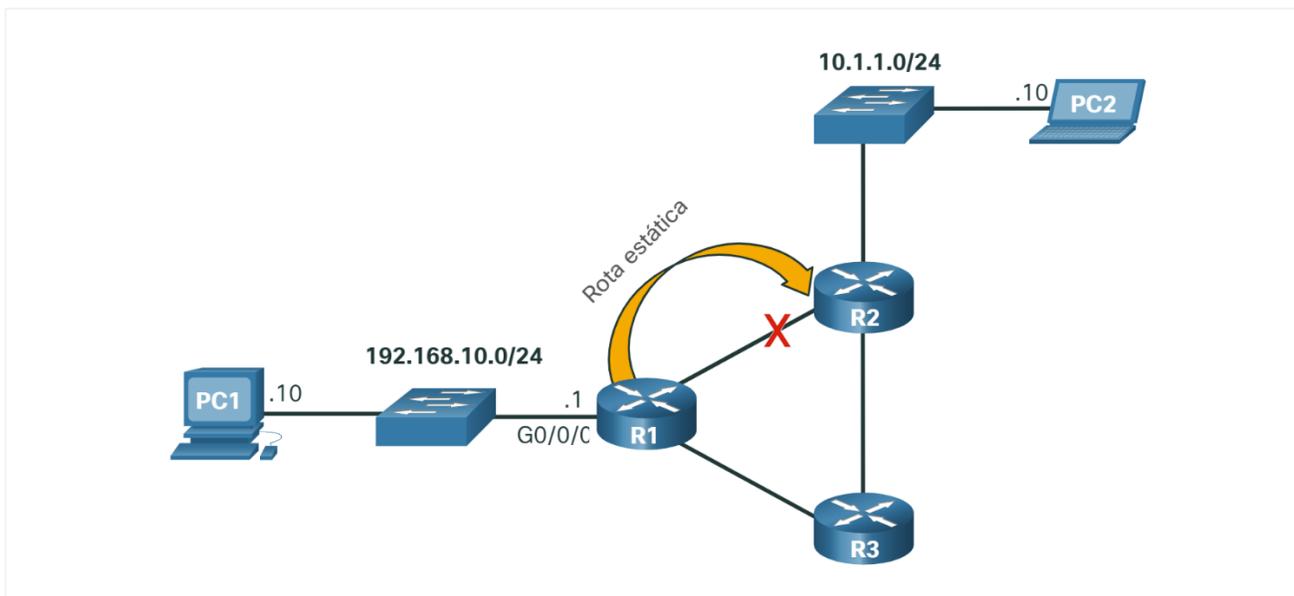
Rotas estáticas são entradas de rota configuradas manualmente. A figura mostra um exemplo de uma rota estática configurada manualmente no roteador R1. A rota estática inclui o endereço de rede remota e o endereço IP do roteador de salto seguinte.

O diagrama é uma topologia de rede que mostra uma configuração de rota estática para alcançar uma rede remota. O host PC1, com um endereço de .10, está conectado a um switch na rede 192.168.10.0/24 que está conectado à interface G0/0/0 do roteador R1 com um endereço de .1. Rede 209.165.200.224/30 conecta a interface G0/0/1 em R1, endereço .225, a outro roteador, R2 no endereço .226. R2 tem uma interface com o endereço .1 conectada a um switch na rede 10.1.1.0/24 ao qual o host PC2, endereço .10, está conectado. O R2 também possui uma conexão com uma nuvem da Internet. Uma configuração de rota estática no R1 para a rede 10.1.1.0/24 diz: R1(config)#ip route 10.1.1.0 255.255.255.0 209.165.200.226. Na configuração, 10.1.1.0 255.255.255.0 é rotulado como rede remota e 209.165.200.226 é rotulado como endereço IP do próximo roteador de salto.



O R1 é configurado manualmente com uma rota estática para alcançar a rede 10.1.1.0/24. Se esse caminho mudar, R1 exigirá uma nova rota estática.

Se houver uma alteração na topologia da rede, a rota estática não será atualizada automaticamente e deverá ser reconfigurada manualmente. Por exemplo, na figura R1 tem uma rota estática para alcançar a rede 10.1.1.0/24 via R2. Se esse caminho não estiver mais disponível, R1 precisaria ser reconfigurado com uma nova rota estática para a rede 10.1.1.0/24 via R3. Portanto, o roteador R3 precisaria ter uma entrada de rota em sua tabela de roteamento para enviar pacotes destinados a 10.1.1.0/24 para R2.



O diagrama é uma topologia de rede mostrando um link com falha em uma rota estática. O host PC1, com um endereço de .10, está conectado a um switch na rede 192.168.10.0/24 que está conectado à interface G0 / 0/0 do roteador R1 com um endereço de .1. R1 está conectado ao roteador R2 e roteador R3 que também são direcionados conectados. R2 está conectado a um switch na rede 10.1.1.0/24 ao qual é o host PC2, endereço .10, está conectado. Uma rota estática foi configurada em R1 que aponta para R2 como o próximo salto. Um X vermelho indica que este link falhou. Rota estática

Se a rota de R1 via R2 não estiver mais disponível, uma nova rota estática via R3 precisaria ser configurada. Uma rota estática não se ajusta automaticamente para alterações de topologia.

O roteamento estático tem as seguintes características:

- Uma rota estática deve ser configurada manualmente.
- O administrador precisa reconfigurar uma rota estática se houver uma alteração na topologia e a rota estática não for mais viável.
- Uma rota estática é apropriada para uma rede pequena e quando há poucos ou nenhum vínculo redundante.
- Uma rota estática é comumente usada com um protocolo de roteamento dinâmico para configurar uma rota padrão.

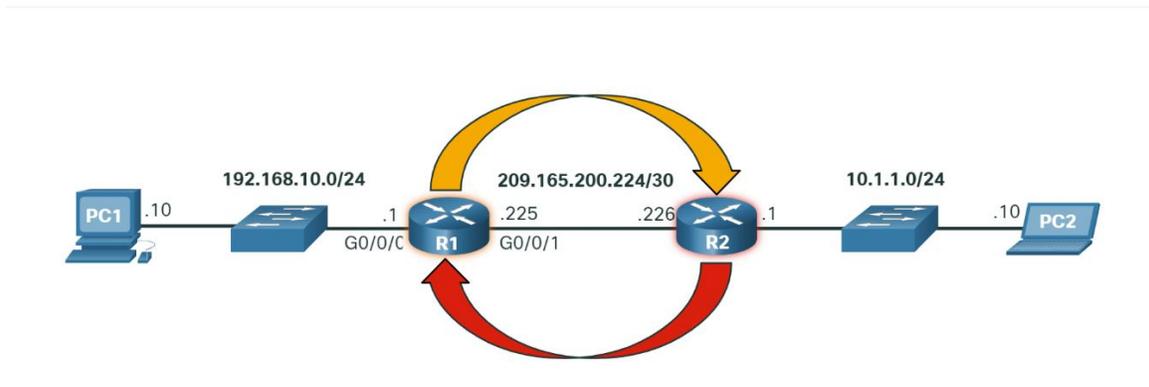
8.5.4 Roteamento dinâmico

Um protocolo de roteamento dinâmico permite que os roteadores aprendam automaticamente sobre redes remotas, incluindo uma rota padrão, de outros roteadores. Os roteadores que usam protocolos de roteamento dinâmico compartilham automaticamente informações de roteamento com outros roteadores e compensam qualquer alteração de topologia sem envolver o administrador da rede. Se houver uma alteração na topologia de rede, os roteadores compartilham essas informações usando o protocolo de roteamento dinâmico e atualizam automaticamente suas tabelas de roteamento.

Os protocolos de roteamento dinâmico incluem OSPF e Enhanced Interior Gateway Routing Protocol (EIGRP). A figura mostra um exemplo de roteadores R1 e R2 compartilhando automaticamente informações de rede usando o protocolo de roteamento OSPF.

O diagrama é uma topologia de rede que mostra roteadores usando protocolos de roteamento dinâmico para trocar informações. O host PC1, com um endereço de .10, está conectado a um switch na rede 192.168.10.0/24 que está conectado à interface G0 / 0/0 do roteador R1 com um endereço de .1. Rede 209.165.200.224/30 conecta uma interface G0 / 0/1 em R1, endereço .225, outro roteador, R2 no endereço .226. O R2 tem uma interface com o endereço .1 conectado a um switch na rede 10.1.1.0/24 para qual host PC2, endereço .10, está conectado.

As setas mostram R1 e R2 compartilhando informações entre si.
10.1.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0PC2R2R1PC1



- R1 está usando o protocolo de roteamento OSPF para informar R2 sobre a rede 192.168.10.0/24.
- R2 está usando o protocolo de roteamento OSPF para deixar R1 saber sobre a rede 10.1.1.0/24.

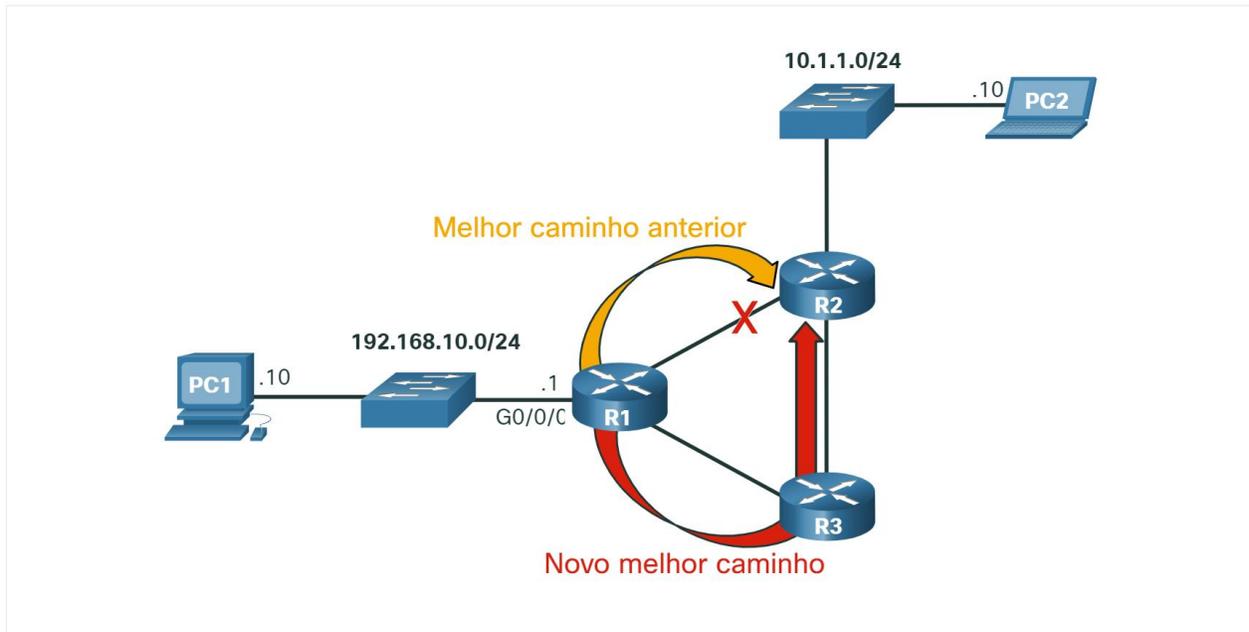
A configuração básica requer apenas que o administrador de rede habilite as redes conectadas diretamente dentro do protocolo de roteamento dinâmico. O protocolo de roteamento dinâmico fará automaticamente o seguinte:

- Descobrir redes remotas;
- Manter as informações de roteamento atualizadas;
- Escolha o melhor caminho para as redes de destino;
- Tente encontrar um novo melhor caminho se o caminho atual não estiver mais disponível.

Quando um roteador é configurado manualmente com uma rota estática ou aprende sobre uma rede remota dinamicamente usando um protocolo de roteamento dinâmico, o endereço de rede remota e o endereço de próximo salto são inseridos na tabela de roteamento IP. Conforme mostrado na figura, se houver uma alteração na topologia de rede, os roteadores ajustarão automaticamente e tentarão encontrar um novo melhor caminho.

O diagrama mostra uma topologia de rede na qual os roteadores que usam protocolos de roteamento dinâmico estão ajustando os melhores caminhos após uma alteração de topologia. O host PC1, com um endereço de .10, está conectado a um switch na rede 192.168.10.0/24 que está conectado à interface G0 / 0/0 do roteador R1 com um endereço de .1. R1 está conectado ao roteador R2 e roteador R3 que também são direcionados. R2 está conectado a um switch na rede 10.1.1.0/24 ao qual é o host PC2, endereço .10, está conectado. Um X vermelho indica que o link entre R1 e R2, rotulado como o melhor caminho anterior, falhou. Um novo melhor caminho é mostrado indo de R1 para R3 para R2.

.10.1192.168.10.0/24G0/0/0PC2R2R1PC1R310.1.1.0/24.10



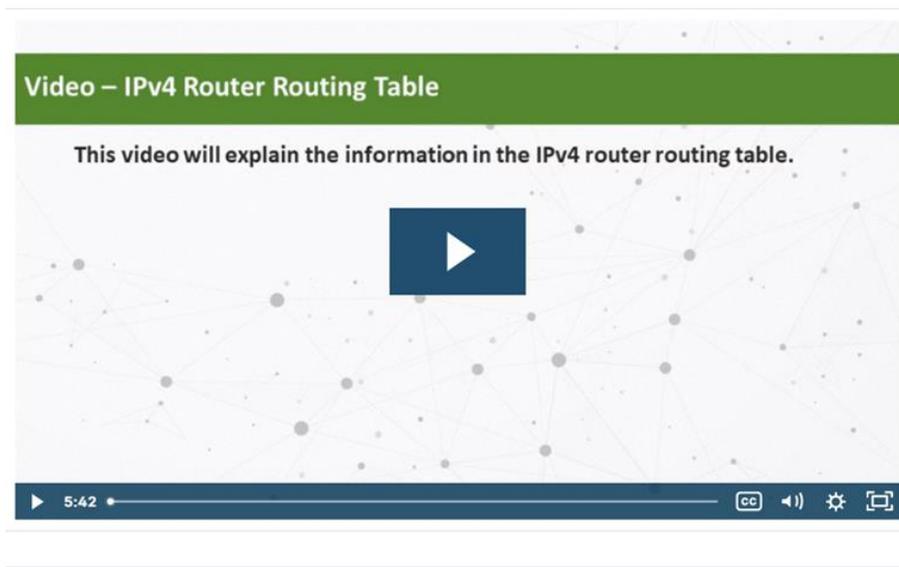
R1, R2 e R3 estão usando o protocolo de roteamento dinâmico OSPF. Se houver uma alteração na topologia de rede, eles poderão ajustar automaticamente para encontrar um novo caminho melhor.

Observação: É comum que alguns roteadores usem uma combinação de rotas estáticas e um protocolo de roteamento dinâmico.

8.5.5 Tabelas de roteamento de roteador de vídeo- IPv4

Ao contrário de uma tabela de roteamento de computadores host, não há títulos de coluna que identifiquem as informações contidas na tabela de roteamento de um roteador. É importante compreender o significado dos diferentes itens incluídos em cada entrada da tabela de roteamento.

Clique em Reproduzir na figura para ver a apresentação de uma tabela de roteamento IPv4.



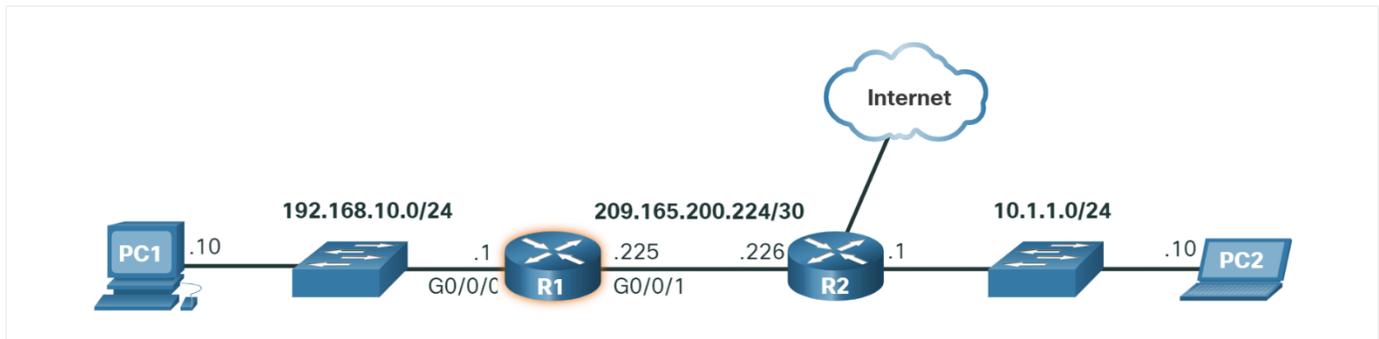
Duração: 5:42

8.5.6 Introdução a uma tabela de roteamento IPv4

Observe na figura que R2 está conectado à internet. Portanto, o administrador configurou R1 com uma rota estática padrão enviando pacotes para R2 quando não há nenhuma entrada específica na tabela de roteamento que

corresponda ao endereço IP de destino. R1 e R2 também estão usando roteamento OSPF para anunciar redes conectadas diretamente.

O host PC1, com um endereço de .10, está conectado a um switch na rede 192.168.10.0/24 que está conectado à interface G0 / 0/0 do roteador R1 com um endereço de .1. Rede 209.165.200.224/30 conecta uma interface G0 / 0/1 em R1, endereço .225, outro roteador, R2 no endereço .226. R2 está conectado a um switch na rede 10.1.1.0/24 ao qual é o host PC2, endereço .10, está conectado. O R2 também possui uma conexão com uma nuvem da Internet. 10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0PC2R2R1P



```
R1# show ip route
Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - área inter IS-IS, * - padrão candidato, U - rota estática por usuário
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - rota replicada, % - substituição do próximo salto, p - substituições de Pfr
Gateway de último recurso é 209.165.200.226 para a rede 0.0.0.0
S* 0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
    10.0.0.0/24 está em sub-rede, 1 sub-redes
O 10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigaBeTheNet0/0/1
    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 está conectado diretamente, GigabitEthernet0 / 0/0
L 192.168.10.1/32 está conectado diretamente, GigabitEthernet0 / 0/0
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 está conectado diretamente, GigabitEthernet0 / 0/1
L 209.165.200.225/32 está conectado diretamente, GigabitEthernet0 / 0/1
R1#
```

O comando de modo EXEC **show ip route** privilegiado é usado para exibir a tabela de roteamento IPv4 em um roteador Cisco IOS. O exemplo mostra a tabela de roteamento IPv4 do roteador R1. No início de cada entrada de tabela de roteamento é um código que é usado para identificar o tipo de rota ou como a rota foi aprendida. As fontes comuns de rotas (códigos) incluem:

- **L** - Endereço IP da interface local diretamente conectado
- **C** - Rede diretamente conectada
- **S** — A rota estática foi configurada manualmente por um administrador
- **O** - OSPF
- **D** - EIGRP

A tabela de roteamento exibe todas as rotas de destino IPv4 conhecidas para R1.

Uma rota diretamente conectada é criada automaticamente quando uma interface do roteador é configurada com informações de endereço IP e é ativada. O roteador adiciona duas entradas de rota com os códigos C (ou seja, a rede conectada) e L (ou seja, o endereço IP da interface local da rede conectada). As entradas de rota também identificam a interface de saída a ser usada para alcançar a rede. As duas redes diretamente conectadas neste exemplo são 192.168.10.0/24 e 209.165.200.224/30.

Os roteadores R1 e R2 também estão usando o protocolo de roteamento dinâmico OSPF para trocar informações do roteador. Na tabela de roteamento de exemplo, R1 tem uma entrada de rota para a rede 10.1.1.0/24 que aprendeu dinamicamente do roteador R2 por meio do protocolo de roteamento OSPF.

Uma rota padrão tem um endereço de rede de todos os zeros. Por exemplo, o endereço de rede IPv4 é 0.0.0.0. Uma entrada de rota estática na tabela de roteamento começa com um código de S*, conforme destacado no exemplo.

8.5.7 Verifique sua compreensão - Introdução ao roteamento

Verifique sua compreensão da introdução ao roteamento e selecione a melhor resposta para as seguintes perguntas.

1. Qual é o comando usado em um roteador Cisco IOS para exibir a tabela de roteamento?
 - netstart -r
 - route print
 - show ip route
 - show routing table
2. O que um código de “O” indica ao lado de uma rota na tabela de roteamento?
 - uma rota diretamente conectada
 - uma rota com uma distância administrativa de 0
 - um portal de último recurso
 - uma rota aprendida dinamicamente do OSPF
3. Esse tipo de rota também é conhecido como gateway de último recurso.
 - rota estática
 - rota remota
 - rota padrão
 - rota diretamente conectada
4. Qual é uma característica das rotas estáticas?
 - Eles são configurados manualmente.
 - Eles são anunciados para vizinhos diretamente conectados.
 - Eles são apropriados quando há muitos links redundantes.
 - Eles se ajustam automaticamente a uma alteração na topologia de rede.
5. Verdadeiro ou falso? Um roteador pode ser configurado com uma combinação de rotas estáticas e um protocolo de roteamento dinâmico.
 - Verdadeiro
 - Falso

 **Bom trabalho!**

Você identificou com sucesso as respostas corretas.

1. O **show ip route** comando é usado para visualizar a tabela de roteamento em um roteador Cisco.
2. Os códigos no início de cada entrada da tabela de roteamento são usados para identificar o tipo de rota ou como a rota foi aprendida. Um código "O" indica que a rota foi aprendida no OSPF.
3. Uma rota padrão também é conhecida como gateway de último recurso.
4. As rotas estáticas são configuradas manualmente e não se ajustam às alterações na topologia da rede e não são anunciadas para roteadores vizinhos.
5. A resposta correta é verdadeira. Os roteadores podem ser configurados com rotas estáticas e com um protocolo de roteamento dinâmico.

Você respondeu 5 das 5 perguntas corretamente.

1. Qual é o comando usado em um roteador Cisco IOS para exibir a tabela de roteamento?

Você entendeu!

- netstart -r
- route print
- show ip route
- show routing table

2. O que um código de "O" indica ao lado de uma rota na tabela de roteamento?

Você entendeu!

- uma rota diretamente conectada
- uma rota com uma distância administrativa de 0
- um portal de último recurso
- uma rota aprendida dinamicamente do OSPF

3. Esse tipo de rota também é conhecido como gateway de último recurso.

Você entendeu!

- rota estática
- rota remota
- rota padrão
- rota diretamente conectada

4. Qual é uma característica das rotas estáticas?

Você entendeu!

- Eles são configurados manualmente.
- Eles são anunciados para vizinhos diretamente conectados.
- Eles são apropriados quando há muitos links redundantes.
- Eles se ajustam automaticamente a uma alteração na topologia de rede.

5. Verdadeiro ou falso? Um roteador pode ser configurado com uma combinação de rotas estáticas e um protocolo de roteamento dinâmico.

Você entendeu!

- Verdadeiro
- Falso

8.6 Módulo Prática e Quiz

8.6.1 O que eu aprendi neste módulo?

Características da camada de rede

A camada de rede (Camada OSI 3) fornece serviços para permitir que dispositivos finais troquem dados entre redes. IPv4 e IPv6 são os principais protocolos de comunicação de camada de rede. A camada de rede também inclui o protocolo de roteamento OSPF e protocolos de mensagens, como ICMP. Os protocolos de camada de rede executam quatro operações básicas: endereçamento de dispositivos finais, encapsulamento, roteamento e desencapsulamento. IPv4 e IPv6 especificam a estrutura de pacotes e o processamento usado para transportar os dados de um host para outro host. O IP encapsula o segmento da camada de transporte adicionando um cabeçalho IP, usado para entregar o pacote ao host de destino. O cabeçalho IP é examinado por dispositivos da Camada 3 (ou seja, roteadores) à medida que viaja através de uma rede até seu destino. As características do IP são que ele é sem conexão, melhor esforço e independente de mídia. O IP não tem conexão, o que significa que nenhuma conexão ponta a ponta é criada pelo IP antes dos dados enviados. O protocolo IP não garante que o pacote enviado seja, de fato, recebido. Esta é a definição da característica não confiável, ou melhor esforço. O IP opera independentemente da mídia que transporta os dados nas camadas inferiores da pilha de protocolos.

Pacote IPv4

Um cabeçalho de pacote IPv4 consiste em campos que contêm informações sobre o pacote. Esses campos contêm números binários que são examinados pelo processo da Camada 3. Os valores binários de cada campo identificam várias configurações do pacote IP. Campos significativos no cabeçalho IPv6 incluem: versão, DS, soma de verificação de cabeçalho, TTL, protocolo e os endereços IPv4 de origem e destino.

Pacote IPv6

O IPv6 foi projetado para superar as limitações do IPv4, incluindo: esgotamento de endereços IPv4, falta de conectividade de ponta a ponta e maior complexidade da rede. O IPv6 aumenta o espaço de endereço disponível, melhora o manuseio de pacotes e elimina a necessidade de NAT. Os campos no cabeçalho do pacote IPv6 incluem: versão, classe de tráfego, rótulo de fluxo, comprimento da carga útil, próximo cabeçalho, limite de salto e os endereços IPv6 de origem e destino.

Como um host é roteado

Um host pode enviar um pacote para si mesmo, outro host local e um host remoto. No IPv4, o dispositivo de origem usa sua própria máscara de sub-rede juntamente com seu próprio endereço IPv4 e o endereço IPv4 de destino para determinar se o host de destino está na mesma rede. No IPv6, o roteador local anuncia o endereço de rede local (prefixo) para todos os dispositivos na rede, para fazer essa determinação. O gateway padrão é o dispositivo de rede (ou seja, roteador) que pode rotear o tráfego para outras redes. Em uma rede, um gateway padrão geralmente é um roteador que tem um endereço IP local no mesmo intervalo de endereços que outros hosts na rede local, pode aceitar dados na rede local e encaminhar dados para fora da rede local e rotear o tráfego para outras redes. Uma tabela de roteamento do host normalmente inclui um gateway padrão. No IPv4, o host recebe o endereço IPv4 do gateway padrão dinamicamente via DHCP ou é configurado manualmente. No IPv6, o roteador anuncia o endereço de gateway padrão ou o host pode ser configurado manualmente. Em um host do Windows, o comando **route print** ou **netstat -r** pode ser usado para exibir a tabela de roteamento do host.

Introdução ao roteamento

Quando um host envia um pacote para outro host, ele consulta sua tabela de roteamento para determinar para onde enviar o pacote. Se o host de destino estiver em uma rede remota, o pacote será encaminhado para o gateway padrão, que geralmente é o roteador local. O que acontece quando um pacote chega na interface do roteador? O roteador examina o endereço IP de destino do pacote e pesquisa sua tabela de roteamento para determinar para onde encaminhar o pacote. A tabela de roteamento contém uma lista de todos os endereços de rede conhecidos (prefixos) e para onde encaminhar o pacote. Essas entradas são conhecidas como entradas de rota ou rotas. O roteador encaminhará o pacote usando a melhor (mais longa) entrada de rota correspondente. A tabela de roteamento de um roteador armazena três tipos de entradas de rota: redes conectadas diretamente, redes remotas e uma rota padrão. Os roteadores aprendem sobre redes remotas manualmente ou dinamicamente usando um protocolo de roteamento dinâmico. Rotas estáticas são entradas de rota configuradas manualmente. As rotas estáticas incluem o endereço de rede remota e o endereço IP do roteador de salto seguinte. OSPF e EIGRP são dois protocolos de roteamento dinâmico. O comando de modo EXEC **show ip route** privilegiado é usado para exibir a tabela de roteamento IPv4 em um roteador Cisco IOS. No início de uma tabela de roteamento IPv4 é um código que é usado para identificar o tipo de rota ou como a rota foi aprendida. As fontes comuns de rotas (códigos) incluem:

- L** - Endereço IP da interface local diretamente conectado
- C** - Rede diretamente conectada
- S** - A rota estática foi configurada manualmente por um administrador
- O** - Abrir caminho mais curto primeiro (OSPF)
- D** - Protocolo de roteamento de gateway interno aprimorado (EIGRP)

8.6.2 Teste de Módulo - Camada de Rede

1. Qual comando pode ser usado em um host Windows para exibir a tabela de roteamento?
 - Endereço IP origem
 - Endereço de link de dados de destino
 - endereço IP de destino
 - Endereço de link de dados de origem
2. Quais informações são adicionadas à camada 3 do modelo OSI durante o encapsulamento?
 - Protocolo de aplicação origem e destino
 - Endereço IP origem e destino
 - Número da porta de origem e destino
 - Endereços MAC origem e destino
3. Como a camada de rede usa o valor de MTU?
 - A camada de rede depende das camadas de nível superior para determinar o MTU.
 - A camada de rede depende da camada de link de dados para definir o MTU e ajustará a velocidade da transmissão para acomodá-lo.
 - Para aumentar a velocidade de entrega, a camada de rede ignora o MTU.
 - O MTU é transmitido para a camada de rede pela camada de link de dados.
4. Um roteador recebe um pacote da interface Gigabit 0/0 e determina que o pacote precisa ser encaminhado para fora da interface Gigabit 0/1. O que o roteador fará a seguir?
 - O cabeçalho IPv6 é mais simples que o cabeçalho IPv4, o que melhora o processamento de pacotes.
 - O espaço de endereço do IPv6 é quatro vezes maior que o do IPv4.
 - Os endereços IPv6 utilizam um endereçamento plano de 128 bits, ao contrário dos endereços IPv4, que utilizam endereçamento hierárquico de 32 bits.
 - Tanto o IPv4 quanto o IPv6 são compatíveis com a autenticação, mas somente o IPv6 aceita os recursos de privacidade.
5. Qual declaração descreve com precisão uma característica do IPv4?
 - Um cabeçalho IPv4 tem menos campos do que um cabeçalho IPv6 tem.
 - Todos os endereços IPv4 podem ser atribuídos a hosts.
 - IPv4 suporta nativamente IPsec.
 - O IPv4 tem um espaço de endereço de 32 bits.
6. Quando um roteador recebe um pacote, quais informações devem ser analisadas para que o pacote seja encaminhado a um destino remoto?
 - Endereço MAC destino
 - Endereço IP origem
 - Endereço MAC origem
 - Endereço IP destino
7. Um computador tem de enviar um pacote para um anfitrião de destino na mesma LAN. Como o pacote será enviado?
 - O pacote será enviado diretamente para o host de destino.
 - O pacote será enviado apenas para o gateway padrão.
 - O pacote será enviado primeiro para o gateway padrão e, em seguida, dependendo da resposta do gateway, ele pode ser enviado para o host de destino.
 - O pacote será enviado primeiro para o gateway padrão e, em seguida, a partir do gateway padrão, ele será enviado diretamente para o host de destino.
8. Qual endereço IPv4 um host pode usar para fazer ping na Interface de Loopback?
 - O espaço de endereço do IPv6 é quatro vezes maior que o do IPv4.
 - 126.0.0.1
 - O cabeçalho IPv6 é mais simples que o cabeçalho IPv4, o que melhora o processamento de pacotes.
 - Tanto o IPv4 quanto o IPv6 são compatíveis com a autenticação, mas somente o IPv6 aceita os recursos de privacidade.

9. Quando um protocolo sem conexão está em uso em uma camada inferior do modelo OSI, como os dados ausentes são detectados e retransmitidos, se necessário?
- O processo de entrega de melhor-esforço garante que todos os pacotes enviados sejam recebidos.
 - Protocolos orientados a conexão da camada superior rastreiam os dados recebidos e podem requisitar a retransmissão desses protocolos no host emissor.
 - Protocolos IP de camada de rede gerenciam as sessões de comunicação, se serviços de transporte orientados a conexão não estiverem disponíveis.
 - Confirmações sem conexão são usadas para requisitar a retransmissão.
10. Qual foi o motivo para a criação e a implementação do IPv6?
- Para aliviar a redução de endereços IPv4
 - Para permitir o suporte de NAT para o endereçamento privado
 - Para fornecer mais espaço de endereço no registro de nomes de Internet
 - Para facilitar a leitura de um endereço de 32 bits
11. Quais informações são usadas pelos roteadores para encaminhar um pacote de dados para seu destino?
- Endereço de link de dados de destino
 - endereço IP de destino
 - Endereço IP origem
 - Endereço de link de dados de origem
12. Qual campo em um cabeçalho de pacote IPv4 normalmente permanecerá o mesmo durante sua transmissão?
- 126.0.0.1
 - Comprimento do Pacote
 - Vida útil (TTL)
 - Endereço Destino
13. Qual campo em um pacote IPv6 é usado pelo roteador para determinar se um pacote expirou e deve ser descartado?
- Limite de saltos
 - Para facilitar a leitura de um endereço de 32 bits
 - Endereço inacessível
 - Nenhuma rota para o destino

1. Qual comando pode ser usado em um host Windows para exibir a tabela de roteamento?

✔ Tópico 8.4.0 - Em um host do Windows, os comandos **route print** ou **netstat -r** podem ser usados para exibir a tabela de roteamento de host. O **show ip route** comando é usado em um roteador para exibir sua tabela de roteamento. O **netstat -s** comando é usado para exibir estatísticas por protocolo. O **tracert** comando é usado para exibir o caminho que um pacote viaja para seu destino.

- Endereço de link de dados de destino
- Endereço IP origem
- endereço IP de destino
- Endereço de link de dados de origem

2. Quais informações são adicionadas à camada 3 do modelo OSI durante o encapsulamento?

✔ Tópico 8.1.0 - IP é um protocolo de Camada 3. Os dispositivos de camada 3 podem abrir o cabeçalho da camada 3 para inspecionar o cabeçalho da camada que contém informações relativas ao IP, incluindo os endereços IP origem e destino.

- Número da porta de origem e destino
- Endereços MAC origem e destino
- Protocolo de aplicação origem e destino
- Endereço IP origem e destino

3. Como a camada de rede usa o valor de MTU?

✔ Tópico 8.1.0 - A camada de enlace de dados indica para a camada de rede o MTU do meio que está sendo usado. A camada de rede usa essas informações para determinar o maior tamanho possível para o envio do pacote. Quando os pacotes são recebidos em um meio e enviados em um meio físico com uma MTU menor, o dispositivo da camada de rede pode fragmentar o pacote para acomodar o menor tamanho.

- Para aumentar a velocidade de entrega, a camada de rede ignora o MTU.
- A camada de rede depende da camada de link de dados para definir o MTU e ajustará a velocidade da transmissão para acomodá-lo.
- A camada de rede depende das camadas de nível superior para determinar o MTU.
- O MTU é transmitido para a camada de rede pela camada de link de dados.

4. Um roteador recebe um pacote da interface Gigabit 0/0 e determina que o pacote precisa ser encaminhado para fora da interface Gigabit 0/1. O que o roteador fará a seguir?

✔ Tópico 8.5.0 - Uma vez que um roteador recebe um pacote e procura dentro do cabeçalho para determinar a rede de destino, o roteador compara a rede de destino com a tabela de roteamento para determinar se o pacote deve ser roteado ou descartado. Se roteado, o roteador anexará um novo cabeçalho de Camada 2 com base na tecnologia usada pela porta de saída usada. O pacote é então roteado para fora da porta de destino conforme designado pela tabela de roteamento. O cache ARP é usado para corresponder um endereço IP com um endereço MAC.

- O espaço de endereço do IPv6 é quatro vezes maior que o do IPv4.
- Os endereços IPv6 utilizam um endereçamento plano de 128 bits, ao contrário dos endereços IPv4, que utilizam endereçamento hierárquico de 32 bits.
- O cabeçalho IPv6 é mais simples que o cabeçalho IPv4, o que melhora o processamento de pacotes.
- Tanto o IPv4 quanto o IPv6 são compatíveis com a autenticação, mas somente o IPv6 aceita os recursos de privacidade.

5. Qual declaração descreve com precisão uma característica do IPv4?

✔ Tópico 8.2.0 - O IPv4 tem um espaço de endereço de 32 bits, fornecendo 4.294.967.296 endereços exclusivos, mas apenas 3.7 bilhões são atribuíveis, um limite devido à reserva de endereço para multicasting e testes. O IPv4 não fornece suporte nativo para IPsec. O IPv6 tem um cabeçalho simplificado com menos campos do que o IPv4 tem.

- Todos os endereços IPv4 podem ser atribuídos a hosts.
- O IPv4 tem um espaço de endereço de 32 bits.
- Um cabeçalho IPv4 tem menos campos do que um cabeçalho IPv6 tem.
- IPv4 suporta nativamente IPsec.

6. Quando um roteador recebe um pacote, quais informações devem ser analisadas para que o pacote seja encaminhado a um destino remoto?

✔ Tópico 8.4.0 - Quando um roteador recebe um pacote, ele examina o endereço de destino do pacote e usa a tabela de roteamento para procurar o melhor caminho para essa rede.

- Endereço MAC origem
- Endereço IP destino
- Endereço MAC destino
- Endereço IP origem

7. Um computador tem de enviar um pacote para um host de destino na mesma LAN. Como o pacote será enviado?

Tópico 8.4.0 - Se o host de destino estiver na mesma LAN que o host de origem, não há necessidade de um gateway padrão. Um gateway padrão é necessário se um pacote precisar ser enviado fora da LAN.

- O pacote será enviado apenas para o gateway padrão.
- O pacote será enviado primeiro para o gateway padrão e, em seguida, dependendo da resposta do gateway, ele pode ser enviado para o host de destino.
- O pacote será enviado primeiro para o gateway padrão e, em seguida, a partir do gateway padrão, ele será enviado diretamente para o host de destino.
- O pacote será enviado diretamente para o host de destino.

8. Qual endereço IPv4 um host pode usar para fazer ping na Interface de Loopback?

Tópico 8.4.0 - Um host pode executar ping na interface de envio de retorno enviando um pacote para um endereço IPv4 especial na rede 127.0.0.0/8.

- 126.0.0.1
- O cabeçalho IPv6 é mais simples que o cabeçalho IPv4, o que melhora o processamento de pacotes.
- Tanto o IPv4 quanto o IPv6 são compatíveis com a autenticação, mas somente o IPv6 aceita os recursos de privacidade.
- O espaço de endereço do IPv6 é quatro vezes maior que o do IPv4.

9. Quando um protocolo sem conexão está em uso em uma camada inferior do modelo OSI, como os dados ausentes são detectados e retransmitidos, se necessário?

Tópico 8.1.0 - Quando protocolos sem conexão estão em uso em uma camada inferior do modelo OSI, os protocolos de nível superior podem precisar trabalhar juntos nos hosts de envio e recebimento para contabilizar e retransmitir dados perdidos. Em alguns casos, isto não é necessário, pois para algumas aplicações é tolerável um determinado volume de perda de dados.

- Protocolos IP de camada de rede gerenciam as sessões de comunicação, se serviços de transporte orientados a conexão não estiverem disponíveis.
- Protocolos orientados a conexão da camada superior rastreiam os dados recebidos e podem requisitar a retransmissão desses protocolos no host emissor.
- O processo de entrega de melhor-esforço garante que todos os pacotes enviados sejam recebidos.
- Confirmações sem conexão são usadas para requisitar a retransmissão.

10. Qual foi o motivo para a criação e a implementação do IPv6?

Tópico 8.3.0 - O espaço de endereçamento IPv4 é esgotado pelo rápido crescimento da Internet e dos dispositivos conectados à Internet. O IPv6 expande o espaço do endereçamento IP ao aumentar o comprimento do endereço de 32 bits para 128 bits, o que deve fornecer endereços suficientes para as futuras necessidades de crescimento da Internet por muitos anos.

- Para aliviar a redução de endereços IPv4
- Para permitir o suporte de NAT para o endereçamento privado
- Para facilitar a leitura de um endereço de 32 bits
- Para fornecer mais espaço de endereço no registro de nomes de Internet

11. Quais informações são usadas pelos roteadores para encaminhar um pacote de dados para seu destino?

Tópico 8.4.0 - O endereço IP de destino é o endereço IP do dispositivo receptor. Esse endereço IP é usado por roteadores para encaminhar o pacote para seu destino.

- Endereço de link de dados de origem
- Endereço IP origem
- Endereço de link de dados de destino
- endereço IP de destino

12. Qual campo em um cabeçalho de pacote IPv4 normalmente permanecerá o mesmo durante sua transmissão?

Tópico 8.1.0 - O valor no campo Endereço de Destino em um cabeçalho IPv4 permanecerá o mesmo durante sua transmissão. As outras opções podem mudar durante a sua transmissão.

- Vida útil (TTL)
- Comprimento do Pacote
- 126.0.0.1
- Endereço Destino

13. Qual campo em um pacote IPv6 é usado pelo roteador para determinar se um pacote expirou e deve ser descartado?

Tópico 8.3.0 - O ICMPv6, como o IPv4, envia uma mensagem de tempo excedido se o roteador não puder encaminhar um pacote IPv6 porque o pacote expirou. No entanto, o pacote IPv6 não tem um campo TTL. Em vez disso, ele usa o campo Limite de Hop para determinar se o pacote expirou.

- Nenhuma rota para o destino
- Limite de saltos
- Para facilitar a leitura de um endereço de 32 bits
- Endereço inacessível