**Introdução**

5.0.1

**Por que devo cursar este módulo?**

Todos nós nos comunicamos em redes diariamente. Olhar para as redes sociais, transmitir vídeos ou pesquisar informações na internet são atividades comuns nas quais normalmente não pensamos muito. No entanto, inúmeros processos tecnológicos estão em ação para nos trazer o conteúdo que queremos da web.

Neste módulo, você aprenderá como os protocolos de rede funcionam juntos para nos permitir solicitar informações e retornar essas informações para nós através da rede.

5.0.2

**O que vou aprender neste módulo?**

**Título do módulo**: protocolos de rede

**Objetivo do módulo**: Explicar como os protocolos permitem operações de rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Processo de comunicação de rede | Explique a operação básica das comunicações em rede de dados. |
| Protocolos de comunicação | Explicar como os protocolos viabilizam as operações de rede. |
| Encapsulamento de dados | Explicar como o encapsulamento permite que os dados sejam transportados pela rede. |

# Processo de comunicação de rede

5.1.1

## Redes de Vários Tamanhos

Existem redes de vários tamanhos. Eles variam de redes simples, que consistem em dois computadores, a redes que conectam milhões de dispositivos.

As redes domésticas simples permitem que você compartilhe recursos, como impressoras, documentos, imagens e música, entre alguns dispositivos finais locais.

As redes de pequeno escritório e escritório doméstico (SOHO) permitem que as pessoas trabalhem em casa ou em um escritório remoto. Muitos trabalhadores independentes usam esses tipos de redes para anunciar e vender produtos, pedir suprimentos e se comunicar com os clientes.

Empresas e grandes organizações usam redes para fornecer consolidação, armazenamento e acesso a informações em servidores de rede. As redes fornecem e-mail, mensagens instantâneas e colaboração entre funcionários. Muitas organizações usam a conexão de sua rede à Internet para fornecer produtos e serviços aos clientes.

A internet é a maior rede existente. Na verdade, o termo Internet significa uma “rede de redes”. É uma coleção de redes públicas e privadas interconectadas.

Em pequenas empresas e residências, muitos computadores funcionam como servidores e clientes na rede. Esse tipo de rede é chamado de rede ponto a ponto.

**Redes domésticas pequenas**

As redes domésticas pequenas conectam alguns computadores entre si e com a Internet.



**Redes para pequenos escritórios e escritórios domésticos**

A rede SOHO permite que computadores em um escritório em casa ou em um escritório remoto se conectem a uma rede corporativa, ou acessem recursos compartilhados centralizados.



**Redes médias a grandes**

Redes de médio a grande porte, como as usadas por empresas e escolas, podem ter muitos locais com centenas ou milhares de hosts interconectados

**Rede Mundial**

A internet é uma rede de redes que conecta centenas de milhões de computadores em todo o mundo.

redes mundiais mostrando um mapa global com cinco edifícios

5.1.2

## Comunicações cliente-servidor

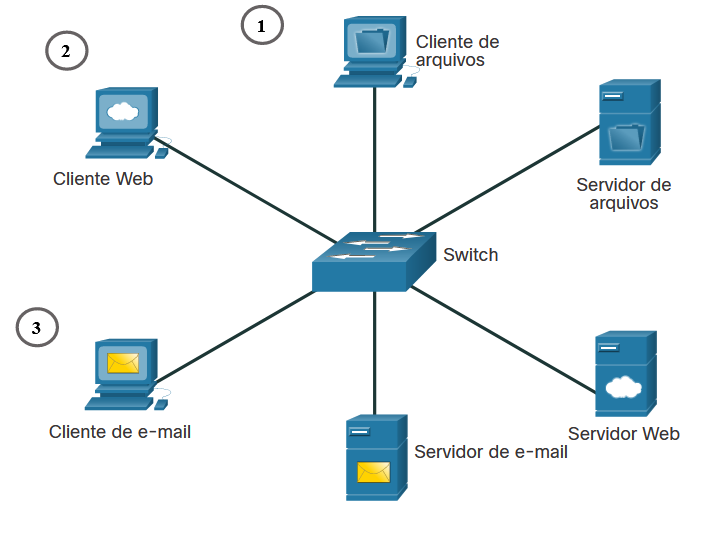
Todos os computadores que estão conectados a uma rede e participam diretamente da comunicação em rede são classificados como hosts. Os hosts também são chamados de dispositivos finais, terminais ou nós. Grande parte da interação entre dispositivos finais é o tráfego cliente-servidor. Por exemplo, quando você acessa uma página da Web na Internet, seu navegador (o cliente) está acessando um servidor. Quando você envia uma mensagem de e-mail, seu cliente de e-mail se conectará a um servidor de e-mail.

Servidores são simplesmente computadores com software especializado. Este software permite que os servidores forneçam informações a outros dispositivos finais na rede. Um servidor pode ser de propósito único, fornecendo apenas um serviço, como páginas da Web. Um servidor pode ser multiuso, fornecendo uma variedade de serviços, como páginas da Web, e-mail e transferências de arquivos.

Os computadores cliente têm software instalado, como navegadores da Web, clientes de email e aplicativos de transferência de arquivos. Este software permite que eles solicitem e exibam as informações obtidas do servidor. Um único computador pode também executar vários tipos de software cliente. Por exemplo, um usuário pode verificar e-mail e visualizar uma página da web enquanto ouve rádio na Internet.

* **Servidor de arquivos** - o servidor de arquivos armazena arquivos corporativos e de usuários em um local central.
* **Servidor Web** - O servidor web executa software de servidor web que permite que muitos computadores acessem páginas da web.
* **Servidor de e-mail** - O servidor de e-mail executa o software de servidor de e-mail que permite que os e-mails sejam enviados e recebidos.

A figura mostra um switch com computadores com fio conectados a ele. O computador superior é um cliente de arquivos e à direita dele está o servidor de arquivos. Ao lado do cliente de arquivo há um número um. As palavras associadas são as seguintes: O servidor de arquivos armazena arquivos corporativos e de usuários em um local central. Os dispositivos cliente acessam esses arquivos com software cliente, como o Windows Explorer. Há também um computador rotulado como cliente web e um servidor web. O número 2 ao lado do cliente da web tem as seguintes palavras: O servidor da web executa o software do servidor da web e os clientes usam o software do navegador, como o Windows Internet Explorer, para acessar páginas da web no servidor. Há um computador cliente de e-mail e um servidor de e-mail. O cliente de e-mail tem o número 3 ao lado com as seguintes palavras: O servidor de e-mail executa o software do servidor de e-mail e os clientes usam seu software cliente de e-mail, como o Microsoft Outlook, para acessar o e-mail no servidor.

1. O servidor de arquivos armazena arquivos corporativos e de usuários em um local central. Os dispositivos clientes acessam esses arquivos com softwares clientes, como o Windows Explorer.
2. O servidor da Web executa um software de servidor da Web e os clientes usam seu software de navegador, como o Windows Microsoft Edge, para acessar páginas da Web no servidor.
3. O Servidor de e-mail executa o software do servidor de e-mail. Os clientes usam o software de cliente de e-mail, como o Microsoft Outlook, para acessar os e-mails no servidor.

[Ir para o conteúdo](https://contenthub.netacad.com/cyberops/5.0.1?lng=pt-br#chunks-container)

*                                                    
*         
*           
*           
*                 
*                                   

1. Protocolos de rede
2. Processo de comunicação de rede

# Processo de comunicação de rede

5.1.1

## Redes de Vários Tamanhos

Existem redes de vários tamanhos. Eles variam de redes simples, que consistem em dois computadores, a redes que conectam milhões de dispositivos.

As redes domésticas simples permitem que você compartilhe recursos, como impressoras, documentos, imagens e música, entre alguns dispositivos finais locais.

As redes de pequeno escritório e escritório doméstico (SOHO) permitem que as pessoas trabalhem em casa ou em um escritório remoto. Muitos trabalhadores independentes usam esses tipos de redes para anunciar e vender produtos, pedir suprimentos e se comunicar com os clientes.

Empresas e grandes organizações usam redes para fornecer consolidação, armazenamento e acesso a informações em servidores de rede. As redes fornecem e-mail, mensagens instantâneas e colaboração entre funcionários. Muitas organizações usam a conexão de sua rede à Internet para fornecer produtos e serviços aos clientes.

A internet é a maior rede existente. Na verdade, o termo Internet significa uma “rede de redes”. É uma coleção de redes públicas e privadas interconectadas.

Em pequenas empresas e residências, muitos computadores funcionam como servidores e clientes na rede. Esse tipo de rede é chamado de rede ponto a ponto.

Clique em cada botão abaixo para obter mais informações.

**Rede Mundial**

A internet é uma rede de redes que conecta centenas de milhões de computadores em todo o mundo.

redes mundiais mostrando um mapa global com cinco edifícios

5.1.2

## Comunicações cliente-servidor

Todos os computadores que estão conectados a uma rede e participam diretamente da comunicação em rede são classificados como hosts. Os hosts também são chamados de dispositivos finais, terminais ou nós. Grande parte da interação entre dispositivos finais é o tráfego cliente-servidor. Por exemplo, quando você acessa uma página da Web na Internet, seu navegador (o cliente) está acessando um servidor. Quando você envia uma mensagem de e-mail, seu cliente de e-mail se conectará a um servidor de e-mail.

Servidores são simplesmente computadores com software especializado. Este software permite que os servidores forneçam informações a outros dispositivos finais na rede. Um servidor pode ser de propósito único, fornecendo apenas um serviço, como páginas da Web. Um servidor pode ser multiuso, fornecendo uma variedade de serviços, como páginas da Web, e-mail e transferências de arquivos.

Os computadores cliente têm software instalado, como navegadores da Web, clientes de email e aplicativos de transferência de arquivos. Este software permite que eles solicitem e exibam as informações obtidas do servidor. Um único computador pode também executar vários tipos de software cliente. Por exemplo, um usuário pode verificar e-mail e visualizar uma página da web enquanto ouve rádio na Internet.

* **Servidor de arquivos** - o servidor de arquivos armazena arquivos corporativos e de usuários em um local central.
* **Servidor Web** - O servidor web executa software de servidor web que permite que muitos computadores acessem páginas da web.
* **Servidor de e-mail** - O servidor de e-mail executa o software de servidor de e-mail que permite que os e-mails sejam enviados e recebidos.

A figura mostra um switch com computadores com fio conectados a ele. O computador superior é um cliente de arquivos e à direita dele está o servidor de arquivos. Ao lado do cliente de arquivo há um número um. As palavras associadas são as seguintes: O servidor de arquivos armazena arquivos corporativos e de usuários em um local central. Os dispositivos cliente acessam esses arquivos com software cliente, como o Windows Explorer. Há também um computador rotulado como cliente web e um servidor web. O número 2 ao lado do cliente da web tem as seguintes palavras: O servidor da web executa o software do servidor da web e os clientes usam o software do navegador, como o Windows Internet Explorer, para acessar páginas da web no servidor. Há um computador cliente de e-mail e um servidor de e-mail. O cliente de e-mail tem o número 3 ao lado com as seguintes palavras: O servidor de e-mail executa o software do servidor de e-mail e os clientes usam seu software cliente de e-mail, como o Microsoft Outlook, para acessar o e-mail no servidor.

3 2

1

Servidor de e-mailServidor WebCliente de e-mailCliente WebCliente de arquivosServidor de arquivosSwitch

1. O servidor de arquivos armazena arquivos corporativos e de usuários em um local central. Os dispositivos clientes acessam esses arquivos com softwares clientes, como o Windows Explorer.
2. O servidor da Web executa um software de servidor da Web e os clientes usam seu software de navegador, como o Windows Microsoft Edge, para acessar páginas da Web no servidor.
3. O Servidor de e-mail executa o software do servidor de e-mail. Os clientes usam o software de cliente de e-mail, como o Microsoft Outlook, para acessar os e-mails no servidor.

5.1.3

## Sessões Típicas

Aluno

Um usuário típico de rede na escola, em casa ou no escritório normalmente usa algum tipo de dispositivo de computação para estabelecer muitas conexões com servidores de rede. Esses servidores podem estar localizados na mesma sala ou em todo o mundo. Vejamos algumas sessões típicas de comunicação em rede.

Terry é uma estudante do ensino médio cuja escola começou recentemente um programa “traga seu próprio dispositivo” (BYOD). Os alunos são incentivados a usar seus telefones celulares ou outros dispositivos, como tablets ou laptops, para acessar recursos de aprendizagem. Terry acaba de receber uma tarefa na aula de artes linguísticas para pesquisar os efeitos da Primeira Guerra Mundial sobre a literatura e arte da época. Ela insere os termos de pesquisa que escolheu em um aplicativo de mecanismo de busca que ela abriu em seu celular.

Terry conectou o telefone dela à rede Wi-Fi da escola. Sua pesquisa é enviada de seu telefone para a rede da escola sem fio. Antes que sua busca possa ser enviada, os dados devem ser endereçados para que ele possa encontrar seu caminho de volta para Terry. Seus termos de pesquisa são então representados como uma cadeia de dados binários que foi codificada em ondas de rádio. Sua seqüência de pesquisa é então convertida em sinais elétricos que viajam na rede com fio da escola até que eles cheguem ao local em que a rede da escola se conecta à rede do provedor de serviços de Internet (ISP). Uma combinação de tecnologias leva a busca de Terry para o site do motor de busca.

Por exemplo, os dados de Terry fluem com os dados de milhares de outros usuários ao longo de uma rede de fibra óptica que conecta o ISP de Terry com os vários outros ISPs, incluindo o ISP que é usado pela empresa do mecanismo de busca. Eventualmente, a string de busca de Terry entra no site da empresa do mecanismo de busca e é processada por seus poderosos servidores. Os resultados são então codificados e endereçados à escola de Terry e seu dispositivo.

Todas essas transições e conexões acontecem em uma fração de segundo, e Terry começou seu caminho para aprender sobre seu assunto.



Jogador

Michelle adora jogos de computador. Ela tem um poderoso console de jogos que ela usa para jogar contra outros jogadores, assistir filmes e reproduzir música. Michelle conecta seu console de jogos diretamente à sua rede com um cabo de rede de cobre.

A rede de Michelle, como muitas redes domésticas, se conecta a um ISP usando um roteador e um modem a cabo. Estes dispositivos permitem que a rede doméstica da Michelle se conecte a uma rede de TV a cabo que pertence ao ISP da Michelle. Os cabos da vizinhança da Michelle ligam-se a um ponto central num poste telefónico e ligam-se a uma rede de fibra óptica. Esta rede de fibra óptica conecta muitos bairros que são servidos pelo ISP de Michelle.

Todos esses cabos de fibra óptica se conectam a serviços de telecomunicações que fornecem acesso às conexões de alta capacidade. Essas conexões permitem que milhares de usuários em residências, escritórios governamentais e empresas conectem destinos de internet em todo o mundo.

Michelle conectou seu console de jogos a uma empresa que hospeda um jogo online muito popular. Michelle está registrada na empresa, e seus servidores acompanham as pontuações, experiências e ativos de jogos de Michelle. As ações de Michelle em seu jogo se tornam dados que são enviados para a rede de jogadores. Os movimentos de Michelle são divididos em grupos de dados binários que cada um consistem em uma cadeia de zeros e uns. Informações que identificam Michelle, o jogo que ela está jogando e a localização de rede de Michelle são adicionadas aos dados do jogo. Os dados que representam o jogo de Michelle são enviados em alta velocidade para a rede do provedor de jogos. Os resultados são devolvidos a Michelle na forma de gráficos e sons.

Tudo isso acontece tão rapidamente que Michelle pode competir com centenas de outros jogadores em tempo real.

Cirurgião

Dr. Ismael Awad é um oncologista que realiza cirurgia em pacientes com câncer. Ele freqüentemente precisa consultar radiologistas e outros especialistas em casos de pacientes. O hospital para o qual o Dr. Awad trabalha assina um serviço especial chamado nuvem. A nuvem permite que dados médicos, incluindo raios-X e ressonâncias magnéticas de pacientes, sejam armazenados em um local central que é acessado pela Internet. Desta forma, o hospital não precisa gerenciar registros de pacientes em papel e filmes de raios-X.

Quando um paciente faz um raio-X, a imagem é digitalizada como dados do computador. O raio-X é então preparado por computadores hospitalares para ser enviado para o serviço de nuvem médica. Como a segurança é muito importante ao trabalhar com dados médicos, o hospital usa serviços de rede que criptografam os dados da imagem e as informações do paciente. Esses dados criptografados não podem ser interceptados e lidos à medida que viajam pela Internet para os data centers do provedor de serviços de nuvem. Os dados são endereçados para que possam ser roteados para o data center do provedor de nuvem para alcançar os serviços corretos que fornecem armazenamento e recuperação de imagens digitais de alta resolução.

Dr. Awad e a equipe de atendimento do paciente podem se conectar a este serviço especial, se reunir com outros médicos em audioconferências e discutir registros de pacientes para decidir sobre o melhor tratamento que pode ser fornecido ao paciente. Dr. Awad pode trabalhar com especialistas de diversos locais para visualizar as imagens médicas e outros dados de pacientes e discutir o caso.

Toda essa interação é digital e ocorre usando serviços em rede que são fornecidos pelo serviço de nuvem médica.

5.1.4

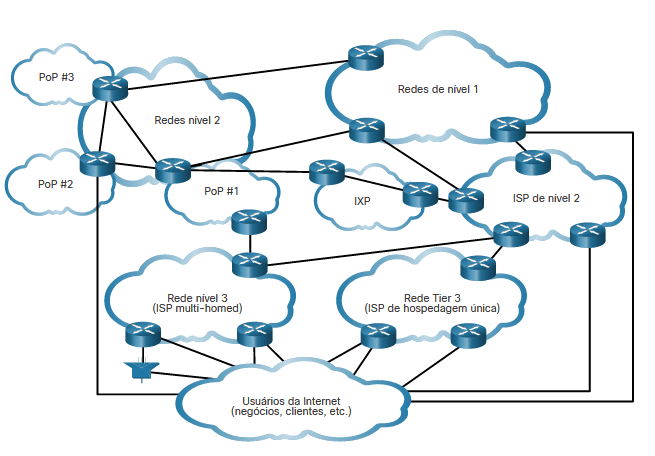
**Traçando o Caminho**

Nós tendemos a pensar sobre as redes de dados que usamos em nossas vidas diárias como pensamos em dirigir um carro. Nós realmente não nos importamos com o que acontece no motor, desde que o carro nos leve para onde queremos ir. No entanto, assim como o mecânico de um carro conhece os detalhes de como um carro opera, analistas de segurança cibernética precisam ter uma compreensão profunda de como as redes operam.

Quando nos conectamos a um site para ler mídias sociais ou fazer compras, raramente nos preocupamos com como nossos dados chegam ao site e como os dados do site nos acessam. Não estamos cientes das muitas tecnologias que nos permitem usar a internet. Uma combinação de cabos de cobre e fibra óptica que passam por terra e sob o oceano transportam tráfego de dados. Tecnologias sem fio e satélite de alta velocidade também são usadas. Essas conexões conectam instalações de telecomunicações e provedores de serviços de internet (ISP) que são distribuídos em todo o mundo, como mostrado na figura. Esses ISPs globais de Nível 1 e Nível 2 conectam partes da Internet, geralmente por meio de um Ponto de Troca de Internet (IXP). Redes maiores se conectarão a redes Nível 2 por meio de um Ponto de Presença (PoP), que geralmente é um local no edifício onde as conexões físicas com o ISP são feitas. Os ISPs de Nível 3 conectam residências e empresas à Internet.

Devido às diferentes relações entre ISPs e empresas de telecomunicações, o tráfego de um computador para um servidor de Internet pode tomar muitos caminhos. O tráfego de um usuário em um país pode tomar um caminho muito indireto para chegar ao seu destino. O tráfego pode primeiro viajar do ISP local para uma instalação que tenha conexões com muitos outros ISPs. O tráfego de internet de um usuário pode ir muitas centenas de milhas em uma direção apenas para ser roteado em uma direção completamente diferente para chegar ao seu destino. Parte do tráfego pode tomar certas rotas para chegar ao destino e, em seguida, tomar rotas completamente diferentes para retornar.

Os analistas de segurança cibernética devem ser capazes de determinar a origem do tráfego que entra na rede e o destino do tráfego que a deixa. Entender o caminho que o tráfego de rede leva é essencial para isso.



# Protocolos de comunicação

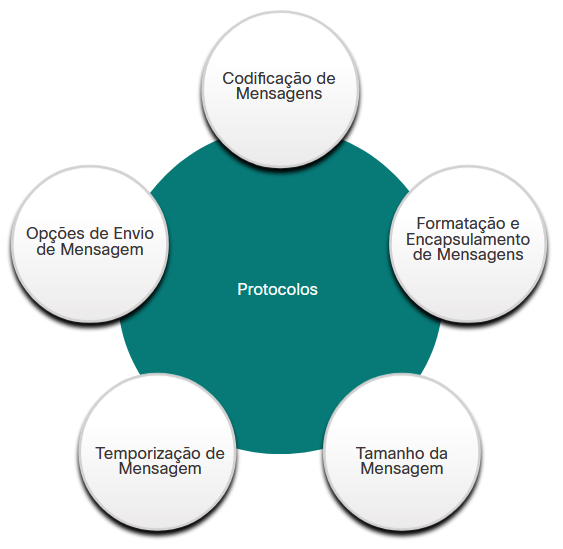
5.2.1

## O que são Protocolos?

Simplesmente ter uma conexão física com ou sem fio entre os dispositivos finais não é suficiente para permitir a comunicação. Para que ocorra comunicação, os dispositivos devem saber “como” se comunicar. A comunicação, seja cara a cara ou em rede, é governada por regras chamadas de protocolos. Esses protocolos são específicos para o tipo de método de comunicação em questão.

Por exemplo, considere duas pessoas se comunicando cara a cara. Antes da comunicação, devem concordar sobre como se comunicar. Se a comunicação for através de voz, devem primeiro acordar o idioma. Em seguida, quando há uma mensagem para compartilhar, eles devem formatar a mensagem de forma que seja compreensível. Por exemplo, se alguém usa o idioma inglês, mas a estrutura de frases for fraca, a mensagem poderá facilmente ser mal interpretada.

Da mesma forma, os protocolos de rede especificam muitos recursos da comunicação de rede, como mostrado na figura.



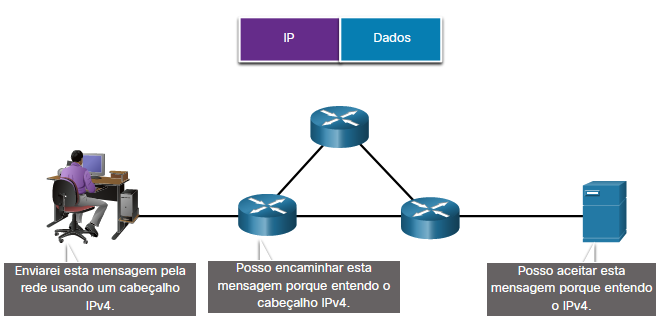
5.2.2

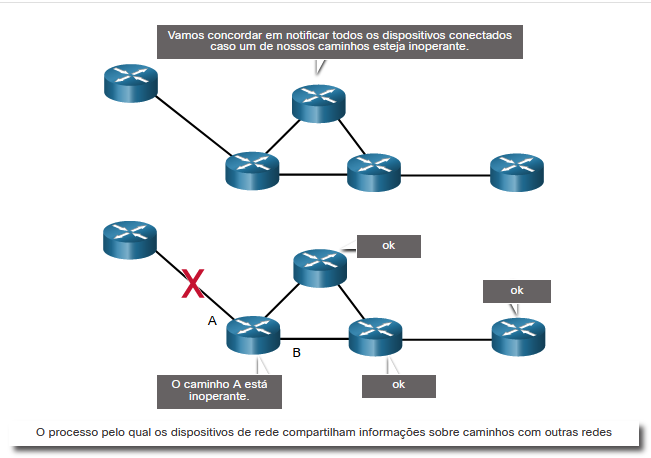
**Protocolos de rede**

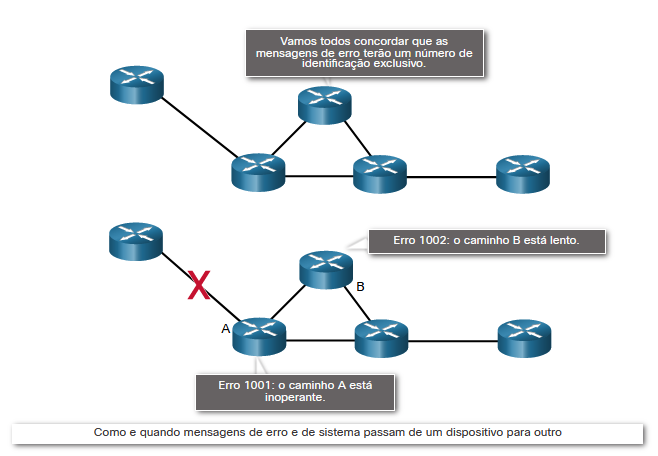
Os protocolos de rede fornecem os meios para que os computadores se comuniquem em redes. Os protocolos de rede determinam as opções de codificação, formatação, encapsulamento, tamanho, tempo e entrega da mensagem. Os protocolos de rede definem um formato e um conjunto de regras comuns para a troca de mensagens entre dispositivos. Estes são alguns protocolos de rede comuns: Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP) e Internet Protocol (IP). Como analista de segurança cibernética, você deve estar muito familiarizado com a estrutura dos dados de protocolo e como os protocolos funcionam nas comunicações de rede.

**Observação**: neste curso, IP se refere aos pr

otocolos IPv4 e IPv6. IPv6 é a versão mais recente do IP e eventualmente substituirá o IPv4 mais comum.





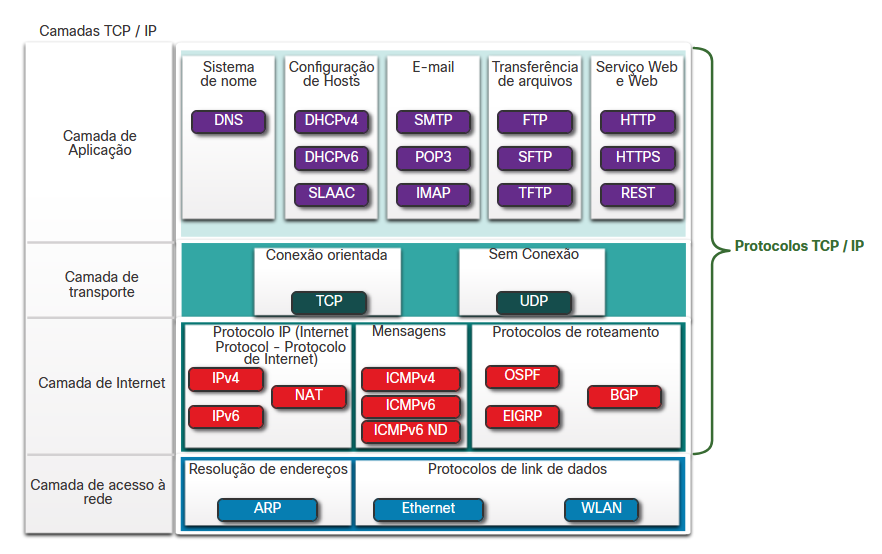




5.2.3

**Conjunto de protocolos TCP/IP**

Hoje, o conjunto de protocolos TCP/IP inclui muitos protocolos e continua a evoluir para oferecer suporte a novos serviços. A Figura mostra alguns dos mais populares.



TCP/IP é o conjunto de protocolos usado pela internet e as redes de hoje. O TCP/IP tem dois aspectos importantes para fornecedores e fabricantes:

* **Conjunto de protocolos de padrão aberto** - Isso significa que está disponível gratuitamente ao público e pode ser usado por qualquer fornecedor em seu hardware ou software.
* **Conjunto de protocolos com base em padrões** - isso significa que foi endossado pela indústria de rede e aprovado por uma organização de padrões. Isso garante que produtos de diferentes fabricantes possam interoperar com êxito.

## Camada de aplicação

**Camada de aplicação**

Sistema de nomes

* **DNS** - Sistema de nomes de domínio. Converte nomes de domínio, como cisco.com, em endereços IP.

Configuração de hosts

* **DHCPv4** - Protocolo de configuração de host dinâmico para IPv4. Um servidor DHCPv4 atribui dinamicamente informações de endereçamento IPv4 aos clientes DHCPv4 na inicialização e permite que os endereços sejam reutilizados quando não forem mais necessários.
* **DHCPv6** - Protocolo de Configuração do Host Dinâmico para IPv6. DHCPv6 é semelhante ao DHCPv4. Um servidor DHCPv6 atribui dinamicamente informações de endereçamento IPv6 aos clientes DHCPv6 na inicialização.
* **SLAAC** - Configuração automática de endereço sem estado. Um método que permite que um dispositivo obtenha suas informações de endereçamento IPv6 sem usar um servidor DHCPv6.

E-mail

* **SMTP** -Protocolo de transferência de correio simples. Permite que os clientes enviem e-mails para um servidor de e-mail e permite que os servidores enviem e-mails para outros servidores.
* **POP3** - Post Office Protocol versão 3. Permite que os clientes recuperem e-mails de um servidor de e-mail e baixem o e-mail para o aplicativo de e-mail local do cliente.
* **IMAP** - Protocolo de Acesso à Mensagem na Internet. Permite que os clientes acessem o e-mail armazenado em um servidor de e-mail e também mantenham o e-mail no servidor.

Transferência de arquivos

* **FTP** - Protocolo de transferência de arquivos. Define as regras que permitem que um usuário em um host acesse e transfira arquivos para e de outro host em uma rede. O FTP é um protocolo de entrega de arquivos confiável, orientado a conexão e reconhecido.
* **SFTP** - Protocolo de transferência de arquivos SSH. Como uma extensão do protocolo Secure Shell (SSH), o SFTP pode ser usado para estabelecer uma sessão segura de transferência de arquivos na qual a transferência é criptografada. SSH é um método para login remoto seguro que normalmente é usado para acessar a linha de comando de um dispositivo.
* **TFTP** - Protocolo de Transferência de Arquivos Trivial. Um protocolo de transferência de arquivos simples e sem conexão com entrega de arquivos não confirmada e de melhor esforço. Ele usa menos sobrecarga que o FTP.

Web e serviço Web

* **HTTP** - Protocolo de transferência de hipertexto. Um conjunto de regras para a troca de texto, imagens gráficas, som, vídeo e outros arquivos multimídia na World Wide Web.
* **HTTPS** - HTTP seguro. Uma forma segura de HTTP que criptografa os dados que são trocados pela World Wide Web.
* **REST** - Representational State Transfer. Um serviço Web que utiliza interfaces de programação de aplicações (APIs) e pedidos HTTP para criar aplicações Web.

## Camada de transporte

**Camada de transporte**

Conexão orientada

* **TCP** - Protocolo de controle de transmissão. Permite a comunicação confiável entre processos executados em hosts separados e fornece transmissões confiáveis e reconhecidas que confirmam a entrega bem-sucedida.

Sem Conexão

* **UDP** - Protocolo de datagrama do usuário. Permite que um processo em execução em um host envie pacotes para um processo em execução em outro host. No entanto, o UDP não confirma a transmissão bem-sucedida do datagrama.

## Camada de internet

**Camada de Internet**

Protocolo IP (Internet Protocol)

* **IPv4** - Protocolo da Internet versão 4. Recebe segmentos de mensagem da camada de transporte, empacota mensagens em pacotes e endereça pacotes para entrega de ponta a ponta através de uma rede. O IPv4 usa um endereço de 32 bits.
* **IPv6** - IP versão 6. Semelhante ao IPv4, mas usa um endereço de 128 bits.
* **NAT** - Tradução de endereços de rede. Converte endereços IPv4 de uma rede privada em endereços IPv4 públicos globalmente exclusivos.

Mensagens

* **ICMPv4** - Protocolo de mensagens de controle da Internet para IPv4. Fornece feedback de um host de destino para um host de origem sobre erros na entrega de pacotes.
* **ICMPv6** - ICMP para IPv6. Funcionalidade semelhante ao ICMPv4, mas é usada para pacotes IPv6.
* **ICMPv6 ND** - descoberta de vizinho ICMPv6. Inclui quatro mensagens de protocolo que são usadas para resolução de endereço e detecção de endereço duplicado.

Protocolos de roteamento

* **OSPF** - Abrir o caminho mais curto primeiro. Protocolo de roteamento de estado de link que usa um experimento hierárquico baseado em áreas. OSPF é um protocolo de roteamento interno padrão aberto.
* **EIGRP** - Protocolo de roteamento de gateway interno aprimorado. Um protocolo de roteamento de padrão aberto desenvolvido pela Cisco que usa uma métrica composta com base na largura de banda, atraso, carga e confiabilidade.
* **BGP** - Protocolo de gateway de fronteira. Um protocolo de roteamento de gateway externo padrão aberto usado entre os Internet Service Providers (ISPs). O BGP também é comumente usado entre os ISPs e seus grandes clientes particulares para trocar informações de roteamento.

## Camada de acesso à rede

Resolução de endereços

* **ARP** - Protocolo de Resolução de Endereço. Fornece mapeamento de endereço dinâmico entre um endereço IPv4 e um endereço de hardware.

**Observação**: Você pode ver outro estado de documentação que o ARP opera na Camada da Internet (Camada OSI 3). No entanto, neste curso, afirmamos que o ARP opera na camada de Acesso à Rede (OSI Camada 2) porque seu objetivo principal é descobrir o endereço MAC do destino. Um endereço MAC é um endereço da camada 2.

Protocolos de link de dados

* **Ethernet** - define as regras para os padrões de fiação e sinalização da camada de acesso à rede.
* **WLAN** - Rede local sem fio. Define as regras para sinalização sem fio nas frequências de rádio de 2,4 GHz e 5 GHz.

5.2.4

**Formatação e Encapsulamento de Mensagens**

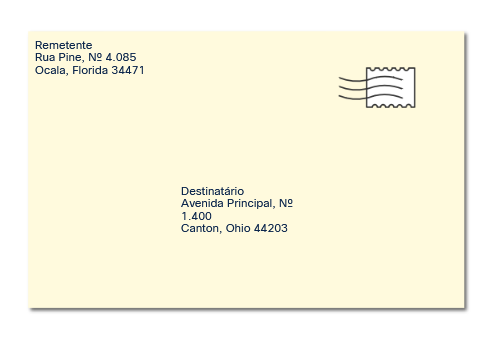
Quando uma mensagem é enviada da origem para o destino, deve usar um formato ou uma estrutura específica. Os formatos da mensagem dependem do tipo de mensagem e do canal usado para entregá-la.

**Analogia**

Um exemplo comum de exigir o formato correto nas comunicações humanas é ao enviar uma carta. Clique em Reproduzir na figura para exibir uma animação de formatação e encapsulamento de uma letra.

Um envelope tem o endereço do remetente e do destinatário, cada um localizado no local apropriado no envelope. Se o endereço destino e a formatação não estiverem corretos, a carta não será entregue.

O processo de colocar um formato de mensagem (a carta) em outro formato de mensagem (o envelope) é chamado encapsulamento. O desencapsulamento ocorre quando o processo é invertido pelo destinatário e a carta é retirada do envelope.

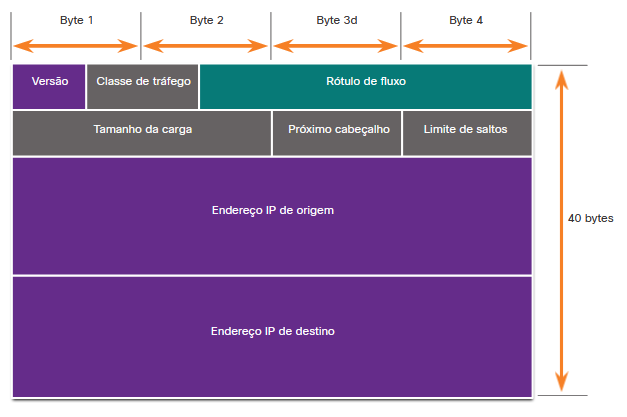


**Rede**

Semelhante ao envio de uma carta, uma mensagem enviada por uma rede de computadores segue regras específicas de formato para que ela seja entregue e processada.

Internet Protocol (IP) é um protocolo com uma função semelhante ao exemplo de envelope. Na figura, os campos do pacote IPv6 (Internet Protocol versão 6) identificam a origem do pacote e seu destino. IP é responsável por enviar uma mensagem da origem da mensagem para o destino através de uma ou mais redes.

**Nota**: Os campos do pacote IPv6 são discutidos em detalhes em outro módulo.



5.2.5

**Tamanho da Mensagem**

Outra regra de comunicação é o tamanho da mensagem.

**Analogia**

Quando as pessoas se comunicam entre si, as mensagens que enviam geralmente são quebradas em partes ou sentenças menores. Essas sentenças são limitadas em tamanho ao que a pessoa receptora pode processar de uma só vez, conforme mostrado na figura. Também torna mais fácil para o receptor ler e compreender.

**Rede**

Do mesmo modo, quando uma mensagem longa é enviada de um host a outro em uma rede, é necessário dividir a mensagem em partes menores, como mostra a Figura 2. As regras que regem o tamanho das partes, ou quadros, transmitidos pela rede são muito rígidas. Também podem diferir, dependendo do canal usado. Os quadros que são muito longos ou muito curtos não são entregues.

As restrições de tamanho dos quadros exigem que o host origem divida uma mensagem longa em pedaços individuais que atendam aos requisitos de tamanho mínimo e máximo. A mensagem longa será enviada em quadros separados, e cada um contém uma parte da mensagem original. Cada quadro também terá suas próprias informações de endereço. No host destino, as partes individuais da mensagem são reconstruídas na mensagem original.

5.2.6

## Temporização de Mensagem

O tempo de mensagens também é muito importante nas comunicações de rede. A temporização da mensagem inclui o seguinte:

* **Controle de fluxo** - este é o processo de gerenciamento da taxa de transmissão de dados. O controle de fluxo define quanta informação pode ser enviada e a velocidade com que pode ser entregue. Por exemplo, se uma pessoa fala muito rapidamente, pode ser difícil para o receptor ouvir e entender a mensagem. Na comunicação de rede, existem protocolos de rede usados pelos dispositivos de origem e destino para negociar e gerenciar o fluxo de informações.
* **Tempo limite de resposta** - se uma pessoa fizer uma pergunta e não ouvir uma resposta dentro de um período de tempo aceitável, a pessoa presumirá que não haverá resposta e reagirá de acordo. A pessoa pode repetir a pergunta ou prosseguir com a conversa. Os hosts da rede usam protocolos de rede que especificam quanto tempo esperar pelas respostas e que ação executar se ocorrer um tempo limite de resposta.
* **Método de acesso -** determinar quando alguém pode enviar uma mensagem. Clique em Reproduzir na figura para ver uma animação de duas pessoas conversando ao mesmo tempo e, em seguida, ocorre uma "colisão de informações", e é necessário que as duas se afastem e iniciem novamente. Da mesma forma, quando um dispositivo deseja transmitir em uma LAN sem fio, é necessário que a placa de interface de rede (NIC) da WLAN determine se a mídia sem fio está disponível.

5.2.7

**Unicast, broadcast ou multicast**

Uma mensagem pode ser entregue de diferentes maneiras. Às vezes, uma pessoa deseja transmitir informações a uma única pessoa. Em outros casos, a pessoa pode precisar enviar informações a um grupo de uma só vez, ou até mesmo para todas as pessoas na mesma área.

Hosts em uma rede usam opções de entrega semelhantes para se comunicar. Esses métodos de comunicação são chamados unicast, multicast e broadcast.

5.2.8

## Os Benefícios de Se Usar um Modelo de Camadas

Você não pode realmente assistir a pacotes reais viajando através de uma rede real da mesma forma que pode assistir os componentes de um carro sendo montados em uma linha de montagem. Então ajuda ter um jeito de pensar em rede para você imaginar o que está acontecendo. Um modelo é útil nessas situações.

Conceitos complexos, como a forma como uma rede opera, podem ser difíceis de explicar e compreender. Por esta razão, um modelo em camadas é usado para modularizar as operações de uma rede em camadas gerenciáveis.

Estes são os benefícios do uso de um modelo em camadas para descrever protocolos e operações de rede:

* Auxiliar no projeto de protocolo porque os protocolos que operam em uma camada específica têm informações definidas sobre as quais eles atuam e uma interface definida para as camadas acima e abaixo
* Estimular a competição porque os produtos de diferentes fornecedores podem trabalhar em conjunto.
* Impedir que mudanças de tecnologia ou capacidade em uma camada afetem outras camadas acima e abaixo.
* Fornecer um idioma comum para descrever funções e capacidades de rede.

Como mostrado na figura, existem dois modelos em camadas que são usados para descrever operações de rede:

* Modelo de referência OSI (Open System Interconnection)
* Modelo de referência TCP/IP



5.2.9

**O Modelo de Referência OSI**

O modelo de referência OSI fornece uma extensa lista de funções e serviços que podem ocorrer em cada camada. Esse tipo de modelo fornece consistência em todos os tipos de protocolos e serviços de rede, descrevendo o que deve ser feito em uma camada específica, mas não prescrevendo como deve ser realizado.

Ele também descreve a interação de cada camada com as camadas diretamente acima e abaixo. Os protocolos TCP/IP discutidos neste curso estão estruturados com base nos modelos OSI e TCP/IP. A tabela mostra detalhes sobre cada camada do modelo OSI. A funcionalidade de cada camada e o relacionamento entre elas ficarão mais evidentes no decorrer deste curso, conforme os protocolos são discutidos com mais detalhes.

| **Camada de modelo OSI** | **Descrição** |
| --- | --- |
| **7 - Aplicação** | A camada de aplicação contém protocolos usados para comunicações processo a processo. |
| **6 - Apresentação** | A camada de apresentação fornece a representação comum de dados transferidos entre serviços da camada de aplicação. |
| **5 - Sessão** | A camada de sessão fornece serviços à camada de apresentação para organizar o diálogo e gerenciar a troca de dados. |
| **4 - Transporte** | A camada de transporte define serviços para segmentar, transferir e reagrupar os dados para comunicações individuais entre os dispositivos finais. |
| **3 - Rede** | A camada de rede fornece serviços para trocar partes individuais de dados na rede entre dispositivos finais identificados. |
| **2 - Link** de dados | Os protocolos da camada de enlace descrevem métodos para a troca de quadros de dados entre dispositivos em uma mídia comum |
| **1 - Físico** | Os protocolos da camada física descrevem os meios mecânicos, elétricos, funcionais e procedimentais para ativar, manter e desativar conexões físicas para uma transmissão de bits de e para um dispositivo de rede. |

**Nota**: Enquanto as camadas do modelo TCP / IP são referenciadas apenas pelo nome, as sete camadas do modelo OSI são mais frequentemente referenciadas pelo número do que pelo nome. Por exemplo, a camada física é referida como Camada 1 do modelo OSI, a camada de enlace de dados é a Camada 2 e assim por diante.

5.2.10

**O Modelo de Protocolo TCP/IP**

O modelo de protocolo TCP / IP para comunicações entre redes foi criado no início dos anos 70 e às vezes é chamado de modelo da Internet. Esse tipo de modelo corresponde à estrutura de um conjunto de protocolos específico. O modelo TCP/IP é um modelo de protocolo porque descreve as funções que ocorrem em cada camada de protocolos dentro da suíte TCP/IP. O TCP/IP também é usado como um modelo de referência. A tabela mostra detalhes sobre cada camada do modelo OSI.

| **Camada do modelo TCP/IP** | **Descrição** |
| --- | --- |
| **4 - Aplicação** | Representa dados para o usuário, além do controle de codificação e de diálogo. |
| **3 - Transporte** | Permite a comunicação entre vários dispositivos diferentes em redes distintas. |
| **2 - Internet** | Determina o melhor caminho pela rede. |
| **1 - Acesso à Rede** | Controla os dispositivos de hardware e o meio físico que formam a rede. |

As definições do padrão e dos protocolos TCP/IP são discutidas em um fórum público e definidas em um conjunto publicamente disponível de documentos de solicitação de comentário (RFC) da IETF. Um RFC é criado por engenheiros de rede e enviado a outros membros do IETF para comentários.

# Encapsulamento de dados

5.3.1

## Segmentando Mensagens

Conhecer o modelo de referência OSI e o modelo de protocolo TCP/IP será útil quando você aprender sobre como os dados são encapsulados à medida que eles se movem através de uma rede. Não é tão simples como uma carta física sendo enviada através do sistema de correio.

Em teoria, uma única comunicação, como um vídeo ou uma mensagem de e-mail com muitos anexos grandes, poderia ser enviada através de uma rede de uma fonte para um destino como um fluxo maciço e ininterrupto de bits. No entanto, isso criaria problemas para outros dispositivos que precisassem usar os mesmos canais de comunicação ou links. Esses grandes fluxos de dados resultariam em atrasos consideráveis. Além disso, se algum link na infra-estrutura de rede interconectada falhasse durante a transmissão, a mensagem completa seria perdida e teria que ser retransmitida na íntegra.

Uma melhor abordagem é dividir os dados em pedaços menores e mais gerenciáveis para o envio pela rede. Segmentação é o processo de dividir um fluxo de dados em unidades menores para transmissões através da rede. A segmentação é necessária porque as redes de dados usam o conjunto de protocolos TCP/IP enviar dados em pacotes IP individuais. Cada pacote é enviado separadamente, semelhante ao envio de uma carta longa como uma série de cartões postais individuais. Pacotes que contêm segmentos para o mesmo destino podem ser enviados por caminhos diferentes.

Isso leva à segmentação de mensagens com dois benefícios principais:

* **Aumenta a velocidade** - como um grande fluxo de dados é segmentado em pacotes, grandes quantidades de dados podem ser enviadas pela rede sem obstruir um link de comunicação. Isso permite que muitas conversas diferentes sejam intercaladas na rede chamada multiplexação.
* **Aumenta a eficiência** - se um único segmento não consegue alcançar seu destino devido a uma falha na rede ou congestionamento da rede, apenas esse segmento precisa ser retransmitido em vez de reenviar todo o fluxo de dados.
* 5.3.2
* **Sequenciamento**
* O desafio de utilizar segmentação e multiplexação para a transmissão de mensagens por uma rede é o nível de complexidade que é agregado ao processo. Imagine se você tivesse que enviar uma carta de 100 páginas, mas cada envelope poderia conter apenas uma página. Portanto, seriam necessários 100 envelopes e cada envelope precisaria ser endereçado individualmente. É possível que a carta de 100 páginas em 100 envelopes diferentes chegue fora de ordem. Consequentemente, as informações contidas no envelope teriam de incluir um número sequencial para garantir que o destinatário pudesse remontar as páginas na ordem correcta.
* Nas comunicações em rede, cada segmento da mensagem deve passar por um processo semelhante para garantir que chegue ao destino correto e possa ser remontado no conteúdo da mensagem original, conforme mostrado na figura. O TCP é responsável por sequenciar os segmentos individuais.



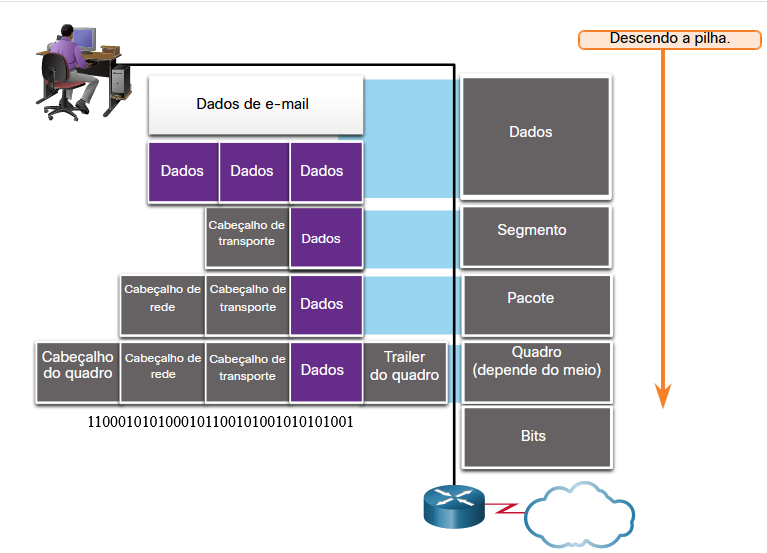
5.3.3

**Unidades de Dados de Protocolo**

À medida que os dados da aplicação são passados pela pilha de protocolos em seu caminho para serem transmitidos pelo meio físico de rede, várias informações de protocolos são adicionadas em cada nível. Isso é conhecido como o processo de encapsulamento.

**Nota**: Embora o UDP PDU seja chamado de datagrama, os pacotes IP às vezes também são chamados de datagramas IP.

O formato que uma parte de dados assume em qualquer camada é chamado de unidade de dados de protocolo (PDU). Durante o encapsulamento, cada camada sucessora encapsula a PDU que recebe da camada superior de acordo com o protocolo sendo usado. Em cada etapa do processo, uma PDU possui um nome diferente para refletir suas novas funções. Embora não haja uma convenção de nomenclatura universal para PDUs, neste curso, as PDUs são nomeadas de acordo com os protocolos do conjunto TCP / IP. As PDUs para cada forma de dados são mostradas na figura.



Aplicação

Transporte

Fisico

Enlace

Rede

A figura mostra as unidades de dados de protocolo (PDUs) em várias camadas do modelo OSI. Na parte superior da imagem é uma pessoa sentada em uma estação de trabalho de computador enviando dados de e-mail. Esses dados são passados pela pilha e encapsulados em uma nova PDU em cada camada. Na parte superior, os dados de e-mail são divididos em pequenos pedaços de dados. Abaixo disso, um cabeçalho de transporte é adicionado na frente do pedaço de dados e torna-se um segmento. Abaixo disso, um cabeçalho de rede é adicionado na frente do cabeçalho de transporte e torna-se um pacote. Abaixo disso, um cabeçalho de quadro é adicionado na frente do cabeçalho da rede e um trailer de quadro é adicionado atrás dos dados e torna-se um quadro (dependente médio). O quadro é mostrado como um fluxo de bits antes de ser recebido por um roteador que está conectado à nuvem. O texto na parte inferior lê: Dados - O termo geral para a PDU usada na camada do aplicativo; Segmento - PDU da camada de transporte; Pacote - PDU da camada de rede; Frame - PDU da camada de link de dados; Bits - PDU da camada física usada ao transmitir dados fisicamente pelo meio. Nota: Se o cabeçalho Transporte for TCP, será um segmento. Se o cabeçalho Transporte é UDP, então é um datagrama.

* Dados - o termo genérico para a PDU usada na camada de aplicação;
* Segmento - PDU da camada de transporte;
* Pacote - PDU da camada de rede;
* Quadro - PDU da camada de enlace de dados
* Bits - PDU da camada física usada ao transmitir dados fisicamente pela mídia.

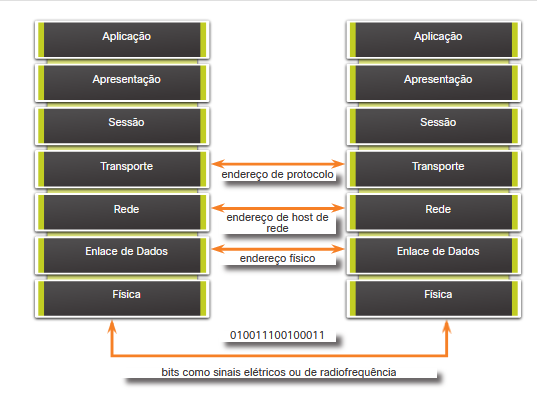
**Nota**: Se o cabeçalho de transporte é TCP, então é um segmento. Se o cabeçalho Transporte é UDP, então é um datagrama.

5.3.4

**Três Endereços**

Os protocolos de rede exigem que os endereços sejam usados para comunicação de rede. O endereçamento é usado pelo cliente para enviar solicitações e outros dados para um servidor. O servidor usa o endereço do cliente para retornar os dados solicitados ao cliente que o solicitou.

Todas as camadas de transporte OSI, rede e link de dados usam endereçamento de alguma forma. A camada de transporte usa endereços de protocolo na forma de números de porta para identificar aplicativos de rede que devem manipular dados de cliente e servidor. A camada de rede especifica endereços que identificam as redes às quais os clientes e servidores estão conectados e os próprios clientes e servidores. Finalmente, a camada de link de dados especifica os dispositivos na LAN local que devem lidar com quadros de dados. Todos os três endereços são necessários para a comunicação cliente-servidor, como mostrado na figura.

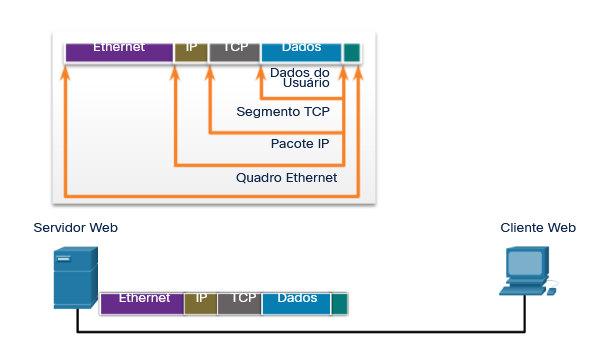


5.3.5

**Exemplo de Encapsulamento**

Quando as mensagens estão sendo enviadas em uma rede, o processo de encapsulamento funciona de cima para baixo. Em cada camada, as informações da camada superior são consideradas dados encapsulados no protocolo. Por exemplo, o segmento TCP é considerado dados dentro do pacote IP.

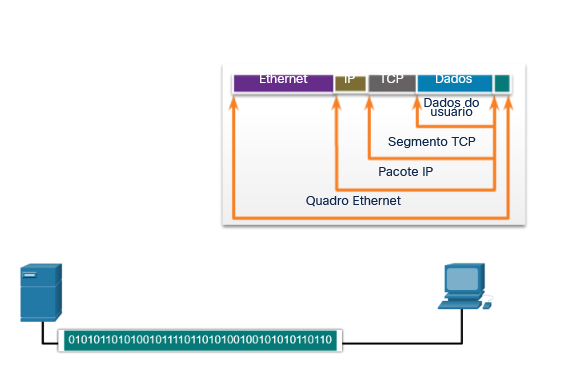
Você viu essa animação anteriormente neste módulo. Dessa vez, clique em Reproduzir e concentre-se no processo de encapsulamento, pois um servidor da Web envia uma página da Web para um cliente da Web.



5.3.6

**Exemplo de desencapsulamento**

Esse processo é revertido no host de recebimento e é conhecido como desencapsulamento. O desencapsulamento é o processo usado por um dispositivo receptor para remover um ou mais cabeçalhos de protocolo. Os dados são desencapsulados à medida que se movem na pilha em direção à aplicação do usuário final.



# Resumo de protocolos de rede

5.4.1

## O que aprendi neste módulo?

**Comunicações em Rede**

As redes vêm em todos os tamanhos e podem ser encontradas em casas, empresas e outras organizações. A Internet é a maior rede existente. Todos os computadores que se conectam a uma rede são conhecidos como hosts ou dispositivos finais. Grande parte da interação entre hosts é o tráfego cliente-servidor. Os hosts podem operar como clientes ou servidores ou clientes e servidores em redes ponto a ponto. Servidores são hosts que usam software especializado para permitir que eles respondam a solicitações de diferentes tipos de dados de clientes. Os clientes são hosts que usam aplicativos de software como navegadores da Web, clientes de email ou aplicativos de transferência de arquivos para solicitar dados de servidores. Quando usamos a internet, usamos uma combinação de cabos de cobre e fibra óptica ou comunicações sem fio e satélite para transportar nosso tráfego de dados. As conexões com a Internet são feitas por provedores de serviços de Internet que se conectam entre si usando ISPs globais de Nível 1 e Nível 2 que se conectam entre si por meio de Pontos de Troca de Internet (IXP). Empresas maiores podem se conectar a ISPs de Nível 2 por meio de um Ponto de Presença (POP). Os ISPs de Nível 3 conectam residências e empresas à Internet. O tráfego entre um computador e um servidor de Internet pode assumir muitos caminhos diferentes. Alguns caminhos podem ser muito diretos, mas outros podem parecer sair do caminho. Além disso, os dados enviados entre um computador e um servidor podem ser enviados em um caminho diferente daquele em que são recebidos.

**Protocolos de comunicação**

A comunicação de dados requer mais do que apenas conexões. Os dispositivos devem saber como se comunicar. Para isso, os dispositivos usam regras ou protocolos de comunicação, assim como as comunicações presenciais entre as pessoas usam regras. Os protocolos de rede especificam muitos recursos de comunicação de rede, como codificação de mensagens, formatação e encapsulamento de mensagens, tamanho da mensagem, tempo de mensagens e opções de entrega. Exemplos de protocolos de rede incluem Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TC) e Internet Protocol (IP). É muito importante que um analista de segurança cibernética conheça a estrutura dos dados de protocolo e como os protocolos funcionam na rede. Os protocolos especificam como as mensagens são estruturadas e a maneira como os dispositivos de rede compartilham informações sobre caminhos para outras redes. Eles também especificam como e quando as mensagens de erro e do sistema são passadas entre os dispositivos. Além disso, os protocolos especificam como as sessões de transferência de dados são configuradas e terminadas. O conjunto de protocolos TCP/IP é usado pela Internet e redes de dados em residências, empresas e outras organizações. O pacote TCP/IP é uma família de protocolos que estão em conformidade com padrões de código aberto disponíveis gratuitamente que são endossados pelo setor de rede e aprovados por organizações de padrões. Isso permite que dispositivos de diferentes fabricantes trabalhem em conjunto. O conjunto de protocolos TCP/IP tem quatro camadas de protocolos que funcionam juntos quando as mensagens são enviadas e recebidas. Protocolos comuns na camada de aplicativo da suíte são DNS, DHCP, POP3 e HTTPS, entre outros. Os protocolos da camada de transporte são TCP e UDP. Exemplos de protocolos de camada de Internet são IPv4, IPv6, ICMP e EIGRP. As mensagens são formatadas de acordo com os padrões de protocolos. Os dados de protocolo são encapsulados colocando dados de camada superior dentro de dados de camada inferior quando os dados são enviados. O processo inverso ocorre quando os dados são recebidos. Os padrões de protocolo especificam o tamanho das mensagens e como as mensagens são codificadas para serem enviadas através de conexões de rede como ondas de rádio, pulsos de luz ou sinais elétricos. O host receptor decodifica as mensagens. Os padrões de protocolo também especificam a taxa na qual os dados são enviados (controle de fluxo), o tempo que um host aguarda para receber uma resposta do destino (tempo limite de resposta) e a maneira pela qual os hosts determinam quando podem enviar dados em uma rede de mídia compartilhada (método de acesso). Mensagens unicast são enviadas para um host de destino. Mensagens multicast são enviadas para um grupo de hosts. As transmissões (broadcasts) são enviadas para todos os hosts na mesma área da rede. Os modelos de comunicação em camadas têm uma série de benefícios. Os modelos auxiliam no design de protocolos e dispositivos. Eles também aumentam a concorrência entre os fabricantes porque os dispositivos devem funcionar em conjunto. Finalmente, os modelos impedem que as alterações em uma camada afetem outras camadas e fornecem uma maneira comum de descrever a operação da rede. Dois modelos são os modelos de referência OSI e TCP/IP. O modelo OSI tem sete camadas. As diferentes camadas têm funções diferentes. O modelo TCP / IP possui quatro camadas.

**Encapsulamento de dados**

Mensagens que consistem em grandes quantidades de dados não podem ser enviadas através da rede como um fluxo maciço de bits. Isso ocorre porque outras pessoas precisariam esperar que toda a comunicação fosse concluída antes que pudessem usar a rede, e se a comunicação falhasse, toda a mensagem precisaria ser enviada novamente. Em vez disso, os dados são divididos em uma série de pedaços menores e enviados pela rede. Isso é chamado de segmentação. A segmentação é necessária pelo conjunto de protocolos TCP/IP. Os dados são enviados como pacotes. Cada pacote é endereçado separadamente e pode seguir caminhos diferentes através de uma rede para chegar ao destino. A segmentação aumenta a velocidade e a eficiência das redes de dados. Maior velocidade é obtida porque muitas conversas de dados podem acontecer ao mesmo tempo na rede. Isso é chamado de multiplexação. A eficiência é obtida porque apenas os dados que não são recebidos por um destino precisam ser reenviados. As mensagens são segmentadas para serem enviadas e devem ser recombinadas quando forem recebidas. À medida que os dados são passados para baixo a pilha de protocolo a ser enviado, informações diferentes são adicionadas por cada camada. Esse processo é chamado de encapsulamento. A forma que os dados assumem em diferentes camadas é chamada de unidade de dados de protocolo (PDU). Durante o encapsulamento, as PDUs são encapsuladas dentro de PDUs na próxima camada abaixo da pilha quando os dados são enviados. O processo inverso ocorre quando os dados são recebidos. Na camada de aplicação OSI, a PDU é geralmente referida simplesmente como dados. Os dados são encapsulados em segmentos ou datagramas na camada de transporte. A PDU da camada de rede é chamada de pacote, encapsulando segmentos. A camada de enlace de dados encapsula os pacotes em quadros. Finalmente, a camada física transmite bits através da rede. As camadas de transporte, rede e enlace do modelo OSI usam endereçamento. A camada de transporte usa endereços de protocolo na forma de números de porta. A camada de rede usa endereços IP para identificar hosts e redes. Finalmente, a camada de enlace usa endereços de hardware para identificar quais hosts na rede local devem lidar com quadros. Estes endereços identificam a origem dos dados e o destino dos dados. Depois que os dados são recebidos, eles são desencapsulados para que os dados possam ser usados pelos aplicativos cliente que os solicitaram.

5.4.2

Módulo 5: Questionário de protocolos de rede

Um host está transmitindo um broadcast. Qual host ou hosts o receberão?

Tópico 5.2.0 - Um broadcast é entregue a cada host que possui um endereço IP na mesma rede.

Qual afirmativa descreve uma característica da computação em nuvem?

Tópico 5.1.0 - A computação em nuvem permite aos usuários acessar aplicativos, fazer backup e armazenar arquivos e realizar tarefas sem a necessidade de software ou servidores adicionais. Os usuários da nuvem acessam os recursos em tempo real, através de serviços de assinatura ou pagamento por uso, usando apenas um navegador web.

Um administrador de rede pode executar ping com êxito no servidor em www.cisco.com, mas não pode executar o ping no servidor web da empresa localizado em um ISP em outra cidade. Que ferramenta ou comando podem ajudar a identificar o roteador específico em que o pacote foi perdido ou atrasado?

Tópico 5.1.0 - O comando traceroute fornece informações de conectividade sobre o caminho que um pacote segue para chegar ao destino e sobre cada roteador (salto) ao longo do caminho. Ele também indica o tempo que um pacote leva para chegar da origem em cada salto e vice-versa.

Qual camada do modelo OSI contém protocolos para comunicação processo a processo?

Tópico 5.2.0 - A camada de aplicação do modelo OSI é responsável pela comunicação entre os processos. Exemplos de protocolos na camada de aplicação são DHCP, DNS e HTTP.

Em qual camada OSI é um número de porta de destino adicionado a uma PDU durante o processo de encapsulamento?

Tópico 5.3.0 - A camada de transporte usa endereços de protocolo na forma de números de porta para identificar aplicativos de rede que devem lidar com dados de cliente e servidor.

Qual processo envolve colocar uma PDU dentro de outra PDU?

Tópico 5.3.0 - Quando uma mensagem é colocada dentro de outra mensagem, isso é conhecido como encapsulamento. Em redes, o encapsulamento ocorre quando uma unidade de dados de protocolo é transportada dentro do campo de dados da próxima unidade de dados de protocolo inferior.

Qual afirmação descreve com precisão um processo de encapsulamento TCP / IP quando um PC está enviando dados para a rede?

Tópico 5.3.0 - Quando os dados estão viajando do PC para a rede, a camada de transporte envia segmentos para a camada de rede. A camada de rede envia pacotes para a camada de acesso à rede, que cria quadros e os converte em bits. Os bits são liberados para a mídia da rede.

Um cliente Web está recebendo uma resposta para uma página da Web de um servidor Web. Do ponto de vista do cliente, qual é a ordem correta da pilha de protocolo que é usada para decodificar a transmissão recebida?

Tópico 5.3.0-1. O HTTP controla a maneira como um servidor da web e um cliente interagem. 2. O TCP gerencia conversas individuais entre servidores da web e clientes. 3. IP é responsável pela entrega através do melhor caminho para o destino. 4. Ethernet pega o pacote do IP e formata-o para transmissão.

Como a BYOD (Bring Your Own Device) muda a maneira como as empresas implementam as redes?

Tópico 5.1.0 - Um ambiente BYOD exige que uma organização acomode uma variedade de dispositivos e métodos de acesso. Dispositivos pessoais, que não estão sob o controle da empresa, podem ser aceitos e, portanto, segurança é um fator essencial. Os custos de hardware no local serão reduzidos, permitindo que a empresa priorize a disponibilização de ferramentas de colaboração e outros softwares para usuários BYOD.

Na comunicação entre computadores, qual é o objetivo da codificação de mensagens?

Tópico 5.2.0 - Antes de uma mensagem ser enviada através de uma rede, ela deve primeiro ser codificada. Codificação é o processo de conversão de dados da mensagem em outro formato adequado a transmissão pelo meio físico. Cada bit da mensagem é codificado em um padrão de sons, de ondas de luz ou de impulsos elétricos, dependendo do meio físico de rede em que os bits são transmitidos. O host destino recebe e decodifica os sinais para interpretar a mensagem.

Qual afirmação é verdadeira sobre os modelos TCP/IP e OSI?​

Tópico 5.2.0 - A camada de rede do TCP / IP fornece a mesma função que a camada de rede OSI. A camada de transporte dos modelos TCP / IP e OSI fornece a mesma função. A camada de aplicação TCP / IP inclui as mesmas funções das camadas OSI 5, 6 e 7.

Que método pode ser usado por dois computadores para garantir que os pacotes não sejam descartados porque muitos dados estão sendo enviados muito rapidamente?

Tópico 5.2.0 - Para que dois computadores possam se comunicar de forma eficaz, deve haver um mecanismo que permita que a origem e o destino definam o tempo de transmissão e recebimento dos dados. O controle de fluxo permite isso, garantindo que os dados não sejam enviados muito rápido para serem recebidos corretamente.

# Introdução

6.0.1

## Por que devo cursar este módulo?

Como os dispositivos sabem enviar e receber informações dentro da rede e da vasta Internet? Cada pedaço de dados que é enviado requer endereços; endereços para destinos e endereços para o retorno de informações para a fonte.

Os analistas de segurança cibernética trabalham para identificar e analisar os indicadores de incidentes de segurança de rede. Esses indicadores consistem em registros de eventos de rede. Esses eventos, que são registrados em arquivos de log de vários dispositivos, são compostos principalmente de detalhes de operações de protocolo de rede. Os endereços identificam quais hosts se conectaram uns aos outros, dentro de uma organização ou a hosts distantes na Internet. Os endereços que são mantidos em arquivos de log também identificam quais hosts externos se conectaram ou tentaram se conectar com hosts dentro de uma organização.

É crucial que um analista de segurança cibernética saiba tudo o que puder sobre Ethernet e endereços IP. Este módulo começa com uma discussão sobre a tecnologia Ethernet, incluindo uma explicação da subcamada MAC da Camada 2 e os campos de quadro Ethernet. O restante do módulo discute os endereços IPv4 e IPv6 da Camada 3 e como eles são usados para rotear pacotes da origem para o destino.

6.0.2

**O que vou aprender neste módulo?**

**Título do módulo: Protocolo** Ethernet e IP

**Objetivo do Módulo:** Explique como os protocolos Ethernet e IP oferecem suporte à comunicação de rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Ethernet | Explicar como a Ethernet oferece suporte à comunicação de rede. |
| IPv4 | Explicar como o protocolo IPv4 oferece suporte às comunicações de rede. |
| Noções básicas de endereçamento IP | Explicar como os endereços IP viabilizam a comunicação de rede. |
| Tipos de endereços IPv4 | Explicar os tipos de endereços IPv4 que viabilizam a comunicação de rede. |
| O gateway padrão | Explicar como o gateway padrão viabiliza a comunicação de rede. |
| IPv6 | Explicar como o protocolo IPv6 oferece suporte às comunicações de rede. |

# Ethernet;

6.1.1

## Encapsulamento Ethernet

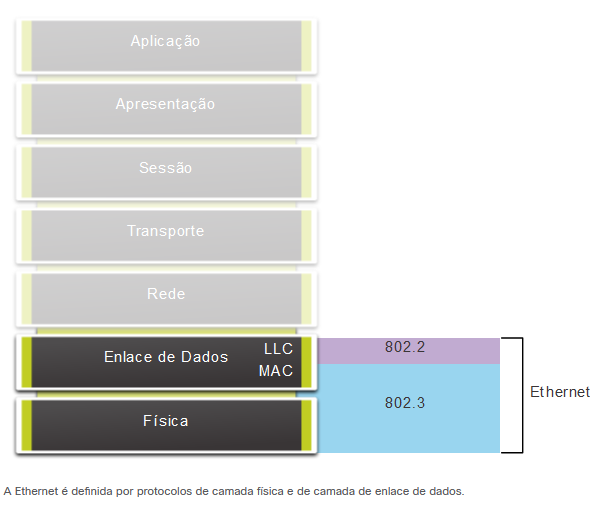
Ethernet e LAN sem fio (WLANs) são as duas tecnologias LAN mais comumente implantadas. Ao contrário da rede sem fio, a Ethernet usa comunicações com fio, incluindo par trançado, links de fibra óptica e cabos coaxiais.

Ela opera na camada de enlace de dados e na camada física. É uma família de tecnologias de rede definidas nos padrões IEEE 802.2 e 802.3. Ethernet oferece suporte às seguintes larguras de banda de dados:

* 10 Mbps
* 100 Mbps
* 1000 Mbps (1 Gbps)
* 10,000 Mbps (10 Gbps)
* 40,000 Mbps (40 Gbps)
* 100,000 Mbps (100 Gbps)

Conforme mostrado na figura, os padrões Ethernet definem os protocolos da camada 2 e as tecnologias da camada 1.

### Ethernet e o modelo OSI



A Ethernet é definida por protocolos de camada física e de camada de enlace de dados.

6.1.2

## Campos de um Quadro Ethernet

O tamanho mínimo de quadro Ethernet é 64 bytes e o máximo é 1518 bytes. Isso inclui todos os bytes do campo de endereço MAC de destino através do campo FCS (Frame Check Sequence). O campo de preâmbulo não é incluído ao descrever o tamanho do quadro.

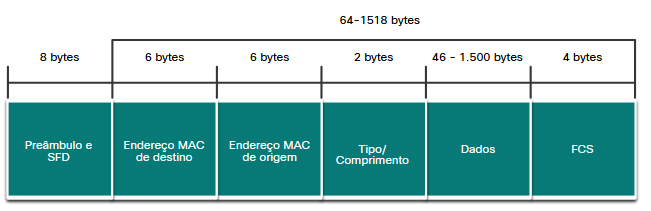
Qualquer quadro com comprimento menor que 64 bytes é considerado um"fragmento de colisão" ou um "quadro desprezível" e é automaticamente descartado pelas estações receptoras. Quadros com mais de 1.500 bytes de dados são considerados “jumbo” ou “baby giant”.

Se o tamanho de um quadro transmitido for menor que o mínimo ou maior que o máximo, o dispositivo receptor descarta o quadro. É provável que quadros perdidos sejam resultado de colisões ou outros sinais indesejados. Eles são considerados inválidos. No entanto, as interfaces Fast Ethernet e Gigabit Ethernet de alguns switches Cisco Catalyst podem ser configuradas para suportar quadros jumbo maiores.

A figura mostra cada campo no quadro Ethernet. Consulte a tabela para obter mais informações sobre a função de cada campo.

O diagrama mostra os campos de um quadro Ethernet. From left to right the fields and their length are: Preamble and SFD, 8 bytes; destination MAC address, 6 bytes; source MAC address, 6 bytes; type / length, 2 bytes; data, 46 - 1500 bytes; and F C S, 4 bytes. Excluding the first field, the total number of bytes in the remaining fields is between 64 – 1518 bytes.

### Campos do quadro Ethernet



| **Campo** | **Descrição** |
| --- | --- |
| Campos Preâmbulo e Delimitador Início de Quadro | O Preâmbulo (7 bytes) e o Delimitador de Quadro Inicial (SFD), também chamado de Início do Frame (1 byte), os campos são usados para sincronização entre o dispositivos de envio e recepção. Estes primeiros oito bytes do quadro são usado para chamar a atenção dos nós de recepção. Essencialmente, o primeiro poucos bytes informam aos receptores para se prepararem para receber um novo quadro. |
| Campo Endereço MAC de Destino | Este campo de 6 bytes é o identificador do destinatário desejado. Como você , esse endereço é usado pela Camada 2 para auxiliar dispositivos no determinar se um quadro é endereçado a eles. O endereço no quadro é em comparação com o endereço MAC no dispositivo. Se houver uma correspondência, o aceita o quadro. Pode ser unicast, multicast ou broadcast endereço: |
| Campo Endereço MAC de Origem | Esse campo de 6 bytes identifica a NIC ou interface de origem do quadro. Um endereço MAC de origem só pode ser um endereço unicast. |
| Tipo/Comprimento | Este campo de 2 bytes identifica o protocolo da camada superior encapsulado em o quadro Ethernet. Os valores comuns são, em hexadecimal, 0x800 para IPv4, 0x86DD para IPv6 e 0x806 para ARP.  **Nota**: Você também pode ver este campo referido como EtherType, Tipo ou Comprimento. |
| Campo Dados | Este campo (46 - 1500 bytes) contém os dados encapsulados de um camada superior, que é uma PDU de Camada 3 genérica, ou mais comumente, um IPv4 pacote. Todos os quadros devem ter pelo menos 64 bytes. Se um pequeno pacote for encapsulado, bits adicionais chamados pad são usados para aumentar o tamanho do quadro para este tamanho mínimo. |
| Campo Sequência de Verificação de Quadro | O campo FCS (Frame Check Sequence) (4 bytes) é usado para detectar erros em um quadro. Ele utiliza uma verificação de redundância cíclica (CRC). O dispositivo de envio inclui os resultados de um CRC no campo FCS do quadro. O comando O dispositivo receptor recebe o quadro e gera um CRC para procurar erros. Se o cálculo corresponder, significa que não houve erro. Cálculos que não coincidem são uma indicação de que os dados foram alterados; Portanto, o quadro é descartado. Uma alteração nos dados pode ser o resultado de um interrupção dos sinais elétricos que representam os bits. |

6.1.3

## Formato do Endereço MAC

A figura é três colunas mostrando os equivalentes decimal e hexadecimais de números binários de 4 bits selecionados. Da esquerda para a direita, os cabeçalhos das colunas são: decimal, binário e hexadecimal. Cada coluna tem 16 linhas abaixo do cabeçalho.

### Equivalentes decimais e binários de 0 a F Hexadecimal



Um endereço MAC Ethernet é um valor binário de 48 bits expresso como 12 dígitos hexadecimais (4 bits por dígito hexadecimal). Os dígitos hexadecimais usam os números de 0 a 9 e as letras de A a F. A figura mostra os valores decimais e hexadecimais equivalentes para 0000 a 1111 binários. Hexadecimal é comumente usado para representar dados binários. Endereços IPv6 são outro exemplo de endereçamento hexadecimal.

Dependendo do dispositivo e do sistema operacional, você verá várias representações de endereços MAC, conforme exibido na figura abaixo.

A Figura 1 mostra uma tabela de valores decimais entre 0 e 15 com o equivalente Binário e Hexadecimal. Esta tabela mostra porque Hexadecimal tem letras de A a F, juntamente com números de 0 a 9. A Figura 2 mostra que um Endereço MAC pode ser representado com traços, dois pontos ou pontos.

### Diferentes Representações de Endereços MAC

Com travessões 00-60-2F-3A-07-BC

Com dois pontos 00:60:2 F:3A:07:BC

Com períodos 0060.2F3A.07BC

Todos os dados que viajam na rede são encapsulados em quadros Ethernet. Um analista de segurança cibernética deve ser capaz de interpretar os dados Ethernet que são capturados por analisadores de protocolo e outras ferramentas.

Qual campo de quadro Ethernet ajuda um host a determinar se o quadro recebido é endereçado a ele?

Endereço de destino

Qual campo de quadro Ethernet notifica os destinos para se prepararem para um novo quadro?

Preâmbulo

Qual campo de quadro Ethernet descreve o protocolo de camada superior que é encapsulado?

Tipo/tamanho

Qual parte do quadro Ethernet ajuda um destino a detectar se há erros em um quadro?

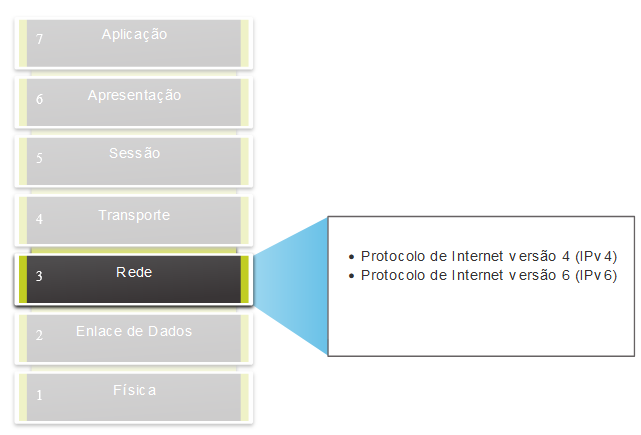
Sequência de verificação de quadro

6.2.1

## 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



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 à 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.

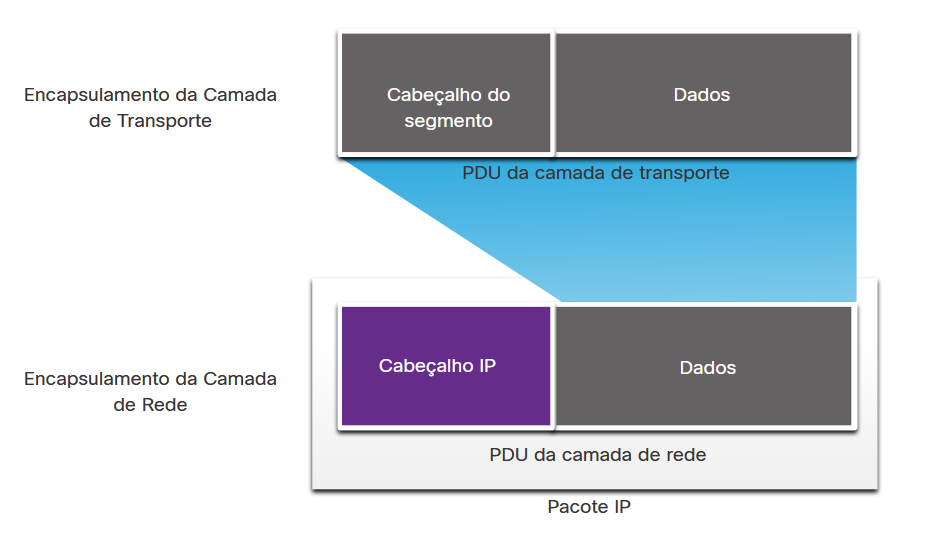
6.2.2

**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.

6.2.3

## 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.

6.2.4

**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.

destinatário com antecedência. A figura resume esse ponto-chave.

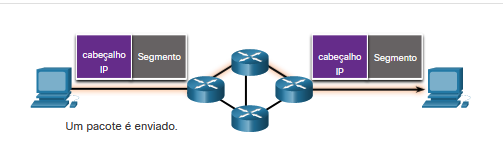
um pacote, que consiste em um cabeçalho e segmento IP, é enviado de uma origem em uma rede para um destino em outra rede

### Sem conexão - Analogia

Uma carta é enviada.CartaCartaCaixa de correio

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



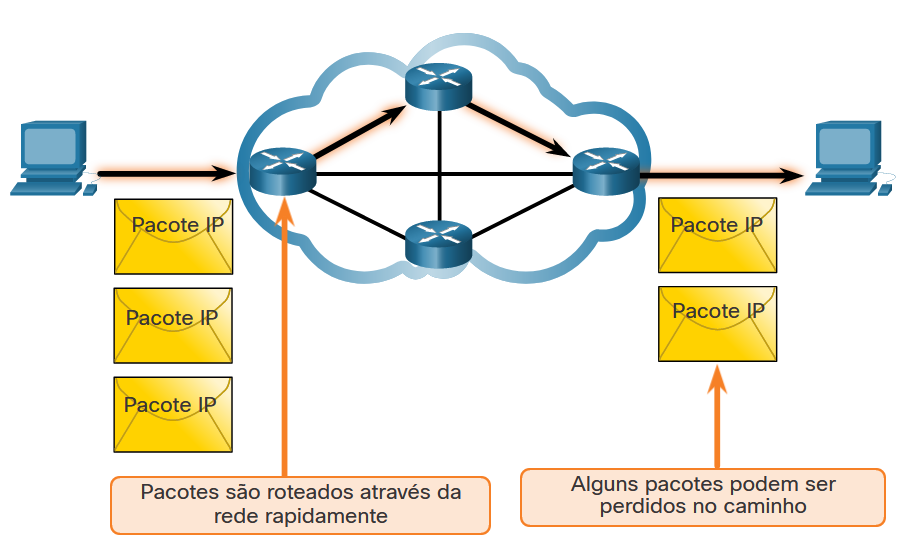
6.2.5

**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.



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.

6.2.6

**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.

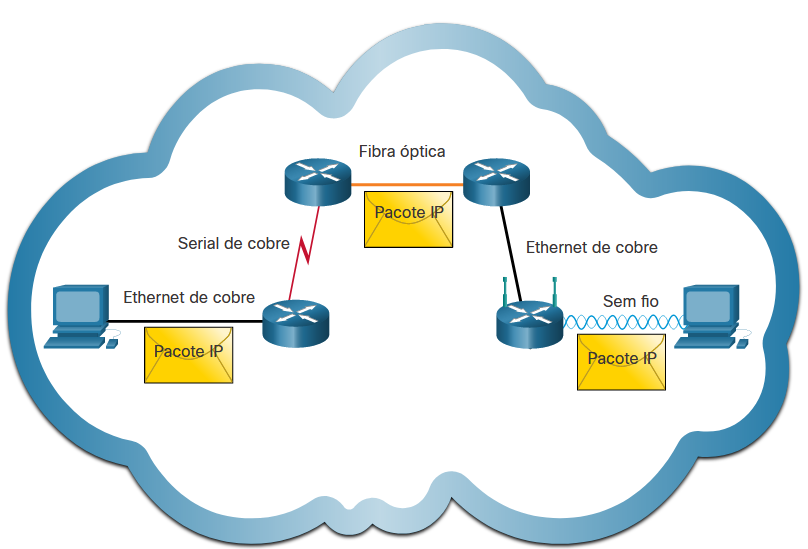
Se os pacotes forem entregues fora de ordem ou estiver faltando algum pacote, as aplicações que usam os dados, ou serviços de camada superior, deverão resolver esses problemas. Isso permite que o IP funcione de forma bem eficiente. No conjunto de protocolos TCP / IP, a confiabilidade é o papel do protocolo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

.

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.

6.2.8

**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.

6.2.9

## 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 isso como um pacote IPv4.
* **Serviços diferenciados ou DiffServ (DS) -** Anteriormente chamado de campo 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).
* **Tempo de vida (TTL) -** TTL contém um valor binário de 8 bits 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 próximo nível de protocolo. 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). Checksum de \* **cabeçalho —** Isso é usado para detectar corrupção no cabeçalho IPv4.
* **Endereço IPv4 de origem -** Contém um valor binário de 32 bits que representa o endereço IPv4 de origem do pacote. O endereço de origem IPv 4 é sempre um endereço unicast.
* **Endereço IPv4 de destino -** Contém um valor binário de 32 bits que representa o endereço IPv4 de 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.

# Noções básicas de endereçamento IP

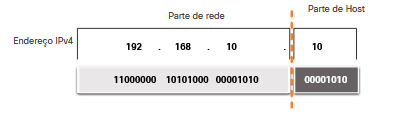
6.3.1

## Partes de Rede e de Host

Um endereço IPv4 é um endereço hierárquico de 32 bits, composto por uma parte da rede e uma parte do host. Ao determinar a parte da rede versus a parte do host, você deve observar o fluxo de 32 bits, conforme mostrado na figura.

O diagrama mostra o detalhamento de um endereço IPv4 nas partes de rede e host. O endereço IPv4 é 192.168.10.10. Abaixo, o endereço é convertido em 11000000 10101000 00001010 00001010. Uma linha rastreada mostra a seleção entre partes da rede e host. Isso ocorre após o terceiro octeto e o 24º bit.

### Endereço IPv4



Os bits na parte de rede do endereço devem ser iguais em todos os dispositivos que residem na mesma rede. Os bits na parte de host do endereço devem ser exclusivos para identificar um host específico dentro de uma rede. Se dois hosts tiverem o mesmo padrão de bits na parte de rede especificada do fluxo de 32 bits, esses dois hosts residirão na mesma rede.

Mas como os hosts sabem qual parte dos 32 bits identifica a rede e qual identifica o host? Esse é o papel da máscara de sub-rede.

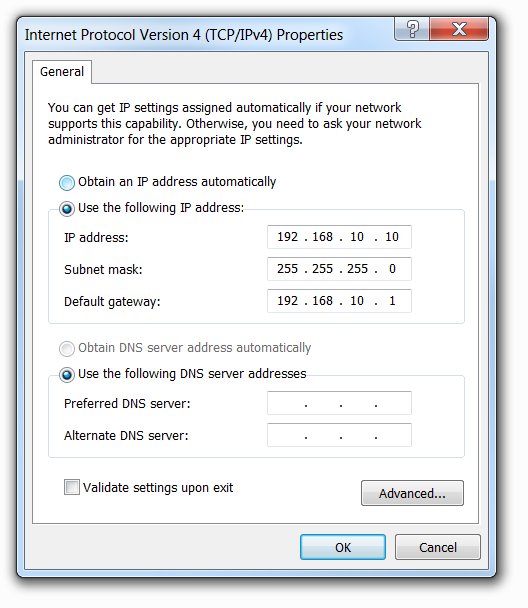
6.3.2

## A Máscara de Sub-Rede

Conforme mostrado na figura, atribuir um endereço IPv4 a um host requer o seguinte:

* **Endereço IPv4** - este é o endereço IPv4 exclusivo do host.
* **Máscara de sub-rede** – É usada para determinar a parte de rede de um endereço IPv4.

### Configuração IPv4 em um computador Windows



**Observação**: Um endereço IPv4 de gateway padrão é necessário para acessar redes remotas e os endereços IPv4 do servidor DNS são necessários para converter nomes de domínio em endereços IPv4.

A máscara de sub-rede IPv4 é usada para diferenciar a parte da rede da parte do host de um endereço IPv4. Quando um endereço IPv4 é atribuído a um dispositivo, a máscara de sub-rede é usada para determinar o endereço de rede do dispositivo. O endereço de rede representa todos os dispositivos na mesma rede.

A próxima figura mostra uma máscara de sub-rede de 32 bits em formatos decimais e binários pontilhados.

máscara de sub-rede de 255.255.255.0 no topo com a representação binária de 11111111 1111111 111111 0000000 abaixo; uma linha tracejada é desenhada após o terceiro octeto e o 24º bit

### Máscara de sub-rede

255 . 255 . 255 . 11111111 00000000 0 11111111

11111111

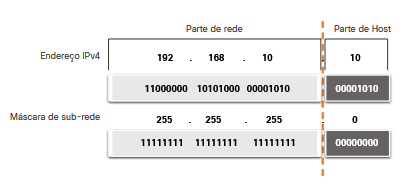
Máscara de sub-rede

Observe como a máscara de sub-rede é uma sequência consecutiva de 1 bits, seguida por uma sequência consecutiva de 0 bits.

Para identificar as partes da rede e do host de um endereço IPv4, a máscara de sub-rede é comparada com o endereço IPv4 bit por bit, da esquerda para a direita, conforme mostrado na figura.

A figura mostra um endereço IPv4, escrito em decimal com ponto e binário, com a máscara de sub-rede abaixo, também escrito em ponto decimal e binário, usado para mostrar a divisão entre a parte da rede e a parte do host do endereço. O endereço IPv4 é 192.168.10.10 que é convertido para 11000000 10101000 00001010 00001010. A máscara de sub-rede é 255.255.255.0 que é convertida para 11111111 111111 111111 00000000. Uma linha rastreada mostra uma seleção entre partes da rede e host. Isso ocorre após o terceiro octeto e 24º bit.

### Associando um endereço IPv4 à sua máscara de sub-rede



Observe que, na verdade, a máscara de sub-rede não contém a parte da rede ou host de um endereço IPv4, apenas informa ao computador onde procurar a parte do endereço IPv4 que é a parte da rede e qual parte é a parte do host.

O processo real usado para identificar a parte da rede e a parte de host é chamado de AND.

6.3.3

## Comprimento do Prefixo

Expressar os endereços de rede e os endereços de host com o endereço da máscara de sub-rede em decimal com pontos pode ser complicado. Felizmente, existe um método alternativo para identificar uma máscara de sub-rede, um método chamado comprimento do prefixo.

O comprimento do prefixo é o número de bits definido como 1 na máscara de sub-rede. Está escrito em "notação de barra", que é anotada por uma barra (/) seguida pelo número de bits definido como 1. Portanto, conte o número de bits da máscara de sub-rede e preceda-o com uma barra.

Consulte a tabela para exemplos. A primeira coluna lista várias máscaras de sub-rede que podem ser usadas com um endereço de host. A segunda coluna mostra o endereço binário de 32 bits convertido. A última coluna mostra o comprimento do prefixo resultante.

| Máscara de sub-rede Endereço de 32 bits Comprimento255.0.0.011111111.00000000.00000000.00000000/8255.255.0.011111111.11111111.00000000.00000000/16255.255.255.011111111.11111111.11111111.00000000/24255.255.255.12811111111.11111111.11111111.10000000/25255.255.255.19211111111.11111111.11111111.11000000/26255.255.255.22411111111.11111111.11111111.11100000/27255.255.255.24011111111.11111111.11111111.11110000/28255.255.255.24811111111.11111111.11111111.11111000/29255.255.255.25211111111.11111111.11111111.11111100/30 | | |
| --- | --- | --- |
| **Máscara de Sub-Rede** | **Endereço de 32 bits** | **Comprimento do Prefixo** |
| 255.0.0.0 | 11111111.00000000.00000000.00000000 | /8 |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | /16 |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | /24 |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | /25 |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | /26 |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | /27 |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | /28 |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | /29 |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | /30 |

**Observação** : Um endereço de rede também é conhecido como prefixo ou prefixo de rede. Portanto, o comprimento do prefixo é o número de 1 bits na máscara de sub-rede.

Ao representar um endereço IPv4 usando um comprimento de prefixo, o endereço IPv4 é gravado seguido do comprimento do prefixo sem espaços. Por exemplo, 192.168.10.10 255.255.255.0 seria gravado como 192.168.10.10/24. O uso de vários tipos de comprimentos do prefixo será discutido mais tarde. Por enquanto, o foco estará no prefixo /24 (ou seja, 255.255.255.0)

6.3.4

## Determinando a rede: Lógica AND

Um AND lógico é uma das três operações booleanas usadas na lógica booleana ou digital. As outras duas são OR e NOT. A operação AND é usada para determinar o endereço de rede.

AND lógico é a comparação de dois bits que produz os resultados mostrados abaixo. Observe como somente 1 AND 1 produz um 1. Qualquer outra combinação resulta em um 0.

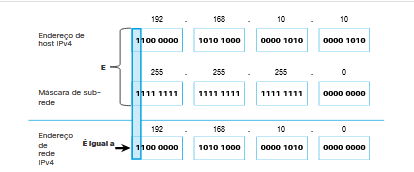
* 1 E 1 = 1
* 0 E 1 = 0
* 1 E 0 = 0
* 0 E 0 = 0

**Observação** : Na lógica digital, 1 representa Verdadeiro e 0 representa Falso. Ao usar uma operação AND, ambos os valores de entrada devem ser Verdadeiro (1) para que o resultado seja Verdadeiro (1).

Para identificar o endereço de rede de um host IPv4, é feito um AND lógico, bit a bit, entre o endereço IPv4 e a máscara de sub-rede. Quando se usa AND entre o endereço e a máscara de sub-rede, o resultado é o endereço de rede.

Para ilustrar como AND é usado para descobrir um endereço de rede, considere um host com endereço IPv4 192.168.10.10 e máscara de sub-rede 255.255.255.0, conforme mostrado na figura:

* **Endereço de host IPv4 (192.168.10.10)** - O endereço IPv4 do host em formatos decimais pontilhados e binários.
* **Máscara de sub-rede (255.255.255.0)** - A máscara de sub-rede do host nos formatos decimal com pontos e binário.
* **Endereço de rede (192.168.10.0)** - A operação lógica AND entre o endereço IPv4 e a máscara de sub-rede resulta em um endereço de rede IPv4 mostrado nos formatos decimal com pontos e binário.



Usando a primeira sequência de bits como exemplo, observe que a operação E é executada no 1 bit do endereço do host com o 1 bit da máscara de sub-rede. Isso resulta em um bit 1 para o endereço de rede. 1 E 1 = 1.

A operação AND entre um endereço de host IPv4 e uma máscara de sub-rede resulta no endereço de rede IPv4 para este host. Neste exemplo, a operação AND entre o endereço de host 192.168.10.10 e a máscara de sub-rede 255.255.255.0 (/24) resulta no endereço de rede IPv4 192.168.10.0/24. Esta é uma operação IPv4 importante, pois informa ao host a qual rede pertence.

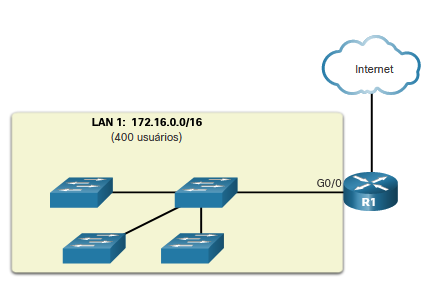
6.3.6

## Sub redes e domínos de Broadcast

A rede 192.168.10.0/24 pode suportar 254 hosts. Redes maiores, como 172.16.0.0/16, podem suportar muitos mais endereços de host (mais de 65.000). No entanto, isso pode potencialmente criar um domínio de Broadcast maior. Um problema desse tipo de domínio é que os hosts podem gerar broadcasts em excesso e afetar a rede de forma negativa. Na figura, a LAN 1 conecta 400 usuários que podem, cada um, gerar tráfego de broadcast. Tanto tráfego de broadcast pode retardar as operações da rede. Ele também pode tornar as operações do dispositivo mais lentas porque cada dispositivo deve aceitar e processar cada pacote de broadcast.

Um roteador, R1, está conectado a um switch via interface G0/0. O switch possui conexões com outros três switches. O domínio de broadcast consiste nos quatro switches e na interface do roteador à qual eles estão conectados. Isso é identificado como LAN1 com um endereço de 172.16.0.0/16. Uma conexão do roteador à Internet não está dentro do domínio de broacast.

### Um Domínio de Broadcast Grande



R1 G0/0

LAN 1: 172.16.0.0/16

Internet(400 usuários)

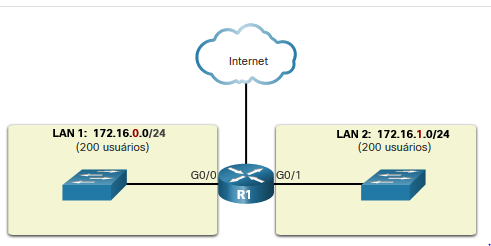
A solução é reduzir o tamanho da rede para criar domínios de broadcast menores em um processo denominado divisão em sub-redes. Os espaços de rede menores são chamados de sub-redes.

Na Figura 2, por exemplo, os 400 usuários da LAN 1 com endereço de rede 172.16.0.0 /16 foram divididos em duas sub-redes de 200 usuários cada: 172.16.0.0 /24 e 172.16.1.0 /24. Os broadcasts são propagados apenas dentro dos domínios de broadcast menores. Portanto, um broadcast em LAN 1 não se propagaria para LAN 2.

Observe como o comprimento do prefixo mudou de /16 para /24. Esta é a base da divisão em sub-redes: usar bits de host para criar sub-redes adicionais.

Um roteador, R1, está conectado a duas LANs que representam dois domínios de difusão diferentes. Conectado à esquerda via G0/0 é um switch que suporta 200 usuários em LAN 1 com um endereço de rede de 172.16.0.0/24. Conectado à direita via G0/1 é um switch que suporta 200 usuários em LAN 2 com um endereço de rede de 172.16.1.0/24.

### Comunicação entre Redes



LAN 1: 172.16.0.0/24 LAN 2: 172.16.1.0/24 G0/1 R1

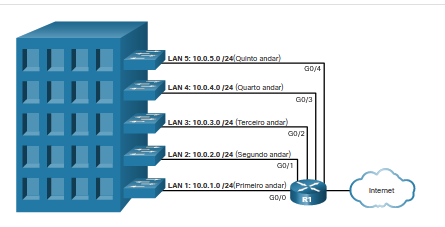
G0/0

Internet(200 usuários)(200 usuários)

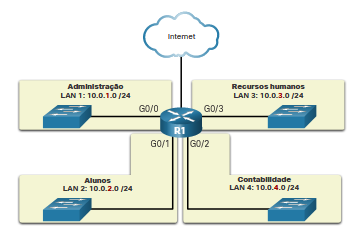
**Observação**: os termos sub-rede e rede costumam ser usados de maneira intercambiável. A maioria das redes são uma sub-rede de um bloco de endereços maior.

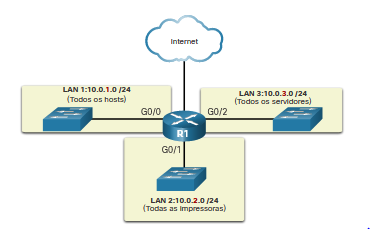
A divisão em sub-redes reduz o tráfego total da rede e melhora seu desempenho. Ele também permite que um administrador implemente políticas de segurança que controlam quais sub-redes têm permissão para se comunicar entre si, por exemplo.

Há várias maneiras de usar sub-redes para gerenciar dispositivos de rede. Os administradores de rede podem agrupar dispositivos e serviços em sub-redes que podem ser determinadas por uma variedade de fatores.



Um analista de segurança cibernética não precisa saber como segregar em sub-rede. No entanto, é importante saber o significado da máscara de sub-rede e que os hosts com endereços em sub-redes diferentes vêm de locais físicos ou virtuais diferentes em uma rede.





Quais duas afirmativas estão corretas sobre endereços IPv4? (Escolha duas.)

Ele contém uma parte do host

Ele contém uma parte do rede

Quais duas instruções estão corretas sobre uma máscara de sub-rede IPv4? (Escolha duas.)

Ele diferencia a parte da rede da parte do host de um endereço ipv4

Os bits 1 determinam a parte de rede de um endereço ipv4 e os 0 bits determinam a parte do host

Quais três declarações estão corretas sobre a operação AND? (Escolha três.)

A operação AND é executada entre um endereço ipv4 e uma máscara de sub-rede

1 0 resultados em um 0

El é usado para determinar as partes de rede e host de um endereço IPV4

Qual é o resultado de uma operação lógica AND de: 10.128.17.4 255.255.240.0?

O endereço de rede ipv4 de 10.128.26.0 255.255.240.0

6.4.1

## Classes de endereços IPv4 e máscaras de sub-rede padrão

Existem vários tipos e classes de endereços IPv4. Embora as classes de endereço estejam se tornando menos importantes na rede, elas ainda são usadas e referenciadas comumente na documentação da rede.

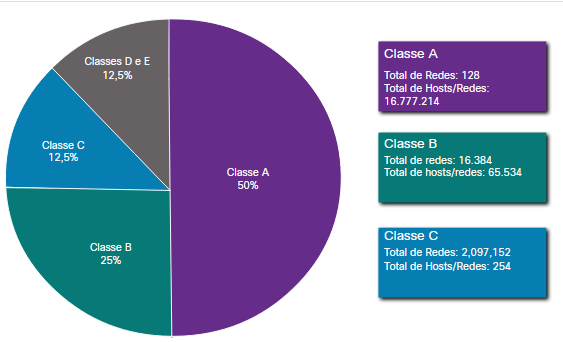
**Classes de endereços**

Em 1981, os endereços IPv4 de Internet eram atribuídos com um endereçamento classful (RFC 790) Os clientes estavam alocados em um endereço de rede em uma das três classes, A, B, ou C. A RFC dividiu os intervalos de unicast em classes específicas chamadas:

* **Classe A** (0.0.0.0/8 a 127.0.0.0/8) - Projetado para suportar redes extremamente grandes com mais de 16 milhões de endereços de host. Usava um prefixo fixo /8 com o primeiro octeto para endereços de rede e os três octetos restantes para endereços de host.
* **Classe B** (128.0.0.0 / 16 - 191.255.0.0 / 16) - Projetada para oferecer suporte às necessidades de redes de tamanho moderado a grande com até aproximadamente 65.000 endereços de host. Usava um prefixo fixo /16 com os dois octetos de mais alta ordem para endereços de rede e os dois octetos restantes para endereços de host.
* **Classe C** (192.0.0.0 / 24 - 223.255.255.0 / 24) - Projetado para oferecer suporte a pequenas redes com no máximo 254 hosts. Usava um prefixo fixo /24 com os primeiros três octetos para endereços de rede e o octeto restante para endereços de host.

**Observação**: Há também um bloco multicast de Classe D consistindo de 224.0.0.0 a 239.0.0.0 e um bloco de endereço experimental de Classe E consistindo de 240.0.0.0 - 255.0.0.0.

Como mostrado na figura, o sistema classful alocava 50% dos endereços IPv4 disponíveis para 128 redes de Classe A, 25% dos endereços para a Classe B, e a Classe C compartilhava os 25% restantes com as Classes D e E. Embora adequado na época, já que a Internet estava em expansão, obviamente esse método era um desperdício de endereços e esgotava o número de endereços de rede IPv4 disponíveis.



O endereçamento classful foi abandonado no fim dos anos de 1990 e substituído por um sistema mais moderno que não usa classe (classless). No entanto, como veremos mais tarde, o endereçamento sem classe era apenas uma solução temporária para o esgotamento de endereços IPv4.

6.4.2

## Endereços privados reservados

Os endereços IPv4 públicos são endereços roteados globalmente entre os roteadores ISP. No entanto, nem todos os endereços IPv4 disponíveis podem ser usados na Internet . Existem blocos de endereços (conhecidos como endereços privados) que são usados pela maioria das organizações para atribuir endereços IPv4 a hosts internos.

Em meados da década de 1990, os endereços IPv4 privados foram introduzidos devido ao esgotamento do espaço de endereços IPv4. Os endereços IPv4 privados são reservados e podem ser usados por uma rede interna.

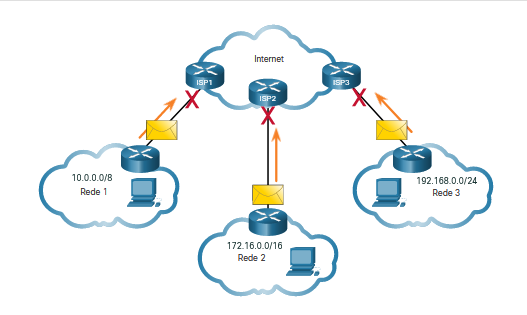
Os blocos de endereços privados

* 10.0.0.0 /8 ou 10.0.0.0 para 10.255.255.255
* 172.16.0.0 /12 ou 172.16.0.0 a 172.31.255.255
* 192.168.0.0 /16 ou 192.168.0.0 a 192.168.255.255

É importante saber que os endereços desses blocos não são permitidos na Internet e devem ser filtrados (descartados) pelos roteadores de Internet. Por exemplo, na figura, os usuários das redes 1, 2 ou 3 estão enviando pacotes para destinos remotos. Os roteadores do ISP constatam que os endereços IPv4 origem nos pacotes são endereços privados e descartam os pacotes.

A figura mostra três redes separadas, rede 1 em 10 ponto 0 ponto 0 ponto 0/8, rede 2 em 172 ponto 16 ponto 0 ponto 0/16 e rede 3 em 192 ponto 168 ponto 0 ponto 0. Cada roteador de rede se conecta ao seu próprio roteador i s p. Os roteadores ISP estão conectados à Internet. As redes são endereçadas de modo privado. Na figura, cada roteador está enviando um pacote endereçado de modo privado para o roteador ISP. Cada roteador ISP tem um X vermelho sobre o link significando que o roteador não aceitará o pacote.

### Endereços privados não podem ser roteados pela Internet



A maioria das organizações usa endereços IPv4 privados para seus hosts internos. No entanto, esses endereços da RFC 1918 não podem ser roteados na Internet e devem ser convertidos em um endereço IPv4 público. A NAT (conversão de endereços de rede) é usada para converter endereços IPv4 privados em endereços IPv4 públicos. Normalmente isso é feito no roteador que conecta a rede interna à rede do ISP.

Roteadores domésticos têm a mesma capacidade. Por exemplo, a maioria dos roteadores atribui endereços IPv4 a seus hosts com e sem fio com base no endereço privado 192.168.1.0 /24. A interface do roteador doméstico que se conecta à rede do provedor de serviços de Internet (ISP) geralmente recebe um endereço IPv4 público para usar na Internet.

# O gateway padrão

6.5.1

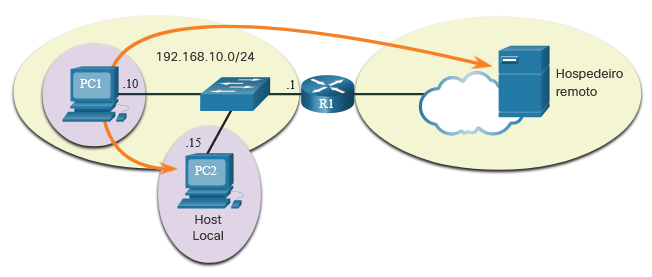
## Decisão de Encaminhamento do Host

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:

* **Próprio** - Um host pode executar ping em si mesmo enviando um pacote para um endereço IPv4 especial de 127.0.0.1 ou um endereço IPv6 :: / 1, conhecido como 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.



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 junto com seu próprio endereço IPv4 e o endereço IPv4 de destino para fazer essa determinação.
* **Em IPv6** - o roteador local anuncia o endereço da rede local (prefixo) para todos os dispositivos da 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).

6.5.2

**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.

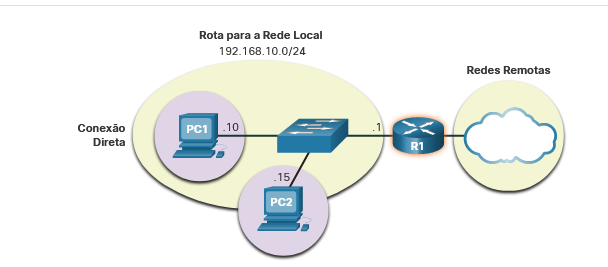
6.5.3

## 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.

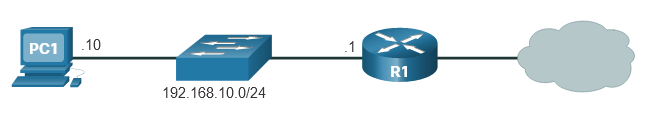
Tanto PC1 quanto PC2 terão uma rota padrão para enviar todo o tráfego destinado a redes remotas para R1.

6.5.4

## 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.

192.168.10.0/24 .10 .1 PC1

R1

### 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 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 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 interface** - lista o endereço de controle de acesso à mídia (MAC) e o número de interface atribuído de cada interface 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.

Qual declaração sobre decisões de encaminhamento de host é verdadeira?

Os hosts locais podem se alcançar sem a necessidade de um roteador

Qual a instrução de gateway padrão é verdadeira?

O endereço do gateway padrão é o endereço IP do roteador na rede local

Quais dois comandos podem ser inseridos em um host Windows para exibir sua tabela de roteamento ipv4 e ipv6 (Escolha duas)

Netstat –r

Route print

# IPv6

6.6.1

## Necessidade de IPv6

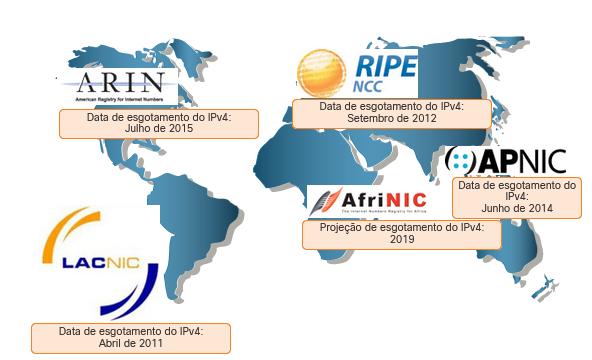
Você já sabe que o IPv4 está ficando sem endereços. É por isso que você precisa aprender sobre IPv6.

Projetado para ser o sucessor do IPv4, o IPv6 tem um maior espaço de endereços de 128 bits, fornecendo 340 undecilhões de endereços (340 seguido por 36 zeros). No entanto, o IPv6 é mais do que apenas endereços maiores.

Quando a IETF começou o desenvolvimento de um sucessor para o IPv4, aproveitou para corrigir as limitações do IPv4 e incluir aprimoramentos. Um exemplo é o ICMPv6 (Internet Control Message Protocol versão 6), que inclui a resolução de endereços e a configuração automática de endereços, não encontradas no ICMP para IPv4 (ICMPv4).

A redução do espaço de endereços IPv4 tem sido o principal fator para migrar para o IPv6. À medida que África, Ásia e outras áreas do mundo ficarem mais conectadas à Internet, não haverá endereços IPv4 suficientes para acomodar esse crescimento. Conforme mostra a figura, quatro dos cinco RIRs estão com endereços IPv4 esgotados.

O gráfico mostra um mapa global dos cinco registros regionais da internet e há datas de exaustão IPv4. A data de exaustão do ARINs IPv4 é julho de 2015, os dados de exaustão do RIPE NCCs são setembro de 2012, a data de exaustão das APNICs é junho de 2014, a data de exaustão de LACNICs é abril de 2011 e a data de exaustão projetada pela AFRINICs é 2020.



O IPv4 tem um máximo teórico de 4,3 bilhões de endereços. Combinados à NAT (tradução de endereços de rede), os endereços privados foram imprescindíveis para retardar a redução do espaço de endereços IPv4. No entanto, o NAT é problemático para muitos aplicativos, cria latência e possui limitações que impedem severamente as comunicações ponto a ponto.

Com o número cada vez maior de dispositivos móveis, os provedores móveis têm liderado o caminho com a transição para o IPv6. Os dois principais provedores de telefonia móvel nos Estados Unidos relatam que mais de 90% de seu tráfego usa IPv6.

A maioria dos principais ISPs e provedores de conteúdo, como YouTube, Facebook e NetFlix, também fizeram a transição. Muitas empresas como Microsoft, Facebook e LinkedIn estão fazendo transição para IPv6 somente internamente. Em 2018, a ISP Comcast de banda larga relatou uma implantação de mais de 65% e a British Sky Broadcasting mais de 86%.

**⁪Internet das Coisas**

A internet de hoje é significativamente diferente da internet das últimas décadas. A internet de hoje é mais do que e-mail, páginas da web e transferências de arquivos entre computadores. A Internet em evolução está se tornando uma Internet das Coisas (IoT). Os únicos dispositivos que acessam a Internet não serão mais computadores, tablets e smartphones. Os dispositivos equipados com sensor e prontos para a Internet de amanhã incluirão tudo, desde automóveis e dispositivos biomédicos, até eletrodomésticos e ecossistemas naturais.

Com uma população cada vez maior na Internet, espaço de endereços IPv4 limitado, problemas com NAT e uma Internet das Coisas, chegou o momento de iniciar a transição para o IPv6.

6.6.2

## Formatos de Endereço IPv6

O primeiro passo para aprender sobre IPv6 em redes é entender a forma como um endereço IPv6 é escrito e formatado. Os endereços IPv6 são muito maiores do que os endereços IPv4, razão pela qual é improvável que fiquemos sem eles.

Os endereços IPv6 têm 128 bits e são escritos como uma sequência de valores hexadecimais. Cada 4 bits são representados por um único dígito hexadecimal, totalizando 32 valores hexadecimais, como mostra a Figura 1. Os endereços IPv6 não diferenciam maiúsculas e minúsculas e podem ser escritos tanto em minúsculas como em maiúsculas.

### Segmentos ou Hextets de 16 bits

X : X : X : X : X : X : X : X 0000 0000 0000 0000 0000 0000 0000 0000 ffff ffff ffff ffff ffff ffff ffff ffff : : : : : : : 1111 1111 1111 1111 0000 0000 0000

0000

4 dígitos hexadecimais = 16 dígitos bináriosatéatéatéatéatéatéatéatéatéatéatéaté

**Formato Preferencial**

Como mostrado na Figura 1, o formato preferencial para escrever um endereço IPv6 é x: x: x: x: x: x: x: x, com cada “x” consistindo de quatro valores hexadecimais. O termo octeto refere-se aos oito bits de um endereço IPv4. No IPv6, um hexteto é o termo não oficial usado para se referir a um segmento de 16 bits ou quatro valores hexadecimais. Cada “x” equivale a um único hexteto, 16 bits ou quatro dígitos hexadecimais.

Formato preferencial significa que o endereço IPv6 é gravado usando todos os 32 dígitos hexadecimais. Isso não significa necessariamente que é o método ideal para representar o endereço IPv6. Existem duas regras que ajudam a reduzir o número de dígitos necessários para representar um endereço IPv6.

A Figura 3 tem exemplos de endereços IPv6 no formato preferencial.

2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000: 0200   
 2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000: 1234   
 2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a: 19ac   
 2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000: 0000   
 fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef   
 fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001   
 fe80 : 0000 : 0000 : 0000 : c012 : 9aff : fe9a: 19ac   
 fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef   
 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001   
 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0000

6.6.3

## Regra 1 - omitir zeros à esquerda

A primeira regra para ajudar a reduzir a notação de endereços IPv6 é omitir os 0s (zeros) à esquerda de qualquer seção de 16 bits ou hexteto. Aqui estão quatro exemplos de maneiras de omitir zeros à esquerda:

* 01AB pode ser representado como 1AB
* 09f0 pode ser representado como 9f0
* 0a00 pode ser representado como a00
* 00ab pode ser representado como ab

Essa regra se aplica somente aos 0s à esquerda, e NÃO aos 0s à direita. Caso contrário, o endereço ficaria ambíguo. Por exemplo, o hexteto “abc” poderia ser “0abc” ou “abc0”, mas essas duas representações não se referem ao mesmo valor.

| TypeFormatPreferred2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200No leading 0s2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200Preferred2001 : 0db8 : 0000 : 00a3 : ab00 : 0ab0 : 00ab : 1234No leading 0s2001 : db8 : 0 : a3 : ab00 : ab0 : ab : 1234Preferred2001 : 0db8 : 000a : 0001 : c012 : 90ff : fe90 : 0001No leading 0s2001 : db8 : a : 1 : c012 : 90ff : fe90 : 1Preferred2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000No leading 0s2001 : db8 : aaaa : 1 : 0 : 0 : 0 : 0Preferredfe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdefNo leading 0sfe80 : 0 : 0 : 0 : 123 : 4567 : 89ab : cdefPreferredfe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001No leading 0sfe80 : 0 : 0 : 0 : 0 : 0 : 0 : 1Preferred0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001No leading 0s 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1Preferred0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000No leading 0s 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 | |
| --- | --- |
| **Tipo** | **Formatar** |
| Preferencial | 2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200 |
| Nenhum 0 à esquerda | 2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200 |
|  |  |
|  |  |
| Preferencial | 2001 : **0**db8 : **000**0 : **00**a3 : ab00 : **0**ab0 : **00**ab : 1234 |
| Nenhum 0 à esquerda | 2001 : db8 : 0 : a3 : ab00 : ab0 : ab : 1234 |
|  |  |
|  |  |
| Preferencial | 2001 : **0**db8 : **000**a : **000**1 : c012 : 90ff : fe90 : **000**1 |
| Nenhum 0 à esquerda | 2001 : db8 : a : 1 : c012 : 90ff : fe90 : 1 |
|  |  |
|  |  |
| Preferencial | 2001 : **0**db8 : aaaa : **000**1 : **000**0 : **000**0 : **000**0 : **000**0 |
| Nenhum 0 à esquerda | 2001 : db8 : aaaa : 1 : 0 : 0 : 0 : 0 |
|  |  |
|  |  |
| Preferencial | fe80 : **000**0 : **000**0 : **000**0 : **0**123 : 4567 : 89ab : cdef |
| Nenhum 0 à esquerda | fe80 : 0 : 0 : 0 : 123 : 4567 : 89ab : cdef |
|  |  |
|  |  |
| Preferencial | fe80 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**1 |
| Nenhum 0 à esquerda | fe80 : 0 : 0 : 0 : 0 : 0 : 0 : 1 |
|  |  |
|  |  |
| Preferencial | **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**1 |
| Nenhum 0 à esquerda | 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1 |
|  |  |
|  |  |
| Preferencial | **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 |
| Nenhum 0 à esquerda | 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 |

6.6.4

## Regra 2 - dois pontos duplos

A segunda regra para ajudar a reduzir a notação de endereços IPv6 é que o uso de dois-pontos duplo (::) pode substituir uma única sequência contígua de um ou mais segmentos de 16 bits (hextetos) compostos exclusivamente por 0s. Por exemplo, 2001:db8:cafe: 1:0:0:0:1 (0s iniciais omitidos) poderia ser representado como 2001:db8:cafe:1::1. O dois-pontos duplos (::) é usado no lugar dos três hextets all-0 (0:0:0).

Os dois-pontos em dobro (::) só podem ser usados uma vez em um endereço; caso contrário, haveria mais de um endereço resultante possível. Quando associada à técnica de omissão dos 0s à esquerda, a notação de endereço IPv6 pode ser bastante reduzida. É o chamado formato compactado.

Aqui está um exemplo do uso incorreto de dois pontos: 2001:db8::abcd::1234.

O dois-pontos duplo é usado duas vezes no exemplo acima. Aqui estão as possíveis expansões deste endereço de formato compactado incorreto:

* 2001:db8::abcd:0000:0000:1234
* 2001:db8::abcd:0000:0000:0000:1234
* 2001:db8:0000:abcd::1234
* 2001:db8:0000:0000:abcd::1234

Se um endereço tiver mais de uma cadeia contígua de todos os hextets 0, a prática recomendada é usar dois pontos duplos (::) na cadeia mais longa. Se as strings forem iguais, a primeira string deve usar dois pontos duplos (::).

| TypeFormatPreferred2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200Compressed/spaces2001 : db8 : 0 : 1111 : : 200Compressed2001:db8:0:1111::200Preferred2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000Compressed/spaces2001 : db8 : 0 : 0 : ab00 :: Compressed2001:db8:0:0:ab00::Preferred2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000Compressed/spaces2001 : db8 : aaaa : 1 ::Compressed2001:db8:aaaa:1::Preferredfe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdefCompressed/spacesfe80 : : 123 : 4567 : 89ab : cdefCompressedfe80::123:4567:89ab:cdefPreferredfe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001Compressed/spacesfe80 : : 1Compressedfe80::0Preferred0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001Compressed/spaces:: 1Compressed::1Preferred0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000Compressed/spaces::Compressed:: | |
| --- | --- |
| **Tipo** | **Formatar** |
| Preferêncial | 2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200 |
| Compressados/espaços | 2001 : db8 : 0 : 1111 : : 200 |
| Compactado | 2001:db8:0:1111::200 |
|  |  |
| Preferencial | 2001 : **0**db8 : **000**0 : **000**0 : ab00 : **0000** : **0000** : **0000** |
| Compressados/espaços | 2001 : db8 : 0 : 0 : ab00 :: |
| Compactado | 2001:db8:0:0:ab00:: |
|  |  |
| Preferencial | 2001 : **0**db8 : aaaa : **000**1 : **0000** : **0000** : **0000** : **0000** |
| Compressados/espaços | 2001 : db8 : aaaa : 1 :: |
| Compactado | 2001:db8:aaaa:1:: |
|  |  |
| Preferencial | fe80 : **0000** : **0000** : **0000** : **0**123 : 4567 : 89ab : cdef |
| Compressados/espaços | fe80 : : 123 : 4567 : 89ab : cdef |
| Compactado | fe80::123:4567:89ab:cdef |
|  |  |
| Preferencial | fe80 : **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **000**1 |
| Compressados/espaços | fe80 : : 1 |
| Compactado | fe80::0 |
|  |  |
| Preferencial | **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **000**1 |
| Compressados/espaços | :: 1 |
| Compactado | ::1 |
|  |  |
| Preferencial | **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **0000** |
| Compressados/espaços | :: |
| Compactado | :: |

6.6.5

## Comprimento do Prefixo IPv6

Lembre-se de que o prefixo (a parte de rede) de um endereço IPv4 pode ser identificado pelo comprimento do prefixo (notação em barra) ou por uma máscara de sub-rede decimal com pontos. Por exemplo, o endereço IPv4 192.168.1.10 com máscara de sub-rede decimal com pontos 255.255.255.0 é equivalente a 192.168.1.10/24.

No IPv4 o /24 é chamado de prefixo. No IPv6 é chamado de comprimento do prefixo. O IPv6 não usa a notação decimal com pontos da máscara de sub-rede. Como o IPv4, o comprimento do prefixo é representado na notação de barra e é usado para indicar a parte da rede de um endereço IPv6.

O comprimento do prefixo pode variar de 0 a 128. O comprimento do prefixo IPv6 recomendado para LANs e a maioria dos outros tipos de redes é /64, conforme mostrado na figura.

O gráfico mostra um endereço IPv6 dividido em um prefixo de 64 bits e um ID de interface de 64 bits. O prefixo de 64 bits é 2001:0db8:000a:0000. O ID da interface de 64 bits é 0000:0000:0000:0000.

### Comprimento do Prefixo IPv6

PrefixoID da interface0000:0000:0000:00002001:0db8:000a:000064 bits64 bitsExemplo: 2001:db8:a::/64

Isso significa que o prefixo ou a parte de rede do endereço é de 64 bits, restando outros 64 bits para a ID da interface (parte de host) do endereço.

É altamente recomendável usar um ID de interface de 64 bits para a maioria das redes. Isso ocorre porque a configuração automática de endereço sem estado (SLAAC) usa 64 bits para o ID de interface. Também facilita a criação e o gerenciamento de sub-redes.

# Resumo de protocolo Ethernet e IP

6.7.1

## O que aprendi neste módulo?

**Ethernet**

Ethernet e LAN sem fio (WLANs) são as duas tecnologias LAN mais populares. A Ethernet opera nas camadas físicas e de link de dados do modelo OSI e são definidas nas normas IEEE 802.2 e 802.3. Ethernet suporta larguras de banda de 10 Mbps a 100.000 Mbps. É importante conhecer os campos de quadro Ethernet. Um endereço MAC Ethernet é um valor binário de 48 bits expresso como 12 dígitos hexadecimais (4 bits por dígito hexadecimal). O endereço MAC pode ser representado usando traços, dois-pontos ou pontos entre os grupos de dígitos.

**IPv4**

Os protocolos de camada de rede permitem que os dispositivos finais troquem dados entre redes e internet. IP versão 4 (IPv4) e IP versão 6 (IPv6) são os principais protocolos de comunicação de camada de rede. Para realizar comunicações ponta a ponta através dos limites da rede, os protocolos da camada de rede executam quatro operações básicas: endereçamento de dispositivos finais, encapsulamento, roteamento e descapsulamento. O IP encapsula o segmento da camada de transporte adicionando um cabeçalho IP que é usado para entregar o pacote, que é examinado pelos dispositivos da Camada 3 (ou seja, roteadores e switches da Camada 3), para chegar ao host de destino. IP é sem conexão, melhor esforço e independente de mídia. É importante estar familiarizado com a estrutura do pacote IP.

**Noções básicas de endereçamento IP**

Um endereço IPv4 é um endereço hierárquico de 32 bits, composto por uma parte da rede e uma parte do host. Os bits na parte de rede do endereço devem ser iguais em todos os dispositivos que residem na mesma rede. Os bits na parte de host do endereço devem ser exclusivos para identificar um host específico dentro de uma rede. Um host recebe um endereço IPv4 e uma máscara de sub-rede. A máscara de sub-rede IPv4 é usada para diferenciar a parte da rede da parte do host de um endereço IPv4. O endereço de rede representa todos os dispositivos na mesma rede. O comprimento do prefixo é o número de bits definidos como 1 na máscara de sub-rede. É escrito em “notação de barra”, que é indicada por uma barra (/) seguida pelo número de bits definido como 1. O processo usado para identificar a parte da rede e a parte do host é denominado AND. A sub-rede cria domínios de difusão menores para reduzir o tráfego geral da rede, melhorar o desempenho da rede e implementar políticas de segurança. As sub-redes podem ser usadas para agrupar dispositivos por local, departamento ou tipo de dispositivo.

**Tipos de endereços IPv4**

As primeiras implementações do IPv4 forneceram endereços de rede roteáveis globalmente baseados no sistema clássico usando Classe A, Classe B e Classe C, cada um com diferentes intervalos de endereços IP. No entanto, o sistema de endereçamento clássico era defeituoso e rapidamente esgotado endereços de rede disponíveis e, portanto, foi substituído pelo sistema de endereçamento sem classes. Existem endereços IPv4 públicos e endereços IPv4 privados. Os endereços privados devem ser usados por organizações e não são propagados na internet. Existem três blocos de endereços privados disponíveis.

**O gateway padrão**

Se um pacote é destinado a um host local ou a um host remoto é determinado pelo dispositivo final de origem. Em redes IPv4, o dispositivo de origem usa sua própria máscara de sub-rede junto com seu próprio endereço IPv4 e o endereço IPv4 de destino para fazer essa determinação. Em uma rede IPv6, o roteador local anuncia o endereço da rede local (prefixo) para todos os dispositivos da rede. O roteador conectado ao segmento de rede local é conhecido como gateway padrão. 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 também roteia o tráfego para outras redes. Uma rota padrão é a rota ou o caminho que o computador usa quando tenta entrar em contato com uma rede remota. Em um host do Windows, o comando **route print** ou **netstat -r** pode ser usado para exibir a tabela de roteamento do host.

**IPv6**

Um endereço IPv6 é um endereço hierárquico de 128 bits. O espaço de endereço de 128 bits fornece um pool muito maior de endereços IP disponíveis publicamente (ou seja, 340 undecillion) do que IPv4 (ou seja, 4,3 bilhões). O IPv6 também inclui o Internet Control Message Protocol versão 6 (ICMPv6), que fornece resolução de endereço e configuração automática de endereço. Esses recursos não são encontrados no ICMPv4. Os endereços IPv6 são escritos como uma string de valores hexadecimais. A cada quatro bits é representado por um único dígito hexadecimal; para um total de 32 valores hexadecimais. Existem duas regras que ajudam a reduzir o número de dígitos necessários para representar um endereço IPv6. A primeira regra é omitir os 0s (zeros) iniciais em qualquer hexteto. A segunda regra é que dois pontos duplos (: :) podem substituir qualquer string única contígua de um ou mais hextetos de 16 bits que consistem em todos os zeros. IPv6 usa o comprimento do prefixo em notação de barra para indicar a parte da rede de um endereço IPv6. O comprimento do prefixo pode variar de 0 a 128. O comprimento recomendado do prefixo IPv6 para LANs e a maioria dos outros tipos de redes é / 64. Isso ocorre porque a configuração automática de endereço sem estado (SLAAC) usa 64 bits para o ID de interface. Também facilita a criação e o gerenciamento de sub-redes.

6.7.2

Módulo 6: Teste de protocolo Ethernet e IP

Quais duas características descrevem a tecnologia Ethernet? (Escolha duas.)

É suportado pelos padrões IEEE 802.3

Ele usa o método e controle de acesso CSMA/CD

Tópico 6.1.0 - O padrão Ethernet 802.3 especifica que uma rede implementa o método de controle de acesso CSMA / CD.

Quais são os serviços fornecidos pela camada de rede do modelo OSI? (Escolha duas.)

Tópico 6.2.0 - A camada de rede do modelo OSI fornece vários serviços para permitir a comunicação entre dispositivos:

endereçamento

encapsulamento

roteamento

desencapsulamento

Detecção de erro, colocação de quadros no meio físico e detecção de colisão são funções da camada de enlace de dados.

Roteamento de pacotes em direção ao destino

Encapsulamento de PDUs da camada de transporte

Como os hosts garantem que seus pacotes sejam direcionados para o destino correto da rede?

Eles precisam manter sua própria tabela e roteamento local que contém uma rota para a interface de loopack, uma rota de rede local e uma rota padrão remota.

Tópico 6.5.0 - Os hosts devem manter sua própria tabela de roteamento local para garantir que os pacotes da camada de rede sejam direcionados à rede de destino correta. Esta tabela local normalmente contém uma rota para a interface de loopback, uma rota para a rede à qual o host está conectado e uma rota padrão local, que representa a rota que os pacotes devem tomar para alcançar todos os endereços de rede remotos.

Um técnico usa o comando ping 127.0.0.1. O que o técnico está testando?

A pilha TCP/IP em um host de rede

Tópico 6.4.0 - 127.0.0.1 é o endereço de loopback local em qualquer dispositivo de rede TCP/IP. Fazendo ping neste endereço, o técnico está verificando a pilha do protocolo TCP / IP naquele dispositivo específico.

Qual é o formato compactado correto do endereço IPv6 2001:0db8:eeff:000a:0000:0000:0000:0001?

2001:db8:eeff:a::1

Tópico 6.6.0 - Existem duas regras para compactação de endereços IPv6. Regra 1: os zeros iniciais em qualquer hexteto podem ser removidos. Regra 2: os hextextos contíguos iguais a zero podem ser compactados em dois pontos duplo. A regra dois só pode ser aplicada uma vez.

Qual função ou operação é executada pela subcamada LLC?

Ele se comunica com camadas de protocolo superiores

Tópico 6.1.0 - A subcamada Ethernet LLC tem a responsabilidade de lidar com a comunicação entre as camadas superiores e inferiores da pilha de protocolos. O LLC é implementado em software e se comunica com as camadas superiores do aplicativo para fazer a transição do pacote para as camadas inferiores para entrega.

Quantos endereços IP úteis estão disponíveis na rede 192.168.1.0/27?

1) 32 – 27 = 5; 2) 2 ^ 5 – 2 = 30

Tópico 6.3.0 - A máscara A / 27 é igual a 255.255.255.224. Restam 5 bits de host. Com 5 bits de host, é possível obter 32 endereços IP, porém um endereço representa o número de sub-rede e outro representa o endereço de broadcast. Sendo assim, 30 endereços podem ser atribuídos a dispositivos de rede.

At the top is a screen capture with the following words: Ethernet adapter Local Area Connection: Connection-specific DNS Suffix: launchmodem.com IP Address: 192.168.1.95 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254. Under these words from left bottom to right top is the following: PC2 is connected with a straight line to Switch2. Switch2 connects with a straight line to Router2. Router2 has a line that extends into a cloud. Out of the cloud is a line that attaches to Router1. Router1 also has a straight line to connect to Switch1. Switch1 has a straight line that attaches to PC1.

É o endereço IP da interface Router 1 que conecta PC1 a outros dispositivos na mesma LAN

Consulte a figura. Considere a configuração do endereço IP mostrada a partir do PC1. Qual é a descrição do endereço do gateway padrão?

Tópico 6.5.0 - O gateway padrão é usado para rotear pacotes destinados a redes remotas. O endereço IP do gateway padrão é o endereço do primeiro dispositivo da Camada 3 (a interface do roteador) que se conecta à mesma rede.

Para que é utilizado o comando netstat -r?

Para exibir a tabla de roteamento do host

Tópico 6.5.0 - O comando netstat -r exibe a tabela de roteamento do host para verificar as rotas e os custos que um computador usa para se comunicar com determinadas redes.

Um dispositivo tem um endereço IPv6 2001:0DB8:75a3:0214:0607:1234:aa10:ba01 /64. Qual é a identificação de host do dispositivo?

0607:1234:aa10:ba01

Tópico 6.6.0 - Um endereço IPv6 é composto de 128 bits que são representados como oito blocos de quatro dígitos hexadecimais que são chamados de hextetos. Como cada dígito hexadecimal representa quatro bits, cada hexteto representa 16 bits. O prefixo de rede /64 indica que os primeiros 64 bits, ou os primeiros quatro hextetos, representam a porção de rede do endereço. Como há 128 bits em um endereço IPv6, isso deixa os últimos 64 bits, ou os últimos quatro hextetos, para representar a identificação do host. O valor dos últimos quatro hextetos é 0607:1234:aa10:ba01.

Qual afirmação descreve melhor um endereço MAC?

É um endereço físico atribuído a uma placa de rede Ethernt pelo fabricante

Tópico 6.1.0 - O endereço Media Access Control (MAC) é um endereço físico atribuído a cada NIC Ethernet pelos fabricantes. Tem 48 bits de comprimento. O endereço MAC é usado para identificar a origem e o destino em uma rede Ethernet local. Ele não pode ser roteado para redes remotas.

Por que um dispositivo da camada 3 executa um AND entre um endereço IP destino e a máscara de sub-rede?

Para identificar o endreço da rede destino

O tópico 6.3.0 - AND nos permite identificar o endereço de rede a partir do endereço IP e da máscara de rede.

Quais são duas características do IP? (Escolha duas.)

Opera independente do meio físico de rede

Não requer uma conexão fim a fim dedicada

Tópico 6.2.0 - O Protocolo de Internet (IP) é um protocolo de melhor esforço sem conexão. Isto significa que o protocolo IP não requer conexões fim a fim, bem como não garante a entrega dos pacotes. O protocolo IP é também independente de meio físico, o que significa que opera independente do meio físico de rede no transporte dos pacotes.

Quais são os três endereços IP privados? (Escolha três.)

192.168.5.5

172.16.4.4

10.1.1.1

Tópico 6.4.0 - Os endereços IP privados estão dentro destes três intervalos:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

# Introdução

7.0.1

## Por que devo cursar este módulo?

As redes nunca param? É claro que elas param. Felizmente, os desenvolvedores dos protocolos IP incluíram um protocolo de teste chamado ICMP. As ferramentas ICMP criam pacotes especiais que testam redes. Os analistas de segurança cibernética devem compreender a rede em que os dados normais viajam para que possam detectar comportamentos anormais. O ICMP pode ajudá-lo a entender o comportamento normal e anormal da rede.

Este módulo fornece uma visão geral de como usar as ferramentas de verificação de conectividade de rede ICMP: ping e traceroute.

7.0.2

## O que vou aprender neste 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. |

# ICMP

7.1.1

## Mensagens ICMPv4

Embora o IP seja apenas um protocolo de melhor esforço, a suíte TCP/IP prevê o envio de mensagens no caso de certos erros. Essas mensagens são enviadas com os serviços do ICMP. O objetivo dessas mensagens é dar feedback sobre questões relativas ao processamento de pacotes IP sob certas condições, e não tornar o IP confiável. 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 o IPv4. O ICMPv6 fornece os mesmos serviços para o IPv6, mas inclui funcionalidade adicional. Neste curso, o termo ICMP será usado indistintamente quando falarmos de ICMPv4 e ICMPv6.

São muitos os tipos de mensagens ICMP e os motivos pelos quais elas são enviadas. Vamos apresentar algumas das mensagens mais comuns.

Estas são as mensagens ICMP mais comuns para ICMPv4 e ICMPv6:

* Confirmação de host
* Destino ou serviço inalcançável;
* Tempo excedido..
* Redirecionamento de rota

**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). Clique em Reproduzir na figura para ver uma animação de Echo Request/Echo Reply do ICMP Esse uso das mensagens de eco ICMP é a base do utilitário ping.

animação do host 1 enviando uma solicitação de eco ICMP ping para o host 2 e a resposta de eco ICMP do host 2 de volta para o host 1

Sim, estou aqui.

**ping 192.168.30.1**

**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.

Estes são alguns dos códigos de destino inacessível para ICMPv4:

* **0** - Net unreachable (Rede Inacessível)
* **1** - Host unreachable (Host Inacessível)
* **2** - Protocol unreachable (Protocolo Inacessível)
* **3** - Port unreachable (Porta Inacessível)

**nota**: O ICMPv6 possui códigos semelhantes, mas ligeiramente diferentes, para mensagens de Destino Inacessível.

**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.

7.1.2

## Mensagens ICMPv6 RS e RA

As mensagens informativas e de erro encontradas no ICMPv6 são muito semelhantes às mensagens de controle e de erros implementadas pelo ICMPv4. No entanto, o ICMPv6 tem funcionalidade aprimorada e novos recursos que não são encontrados no ICMPv4. As mensagens ICMPv6 são encapsuladas no IPv6.

O ICMPv6 inclui quatro novos protocolos como parte do protocolo ND ou NDP (Neighbor Discovery Protocol):

Mensagens entre um roteador IPv6 e um dispositivo IPv6:

* Mensagem de Solicitação de Roteador (RS)
* Mensagem de Anúncio de Roteador (RA)

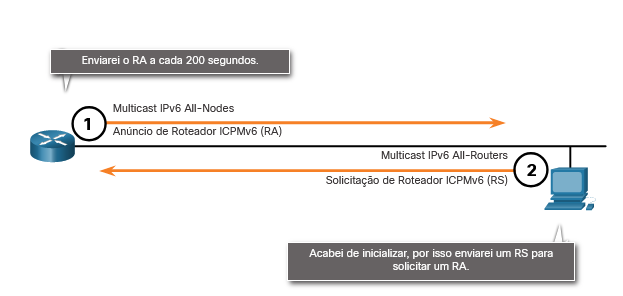
Mensagens entre dispositivos IPv6:

* Mensagem de solicitação de vizinhos (NS)
* Mensagem de anúncio de vizinhos (NA)

Solicitação de roteador

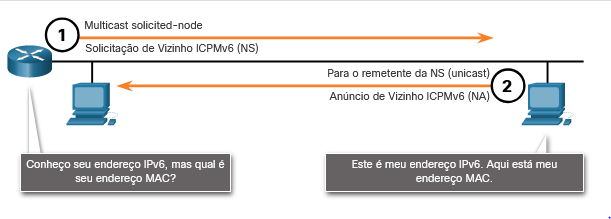
1. As mensagens de RA são enviadas por roteadores para fornecer informações de endereçamento aos hosts usando a configuração automática de endereço sem estado (SLAAC). A mensagem RA pode incluir informações de endereçamento para o host, como prefixo, comprimento do prefixo, endereço DNS e nome de domínio. 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.
2. 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.

A figura para solicitação de roteador mostra um roteador e um PC estão conectados. Acima do roteador há uma caixa de diálogo que diz que enviarei o R A a cada 200 segundos. Ao lado do roteador está o número 1 circulado com uma seta apontando para o PC e as palavras Para todos os dispositivos i p v 6 multicast i c m p v 6 anúncio do roteador. Ao lado de p c está a caixa de diálogo que diz Acabei de inicializar, então enviarei um R S para solicitar um R A. Há uma seta apontando em direção ao roteador com as palavras para todos os roteadores ip v 6 multicast i c m p v 6 solicitação de roteador.



Resolução de endereços

1. 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.
2. 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.



Detecção de Endereço Duplicado

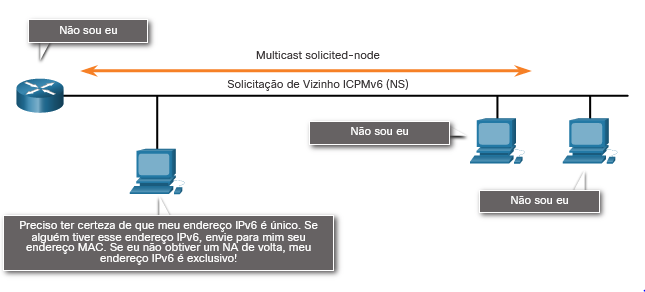
**Detecção de Endereços Duplicados (DAD)**

Quando um dispositivo recebe um unicast global ou um endereço unicast de link local, é recomendável executar DAD no endereço para garantir que ele seja único. Para verificar a exclusividade de um endereço, o dispositivo enviará uma mensagem NS com seu próprio endereço IPv6 como o endereço IPv6 de destino, mostrado na figura. Se outro dispositivo na rede tiver esse endereço, ele responderá com uma mensagem de NA. Essa mensagem de NA notificará o dispositivo emissor 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.

**Nota**: O DAD não é necessário, mas o RFC 4861 recomenda que o DAD seja executado em endereços unicast.

A figura para detecção de endereço duplicado mostra um roteador com uma linha estendida a partir dele. Também anexados à linha estão três PCs. O PC mais próximo do roteador tem uma caixa de diálogo que diz: deixe-me verificar se meu endereço ip v 6 é exclusivo. Quem já tiver esse endereço ipv6, me mande seu endereço MAC. Se eu não obtiver um NA de volta, meu endereço ip v 6 será exclusivo! As caixas de diálogo do roteador e de dois outros PCs não dizem eu. Há uma linha com setas em ambas as extremidades que se estendem acima da linha que conecta os dispositivos com as palavras para multicast de nó solicitado i c m p v 6 solicitação de vizinho.

### Detecção de Endereço Duplicado (DAD)



# Utilitários Ping e Traceroute

7.2.1

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

7.2.2

**Ping - Testar conectividade**

No tópico anterior, você foi apresentado às ferramentas **ping** e traceroute (**tracert**). Neste tópico, você aprenderá sobre as situações em que cada ferramenta é usada e como usá-las. 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, **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. Isso pode indicar que há um problema, mas também pode indicar que os recursos de segurança que bloqueiam as mensagens de ping foram ativados na rede. É comum o primeiro ping para o tempo limite se a resolução de endereço (ARP ou ND) precisar ser executada antes de enviar a Solicitação de eco ICMP.

Depois que todas as solicitações são enviadas, o **ping** utilitário fornece um resumo que inclui a taxa de sucesso e o tempo médio de ida e volta para o destino.

O tipo de testes de conectividade realizados com **ping** incluem o seguinte:

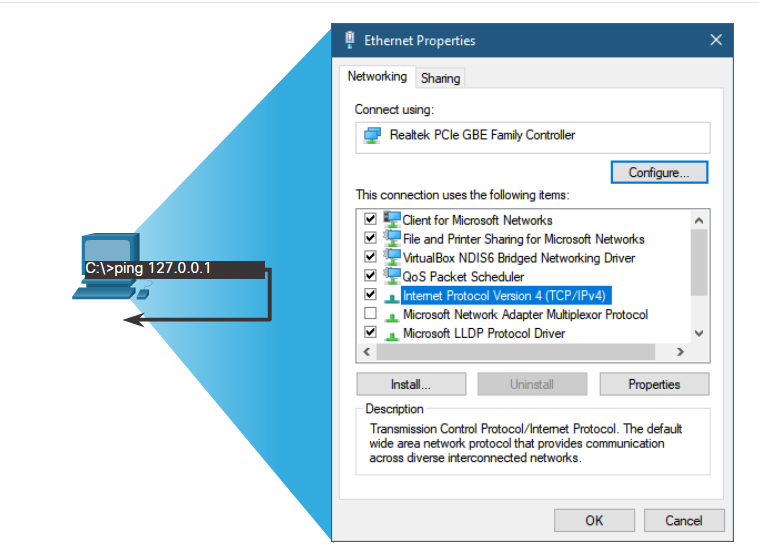
* Fazendo ping no loopback local
* Fazendo ping no gateway padrão
* Fazendo ping no host remoto

7.2.3

**Fazer ping no loopback**

O ping pode ser usado para testar a configuração interna do IPv4 ou IPv6 no host local. Para executar este teste, **ping** o endereço de loopback local 127.0.0.1 para IPv4 (:: 1 para 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. No entanto, ela não significa que os endereços, as máscaras ou os gateways estão configurados adequadamente, Nem indica o status da camada inferior da pilha de rede. Ela simplesmente testa o IP até a camada de rede do IP. Uma mensagem de erro indica que o TCP/IP não está operacional no host.



C:\>ping 127.0.0.1

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.

7.2.4

## Executar ping no gateway padrão

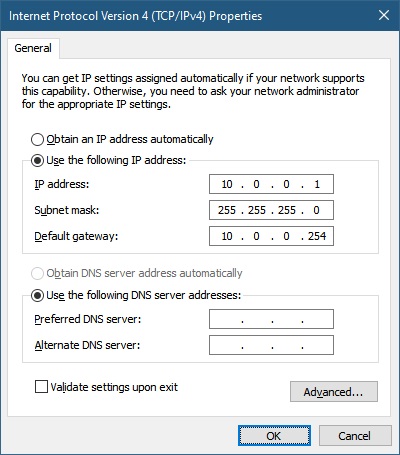
Você também pode usar **ping** para testar a capacidade de um host de se comunicar na rede local. Isso geralmente é feito através do ping do endereço IP do gateway padrão do host. Um êxito **ping** no gateway padrão indica que o host e a interface do roteador servindo como gateway padrão estão operacionais na rede local.

Para este teste, o endereço de gateway padrão é usado com mais frequência porque o roteador normalmente está sempre operacional. Se o endereço de gateway padrão não responder, um **ping** poderá ser enviado para o endereço IP de outro host na rede local que se sabe estar 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 de gateway padrão errado tenha sido configurado no host. Outra possibilidade é que a interface do roteador esteja plenamente operacional, mas tenha segurança aplicada a ela que a impeça de processar ou responder a solicitações ping.

O gráfico mostra a caixa de diálogo Propriedades Ethernet configurada com um endereço IP estático, máscara de sub-rede e gateway padrão. A topologia mostra o PC enviando uma solicitação de eco para o gateway padrão do roteador e os roteadores ecoam resposta.



SOLICITAÇÃO DE ECO (ECHO REQUEST)RESPOSTA DE ECO (ECHO REPLY)10.0.0.1  
255.255.255.010.0.0.254  
255.255.255.0G0/0/0

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.

7.2.5

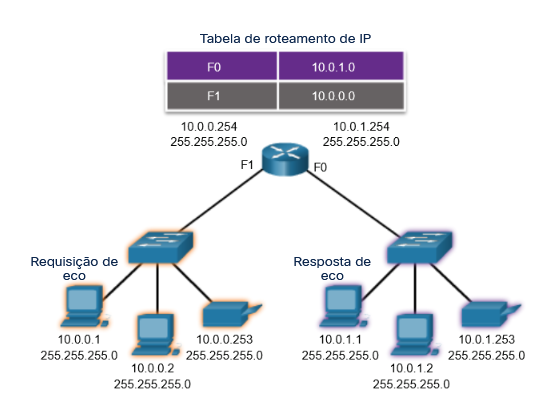
## Efetuar ping em um host remoto

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 fazer ping em um host IPv4 operacional de uma rede remota, como mostrado na figura. O roteador usa sua tabela de roteamento IP para encaminhar os pacotes.

Se esse ping tiver êxito, a operação de uma grande parte da rede interconectada poderá ser verificada. Um êxito **ping** na rede confirma a comunicação na rede local, a operação do roteador que serve como gateway padrão e a operação de todos os outros roteadores que possam estar no caminho entre a rede local e a rede do host remoto.

Além disso, a funcionalidade do host remoto pode ser verificada. Se o host remoto não conseguir se comunicar para fora de sua rede local, ele não responderá.

**Nota**: Muitos administradores de rede limitam ou proíbem a entrada de mensagens ICMP na rede corporativa; portanto, a falta de \*\*ping\*\*resposta pode ser devido a restrições de segurança.



7.2.6

## 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.

**Tempo de Ida e Volta (RTT)**

O uso do traceroute fornece tempo de ida e volta para cada salto ao longo do caminho e indica se um salto falha na resposta. 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.

**TTL no IPv4 e Limite de Saltos no IPv6**

O Traceroute utiliza uma função do campo TTL no IPv4 e do campo Limite de saltos no IPv6 nos cabeçalhos da camada 3, junto com a mensagem ICMP Time Exceded.

Execute a animação na figura para ver como o traceroute tira proveito do TTL.

a animação mostra um traceroute para uma rede remota que atravessa três roteadores. O traceroute levará 4 solicitações de eco para chegar ao seu destino

Resposta de Eco ICMP

ICMP  
Tempo excedido

ICMP  
Tempo excedido

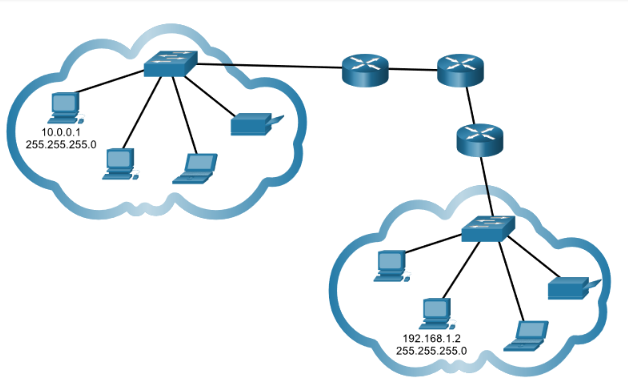
ICMP  
Tempo excedido

Traceroute  
192.168.1.2  
(TTL = 4)

Traceroute  
192.168.1.2  
(TTL = 3)

Traceroute  
192.168.1.2  
(TTL = 2)

Traceroute  
192.168.1.2  
(TTL = 1)



A primeira sequência de mensagens enviadas pelo traceroute terá um campo TTL de valor 1. Isso faz com que o TTL coloque um tempo limite no pacote IPv4 que ocorrerá 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 ser aumentado até alcançar o destino ou até atingir um valor máximo pré-determinado.

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.

7.2.7

## Formato de pacote ICMP

O ICMP é encapsulado diretamente em pacotes IP. Nesse sentido, é quase como um protocolo da camada de transporte, pois é encapsulado em um pacote, porém é considerado um protocolo da Camada 3. O ICMP atua como uma carga útil de dados dentro do pacote IP. Possui um campo de dados de cabeçalho especial, conforme mostrado na figura.

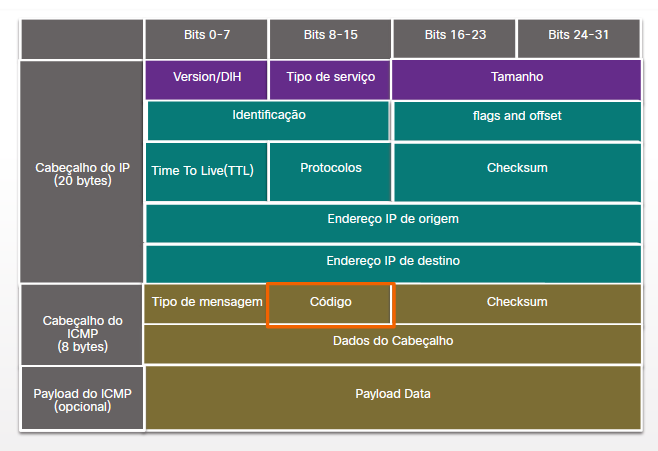
ICMP usa códigos de mensagem para diferenciar entre diferentes tipos de mensagens ICMP. Estes são alguns códigos de mensagem comuns:

* **0** — Echo reply (resposta a um ping)
* **3** – Destination Unreachable (Destino Inalcançável)
* **5** — Redirect (use outra rota para o seu destino)
* **8** — Echo request (para ping)
* **11** — Time Exceeded (TTL tornou-se 0)

Como você verá posteriormente no curso, um analista de segurança cibernética sabe que o campo opcional de carga útil do ICMP pode ser usado em um vetor de ataque para exfiltrar dados.

A figura mostra um datagrama i p com o cabeçalho i p de 20 bytes e os diferentes campos no topo com o cabeçalho I C M P de 8 bytes abaixo do cabeçalho I P. O primeiro byte do cabeçalho I C M P é o tipo de campo de mensagem seguido pelo campo de código que também é de 1 byte. O campo de checksum é um campo de 2 bytes e os dados do cabeçalho são um campo de 4 bytes. O campo de código é o foco. Sob o cabeçalho I C M P está a seção opcional de carga útil I C M P, onde 32 bits ou 4 bytes de dados de carga podem ser inseridos.

### Datagrama IP



# Resumo de Verificação de Conectividade

7.3.1

## O que aprendi neste módulo?

**ICMP**

O conjunto TCP / IP envia mensagens ICMP quando os pacotes IP encontram problemas de encaminhamento. No entanto, as mensagens ICMP não são necessárias e muitas vezes não são permitidas em uma rede por motivos de segurança. 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.

**Utilitários Ping e Traceroute**

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. Isso fornece informações importantes de verificação e solução de problemas. 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.

7.3.2

Módulo 7: Questionário de Verificação de Conectividade

O que é indicado por um ping bem-sucedido para o endereço IPv6: :1?

O ip está instalado corretamente no host

Tópico 7.2.0 - O Endereço IPv6 ::1 é o Endereço de Loopback. Um ping bem-sucedido para esse endereço significa que a pilha TCP/IP está instalada corretamente. Isso não significa que quaisquer endereços estão configurados corretamente.

Um usuário se queixa de que a estação de trabalho não pode acessar a rede. O técnico de rede pede ao usuário para emitir o ping 127.0.0.1comando. Qual é o propósito de usar este comando?

Para verificar se a pilha TCP/IP está operacional

Tópico 7.2.0 - O ping 127.0.0.1comando é usado para verificar a operação apropriada da pilha de protocolos TCP/IP da camada de rede para a camada física - e vice-versa. Esta operação deste comando não coloca um sinal na mídia de rede.

Qual é o procedimento usado no ICMPv6 em situações nas quais um host precisa verificar a exclusividade de um endereço IPv6 antes de configurá-lo na interface?

DAD

Tópico 7.1.0 - Antes que um host IPv6 possa habilitar e usar um endereço IPv6 atribuído, o host deve verificar se o endereço é exclusivo na rede. Para verificar que nenhum outro host está usando o endereço IPv6, o host realiza o processo de Detecção de endereço duplicado (DAD), ao enviar uma mensagem de Solicitação de vizinho (NS) ao endereço IPv6.

Um administrador de rede consegue fazer ping com êxito no servidor em www.cisco.com, mas não consegue fazer ping no servidor da Web da empresa localizado em um ISP em outra cidade. Que ferramenta ou comando podem ajudar a identificar o roteador específico em que o pacote foi perdido ou atrasado?

traceroute

Tópico 7.2.0 - O comando traceroute fornece informações de conectividade sobre o caminho que um pacote segue para chegar ao destino e sobre cada roteador (salto) ao longo do caminho. Ele também indica o tempo que um pacote leva para chegar da origem em cada salto e vice-versa.

Um usuário executa um traceroute sobre IPv6. Em que momento um roteador no caminho para o dispositivo de destino descartaria o pacote?

Quando o valor do campo limite de salto chegar a zero

Tópico 7.2.0 - Quando um traceroute é executado, o valor no campo Hop Limit de um pacote IPv6 determina quantos saltos de roteador o pacote pode viajar. Uma vez que o campo Limite de Hop atinge um valor de zero, ele não poderá mais ser encaminhado e o roteador de recebimento soltará o pacote.

Qual mensagem ICMPv6 é enviada quando o campo de limite de salto IPv6 de um pacote é diminuído para zero e o pacote não pode ser encaminhado?

Tempo excedido

Tópico 7.1.0 - ICMPv6 usa o campo de limite de salto no cabeçalho do pacote IPv6 para determinar se o pacote expirou. Se o campo limite de salto atingir zero, um roteador enviará uma mensagem de tempo excedido de volta para a origem indicando que o roteador não pode encaminhar o pacote.

Qual mensagem é enviada por um host para verificar a exclusividade de um endereço IPv6 antes de usar esse endereço?

Solicitação de vizinho

Tópico 7.1.0 - No IPv6, a detecção de endereço duplicado (DAD) é usada no lugar do ARP. Um host IPv6 executa DAD enviando uma mensagem de solicitação de vizinho (NS) para seu próprio endereço IPv6 para garantir a exclusividade do endereço antes de usá-lo.

Qual protocolo é usado para pingtestar a conectividade entre hosts de rede?

ICMP

Tópico 7.1.0 - O Internet Control Message Protocol (ICMP) é usado para pingtestar a conectividade entre hosts de rede. O Protocolo de resolução de endereços (ARP) é usado para mapear endereços IP para endereços MAC. O protocolo DHCP (Dynamic Host Configuration Protocol) é usado para atribuir dinamicamente endereços IP aos hosts de rede. O protocolo de controle de transmissão (TCP) é considerado um protocolo confiável que segmenta os dados da camada de aplicação em segmentos para transmissão.

Um usuário emite umping 2001:db8:3040:114::88 comando e recebe uma resposta que inclui um código de 3. O que esse código representa?

Porta inacessível

Tópico 7.1.0 -

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. Estes são alguns dos códigos de destino inacessível para ICMPv4:

0 : net unreachable

1 : host unreachable

2 : protocol unreachable

3 : port unreachable

Um usuário emite um comando ping 192.168.219.8 e recebe uma resposta que inclui um código de 0. O que esse código representa?

Rede inacessível

Tópico 7.1.0 -

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. Estes são alguns dos códigos de destino inacessível para ICMPv4:

0 : net unreachable

1 : host unreachable

2 : protocol unreachable

3 : port unreachable

O que caracteriza um utilitário traceroute?

Ele identifica os roteadores no caminho de um host de origem para um host de destino

Tópico 7.2.0 - Traceroute é um utilitário que gera uma lista de saltos (ou roteadores) ao longo do caminho de um host de origem para o host de destino.

Por que um gerente precisaria usar o tracert comando?

Para exibir uma lista das interfaces do lado do roteador entre o dispositivo de origem e o dispositivo de destino

Tópico 7.2.0 - 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 problemas.Se os dados chegarem ao 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.

Qual protocolo oferece suporte à configuração automática de endereço sem estado (SLAAC) para atribuição dinâmica de endereços IPv6 a um host?

ICMPv6

Tópico 7.1.0 - SLAAC usa mensagens ICMPv6 ao atribuir dinamicamente um endereço IPv6 a um host.DHCPv6 é um método alternativo de atribuição de endereços IPv6 a um host.O ARPv6 não existe. O Neighbour Discovery Protocol (NDP) fornece a funcionalidade do ARP para redes IPv6.UDP é o protocolo da camada de transporte usado porDHCPv6.

# Introdução

8.0.1

## Por que devo fazer este módulo?

Você já se perguntou como as informações que você envia são entregues para o dispositivo correto? Este módulo explicará como a combinação de um endereço lógico e um endereço físico permite a comunicação entre dois hosts. Você aprenderá como o ARP (Address Resolution Protocol) é usado em uma rede IPv4 para criar essa associação. Continue lendo para saber como funciona o processo ARP e o que pode ser feito para evitar possíveis problemas.

8.0.2

## O que vou aprender neste módulo?

**Título do Módulo:** Resolução de endereço

**Objetivo do Módulo**: Analisar as PDUs do protocolo ARP em uma rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| MAC e IP | Comparar as funções do endereço MAC e do endereço IP. |
| ⁪ARP | Analisar o ARP examinando os quadros Ethernet. |
| Problemas do ARP | Explique como as solicitações ARP afetam o desempenho da rede e do host, bem como os riscos potenciais à segurança. |

# MAC e IP

8.1.1

## Destino na Mesma Rede

Há dois endereços principais atribuídos a um dispositivo em uma rede LAN Ethernet:

* **Endereço físico (o endereço MAC)** – Isso é usado para comunicações Ethernet NIC para Ethernet NIC na mesma rede.
* **Endereço lógico (o endereço IP)** – Isso é usado para enviar o pacote da fonte original ao destino final.

Os endereços IP são usados para identificar o endereço do dispositivo de origem original e o dispositivo de destino final. O endereço IP de destino pode estar na mesma rede IP que a origem ou em uma rede remota.

**Nota**: A maioria dos aplicativos usa DNS (Sistema de Nome de Domínio) para determinar o endereço IP quando recebe um nome de domínio como www.cisco.com. O DNS é discutido em um módulo posterior.

Os endereços MAC Ethernet têm uma finalidade diferente. Esses endereços servem para entregar o quadro de enlace de dados com o pacote IP encapsulado de uma NIC para outra na mesma rede. Se o endereço IP de destino estiver na mesma rede, o endereço MAC de destino será o do dispositivo de destino.

A figura mostra os endereços MAC Ethernet e endereço IP de PC-A enviando um pacote IP para o servidor de arquivos na mesma rede.

O quadro Ethernet da Camada 2 contém:

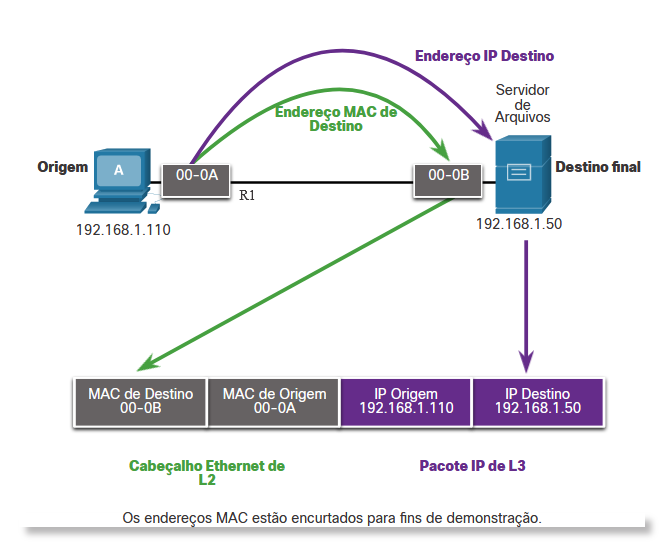
* **Endereço MAC de destino** – Este é o endereço MAC da placa de rede Ethernet do servidor de arquivos.
* **Endereço MAC de origem** – Este é o endereço MAC da placa de rede Ethernet do PC-A.

O pacote IP da Camada 3 contém:

* **Endereço IP de origem** – Este é o endereço IP da fonte original, PC-A.
* **Endereço IP de destino** – Este é o endereço IP do destino final, o servidor de arquivos.

A figura mostra um P C conectado a um servidor. O P C está enviando dados para o servidor. O P C coloca os endereços IP de origem e destino da camada 3 no cabeçalho do pacote e, em seguida, coloca os endereços MAC de origem e destino da camada 2 no cabeçalho do quadro.

### Comunicação em uma Rede Local



[Ir para o conteúdo](https://contenthub.netacad.com/cyberops/5.0.1?lng=pt-br#chunks-container)

*                  
*               
*                                       

1. Protocolo de Resolução de Endereços (ARP)
2. MAC e IP

# MAC e IP

8.1.1

## Destino na Mesma Rede

Há dois endereços principais atribuídos a um dispositivo em uma rede LAN Ethernet:

* **Endereço físico (o endereço MAC)** – Isso é usado para comunicações Ethernet NIC para Ethernet NIC na mesma rede.
* **Endereço lógico (o endereço IP)** – Isso é usado para enviar o pacote da fonte original ao destino final.

Os endereços IP são usados para identificar o endereço do dispositivo de origem original e o dispositivo de destino final. O endereço IP de destino pode estar na mesma rede IP que a origem ou em uma rede remota.

**Nota**: A maioria dos aplicativos usa DNS (Sistema de Nome de Domínio) para determinar o endereço IP quando recebe um nome de domínio como www.cisco.com. O DNS é discutido em um módulo posterior.

Os endereços MAC Ethernet têm uma finalidade diferente. Esses endereços servem para entregar o quadro de enlace de dados com o pacote IP encapsulado de uma NIC para outra na mesma rede. Se o endereço IP de destino estiver na mesma rede, o endereço MAC de destino será o do dispositivo de destino.

A figura mostra os endereços MAC Ethernet e endereço IP de PC-A enviando um pacote IP para o servidor de arquivos na mesma rede.

O quadro Ethernet da Camada 2 contém:

* **Endereço MAC de destino** – Este é o endereço MAC da placa de rede Ethernet do servidor de arquivos.
* **Endereço MAC de origem** – Este é o endereço MAC da placa de rede Ethernet do PC-A.

O pacote IP da Camada 3 contém:

* **Endereço IP de origem** – Este é o endereço IP da fonte original, PC-A.
* **Endereço IP de destino** – Este é o endereço IP do destino final, o servidor de arquivos.

A figura mostra um P C conectado a um servidor. O P C está enviando dados para o servidor. O P C coloca os endereços IP de origem e destino da camada 3 no cabeçalho do pacote e, em seguida, coloca os endereços MAC de origem e destino da camada 2 no cabeçalho do quadro.

### Comunicação em uma Rede Local

R1

OrigemDestino final00-0A00-0BEndereço IP DestinoServidor de Arquivos192.168.1.110192.168.1.50Os endereços MAC estão encurtados para fins de demonstração.Endereço MAC de DestinoMAC de Destino  
00-0BMAC de Origem  
00-0AIP Origem  
192.168.1.110Cabeçalho Ethernet de L2Pacote IP de L3IP Destino  
192.168.1.50

8.1.2

## Destino na Rede Remota

Quando o endereço IP de destino estiver em uma rede remota, o endereço MAC de destino será o endereço do gateway padrão do host. O endereço padrão do gateway é o endereço da NIC do roteador, conforme mostrado na figura. Fazendo uma analogia com os correios, seria semelhante a uma pessoa levar uma carta até a agência postal local. Eles só precisam deixar a carta nos correios. Cabe então aos correios encaminhar a carta para o seu destino final.

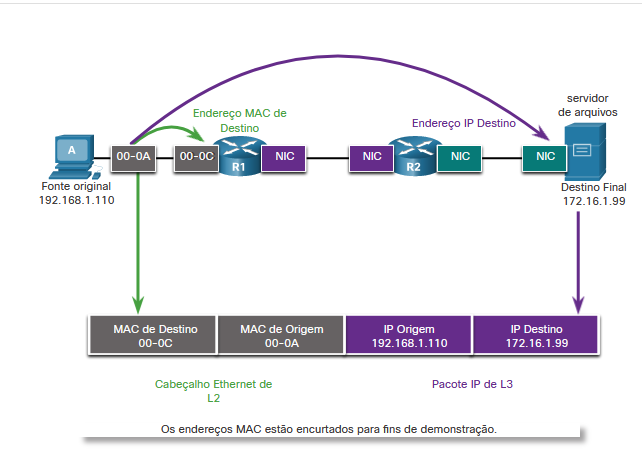
A figura mostra os endereços de Ethernet MAC e endereços IPv4 para PC-A. Ele está enviando um pacote IP para um servidor de arquivos em uma rede remota. Os roteadores examinam o endereço IPv4 destino para determinar o melhor caminho para encaminhar o pacote IPv4. É um processo semelhante à forma como os correios encaminham correspondência com base no endereço do destinatário.

Quando o roteador recebe o quadro Ethernet, ele desencapsula as informações da Camada 2. Usando o endereço IP de destino, ele determina o dispositivo do próximo salto e encapsula o pacote IP em um novo quadro de enlace de dados para a interface de saída. Em cada link ao longo do caminho, um pacote IP é encapsulado em um quadro específico para a tecnologia de enlace de dados associada a esse link, como a Ethernet. Se o dispositivo do próximo salto for o destino final, o endereço MAC de destino será o da NIC Ethernet do dispositivo.

Como os endereços IPv4 dos pacotes IPv4 em um fluxo de dados são associados aos endereços MAC em cada link ao longo do caminho até o destino? Isso é feito através de um processo chamado protocolo ARP (Address Resolution Protocol).

A figura mostra P C A conectado ao roteador r 1, que está conectado a R 2. R 2 está conectado a um servidor de arquivos. P C A está enviando dados para o servidor de arquivos. P C A constrói um pacote com seu próprio endereço I P como a origem e o endereço I P de destino do servidor de arquivos. P C A então constrói um quadro com seu próprio endereço MAC como origem e o endereço MAC para R 1 como destino.

### Comunicação com uma Rede Remota



# ARP

8.2.1

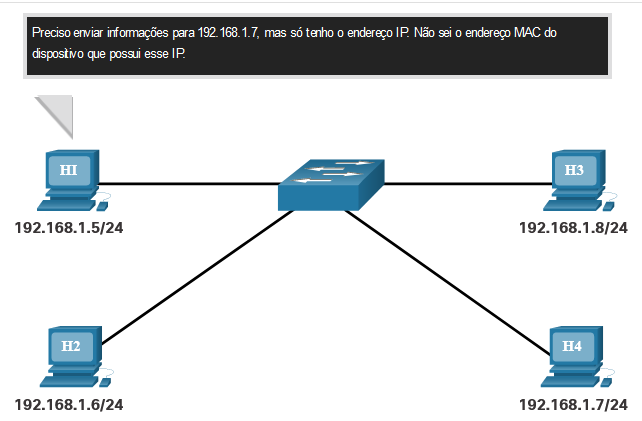
## Visão geral do ARP

Se sua rede estiver usando o protocolo de comunicações IPv4, o Protocolo de Resolução de Endereços ou ARP é o que você precisa para mapear endereços IPv4 para endereços MAC. Este tópico explica como o ARP funciona.

Cada dispositivo IP em uma rede Ethernet tem um endereço MAC Ethernet exclusivo. Quando um dispositivo envia um quadro Ethernet Layer 2, ele contém estes dois endereços:

* **Endereço MAC de destino** - O endereço MAC Ethernet do dispositivo de destino no mesmo segmento de rede local. Se o host de destino estiver em outra rede, o endereço de destino no quadro será o do gateway padrão (ou seja, roteador).
* **Endereço MAC de origem** - O endereço MAC da Ethernet NIC no host de origem.

A figura ilustra o problema ao enviar um quadro para outro host no mesmo segmento em uma rede IPv4.



Para enviar um pacote para outro host na mesma rede IPv4 local, um host deve saber o endereço IPv4 e o endereço MAC do dispositivo de destino. Os endereços IPv4 de destino do dispositivo são conhecidos ou resolvidos pelo nome do dispositivo. No entanto, os endereços MAC devem ser descobertos.

Um dispositivo utiliza o protocolo ARP (Address Resolution Protocol) para determinar o endereço MAC de destino de um dispositivo local quando conhece o endereço IPv4.

O ARP fornece duas funções básicas:

* Resolução de endereços IPv4 em endereços MAC
* Manter uma tabela de mapeamentos de endereços IPv4 para MAC

8.2.2

**Funções do ARP**

Quando um pacote é enviado à camada de enlace de dados para ser encapsulado em um quadro Ethernet, o dispositivo consulta uma tabela em sua memória para encontrar o endereço MAC que é mapeado para o endereço IPv4. Esta tabela é armazenada temporariamente na memória RAM e denominada tabela ARP ou cache ARP.

O dispositivo emissor pesquisará em sua tabela ARP um endereço IPv4 destino correspondente a um endereço MAC.

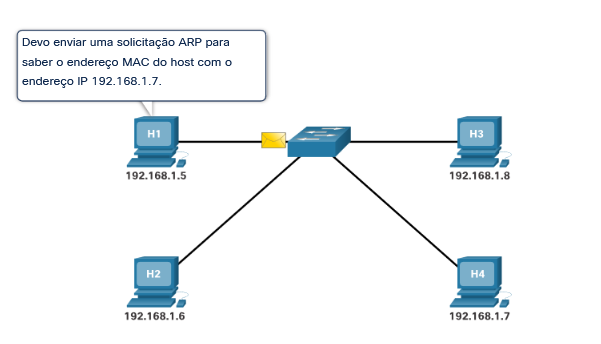
* Se o endereço IPv4 destino do pacote estiver na mesma rede que o endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 destino na tabela ARP.
* Se o endereço IPv4 destino do pacote estiver em uma rede diferente do endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 do gateway padrão na tabela ARP.

Nos dois casos, a pesquisa é por um endereço IPv4 e um endereço MAC correspondente para o dispositivo.

Cada entrada (linha) da tabela ARP vincula um endereço IPv4 a um endereço MAC. Chamamos a relação entre os dois valores de um mapa. Isso significa simplesmente que você pode localizar um endereço IPv4 na tabela e descobrir o endereço MAC correspondente. A tabela ARP salva (armazena em cache) temporariamente o mapeamento dos dispositivos da LAN.

Se o dispositivo localizar o endereço IPv4, seu endereço MAC correspondente será usado como endereço MAC de destino no quadro. Se nenhuma entrada for encontrada, o dispositivo enviará uma requisição ARP.

Clique em Reproduzir na figura para ver uma animação da função ARP.



8.2.3

**Vídeo - Operação ARP - Solicitação ARP**

Uma solicitação ARP é enviada quando um dispositivo precisa determinar o endereço MAC associado a um endereço IPv4 e não possui uma entrada para o endereço IPv4 em sua tabela ARP.

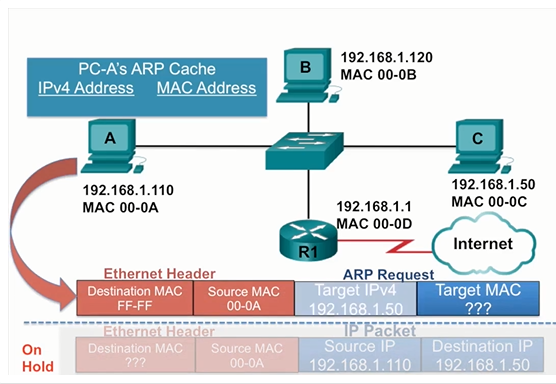
As mensagens do ARP são encapsuladas diretamente em um quadro Ethernet. Não há cabeçalho IPv4. A requisição ARP é encapsulada em um quadro Ethernet usando as seguintes informações de cabeçalho:

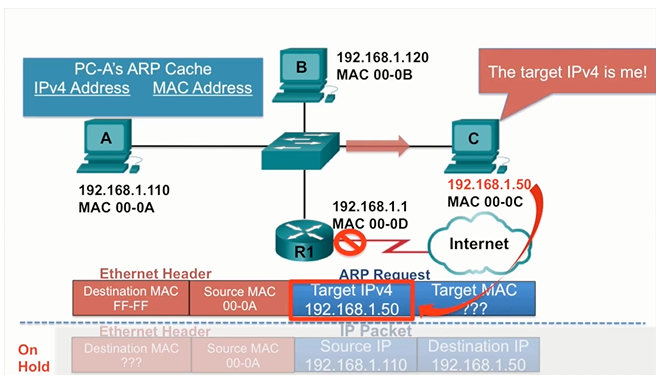
* **Endereço MAC de destino** – Este é um endereço de broadcast FF-FF-FF-FF-FF-FF que requer todos os NICs Ethernet na LAN para aceitar e processar a solicitação ARP.
* **Endereço MAC de origem** - Este é o endereço MAC do remetente da solicitação ARP.
* **Tipo** - As mensagens ARP têm um campo de tipo de 0x806. Ele informa à NIC de recebimento que a parte de dados do quadro precisa ser transferida para o processo ARP.

Como as solicitações de ARP são transmissões, elas são inundadas em todas as portas pelo switch, exceto a porta de recebimento. Todas as NICs Ethernet no processo de LAN transmite e devem entregar a solicitação ARP ao seu sistema operacional para processamento. Cada dispositivo deve processar a requisição ARP para ver se o endereço IPv4 destino corresponde ao seu. Um roteador não encaminhará broadcasts pelas outras interfaces.

Somente um dispositivo na LAN terá um endereço IPv4 correspondente ao endereço IPv4 na requisição ARP. Nenhum outro dispositivo responderá.

Clique em Reproduzir na figura para ver uma demonstração de uma requisição ARP para um endereço IPv4 destino que está na rede local.





8.2.4

**Vídeo - Operação do ARP - Resposta do ARP**

Somente o dispositivo com o endereço IPv4 de destino associado à solicitação ARP responderá com uma resposta ARP. A resposta de ARP é encapsulada em um quadro Ethernet com as seguintes informações de cabeçalho:

* **Endereço MAC de destino** - Este é o endereço MAC do remetente da solicitação ARP.
* **Endereço MAC de origem** - Este é o endereço MAC do remetente da resposta ARP.
* **Tipo** - As mensagens ARP têm um campo de tipo de 0x806. Ele informa à NIC de recebimento que a parte de dados do quadro precisa ser transferida para o processo ARP.

Apenas o dispositivo que enviou originalmente uma requisição ARP receberá a resposta ARP unicast. Depois que a resposta do ARP é recebida, o dispositivo adiciona o endereço IPv4 e o endereço MAC correspondente à sua tabela ARP. Agora os pacotes destinados a esse endereço IPv4 podem ser encapsulados em quadros com o endereço MAC correspondente.

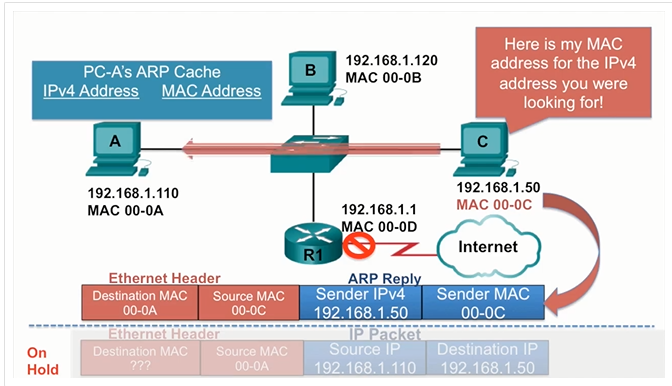
Se nenhum dispositivo responder à requisição ARP, o pacote será descartado porque não será possível criar um quadro.

As entradas na tabela ARP têm carimbo de data/hora (timestamp). Se um dispositivo não receber um quadro de um dispositivo específico antes que o carimbo de data / hora expire, a entrada desse dispositivo será removida da tabela ARP.

Além disso, entradas de mapa estáticas podem ser inseridas em uma tabela ARP, mas isso é raro. As entradas estáticas na tabela ARP não expiram com o tempo e devem ser removidas manualmente.

**Nota**: O IPv6 usa um processo semelhante ao ARP para IPv4, conhecido como ICMPv6 Neighbour Discovery (ND). O IPv6 usa mensagens de requisição e de anúncio de vizinho, semelhantes a solicitações ARP e respostas ARP no IPv4.

Clique em Reproduzir na figura para ver uma demonstração de uma resposta ARP.



8.2.5

## Vídeo - Função ARP na Comunicação Remota

Quando o endereço IPv4 destino não está na mesma rede que o endereço IPv4 origem, o dispositivo de origem precisa enviar o quadro para o gateway padrão. Essa é a interface do roteador local. Sempre que um dispositivo de origem tiver um pacote com um endereço IPv4 em outra rede, ele encapsulará esse pacote em um quadro usando o endereço MAC de destino do roteador.

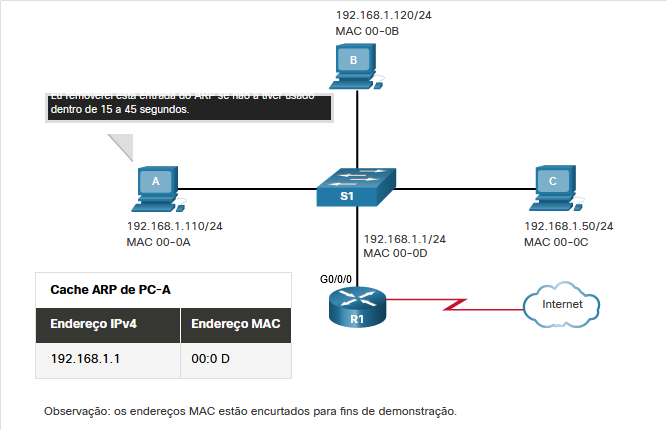
O endereço IPv4 do gateway padrão é armazenado na configuração IPv4 dos hosts. Quando um host cria um pacote para um destino, ele compara o endereço IPv4 destino e seu próprio endereço IPv4 para determinar se os dois endereços IPv4 estão localizados na mesma rede de Camada 3. Se o host de destino não estiver na mesma rede, a origem usará a tabela ARP para obter uma entrada com o endereço IPv4 do gateway padrão. Se não houver uma entrada, ela usará o processo de ARP para determinar um endereço MAC do gateway padrão.

Clique em Reproduzir para ver uma demonstração de uma requisição ARP e de uma resposta ARP associadas ao gateway padrão.

8.2.6

## Remoção de Entradas de uma Tabela ARP

Em cada dispositivo, um temporizador da cache ARP remove entradas ARP que não tenham sido usadas durante um determinado período. Os horários diferem dependendo do sistema operacional do dispositivo. Por exemplo, os sistemas operacionais Windows mais recentes armazenam entradas da tabela ARP entre 15 e 45 segundos, conforme ilustrado na figura.



Os comandos também podem ser usados para remover manualmente algumas ou todas as entradas na tabela ARP. Após a remoção de uma entrada, o processo de envio de uma requisição ARP e de recebimento de uma resposta ARP deve ocorrer novamente para inserir o mapa na tabela ARP.

8.2.7

## Tabelas ARP

Em um roteador Cisco, o comando **show ip arp** é usado para exibir a tabela ARP, conforme mostrado na figura.

R1# **show ip arp**

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.10.1 - a0e0.af0d.e140 ARPA GigabitEthernet0/0/0

Internet 209.165.200.225 - a0e0.af0d.e141 ARPA GigabitEthernet0/0/1

Internet 209.165.200.226 1 a03d.6fe1.9d91 ARPA GigabitEthernet0/0/1

R1#

Em um PC com Windows 10, o comando **arp –a** é usado para exibir a tabela ARP, conforme mostrado na figura.

C:\Users\PC> **arp -a**

Interface: 192.168.1.124 --- 0x10

Internet Address Physical Address Type

192.168.1.1 c8-d7-19-cc-a0-86 dynamic

192.168.1.101 08-3e-0c-f5-f7-77 dynamic

192.168.1.110 08-3e-0c-f5-f7-56 dynamic

192.168.1.112 ac-b3-13-4a-bd-d0 dynamic

192.168.1.117 08-3e-0c-f5-f7-5c dynamic

192.168.1.126 24-77-03-45-5d-c4 dynamic

192.168.1.146 94-57-a5-0c-5b-02 dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.251 01-00-5e-00-00-fb static

239.255.255.250 01-00-5e-7f-ff-fa static

255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Users\PC>

8.2.8

## Laboratório – Usando Wireshark para Examinar Quadros Ethernet

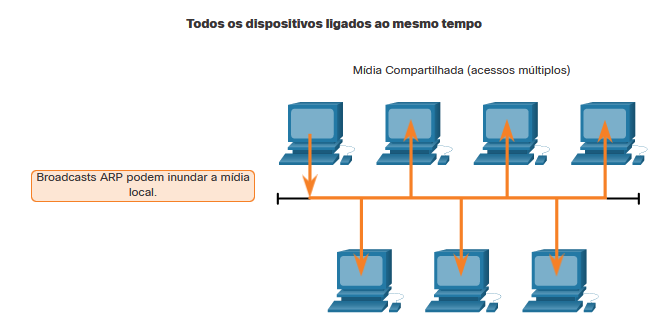
Neste laboratório, você usará o Wireshark para capturar e visualizar quadros Ethernet a fim de investigar ARP e endereçamento IP e MAC. Além disso, você capturará e analisará quadros ICMP.

# Problemas do ARP

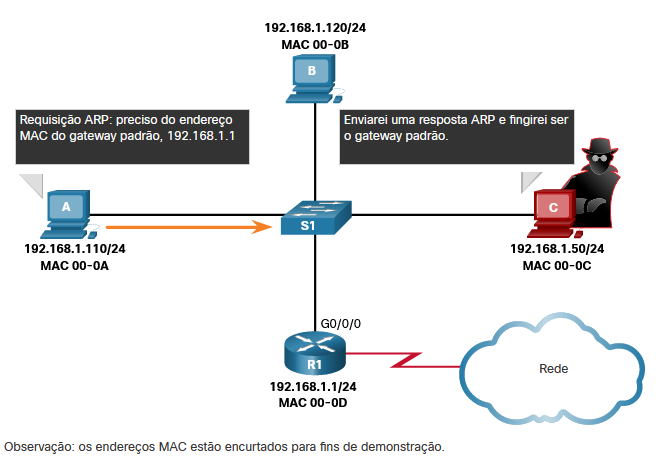
8.3.1

## Problemas de ARP - transmissões de ARP e falsificação de ARP

Como um quadro broadcast, uma requisição ARP é recebida e processada por todos os dispositivos na rede local. Em uma rede corporativa típica, esses broadcasts provavelmente teriam impacto mínimo no desempenho da rede. No entanto, se um grande número de dispositivos precisasse ser ligado e todos começassem a acessar serviços de rede ao mesmo tempo, poderia haver alguma redução no desempenho por um curto período, como mostra a figura. Depois que os dispositivos enviarem os broadcasts ARP iniciais e tiverem reconhecido os endereços MAC necessários, qualquer impacto na rede será minimizado.



Em alguns casos, o uso do ARP pode levar a um risco potencial à segurança. Um ator de ameaça pode usar falsificação ARP para realizar um ataque de envenenamento por ARP. Esta é uma técnica usada por um ator de ameaça para responder a uma solicitação ARP de um endereço IPv4 que pertence a outro dispositivo, como o gateway padrão, conforme mostrado na figura. O agente da ameaça envia uma resposta ARP com seu próprio endereço MAC. O destinatário da resposta ARP adicionará o endereço MAC errado à sua tabela ARP e enviará esses pacotes ao agente de ameaça. Switches de nível corporativo incluem técnicas de mitigação conhecidas como inspeção dinâmica ARP (DAI). A DAI não faz parte do escopo deste curso.



# Resumo do protocolo de resolução de endereço

8.4.1

## O que aprendi neste módulo?

**MAC e IP**

Há dois endereços principais que são atribuídos a um dispositivo em uma LAN Ethernet; o endereço IP, que é atribuído logicamente, e o endereço MAC que é atribuído fisicamente e é exclusivo para a interface de rede. Os endereços IP são usados para identificar o endereço do dispositivo de origem original e o dispositivo de destino final. O endereço IP de destino pode estar na mesma rede IP que a origem ou em uma rede remota. A camada 2 ou os endereços físicos, como endereços MAC Ethernet, têm uma finalidade diferente. Esses endereços servem para entregar o quadro de enlace de dados com o pacote IP encapsulado de uma NIC para outra na mesma rede. Se o endereço IP de destino estiver na mesma rede, o endereço MAC de destino será o do dispositivo de destino.

**ARP**

Ao usar IPv4 para comunicação de rede, o ARP é usado para mapear o endereço IPv4 lógico com o endereço MAC da Camada 2. Para construir um quadro Ethernet, o endereço MAC de destino deve ser conhecido. Quando o endereço IPv4 de destino está na mesma rede que a origem, o processo ARP envia o endereço IPv4 para todos os hosts da rede para que o host com o endereço IPv4 correspondente possa responder com o endereço MAC correspondente. O dispositivo de envio agora tem todas as informações necessárias para construir o quadro Ethernet da Camada 2. O ARP fornece duas funções básicas: resolver endereços IPv4 para endereços MAC e manter uma tabela de mapeamentos de endereços IPv4 para MAC. O dispositivo emissor pesquisará em sua tabela ARP um endereço IPv4 destino correspondente a um endereço MAC. Se o endereço IPv4 destino do pacote estiver na mesma rede que o endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 destino na tabela ARP. Se ele não tiver uma entrada para o endereço IPv4 em sua tabela ARP, o dispositivo de envio enviará uma solicitação ARP para determinar o endereço MAC de destino. Somente o dispositivo com o endereço IPv4 de destino associado à solicitação ARP responderá com uma resposta ARP. A resposta ARP é encapsulada em um quadro Ethernet usando as seguintes informações de cabeçalho: o endereço MAC de destino do host solicitante, o endereço MAC de origem do host respondendo e o tipo, que é um código que identifica os dados como sendo para o processo ARP. As mensagens ARP têm um valor de campo de tipo de 0x806. Se o endereço IPv4 destino do pacote estiver em uma rede diferente do endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 do gateway padrão na tabela ARP. O IPv6 usa um processo semelhante ao ARP em IPv4. É conhecido como ICMPv6 Neighbor Discovery (ND). O IPv6 usa mensagens de requisição e de anúncio de vizinho, semelhantes a solicitações ARP e respostas ARP no IPv4.

**Problemas do ARP**

Como um quadro broadcast, uma requisição ARP é recebida e processada por todos os dispositivos na rede local. Em uma rede corporativa típica, esses broadcasts provavelmente teriam impacto mínimo no desempenho da rede. Se um grande número de dispositivos fosse ligado e todos começassem a acessar os serviços de rede ao mesmo tempo, poderia haver alguma redução no desempenho por um curto período de tempo. Depois que os dispositivos enviarem os broadcasts ARP iniciais e tiverem reconhecido os endereços MAC necessários, qualquer impacto na rede será minimizado. Uma vez que a solicitação ARP é um broadcast, há riscos potenciais de segurança. Um agente de ameaça pode usar ARP spoofing para executar um ataque de envenenamento ARP respondendo a uma solicitação ARP para um endereço IPv4 pertencente a outro dispositivo, como o gateway padrão. O destinatário da resposta ARP adicionará o endereço MAC errado à sua tabela ARP e enviará esses pacotes ao agente de ameaça.

Como o processo ARP usa um endereço IP?

Para determinar o endereço MAC de um dispositivo na mesma rede

Tópico 8.2.0 - O processo ARP é usado para completar o mapeamento necessário dos endereços IP e MAC que estão armazenados na tabela ARP mantida por cada nó em uma LAN. Quando o dispositivo de destino não está na mesma rede que o dispositivo de origem, o endereço MAC do dispositivo da Camada 3 na rede de origem é descoberto e adicionado à tabela ARP do nó de origem.

O que um host fará primeiro ao preparar uma PDU de Camada 2 para transmissão a um host na mesma rede Ethernet?

Irá procurar o endereço Mac do host de destino na tabela ARP

Tópico 8.2.0 - Para encapsular uma PDU da Camada 3 em um quadro, o host remetente precisa saber o endereço MAC do host destino. O host remetente primeiro verifica a tabela ARP. Se uma correspondência for encontrada na tabela, o host usará o endereço MAC como MAC de destino no quadro. Caso contrário, iniciará uma solicitação ARP para obter o MAC de destino.

O gráfico contém as seguintes informações: - saída omitida - Interface: 192.168.1.67 --- 0xa Endereço Internet Tipo de endereço físico 192.168.1.254 64-0f-29-0d-36-91 dinâmico 192.168.1.255 ff-ff-ff-ff -ff-ff estático 224.0.0.22 01-00-5e-00-00-16 estático 224.0.0.251 01-00-5e-00-00-fb estático 224.0.0.252 01-00-5e-00-00-fc estático 255.255.255.255 ff-ff-ff-ff-ff-ff estático Interface: 10.82.253.91 --- 0x10 Endereço de Internet Endereço físico Tipo 10.82.253.92 64-0f-29-0d-36-91 dinâmico 224.0.0.22 01-00 -5e-00-00-16 estático 224.0.0.251 01-00-5e-00-00-fb estático 224.0.0.252 01-00-5e-00-00-fc estático 255.255.255.255 ff-ff-ff-ff- aff-ff estática

Consulte a exposição. Qual protocolo foi responsável pela construção da tabela mostrada?

ARP

Tópico 8.2.0 - A tabela mostrada corresponde à saída do comando arp -a, comando que é usado em um PC Windows para exibir a tabela ARP.

Quando um pacote IP é enviado a um host em uma rede remota, quais informações são fornecidas pelo ARP?

O endereço Mac da interface do roteador mais próxima ao host emissor

Tópico 8.1.0 - Quando um host envia um pacote IP para um destino em uma rede diferente, o quadro Ethernet não pode ser enviado diretamente para o host de destino porque o host não pode ser acessado diretamente na mesma rede. O quadro Ethernet deve ser enviado para outro dispositivo conhecido como roteador ou gateway padrão para encaminhar o pacote IP. O ARP é usado para descobrir o endereço MAC do roteador (ou gateway padrão) e usá-lo como endereço MAC de destino no cabeçalho do quadro.

Um host está tentando enviar um pacote para um dispositivo em um segmento de LAN remota, mas atualmente não há mapeamentos no cache ARP. Como o dispositivo obterá um endereço MAC de destino?

Irá enviar uma requisição arp para o endereço mac do gateway padrão

Tópico 8.2.0 - Ao enviar um pacote para um destino remoto, um host precisará enviar o pacote para um gateway na sub-rede local. Como o gateway será o destino da Camada 2 para o quadro neste segmento da LAN, o endereço MAC de destino deverá ser o endereço do gateway. Se o host ainda não tiver esse endereço no cache ARP, ele deverá enviar uma solicitação ARP para o endereço do gateway.

Qual é o objetivo de um ataque de falsificação de ARP?

Para associar endereços IP para endereços Mac errados

Tópico 8.3.0 - Em um ataque de falsificação de ARP, um host malicioso intercepta solicitações ARP e responde a elas para que os hosts da rede mapeiem um endereço IP para o endereço MAC do host malicioso.

Um host precisa alcançar outro host em uma rede remota, mas o cache ARP não possui entradas de mapeamento. Para qual endereço de destino o host enviará uma solicitação ARP?

O endereço Mac broadcast

Tópico 8.2.0 - Solicitações ARP são enviadas quando um host não possui um mapeamento IP para MAC para um destino no cache ARP. As solicitações ARP são enviadas para a transmissão Ethernet de FF:FF:FF:FF:FF:FF. Neste exemplo, como o endereço do host remoto é desconhecido, uma solicitação ARP é enviada à transmissão Ethernet para resolver o endereço MAC do gateway padrão usado para alcançar o host remoto.

A exposição mostra uma topologia de rede. PC1 e PC2 estão conectados às portas Fa0/1 e Fa0/2 do switch SW1, respectivamente. SW1 é conectado através de sua porta Fa0/3 à interface Fa0/0 do roteador RT1. RT1 é conectado através de seu Fa0/1 à porta Fa0/2 do switch SW2. SW2 é conectado através de sua porta Fa0/1 ao PC3.

Consulte a exposição. PC1 emite uma solicitação ARP porque precisa enviar um pacote para PC2. Neste cenário, o que acontecerá a seguir?

PC2 vai enviar uma reposta ARP com o endereço MAC de PC2

Tópico 8.2.0 - Quando um dispositivo de rede deseja se comunicar com outro dispositivo na mesma rede, ele envia uma solicitação ARP de broadcast. Neste caso, a solicitação conterá o endereço IP do PC2. O dispositivo de destino (PC2) envia uma resposta ARP com o endereço MAC do PC2.

Em que tipo de memória a tabela ARP está armazenada em um dispositivo?

RAM

Tópico 8.2.0 - Quando um pacote é enviado para a camada de enlace de dados para ser encapsulado em um quadro Ethernet, o dispositivo verifica a tabela ARP que está armazenada na RAM. A tabela ARP é usada para mapear o endereço IPv4 de destino para um endereço MAC.

Qual é uma característica das mensagens ARP?

As repostas ARP são unicast

Tópico 8.2.0 - Como as solicitações ARP são broadcasts, todas as portas são inundadas pelo switch, exceto a porta receptora. Somente o dispositivo que enviou originalmente a solicitação ARP receberá a resposta ARP unicast

Que afirmação descreve a função do Protocolo de Resolução de Endereços?

ARP é usado para descobrir o enederço Mac de qualquer host na rede local

Tópico 8.2.0 - Quando um PC deseja enviar dados pela rede, ele sempre sabe o endereço IP do destino. No entanto, também precisa descobrir o endereço MAC do destino. ARP é o protocolo usado para descobrir o endereço MAC de um host que pertence à mesma rede.

Por que um invasor iria querer falsificar um endereço MAC?

para que um switch na LAN comece a encaminhar quadros para o ataque em vez de para o host legítimo

Tópico 8.3.0 - A falsificação de endereço MAC é usada para contornar medidas de segurança, permitindo que um invasor se faça passar por um dispositivo host legítimo, geralmente com a finalidade de coletar tráfego de rede.

Que informações importantes são examinadas no cabeçalho do quadro Ethernet por um dispositivo da Camada 2 para encaminhar os dados adiante?

Endereço MAC de destino

Tópico 8.1.0 - O dispositivo da Camada 2, como um switch, usa o endereço MAC de destino para determinar qual caminho (interface ou porta) deve ser usado para enviar os dados para o dispositivo de destino.

# Introdução

9.0.1

## Por que devo cursar este módulo?

Bem-vindo à Camada de Transporte! A camada de transporte é onde, como o nome indica, os dados são transportados de um host para outro. É aqui que sua rede realmente se move! A camada de transporte usa dois protocolos: TCP e UDP. Pense no TCP como recebendo uma carta registrada pelo correio. Você tem que assinar antes que a transportadora de correio lhe dê. UDP é mais como uma carta regular e carimbada. Ambos os protocolos têm lugar na entrega de dados entre uma origem e um destino. Este tópico mergulha em como TCP e UDP funcionam na camada de transporte.

9.0.2

## O que vou aprender neste módulo?

**Título do Módulo:** A Camada de Transporte

**Objetivo do Módulo**: Explicar como os protocolos da camada de transporte oferecem suporte à funcionalidade de rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Características da Camada de Transporte | Explicar como os protocolos da camada de transporte oferecem suporte à comunicação de rede. |
| Estabelecimento da Sessão da Camada de Transporte | Explicar como a camada de transporte estabelece sessões de comunicação. |
| Confiabilidade da Camada de Transporte | Explicar como a camada de transporte estabelece comunicações confiáveis. |

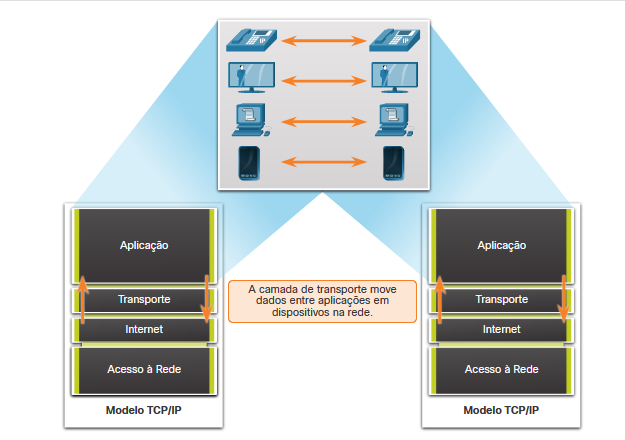
# Características da Camada de Transporte

9.1.1

## Propósito da Camada de Transporte

Os programas da camada de aplicação geram dados que devem ser trocados entre os hosts de origem e de destino. A camada de transporte é responsável pela comunicação lógica entre aplicativos executados em hosts diferentes. Isso pode incluir serviços como o estabelecimento de uma sessão temporária entre dois hosts e a transmissão confiável de informações para um aplicativo.

Como mostra a figura, a camada de transporte é o link entre a camada de aplicação e as camadas inferiores que são responsáveis pela transmissão pela rede.



A camada de transporte não tem conhecimento do tipo de host de destino, o tipo de mídia pela qual os dados devem percorrer, o caminho percorrido pelos dados, o congestionamento em um link ou o tamanho da rede.

A camada de transporte inclui dois protocolos:

* Protocolo TCP
* Protocolo UDP (User Datagram Protocol)

9.1.2

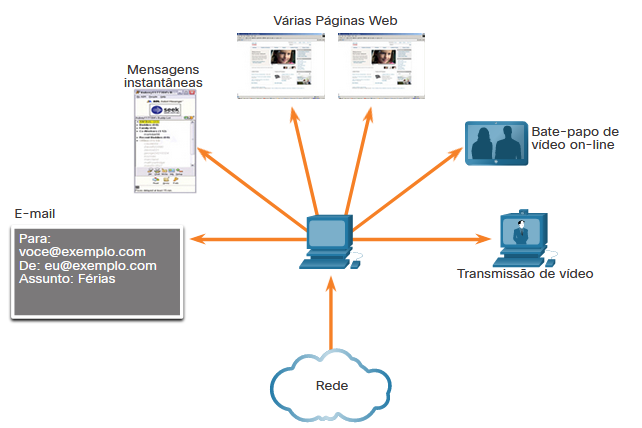
**Responsabilidades da Camada de Transporte**

A camada de transporte tem muitas responsabilidades.

Clique em cada botão abaixo para obter mais informações.

**Rastreamento de Conversações Individuais**

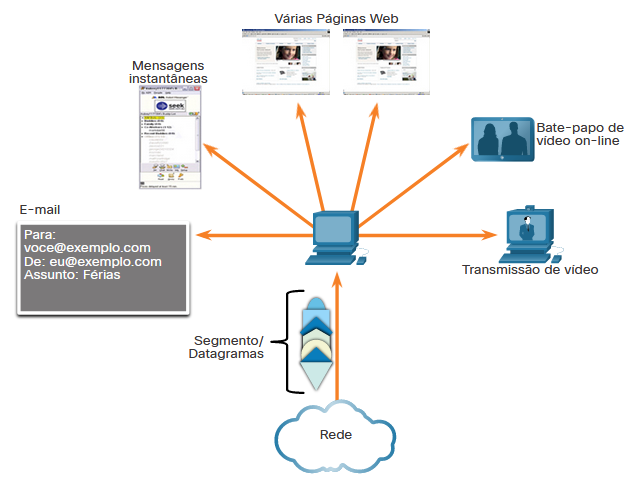
Na camada de transporte, cada conjunto de dados que flui entre um aplicativo de origem e um aplicativo de destino é conhecido como conversa e é rastreado separadamente. É responsabilidade da camada de transporte manter e monitorar essas várias conversações.



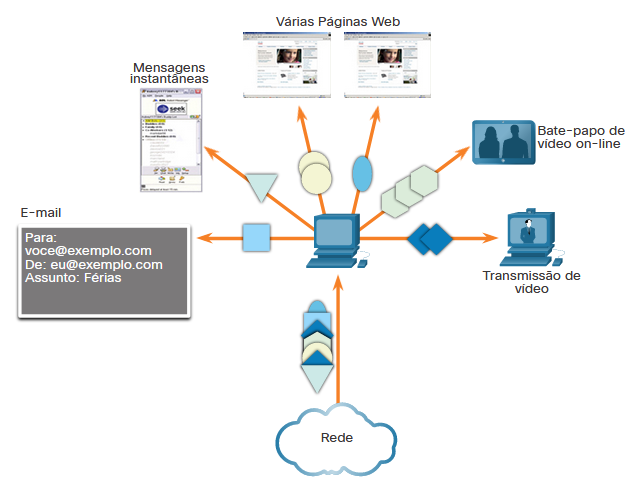
Como ilustrado na figura, um host pode ter vários aplicativos que estão se comunicando pela rede simultaneamente.

A maioria das redes tem uma limitação da quantidade de

**Adicionar Informações de Cabeçalho**

O protocolo da camada de transporte também adiciona informações de cabeçalho contendo dados binários organizados em vários campos a cada bloco de dados. São os valores nesses campos que permitem que os vários protocolos da camada de transporte realizem diferentes funções no gerenciamento da comunicação de dados.

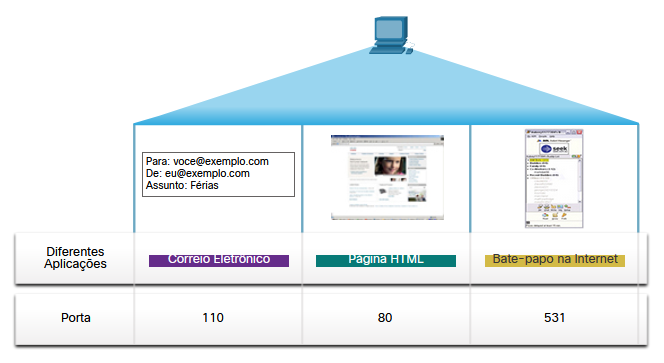
Por exemplo, as informações de cabeçalho são usadas pelo host de recebimento para remontar os blocos de dados em um fluxo de dados completo para o programa de camada de aplicativo de recebimento.



A camada de transporte garante que, mesmo com vários aplicativos em execução em um dispositivo, todos os aplicativos recebam os dados corretos.

**Identificação das Aplicações**

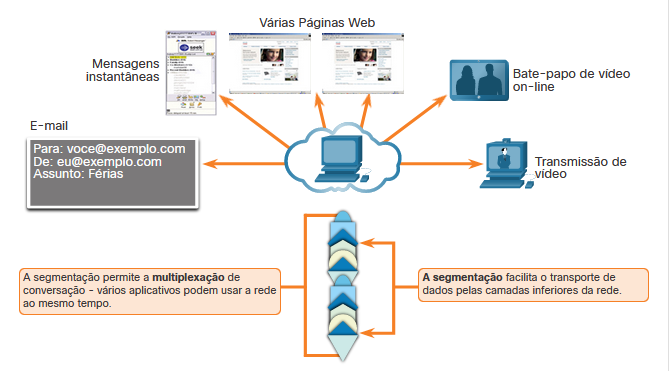
A camada de transporte deve separar e gerenciar várias comunicações com as diferentes necessidades de requisitos de transporte. Para passar fluxos de dados para os aplicativos adequados, a camada de transporte identifica o aplicativo de destino usando um identificador chamado número da porta. Conforme ilustrado na figura, cada processo de software que precisa acessar a rede recebe um número de porta exclusivo para esse host.



**Multiplexação das Conversas**

O envio de alguns tipos de dados (por exemplo, um vídeo de streaming) através de uma rede, como um fluxo de comunicação completo, pode consumir toda a largura de banda disponível. Isso impediria que outras conversas de comunicação ocorressem ao mesmo tempo. Isso também dificultaria a recuperação de erro e retransmissão dos dados danificados.

Como mostrado na figura, a camada de transporte usa segmentação e multiplexação para permitir que diferentes conversas de comunicação sejam intercaladas na mesma rede.



A verificação de erros pode ser realizada nos dados do segmento, para determinar se o segmento foi alterado durante a transmissão.

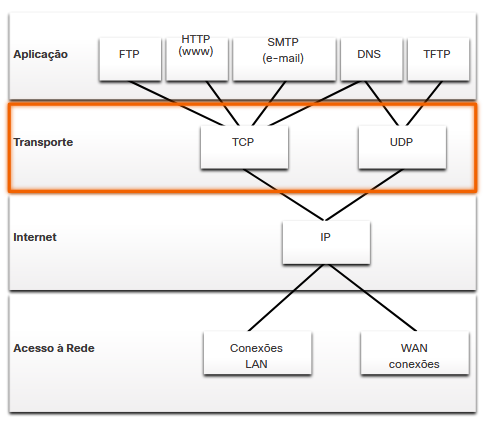
9.1.3

## Protocolos da Camada de Transporte

O IP está preocupado apenas com a estrutura, endereçamento e roteamento de pacotes. O IP não especifica como a entrega ou o transporte de pacotes ocorrem.

Os protocolos de camada de transporte especificam como transferir mensagens entre hosts e são responsáveis pelo gerenciamento dos requisitos de confiabilidade de uma conversa. A camada de transporte inclui os protocolos TCP e UDP.

Diferentes aplicações têm diferentes necessidades de confiabilidade de transporte. Portanto, o TCP/IP fornece dois protocolos de camada de transporte, conforme mostrado na figura.



9.1.4

**Protocolo TCP**

O IP se preocupa apenas com a estrutura, o endereçamento e o roteamento de pacotes, do remetente original ao destino final. A IP não é responsável por garantir a entrega ou determinar se uma conexão entre o remetente e o destinatário precisa ser estabelecida.

O TCP é considerado um protocolo de camada de transporte confiável, completo, que garante que todos os dados cheguem ao destino. O TCP inclui campos que garantem a entrega dos dados do aplicativo. Esses campos exigem processamento adicional pelos hosts de envio e recebimento.

**Nota**: O TCP divide os dados em segmentos.

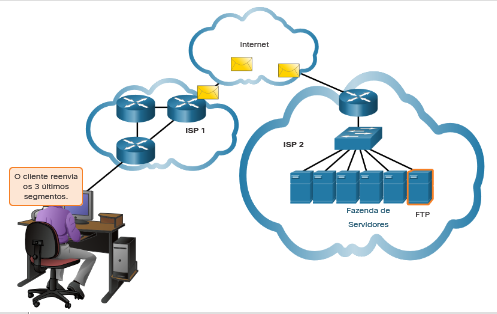
O transporte TCP é análogo a enviar pacotes que são rastreados da origem ao destino. Se um pedido pelo correio estiver dividido em vários pacotes, um cliente poderá verificar on-line a sequência de recebimento do pedido.

O TCP fornece confiabilidade e controle de fluxo usando estas operações básicas:

* Número e rastreamento de segmentos de dados transmitidos para um host específico a partir de um aplicativo específico;
* Confirmar dados recebidos;
* Retransmitir todos os dados não confirmados após um determinado período de tempo
* Dados de sequência que podem chegar em ordem errada
* Enviar dados a uma taxa eficiente que seja aceitável pelo receptor.

Para manter o estado de uma conversa e rastrear as informações, o TCP deve primeiro estabelecer uma conexão entre o remetente e o receptor. É por isso que o TCP é conhecido como um protocolo orientado a conexão.

Clique em Reproduzir na figura para ver como segmentos TCP e as confirmações são transmitidos do remetente ao destinatário.

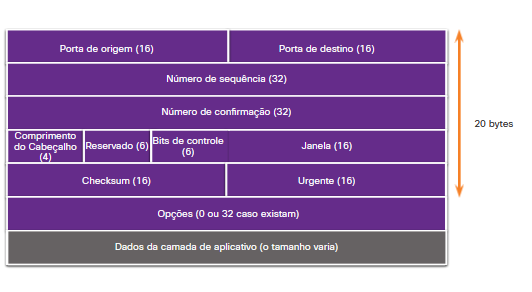


9.1.5

**Cabeçalho TCP**

TCP é um protocolo stateful, o que significa que ele controla o estado da sessão de comunicação. Para manter o controle do estado de uma sessão, o TCP registra quais informações ele enviou e quais informações foram confirmadas. A sessão com estado começa com o estabelecimento da sessão e termina com o encerramento da sessão.

Um segmento TCP adiciona 20 bytes (ou seja, 160 bits) de sobrecarga ao encapsular os dados da camada de aplicativo. A figura mostra os campos em um cabeçalho TCP.



9.1.6

**Campos de cabeçalho TCP**

A tabela identifica e descreve os dez campos em um cabeçalho TCP.

| Descrição do campo do cabeçalho TCP Porta de origem Um campo de 16 bits usado para identificar o aplicativo de origem por número de porta.Destination Porta 16 bits campo usado para identificar o aplicativo de destino pelo número da porta.Número de seqüência A 32 bits campo usado para fins de remontagem de dados.Número de confirmação Um campo de 32 bits usado para indicar que os dados foram recebidos e o próximo byte esperado de o Source.Header Comprimento Um campo de 4 bits conhecido como 'offset' de datas' que indica o comprimento do cabeçalho do segmento TCP.Reservado um campo de 6 bits que está reservado para uso futuro.Bits de controle Um campo de 6 bits usado que inclui códigos de bits ou sinalizadores, que indicam a finalidade e a função do segmento TCP.Window tamanho Um campo de 16 bits usado para indicar o número de bytes que podem ser aceito ao mesmo tempo.Checksum Um campo de 16 bits usado para verificação de erros do cabeçalho de segmento e data.Urgente Um campo de 16 bits usado para indicar se o dados contidos são urgentes. | |
| --- | --- |
| **Campo de cabeçalho TCP** | **Descrição** |
| **Porta de origem** | Um campo de 16 bits usado para identificar o aplicativo de origem por número de porta. |
| **Porta de destino** | Um campo de 16 bits usado para identificar o aplicativo de destino por porta número. |
| **Número sequencial** | Um campo de 32 bits usado para fins de remontagem de dados. |
| **Número de Confirmação** | Um campo de 32 bits usado para indicar que os dados foram recebidos e o próximo byte esperado da fonte. |
| **Comprimento do cabeçalho** | Um campo de 4 bits conhecido como 'offset' de datas' que indica o comprimento do cabeçalho do segmento TCP. |
| **Reservado** | Um campo de 6 bits que é reservado para uso futuro. |
| **Bits de controle** | Um campo de 6 bits que inclui códigos de bits, ou sinalizadores, que indicam a finalidade e função do segmento TCP. |
| **Tamanho da janela** | Um campo de 16 bits usado para indicar o número de bytes que podem ser aceitos de uma só vez. |
| **Checksum** | Um campo de 16 bits usado para verificação de erros do cabeçalho e dos dados do segmento. |
| **Urgente** | Um campo de 16 bits usado para indicar se os dados contidos são urgentes. |

9.1.7

**Protocolo UDP (User Datagram Protocol)**

O UDP é um protocolo de camada de transporte mais simples do que o TCP. Ele não fornece confiabilidade e controle de fluxo, o que significa que requer menos campos de cabeçalho. Como o remetente e os processos UDP receptor não precisam gerenciar confiabilidade e controle de fluxo, isso significa que datagramas UDP podem ser processados mais rápido do que segmentos TCP. O UDP fornece as funções básicas para fornecer datagramas entre os aplicativos apropriados, com muito pouca sobrecarga e verificação de dados.

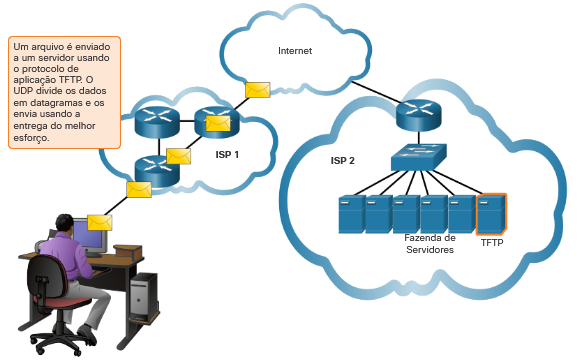
**Nota**: O UDP divide os dados em datagramas que também são chamados de segmentos.

UDP é um protocolo sem conexão. Como o UDP não fornece confiabilidade ou controle de fluxo, ele não requer uma conexão estabelecida. Como o UDP não controla informações enviadas ou recebidas entre o cliente e o servidor, o UDP também é conhecido como um protocolo sem estado.

UDP também é conhecido como um protocolo de entrega de melhor esforço porque não há confirmação de que os dados são recebidos no destino. Com o UDP, não há processo de camada de transporte que informe ao remetente se a entrega foi bem-sucedida.

O UDP é como colocar uma carta regular, não registrada, no correio. O remetente da carta não tem conhecimento se o destinatário está disponível para receber a carta. Nem a agência de correio é responsável por rastrear a carta ou informar ao remetente se ela não chegar ao destino final.

Clique em Reproduzir na figura para ver uma animação dos datagramas UDP sendo transmitidos do remetente para o receptor.



9.1.8

**Cabeçalho UDP**

UDP é um protocolo sem estado, o que significa que nem o cliente nem o servidor rastreiam o estado da sessão de comunicação. Se a confiabilidade for necessária ao usar o UDP como protocolo de transporte, ela deve ser tratada pela aplicação.

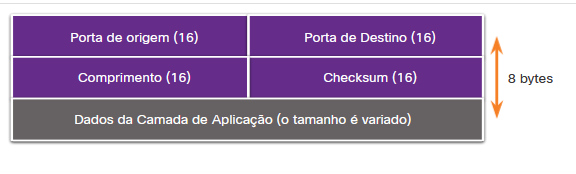
Um dos requisitos mais importantes para transmitir vídeo ao vivo e voz sobre a rede é que os dados continuem fluindo rapidamente. Vídeo ao vivo e aplicações de voz podem tolerar alguma perda de dados com efeito mínimo ou sem visibilidade e são perfeitos para o UDP.

Os blocos de comunicação no UDP são chamados de datagramas ou segmentos. Esses datagramas são enviados como o melhor esforço pelo protocolo da camada de transporte.

O cabeçalho UDP é muito mais simples do que o cabeçalho TCP porque só tem quatro campos e requer 8 bytes (ou seja, 64 bits). A figura mostra os campos em um cabeçalho UDP.

O diagrama de datagrama UDP mostra 4 campos de cabeçalho: porta de origem, porta de destino, comprimento e soma de verificação, bem como os dados da camada de aplicação não cabeçalho

8 bytesPorta de origem (16)Porta de Destino (16)Comprimento (16)Checksum (16)Dados da Camada de Aplicação (o tamanho é variado)



9.1.9

**Campos de Cabeçalho UDP**

A tabela identifica e descreve os quatro campos em um cabeçalho UDP.

| Descrição do campo do cabeçalho UDP Porta de origem Um campo de 16 bits usado para identificar o aplicativo de origem por número de porta.Destination Porta 16 bits campo usado para identificar o aplicativo de destino pelo número da porta.Comprimento Um campo de 16 bits que indica o comprimento do cabeçalho de datagrama UDP. Checksum Um campo de 16 bits usado para verificação de erros do cabeçalho e dos dados do datagrama. | |
| --- | --- |
| **Campo de Cabeçalho UDP** | **Descrição** |
| **Porta de origem** | Um campo de 16 bits usado para identificar o aplicativo de origem por número de porta. |
| **Porta de destino** | Um campo de 16 bits usado para identificar o aplicativo de destino por porta número. |
| **Tamanho** | Um campo de 16 bits que indica o comprimento do cabeçalho do datagrama UDP. |
| **Checksum** | Um campo de 16 bits usado para verificação de erros do cabeçalho e dos dados do datagrama. |

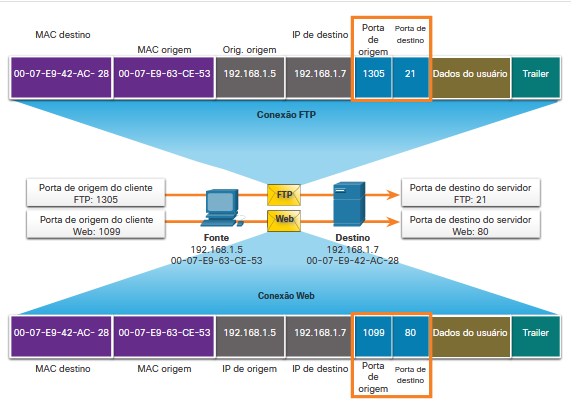
9.1.10

**Pares de Sockets**

As portas origem e destino são colocadas no segmento. Os segmentos são encapsulados em um pacote IP. O pacote IP contém o endereço IP de origem e destino. A combinação do endereço IP de origem e o número de porta de origem, ou do endereço IP de destino e o número de porta de destino é conhecida como um socket.

No exemplo na figura, o PC está solicitando simultaneamente serviços FTP e Web do servidor de destino.

A figura mostra um PC estabelecendo uma conexão FTP e Web com um servidor. The requests have source and destination port numbers which identify the host PC and the requested application service respectively.



No exemplo, a solicitação FTP gerada pelo PC inclui os endereços MAC da Camada 2 e os endereços IP da Camada 3. A solicitação também identifica o número da porta de origem 1305 (ou seja, gerado dinamicamente pelo host) e a porta de destino, identificando os serviços de FTP na porta 21. O host também solicitou uma página da Web do servidor usando os mesmos endereços de Camada 2 e Camada 3. No entanto, ele está usando o número da porta de origem 1099 (ou seja, gerado dinamicamente pelo host) e a porta de destino identificando o serviço Web na porta 80.

O socket é usado para identificar o servidor e o serviço que está sendo solicitado pelo cliente. Um socket do cliente pode ser assim, com 1099 representando o número da porta de origem: 192.168.1.5:1099

O soquete em um servidor da web pode ser 192.168.1.7:80

Juntos, esses dois soquetes se combinam para formar um par de soquetes: 192.168.1.5:1099, 192.168.1.7:80

Os sockets permitem que vários processos em execução em um cliente se diferenciem uns dos outros, e várias conexões com um processo no servidor sejam diferentes umas das outras.

Este número de porta age como um endereço de retorno para a aplicação que faz a solicitação. A camada de transporte rastreia essa porta e a aplicação que iniciou a solicitação, de modo que quando uma resposta é retornada, ela pode ser encaminhada para a aplicação correta.

# Estabelecimento da Sessão da Camada de Transporte

9.2.1

## Processos em Servidores TCP

Você já conhece os fundamentos do TCP. Compreender a função dos números de porta irá ajudá-lo a compreender os detalhes do processo de comunicação TCP. Neste tópico, você também aprenderá sobre os processos de handshake de três vias e terminação de sessão TCP.

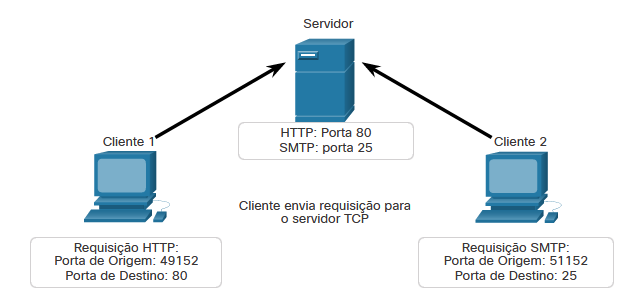
Cada processo de aplicativo em execução em um servidor está configurado para usar um número de porta. O número da porta é atribuído automaticamente ou configurado manualmente por um administrador do sistema.

Um servidor individual não pode ter dois serviços atribuídos ao mesmo número de porta dentro dos mesmos serviços de camada de transporte. Por exemplo, um host executando um aplicativo de servidor web e um aplicativo de transferência de arquivos não pode ter os dois configurados para usar a mesma porta, como a porta TCP 80.

Um aplicativo de servidor ativo atribuído a uma porta específica é considerado aberto, o que significa que a camada de transporte aceita e processa os segmentos endereçados a essa porta. Qualquer solicitação de cliente que chega endereçada ao soquete correto é aceita e os dados são transmitidos à aplicação do servidor. Pode haver muitas portas abertas ao mesmo tempo em um servidor, uma para cada aplicação de servidor ativa.

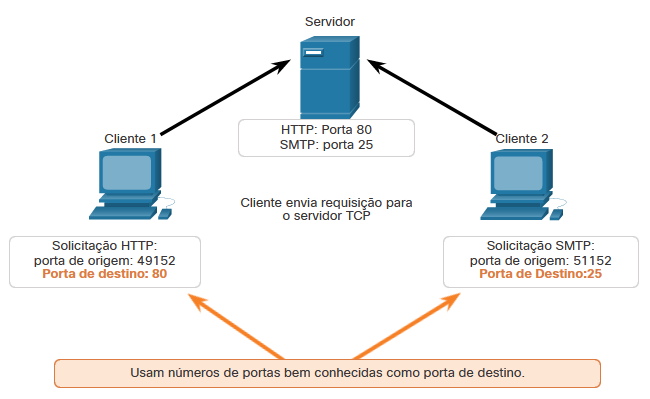
**Clientes Enviando Requisições TCP**

O Cliente 1 está a solicitar serviços Web e o Cliente 2 está a solicitar o serviço de correio electrónico do mesmo servidor.



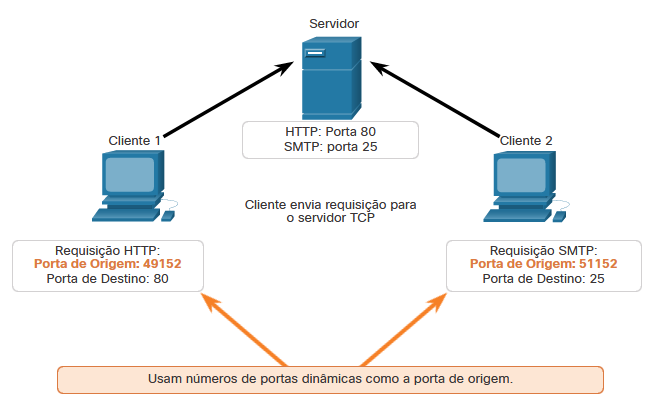
**Portas de Destino das Requisições**

O cliente 1 está solicitando serviços Web usando a porta 80 de destino bem conhecida (HTTP) e o cliente 2 está solicitando o serviço de email usando a porta 25 (SMTP) bem conhecida.



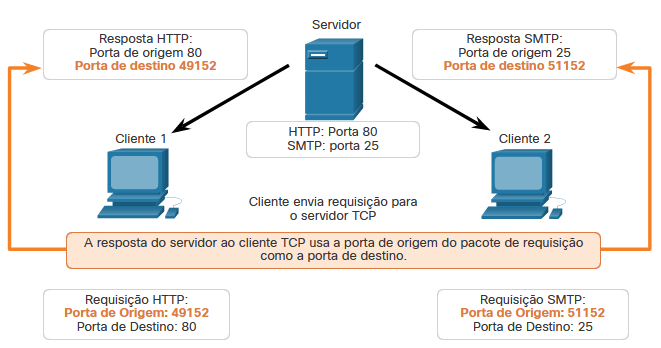
**Portas de Origem das Requisições**

As solicitações do cliente geram dinamicamente um número de porta de origem. Nesse caso, o cliente 1 está usando a porta de origem 49152 e o cliente 2 está usando a porta de origem 51152.



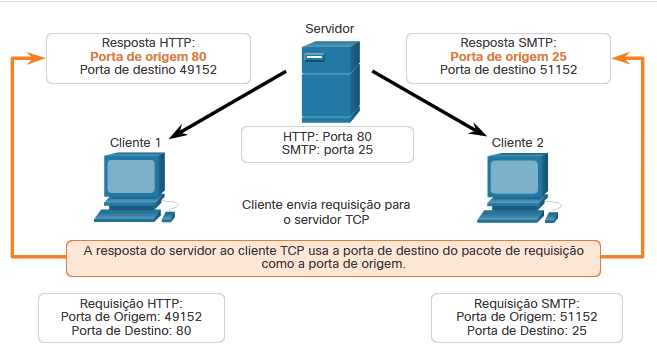
**Portas de Destino das Respostas**

Quando o servidor responde às solicitações do cliente, ele reverte as portas de destino e de origem da solicitação inicial. Observe que a resposta do servidor à solicitação da Web agora tem a porta de destino 49152 e a resposta de e-mail agora tem a porta de destino 51152.



**Portas de Origem das Respostas**

A porta de origem na resposta do servidor é a porta de destino original nas solicitações iniciais.



9.2.2

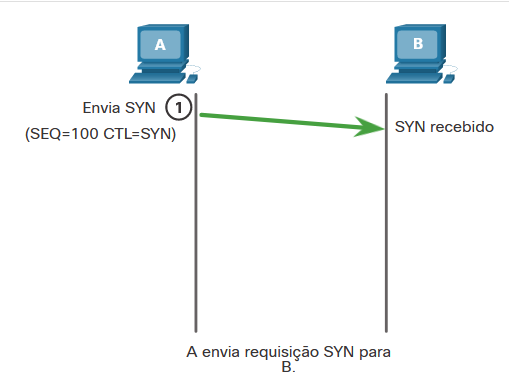
**Estabelecimento de Conexão TCP**

Em algumas culturas, quando duas pessoas se encontram, elas costumam se cumprimentar apertando as mãos. Ambas as partes entendem o ato de apertar as mãos como um sinal para uma saudação amigável. As conexões de rede são semelhantes. Nas conexões TCP, o cliente host estabelece a conexão com o servidor usando o processo de handshake de três vias.

Clique em cada botão para obter mais informações sobre cada etapa de estabelecimento de conexão TCP.

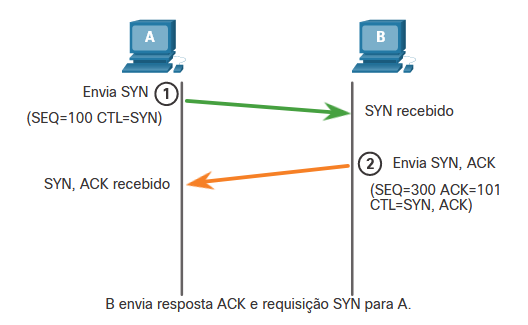
**Etapa 1. SYN**

O cliente iniciador requisita uma sessão de comunicação cliente-servidor com o servidor.



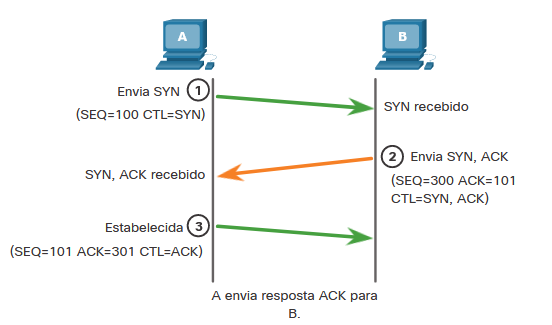
**Etapa 2. ACK e SYN**

O servidor confirma a sessão de comunicação cliente-servidor e requisita uma sessão de comunicação de servidor-cliente.



**Etapa 3. ACK**

O cliente iniciador confirma a sessão de comunicação de servidor-cliente.



O handshake de três vias valida se o host de destino está disponível para comunicação. Neste exemplo, o host A validou que o host B está disponível.

9.2.3

**Encerramento da Sessão**

Para fechar uma conexão, o flag de controle Finish (FIN) deve ser ligado no cabeçalho do segmento. Para terminar cada sessão TCP de uma via, um handshake duplo, consistindo de um segmento FIN e um segmento ACK (Acknowledgment) é usado. Portanto, para terminar uma conversação única permitida pelo TCP, quatro trocas são necessárias para finalizar ambas as sessões. O cliente ou o servidor podem iniciar o encerramento.

No exemplo, os termos cliente e servidor são usados como referência para simplificar, mas dois hosts que possuem uma sessão aberta podem iniciar o processo de finalização.

**Etapa 1. FIN**

Quando o cliente não tem mais dados para enviar no fluxo, ele envia um segmento com um flag FIN ligado.

**Etapa 2. ACK**

O servidor envia ACK para confirmar o recebimento de FIN para encerrar a sessão do cliente com o servidor.

**Etapa 3. FIN**

O servidor envia um FIN ao cliente para encerrar a sessão do servidor-para-cliente.

PCB também envia sua própria fin para PCA para terminar seu lado da sessão

**Etapa 4. ACK**

O cliente responde com um ACK para reconhecer o FIN do servidor.

PCA envia um ack em resposta à barbatana PCBs que termina a conexão

Quando todos os segmentos tiverem sido reconhecidos, a sessão é encerrada.

9.2.4

## Análise do Handshake Triplo do TCP

Os hosts mantêm o estado, rastreiam cada segmento de dados em uma sessão e trocam informações sobre quais dados são recebidos usando as informações no cabeçalho TCP. O TCP é um protocolo full-duplex, em que cada conexão representa duas sessões de comunicação unidirecional. Para estabelecer uma conexão, os hosts realizam um handshake triplo (three-way handshake). Conforme mostrado na figura, os bits de controle no cabeçalho TCP indicam o progresso e o status da conexão.

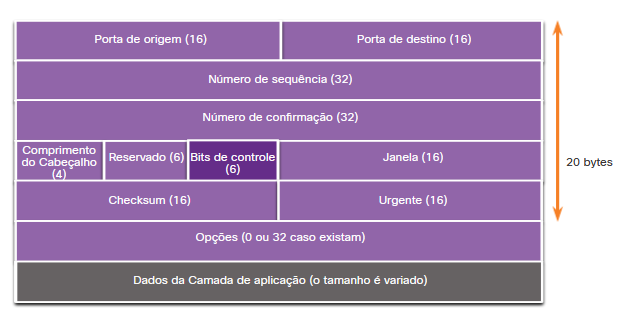
Estas são as funções do handshake de três vias:

* Estabelece que o dispositivo de destino está presente na rede.
* Ele verifica se o dispositivo de destino possui um serviço ativo e está aceitando solicitações no número da porta de destino que o cliente inicial pretende usar.
* Ele informa ao dispositivo de destino que o cliente de origem pretende estabelecer uma sessão de comunicação nesse número de porta.

Após a conclusão da comunicação, as sessões são fechadas e a conexão é encerrada. Os mecanismos de conexão e sessão ativam a função de confiabilidade do TCP.

mostra os campos de cabeçalho do segmento tcp com o campo de bits de controle de 6 bits destacado

### Campo de bits de controle

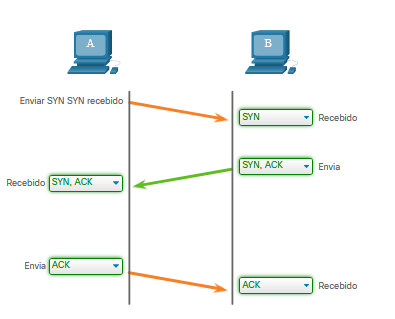


Os seis bits no campo Bits de Controle do cabeçalho do segmento TCP são também conhecidos como flags. Um sinalizador é um pouco definido como ativado ou desativado.

Os seis bits de controle sinalizadores são os seguintes:

* **URG** - Campo de ponteiro urgente significativo.
* **ACK** - Indicador de confirmação usado no estabelecimento de conexão e encerramento de sessão.
* **PSH** - Função Push.
* **RST** - Redefina a conexão quando ocorrer um erro ou tempo limite.
* **SYN** - Sincronizar números de sequência usados no estabelecimento de conexão.
* **FIN** - Não há mais dados do remetente e usados no encerramento da sessão.

Pesquise na Internet para saber mais sobre as bandeiras PSH e URG.



# Confiabilidade da Camada de Transporte

9.3.1

## Confiabilidade do TCP - Entrega garantida e solicitada

A razão pela qual o TCP é o melhor protocolo para alguns aplicativos é porque, ao contrário do UDP, ele reenvia pacotes descartados e números de pacotes para indicar sua ordem correta antes da entrega. O TCP também pode ajudar a manter o fluxo de pacotes para que os dispositivos não fiquem sobrecarregados. Este tópico aborda esses recursos do TCP em detalhes.

Pode haver momentos em que os segmentos TCP não chegam ao seu destino. Outras vezes, os segmentos TCP podem chegar fora de ordem. Para que a mensagem original seja entendida pelo destinatário, todos os dados devem ser recebidos e os dados nesses segmentos devem ser remontados na ordem original. Os números de sequência são atribuídos no cabeçalho de cada pacote para alcançar esse objetivo. O número de sequência representa o primeiro byte de dados do segmento TCP.

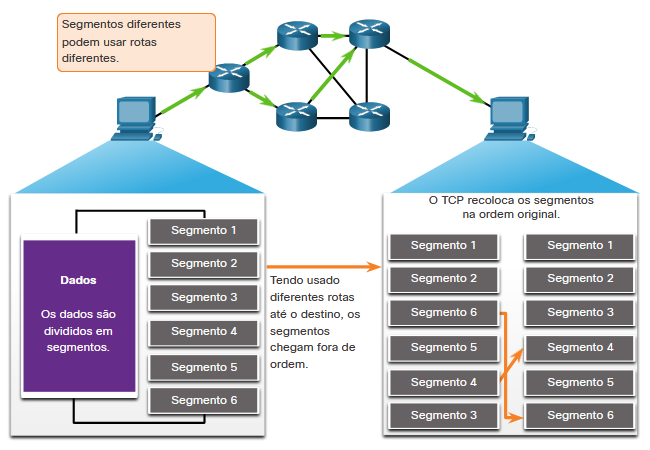
Durante o estabelecimento de uma sessão, um número de sequência inicial (ISN) é definido. Este ISN representa o valor inicial dos bytes que são transmitidos ao aplicativo receptor. À medida que os dados são transmitidos durante a sessão, número de sequência é incrementado do número de bytes que foram transmitidos. Esse rastreamento dos bytes de dados permite que cada segmento seja identificado e confirmado de forma única. Segmentos perdidos podem então, ser identificados.

O ISN não começa em um, mas é efetivamente um número aleatório. Isso é para impedir determinados tipos de ataques maliciosos. Para simplificar os exemplos desse capítulo, usaremos um ISN de 1.

Os números de sequência do segmento indicam como remontar e reordenar os segmentos recebidos, como mostrado na figura.

mostra que, embora os segmentos possam tomar rotas diferentes e chegar fora de ordem no destino, o TCP tem a capacidade de reordenar os segmentos

### Os Segmentos TCP São Reordenados no Destino



O processo TCP receptor coloca os dados de um segmento em um buffer receptor. Os segmentos são então colocados na ordem de sequência correta e passados para a camada de aplicativo quando remontados. Qualquer segmento que chegue com números de sequência fora de ordem são retidos para processamento posterior. Por isso, quando os segmentos com os bytes que faltavam chegam, esses segmentos são processados.

9.3.2

**Vídeo - Confiabilidade TCP - Números de Sequência e Reconhecimentos**

Uma das funções do TCP é garantir que cada segmento chegue ao seu destino. Os serviços TCP no host de destino reconhecem os dados que foram recebidos pelo aplicativo de origem.

Clique em Reproduzir na figura para assistir a uma aula sobre números de sequência TCP e confirmações.

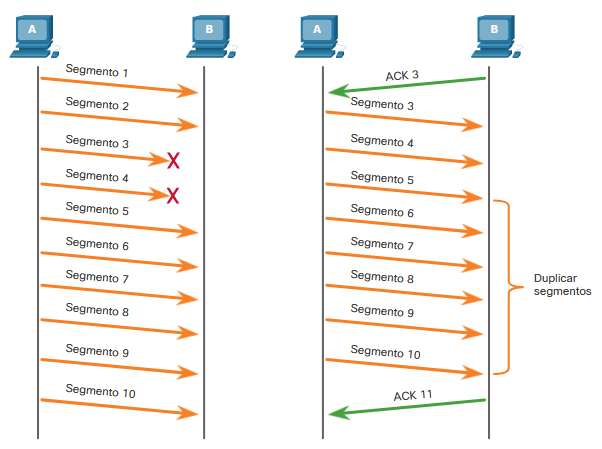
9.3.3

**Confiabilidade do TCP - perda de dados e retransmissão**

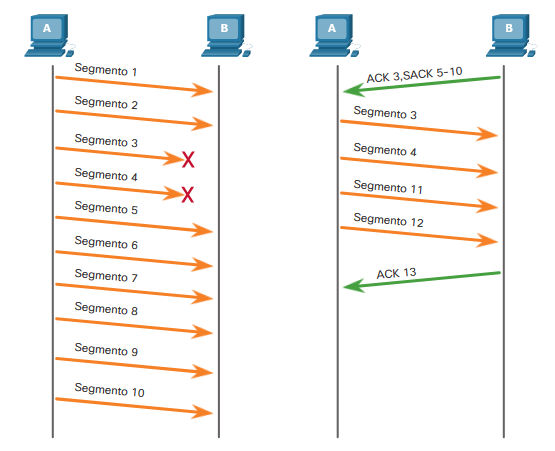
Não importa o quão bem projetada uma rede é, a perda de dados ocasionalmente ocorre. O TCP fornece métodos de gerenciamento dessas perdas de segmento. Entre esses métodos há um mecanismo que retransmite segmentos dos dados não confirmados.

O número de sequência (SEQ) e o número de confirmação (ACK) são usados juntamente para confirmar o recebimento dos bytes de dados contidos nos segmentos. O número SEQ identifica o primeiro byte de dados no segmento que está sendo transmitido. O TCP usa o número de confirmação (ACK) enviado de volta à origem para indicar o próximo byte que o destino espera receber. Isto é chamado de confirmação antecipatória.

Antes de melhorias posteriores, o TCP só podia reconhecer o próximo byte esperado. Por exemplo, na figura, usando números de segmento para simplicidade, o host A envia os segmentos 1 a 10 para o host B. Se todos os segmentos chegarem, exceto os segmentos 3 e 4, o host B responderia com confirmação especificando que o próximo segmento esperado é o segmento 3. O Host A não tem idéia se outros segmentos chegaram ou não. O host A, portanto, reenviaria os segmentos 3 a 10. Se todos os segmentos reenviados chegarem com sucesso, os segmentos 5 a 10 seriam duplicados. Isso pode levar a atrasos, congestionamentos e ineficiências.



Hoje em dia, os sistemas operacionais de host utilizam um recurso TCP opcional chamado reconhecimento seletivo (SACK), negociado durante o handshake de três vias. Se ambos os hosts suportarem SACK, o receptor pode reconhecer explicitamente quais segmentos (bytes) foram recebidos, incluindo quaisquer segmentos descontínuos. O host de envio, portanto, só precisa retransmitir os dados ausentes. Por exemplo, na próxima figura, novamente usando números de segmento para simplicidade, o host A envia segmentos 1 a 10 para o host B. Se todos os segmentos chegarem, exceto os segmentos 3 e 4, o host B pode reconhecer que recebeu segmentos 1 e 2 (ACK 3) e reconhecer seletivamente os segmentos 5 a 10 (SACK 5-10). O host A só precisaria reenviar os segmentos 3 e 4.



**Nota**: O TCP normalmente envia ACKs para todos os outros pacotes, mas outros fatores além do escopo deste tópico podem alterar esse comportamento.

O TCP usa temporizadores para saber quanto tempo esperar antes de reenviar um segmento. Na figura, reproduza o vídeo e clique no link para baixar o arquivo PDF. O vídeo e o arquivo PDF examinam a perda de dados e a retransmissão TCP.

9.3.5

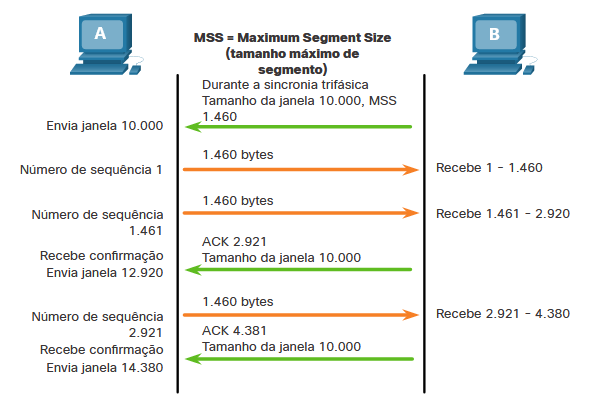
## Controle de Fluxo TCP – Tamanho da Janela e Confirmações

O TCP também fornece mecanismos para controle de fluxo. Controle de fluxo é a quantidade de dados que o destino pode receber e processar de forma confiável. O controle de fluxo ajuda a manter a confiabilidade da transmissão TCP definindo a taxa de fluxo de dados entre a origem e o destino em uma determinada sessão. Para realizar isso, o cabeçalho TCP inclui um campo de 16 bits chamado de tamanho da janela.

A figura mostra um exemplo de tamanho da janela e confirmações.

mostra PCB enviando PCB um tamanho de janela negociado de 10.000 bytes e um tamanho máximo de segmento de 1.460 bytes. PCA começa a enviar segmentos começando com o número de sequência 1. Uma confirmação do PCB pode ser enviada sem esperar até que o tamanho da janela seja atingido e o tamanho da janela possa ser ajustado pela PCA criando uma janela deslizante

### Exemplo de Tamanho da Janela TCP



O tamanho da janela determina o número de bytes que podem ser enviados antes de esperar uma confirmação. O número de reconhecimento é o número do próximo byte esperado.

O tamanho da janela é número de bytes que o dispositivo de destino de uma sessão TCP pode aceitar e processar de uma vez. Neste exemplo, o tamanho da janela inicial do PC B para a sessão TCP é de 10.000 bytes. No caso do primeiro byte ser número 1, o último byte que PC A pode enviar sem receber uma confirmação é o byte 10.000. Isso é conhecido como janela de envio do PC A. O tamanho da janela é incluído em todos os segmentos TCP, para que o destino possa modificar o tamanho da janela a qualquer momento, dependendo da disponibilidade do buffer.

O tamanho da janela inicial é determinado quando a sessão é estabelecida durante o handshake triplo. O dispositivo de origem deve limitar o número de bytes enviados ao dispositivo de destino com base no tamanho da janela do destino. Somente depois que o dispositivo de origem receber uma confirmação de que os bytes foram recebidos, ele poderá continuar a enviar mais dados para a sessão. Normalmente, o destino não esperará que todos os bytes que a sua janela comporta sejam recebidos para responder confirmando. À medida que os bytes forem recebidos e processados, o destino enviará confirmações para informar à origem que pode continuar a enviar bytes adicionais.

Por exemplo, é típico que o PC B não espere até que todos os 10.000 bytes tenham sido recebidos antes de enviar uma confirmação. Isso significa que o PC A pode ajustar sua janela de envio ao receber confirmações do PC B. Como mostrado na figura, quando o PC A recebe uma confirmação com o número de confirmação 2.921, que é o próximo byte esperado. A janela de envio do PC A irá incrementar 2.920 bytes. Isso altera a janela de envio de 10.000 bytes para 12.920. O PC A agora pode continuar enviando até outros 10.000 bytes para o PC B, desde que não envie mais do que sua nova janela de envio em 12.920.

Um destino que envia confirmações enquanto processa os bytes recebidos e o ajuste contínuo da janela de envio de origem é conhecido como janelas deslizantes. No exemplo anterior, a janela de envio do PC A incrementa ou desliza sobre outros 2.921 bytes de 10.000 para 12.920.

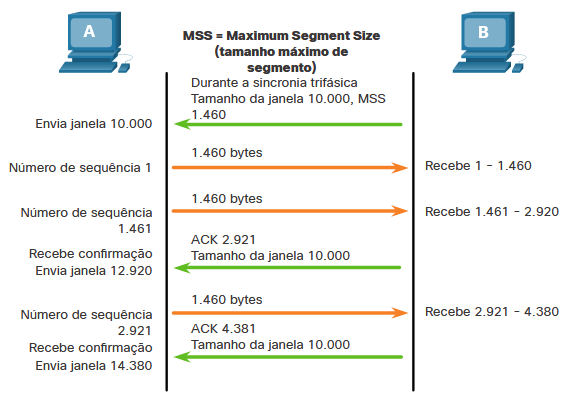
Se a disponibilidade do espaço de buffer do destino diminui, ele pode reduzir o tamanho da sua janela para informar à origem que reduza o número de bytes que ela deveria enviar sem receber uma confirmação.

**Nota**: Os dispositivos hoje usam o protocolo de janelas deslizantes. O receptor normalmente envia uma confirmação após cada dois segmentos que recebe. O número de segmentos recebidos antes de ser confirmado pode variar. A vantagem de janelas móveis é que permite que o emissor transmita continuamente segmentos, desde que o receptor esteja reconhecendo segmentos anteriores. Os detalhes das janelas móveis estão fora do escopo deste curso.

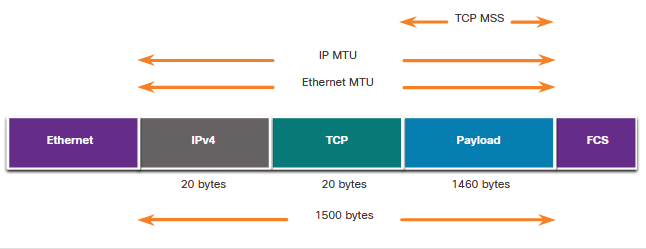
9.3.6

**Controle de Fluxo TCP - Tamanho Máximo do Segmento (MSS)**

Na figura, a fonte está transmitindo 1.460 bytes de dados dentro de cada segmento TCP. Normalmente, este é o tamanho máximo do segmento (MSS) que o dispositivo de destino pode receber. O MSS faz parte do campo de opções no cabeçalho TCP que especifica a maior quantidade de dados, em bytes, que um dispositivo pode receber em um único segmento TCP. O tamanho do MSS não inclui o cabeçalho TCP. O MSS é normalmente incluído durante o handshake de três vias.



Um MSS comum é 1.460 bytes ao usar IPv4. Um host determina o valor do campo de MSS subtraindo os cabeçalhos de IP e de TCP da MTU (Maximum transmission unit, Unidade máxima de transmissão) da Ethernet. Em uma interface Ethernet, a MTU padrão é 1500 bytes. Subtraindo o cabeçalho IPv4 de 20 bytes e o cabeçalho TCP de 20 bytes, o tamanho padrão do MSS será 1460 bytes, conforme mostrado na figura.



9.3.7

## Controle de Fluxo TCP - Prevenção de Congestionamento

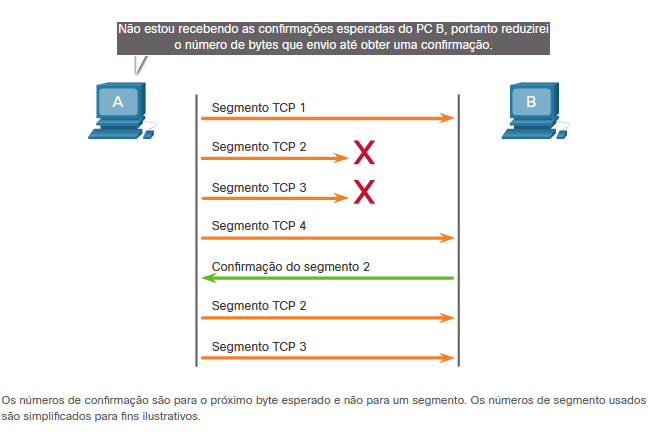
Quando ocorre um congestionamento em uma rede, isso resulta em pacotes sendo descartados pelo roteador sobrecarregado. Quando pacotes contendo segmentos TCP não atingem seu destino, eles são deixados sem serem reconhecidos. Ao determinar a taxa na qual os segmentos TCP são enviados, mas não confirmados, a origem pode pressupor um certo nível de congestionamento da rede.

Sempre que ocorrer um congestionamento, ocorrerá a retransmissão de segmentos TCP perdidos por parte da origem. Se a retransmissão não for devidamente controlada, a retransmissão adicional dos segmentos TCP pode agravar o congestionamento. Não só novos pacotes com segmentos TCP são introduzidos na rede, como também o efeito de feedback dos segmentos retransmitidos que foram perdidos aumentarão o congestionamento. Para evitar e controlar o congestionamento, o TCP emprega alguns mecanismos para lidar com o congestionamento, temporizadores e algoritmos.

Se a origem determina que os segmentos TCP não são confirmados ou não são confirmados em tempo hábil, isso pode reduzir o número de bytes enviados antes do recebimento de uma confirmação. Conforme ilustrado na figura, o PC A detecta que há congestionamento e, portanto, reduz o número de bytes que envia antes de receber uma confirmação do PC B.

mostra PCA enviando segmentos para PCB onde segmentos perdidos e retransmissão podem causar congestionamento

### Controle de Congestionamento TCP



Observe que é a origem que está reduzindo o número de bytes não confirmados que envia e não o tamanho da janela determinado pelo destino.

**Nota:** As explicações sobre os mecanismos, cronômetros e algoritmos reais de tratamento de congestionamento estão além do escopo deste curso.

# O Resumo da Camada de Transporte

9.4.1

## O que aprendi neste módulo?

**Características da Camada de Transporte**

A camada de transporte é o elo entre a camada de aplicação e as camadas inferiores do modelo OSI que são responsáveis pela transmissão da rede. A camada de transporte é responsável pela comunicação lógica entre aplicativos executados em hosts diferentes. A camada de transporte inclui TCP e UDP. Os protocolos de camada de transporte especificam como transferir mensagens entre hosts e é responsável por gerenciar os requisitos de confiabilidade de uma conversa. A camada de transporte é responsável por rastrear conversas (sessões), segmentar dados e remontar segmentos, adicionar informações de cabeçalho de segmento, identificar aplicativos e multiplexar conversas. O TCP é stateful e confiável. Ele reconhece os dados, reenvia os dados perdidos e entrega os dados em ordem sequencial. TCP é usado para e-mail e web. UDP é apátrida e rápido. Ele tem baixa sobrecarga, não requer confirmações, não reenvia dados perdidos e processa os dados na ordem em que eles chegam. UDP é usado para VoIP e DNS.

Os protocolos de camada de transporte TCP e UDP usam números de porta para gerenciar várias conversas simultâneas. É por isso que os campos de cabeçalho TCP e UDP identificam um número de porta de aplicativo de origem e destino. As portas origem e destino são colocadas no segmento. Os segmentos são encapsulados em um pacote IP. A combinação do endereço IP de origem e o número da porta de origem ou o endereço IP de destino e o número da porta de destino são conhecidas como soquetes. O soquete é usado para identificar o servidor e serviço que está sendo solicitado pelo cliente e o host e aplicativo no host que deve lidar com os dados retornados. O intervalo de números de porta é de 0 a 65535.

**Estabelecimento da Sessão da Camada de Transporte**

O handshake triplo estabelece que o dispositivo de destino está presente na rede. Ele verifica se o dispositivo de destino tem um serviço ativo que está aceitando solicitações no número da porta de destino que o cliente inicial pretende usar. Ele também informa ao dispositivo de destino que o cliente de origem pretende estabelecer uma sessão de comunicação naquele número de porta. Os sinalizadores de seis bits de controle são: URG, ACK, PSH, RST, SYN e FIN e são usados para identificar a função de mensagens TCP que são enviadas. Um cliente ou servidor pode encerrar uma única conversa suportada pelo TCP enviando uma sequência de mensagens TCP.

**Confiabilidade da Camada de Transporte**

Para que a mensagem original seja entendida pelo destinatário, todos os dados devem ser recebidos e os dados nesses segmentos devem ser remontados na ordem original. Os números de sequência são atribuídos no cabeçalho de cada pacote. Não importa o quão bem projetada uma rede é, a perda de dados ocasionalmente ocorre. O TCP fornece maneiras de gerenciar perdas de segmento. Existe um mecanismo para retransmitir segmentos para dados não reconhecidos. Os sistemas operacionais host de hoje geralmente empregam um recurso TCP opcional denominado confirmação seletiva (SACK), que é negociado durante o handshake triplo. Se ambos os hosts suportarem SACK, o receptor pode reconhecer explicitamente quais segmentos (bytes) foram recebidos, incluindo quaisquer segmentos descontínuos. O host de envio, portanto, só precisa retransmitir os dados ausentes. O controle de fluxo ajuda a manter a confiabilidade da transmissão TCP, ajustando a taxa de fluxo de dados entre a origem e o destino. Para realizar isso, o cabeçalho TCP inclui um campo de 16 bits chamado de tamanho da janela. O processo de envio de confirmações pelo destino enquanto processa os bytes recebidos, e o ajuste contínuo da janela de envio da origem é conhecido como janelas deslizantes. Uma fonte pode estar transmitindo 1.460 bytes de dados dentro de cada segmento TCP. Este é o tamanho máximo de segmento típico (MSS) que um dispositivo de destino pode receber. Para evitar e controlar o congestionamento, o TCP emprega vários mecanismos de manipulação de congestionamento.

# Introdução

10.0.1

## Por que devo cursar este módulo?

Neste módulo, você aprenderá sobre serviços de rede, incluindo DHCP, NAT, PAT, FTP, TFTP, protocolos de e-mail e DNS. Uma análise recente de ameaças de segurança de rede descobriu que mais de 90% do software malicioso usado para atacar redes usa o sistema DNS para realizar campanhas de ataque! Agora leia mais sobre a segurança desses protocolos.

10.0.2

## O que vou aprender neste módulo?

**Título do módulo:** Serviços de rede

**Objetivo do módulo:** Explicar como os serviços de rede habilitam a funcionalidade da rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| DHCP | Explicar como os serviços de DHCP viabilizam a funcionalidade de rede. |
| DNS | Explicar como os serviços de DNS viabilizam a funcionalidade de rede. |
| NAT | Explicar como os serviços de NAT viabilizam a funcionalidade de rede. |
| Serviços de transferência e compartilhamento de arquivos | Explicar como os serviços de transferência de arquivos viabilizam a funcionalidade de rede. |
| E-mail | Explicar como os serviços de e-mail viabilizam a funcionalidade de rede. |
| HTTP | Explicar como os serviços de HTTP viabilizam a funcionalidade de rede. |

# DHCP

10.1.1

## Protocolo DHCP

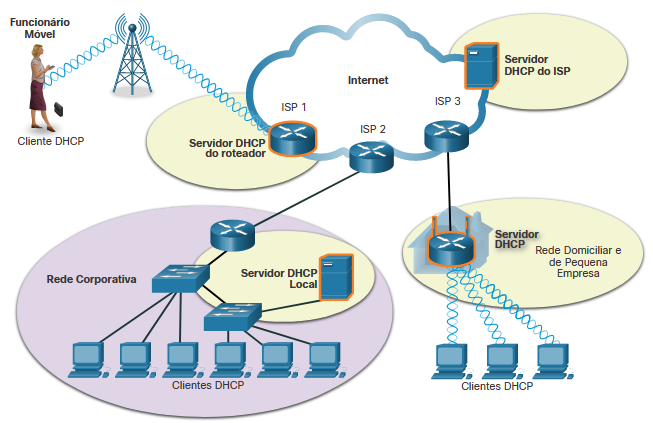
O serviço DHCP para IPv4 torna automática a atribuição de endereços IPv4, máscaras de sub-rede, gateways e outros parâmetros de rede IPv4. Isso é conhecido como o endereçamento dinâmico. A alternativa para o endereçamento dinâmico é o endereçamento estático. Ao usar o endereçamento estático, o administrador de redes insere manualmente informações de endereço IP em hosts.

Quando um host está conectado à Internet, o servidor DHCP é contatado e um endereço é requisitado. O servidor DHCP escolhe um endereço de uma lista configurada de endereços chamada pool e o atribui (aloca) ao host.

Em redes maiores, ou onde a população de usuários muda frequentemente, o DHCP é preferido para atribuição de endereços. Novos usuários podem chegar e precisar de uma conexão; outros podem ter novos computadores que devem ser conectados. Em vez usar endereçamento estático para cada conexão, é mais eficiente ter endereços IPv4 atribuídos automaticamente usando o DHCP.

O DHCP pode alocar endereços IP por um período de tempo configurável, chamado período de concessão. O período de concessão é uma configuração DHCP importante, quando o período de concessão expira ou o servidor DHCP recebe uma mensagem DHCPRELEASE, o endereço é retornado ao pool DHCP para reutilização. Os usuários podem se mover livremente de um local para outro e restabelecer com facilidade conexões de rede com o DHCP.

Como a figura mostra, diversos tipos de dispositivos podem ser servidores DHCP. O servidor DHCP na maioria das redes médias a grandes normalmente é um computador PC com um servidor dedicado. Em redes residenciais, o servidor DHCP é normalmente localizado no roteador local que conecta a rede residencial ao ISP.



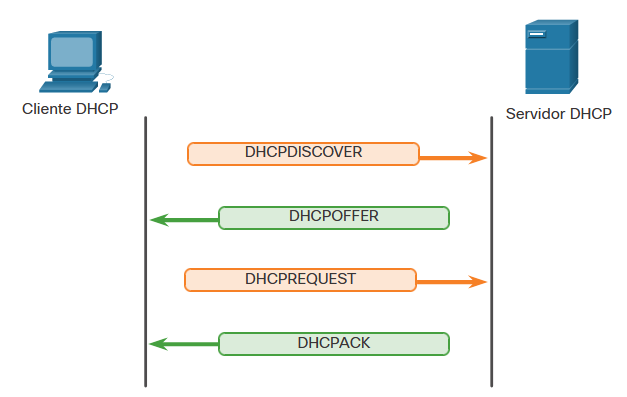
Muitas redes utilizam DHCP e endereçamento estático. O DHCP é usado para hosts de uso geral, como dispositivos de usuário final. O endereçamento estático é usado para dispositivos de rede, como roteadores de gateway, comutadores, servidores e impressoras.

O DHCP para IPv6 (DHCPv6) fornece serviços semelhantes para clientes IPv6. Uma diferença importante é que o DHCPv6 não fornece o endereço do gateway padrão. Isso só pode ser obtido dinamicamente a partir da mensagem Anúncio do roteador do roteador.

10.1.2

**Operação do DHCP**

Como mostra a figura, quando um dispositivo IPv4 configurado com DHCP inicia ou se conecta à rede, o cliente transmite uma mensagem de descoberta DHCP (DHCPDISCOVER) para identificar qualquer servidor DHCP disponível na rede. Um servidor DHCP responde com uma mensagem de oferta DHCP (DHCPOFFER), que oferece uma locação ao cliente. A mensagem de oferta contém o endereço IPv4 e a máscara de sub-rede a serem atribuídos, o endereço IPv4 do servidor DNS e o endereço IPv4 do gateway padrão. A oferta de locação também inclui a duração da locação.



O cliente pode receber várias mensagens DHCPOFFER, caso exista mais de um servidor DHCP na rede local. Portanto, deve escolher entre eles e transmitir uma mensagem de requisição de DHCP (DHCPREQUEST) que identifique o servidor explícito e a oferta de locação que o cliente está aceitando. Um cliente também pode decidir requisitar um endereço que já havia sido alocado pelo servidor.

Presumindo que o endereço IPv4 requisitado pelo cliente, ou oferecido pelo servidor, ainda seja válido, o servidor retornará uma mensagem de confirmação DHCP (DHCPACK) que confirma para o cliente que a locação foi finalizada. Se a oferta não é mais válida, o servidor selecionado responde com uma mensagem de confirmação negativa DHCP (DHCPNAK). Se uma mensagem DHCPNAK for retornada, o processo de seleção deverá recomeçar com a transmissão de uma nova mensagem DHCPDISCOVER. Quando o cliente tiver a locação, ela deverá ser renovada por outra mensagem DHCPREQUEST antes do vencimento.

O servidor DHCP garante que todos os endereços IP sejam exclusivos (um mesmo endereço IP não pode ser atribuído a dois dispositivos de rede diferentes simultaneamente). A maioria dos ISPs usa o DHCP para alocar endereços para seus clientes.

O DHCPv6 possui um conjunto de mensagens semelhantes às do DHCPv4. As mensagens DHCPv6 são SOLICIT, ADVERTISE, INFORMATION REQUEST, e REPLY.

10.1.3

## Formato de Mensagem DHCP

O formato de mensagem DHCPv4 é usado para todas as transações de DHCPv4. As mensagens DHCPv4 são encapsuladas no protocolo de transporte UDP. As mensagens DHCPv4 enviadas do cliente usam a porta de origem UDP 68 e a porta de destino 67. As mensagens de DHCPv4 enviadas do servidor ao cliente usam a porta origem 67 e a porta destino 68 do UDP. A estrutura da mensagem DHCPv4 é mostrada abaixo.

| **8**  Código OP  (1) | **16**  Tipo de hardware  (1) | **24**  Comprimento do endereço de hardware  (1) | **32**  Saltos  (1) |
| --- | --- | --- | --- |
| Identificador de transação | | | |
| Segundos - 2 bytes | | Flags - 2 bytes | |
| Endereço IP do Cliente (CIADDR) - 4 bytes | | | |
| Seu Endereço IP (YIADDR) - 4 bytes | | | |
| Endereço IP do Servidor (SIADDR) - 4 bytes | | | |
| Endereço IP do Gateway (GIADDR) - 4 bytes | | | |
| Endereço de Hardware do Cliente (CHADDR) - 16 bytes | | | |
| Nome do Servidor (SNAME) - 64 bytes | | | |
| Nome do arquivo de inicialização - 128 bytes | | | |
| Opções de DHCP - variável | | | |

Os campos são explicados aqui:

* **Código de operação (OP)** - especifica o tipo geral de mensagem. Um valor igual a 1 indica uma mensagem de solicitação; um valor de 2 é uma mensagem de resposta.
* **Tipo de hardware** - identifica o tipo de hardware usado na rede. Por exemplo, 1 é Ethernet, 15 é Frame Relay e 20 é uma linha serial. Esses são os mesmos códigos utilizados em mensagens ARP.
* **Comprimento do endereço de hardware** - especifica o comprimento do endereço.
* **Salto** - controla o encaminhamento de mensagens. Defina como 0 por um cliente antes de enviar uma solicitação.
* **Identificador de transação** - usado pelo cliente para combinar a solicitação com as respostas recebidas de servidores DHCPv4.
* **Segundos** - identifica o número de segundos decorridos desde que um cliente começou a tentar adquirir ou renovar um endereço. Usado pelos servidores DHCPv4 para priorizar respostas quando as solicitações do cliente são excepcionais.
* **Sinalizadores** - Usados por um cliente que não conhece seu endereço IPv4 ao enviar uma solicitação. Apenas um dos 16 bits é usado, que é a flag de broadcast. Um valor de 1 neste campo informa ao agente de servidor ou retransmissão de DHCPv4 que recebe a solicitação que a resposta deve ser enviada como broadcast.
* **Endereço IP do cliente** - usado por um cliente durante a renovação do aluguel quando o endereço do cliente é válido e utilizável, não durante o processo de aquisição de um endereço. O cliente coloca seu próprio endereço IPv4 nesse campo se, e apenas se, tiver um endereço IPv4 válido no estado limitado; caso contrário, define o campo como 0.
* **Seu endereço IP** - usado pelo servidor para atribuir um endereço IPv4 ao cliente.
* **Endereço IP do servidor** - usado pelo servidor para identificar o endereço do servidor que o cliente deve usar para a próxima etapa do processo de bootstrap, que pode ou não ser o servidor que está enviando esta resposta. O servidor de envio sempre inclui seu próprio endereço IPv4 em um campo especial chamado opção DHCPv4 do Identificador do Servidor.
* **Endereço IP do gateway** - roteia mensagens DHCPv4 quando agentes de retransmissão DHCPv4 estão envolvidos. O endereço de gateway facilita comunicações de solicitações de DHCPv4 e responde entre o cliente e um servidor que estão em sub-redes ou em redes diferentes.
* **Endereço de hardware do cliente** - especifica a camada física do cliente.
* **Nome do servidor** - usado pelo servidor enviando uma mensagem DHCPOFFER ou DHCPACK. O servidor também pode colocar seu nome nesse campo. Isso pode ser um apelido de texto simples ou um nome de domínio DNS, como dhcpserver.netacad.net.
* **Nome do arquivo de inicialização** - opcionalmente usado por um cliente para solicitar um tipo específico de arquivo de inicialização em uma mensagem DHCPDISCOVER. Usado por um servidor em um DHCPOFFER para especificar um diretório e nome do arquivo de inicialização.
* **Opções de DHCP** - contém opções de DHCP, incluindo vários parâmetros necessários para a operação básica de DHCP. Este campo tem comprimento variável. O cliente e o servidor podem usar esse campo.

# DNS

10.2.1

## Visão geral do DNS

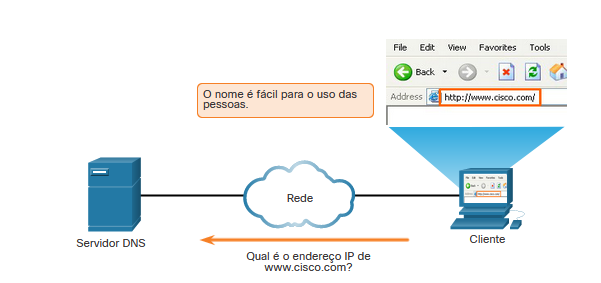
Os servidores web aos quais muitas vezes nos conectamos usando nomes como [www.cisco.com](http://www.cisco.com), são realmente alcançados atribuindo endereços IP a pacotes. Na Internet, esses nomes de domínio são muito mais fáceis para as pessoas lembrarem do que um endereço IP como 74.163.4.161. Se a Cisco decidir alterar o endereço numérico de [www.cisco.com](http://www.cisco.com), é transparente para o usuário porque o nome de domínio permanece o mesmo. O novo endereço é simplesmente vinculado ao nome de domínio atual e a conectividade é mantida.

O Sistema de Nomes de Domínio (DNS) foi desenvolvido para fornecer um meio confiável de gerenciar e fornecer nomes de domínio e seus endereços IP associados. O sistema DNS consiste em uma hierarquia global de servidores distribuídos que contêm bancos de dados de nomes para mapeamentos de endereços IP. O computador cliente na figura enviará uma solicitação ao servidor DNS para obter o endereço IP para [www.cisco.com](http://www.cisco.com) para que ele possa endereçar pacotes para esse servidor.

Uma análise recente das ameaças à segurança da rede descobriu que mais de 90% das explorações de software malicioso utilizam o sistema DNS para realizar campanhas de ataque à rede. Um analista de segurança cibernética deve ter uma compreensão completa do sistema DNS e das maneiras pelas quais o tráfego DNS malicioso pode ser detectado por meio da análise de protocolo e da inspeção de informações de monitoramento de DNS. Além disso, o malware freqüentemente entra em contato com servidores de comando e controle usando o DNS. Isso faz com que os URLs do servidor sejam indicadores de comprometimento para explorações específicas.

A Figura 1 mostra um cliente de computador e um servidor conectado a uma rede. O cliente está tentando acessar a Cisco

### DNS resolve nomes para endereços IP



10.2.2

## A Hierarquia de Domínio DNS

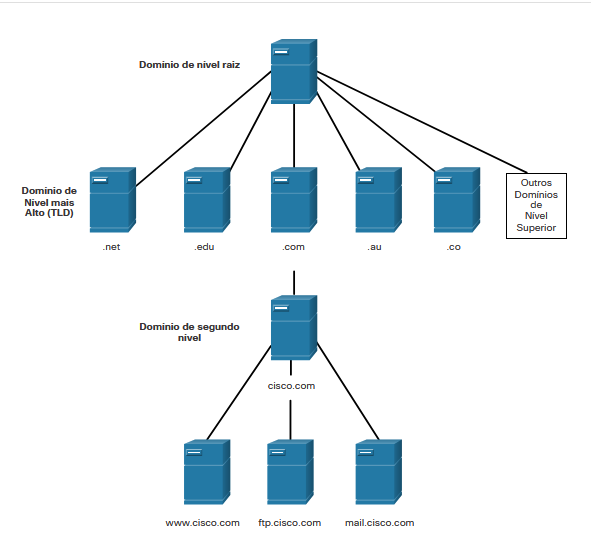
O DNS consiste em uma hierarquia de domínios genéricos de nível superior (gTLD) que consistem em .com, .net, .org, .gov, .edu e vários domínios de nível de país, como .br (Brasil), .es (Espanha), .uk (Reino Unido), etc. No próximo nível da hierarquia DNS estão domínios de segundo nível. Estes são representados por um nome de domínio que é seguido por um domínio de nível superior. Os subdomínios são encontrados no próximo nível da hierarquia DNS e representam alguma divisão do domínio de segundo nível. Finalmente, um quarto nível pode representar um host em um subdomínio. Cada elemento de uma especificação de domínio às vezes é chamado de rótulo. Os rótulos se movem do topo da hierarquia para baixo da direita para a esquerda. Um ponto (“. “) no final de um nome de domínio representa o servidor raiz no topo da hierarquia. A figura ilustra esta hierarquia de domínio DNS.

Os diferentes domínios de nível superior representam o tipo de organização ou país de origem. Exemplos de domínios de nível superior são os seguintes:

* .com - uma empresa ou indústria
* .org - uma organização sem fins lucrativos
* .au - Austrália
* .co - Colômbia

A figura mostra a árvore Hierachy do DNS. No topo está o Domínio de Nível Raiz com os Domínios de Nível Superior (TLD) conectados abaixo do Domínio de Nível Raiz. Os TLDs são .net, .edu, .com, .au, .co e outros domínios de nível superior. Sob o TLD .com está o domínio de Segundo Nível [www.cisco.com](http://www.cisco.com) e sob cisco.com estão [www.cisco.com](http://www.cisco.com), ftp.cisco.com e mail.cisco.com.

Domínio de nível raizDomínio de Nível mais Alto (TLD)Domínio de segundo nívelcisco.comwww.cisco.comftp.cisco.commail.cisco.com.net.edu.com.au.coOutros Domínios de   
Nível Superior



10.2.3

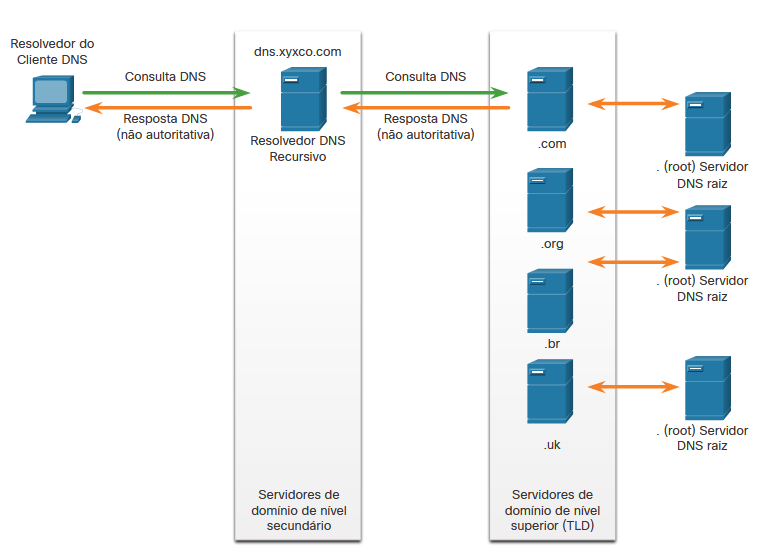
## O Processo de Pesquisa de DNS

Para entender o DNS, os analistas de segurança cibernética devem estar familiarizados com os seguintes termos:

* **Resolvedor** - Um cliente DNS que envia mensagens DNS para obter informações sobre o espaço de nome de domínio solicitado.
* **Recursão** - A ação executada quando um servidor DNS é solicitado a consultar em nome de um resolvedor DNS.
* **Servidor autoritativo** - Um servidor DNS que responde a mensagens de consulta com informações armazenadas em registros de recursos (RRs) para um espaço de nomes de domínio armazenado no servidor.
* **Resolvedor recursivo** - Um servidor DNS que consulta recursivamente as informações solicitadas na consulta DNS.
* **FQDN** - Um nome de domínio totalmente qualificado é o nome absoluto de um dispositivo dentro do banco de dados DNS distribuído.
* **RR** - Um Registro de Recurso é um formato usado em mensagens DNS que é composto dos seguintes campos: NOME, TIPO, CLASSE, TTL, RDLENT e RDATA.
* **Zona** - Um banco de dados que contém informações sobre o espaço de nomes de domínio armazenado em um servidor autoritativo.

Ao tentar resolver um nome para um endereço IP, um host de usuário, conhecido no sistema como um resolvedor, primeiro verificará seu cache DNS local. Se o mapeamento não for encontrado lá, uma consulta será emitida para o servidor DNS ou servidores configurados nas propriedades de endereçamento de rede para o resolvedor. Esses servidores podem estar presentes em uma empresa ou ISP. Se o mapeamento não for encontrado lá, o servidor DNS consultará outros servidores DNS de nível superior que são autoritativos para o domínio de nível superior para localizar o mapeamento. Estes são conhecidos como consultas recursivas.

Devido à carga potencial sobre servidores de domínio de nível superior autoritativos, alguns servidores DNS na hierarquia mantêm caches de todos os registros DNS resolvidos por um período de tempo. Esses servidores DNS de cache podem resolver consultas recursivas sem encaminhar as consultas para servidores de nível superior. Se um servidor exigir dados para uma zona, ele solicitará uma transferência desses dados de um servidor autoritário para essa zona. O processo de transferência de blocos de dados DNS entre servidores é conhecido como transferência de zona.



**Etapa 1**

O usuário digita um FQDN em um campo Endereço do aplicativo do navegador.

esta é uma figura com um cliente entrando em contato com um servidor DNS através da rede com um FQDN digitado em um campo de URL do navegador porque o nome de um site é mais fácil para as pessoas usarem

**Etapa 2**

Uma consulta DNS é enviada para o servidor DNS designado para o computador cliente.

**Etapa 3**

O servidor DNS corresponde ao FQDN com seu endereço IP.

**Etapa 4**

A resposta da consulta DNS é enviada de volta ao cliente com o endereço IP do FQDN.

**Etapa 5**

O computador cliente usa o endereço IP para fazer solicitações do servidor.

esta é uma figura com o computador cliente usando o endereço ip versão 4 para entrar em contato com o servidor [www.cisco.com](http://www.cisco.com) através da rede.

10.2.4

## Formato de Mensagem DNS

O DNS usa a porta UDP 53 para consultas e respostas DNS. As consultas DNS são originadas em um cliente e as respostas são emitidas a partir de servidores DNS. Se uma resposta DNS exceder 512 bytes, como quando DNS dinâmico (DDNS) é usado, a porta TCP 53 é usada para manipular a mensagem. Ele inclui o formato para consultas, respostas e dados. As comunicações do protocolo DNS utilizam um único formato, chamado de mensagem. Este formato de mensagem mostrado na figura é usado para todos os tipos de consultas do cliente e respostas do servidor, mensagens de erro e transferência de informações de registro de recursos entre servidores.

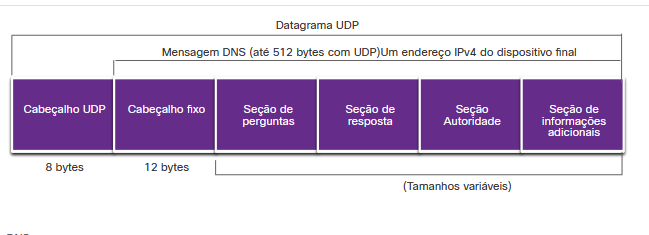
O servidor DNS armazena diferentes tipos de RRs usados para resolver nomes. Esses registros contêm o nome, endereço e tipo de registro. Aqui está uma lista de alguns desses tipos de registro:

* **A** - Um endereço IPv4 do dispositivo final
* **NS** - Um servidor de nomes com autoridade.
* **AAAA** - Um endereço IPv6 do dispositivo final (pronunciado quad-A).
* **MX** - Um registro de troca de correio.

Quando um cliente faz uma consulta, o processo DNS do servidor procura primeiramente em seus próprios registros para resolver o nome. Se ele não puder resolver o nome utilizando seus registros armazenados, entra em contato com outros servidores para concluir a tarefa. Quando uma correspondência é encontrada e retornada ao servidor requisitante original, o servidor temporariamente armazena o número do endereço em questão, no caso do mesmo nome ser requisitado outra vez.

O serviço Cliente DNS nos computadores com Windows também armazena nomes previamente resolvidos na memória. O comando **ipconfig /displaydns** exibe todas as entradas DNS em cache.

A figura mostra a estrutura de uma mensagem DNS dentro de um datagrama UDP. As contas de cabeçalho UDP para 8 bytes, as contas de cabeçalho fixo DNS para 12 bytes e, em seguida, as várias mensagens DNS compõem o restante da mensagem. A mensagem DNS pode ter até 512 bytes de tamanho. O texto no gráfico indica que o DNS usa a mesma mensagem para todos os tipos de consultas do cliente e respostas do servidor, mensagens de erro e transferência de registros de recursos entre servidores.



Datagrama UDPMensagem DNS (até 512 bytes com UDP)Um endereço IPv4 do dispositivo final(Tamanhos variáveis)8 bytes12 bytesCabeçalho UDPCabeçalho fixoSeção de perguntasSeção de respostaSeção AutoridadeSeção de informações adicionais

DNS usa a mesma mensagem para

* Todos os tipos de consultas do cliente e respostas do servidor
* Mensagens de erro
* A transferência de registros de recursos entre servidores

Conforme mostrado na figura, o DNS usa o mesmo formato de mensagem entre servidores, consistindo em uma pergunta, resposta, autoridade e informações adicionais para todos os tipos de consultas do cliente e respostas do servidor, mensagens de erro e transferência de informações de registro de recursos. A tabela descreve cada seção.

| **Seção de mensagens DNS** | **Descrição** |
| --- | --- |
| Pergunta | A pergunta para o servidor. Ele contém o nome de domínio a ser resolvido, a classe de domínio e o tipo de consulta. |
| Atender | O registro de recurso DNS, ou RR, para a consulta, incluindo o endereço IP resolvido, dependendo do tipo de RR. |
| Autoridade | Contém os RRs para a autoridade de domínio. |
| Adicional | Relevante apenas para respostas de consulta. Consiste em RRs que contêm informações adicionais que tornarão a resolução de consultas mais eficiente |

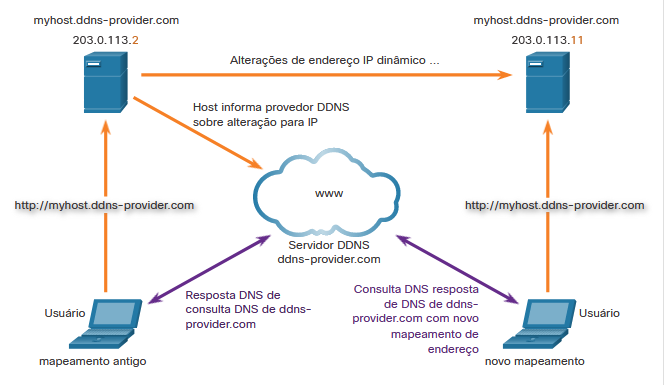
10.2.5

**DNS dinâmico**

O DNS exige que as empresas de registro de domínios aceitem e distribuam mapeamentos DNS de organizações que desejam registrar mapeamentos de nome de domínio e endereço IP. Após a criação do mapeamento inicial, um processo que pode levar 24 horas ou mais, alterações no endereço IP mapeado para o nome de domínio podem ser feitas entrando em contato com o registrador ou usando um formulário on-line para fazer a alteração. No entanto, devido ao tempo que leva para esse processo ocorrer e o novo mapeamento a ser distribuído no sistema de nomes de domínio, a alteração pode levar horas antes que o novo mapeamento esteja disponível para resolvedores. Em situações em que um ISP está usando DHCP para fornecer endereços para um domínio, é possível que o endereço mapeado para o domínio possa expirar e um novo endereço ser concedido pelo ISP. Isso resultaria em uma interrupção da conectividade com o domínio por meio de DNS. Uma nova abordagem era necessária para permitir que as organizações fizerem alterações rápidas no endereço IP mapeado para um domínio.

O DNS dinâmico (DDNS) permite que um usuário ou organização registre um endereço IP com um nome de domínio como no DNS. No entanto, quando o endereço IP do mapeamento muda, o novo mapeamento pode ser propagado através do DNS quase instantaneamente. Para que isso ocorra, um usuário obtém um subdomínio de um provedor DDNS. Esse subdomínio é mapeado para o endereço IP do servidor do usuário ou conexão do roteador doméstico para a Internet. O software cliente é executado no roteador ou em um PC host que detecta uma alteração no endereço IP da Internet do usuário. Quando uma alteração é detectada, o provedor DDNS é imediatamente informado da alteração e o mapeamento entre o subdomínio do usuário e o endereço IP da internet é imediatamente atualizado, conforme mostrado na figura. O DDNS não usa uma entrada DNS verdadeira para o endereço IP de um usuário. Em vez disso, atua como intermediário. O domínio do provedor DDNS é registrado com o DNS, mas o subdomínio é mapeado para um endereço IP totalmente diferente. O serviço do fornecedor DDNS fornece esse endereço IP para o servidor DNS de segundo nível do resolvedor. Esse servidor DNS, na organização ou no ISP, fornece o endereço IP DDNS para o resolvedor.

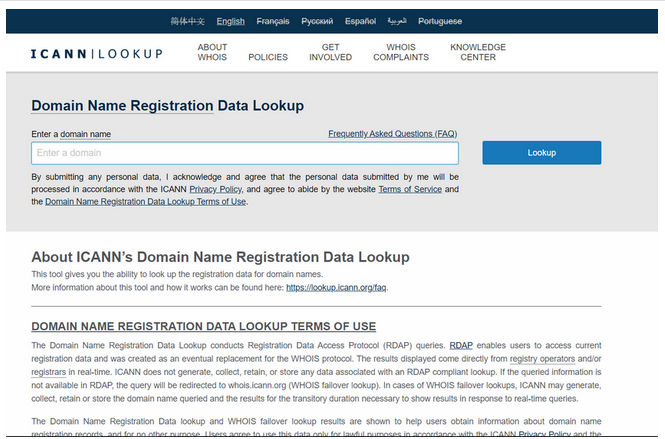
O DNS dinâmico pode ser abusado por atores de ameaças de várias maneiras. Os serviços DDNS gratuitos são especialmente úteis para agentes de ameaça. O DDNS pode ser usado para facilitar a rápida mudança de endereço IP para servidores de comando e controle de malware após o endereço IP atual ter sido amplamente bloqueado. Desta forma, o malware pode ser codificado com uma URL em vez de um endereço IP estático. O DDNS também pode ser usado como uma forma de extrair dados de dentro de uma rede porque o tráfego DNS é muito comum e é frequentemente considerado benigno. O DDNS em si não é maligno, no entanto, monitorar o tráfego DNS que está indo para serviços DDNS conhecidos, especialmente os gratuitos, é muito útil para a detecção de exploits.



10.2.6

**O Protocolo WHOIS**

WHOIS é um protocolo baseado em TCP que é usado para identificar os proprietários de domínios da Internet através do sistema DNS. Quando um domínio da Internet é registrado e mapeado para um endereço IP para o sistema DNS, o registrante deve fornecer informações sobre quem está registrando o domínio. O aplicativo WHOIS usa uma consulta, na forma de um FQDN. A consulta é emitida através de um serviço ou aplicativo WHOIS. O registro oficial de registro de propriedade é devolvido ao usuário pelo serviço WHOIS. Isso pode ser útil para identificar os destinos que foram acessados por hosts em uma rede. O WHOIS tem limitações, e os hackers têm maneiras de esconder suas identidades. No entanto, o WHOIS é um ponto de partida para identificar locais potencialmente perigosos da Internet que podem ter sido alcançados através da rede. Um serviço WHOIS baseado na Internet é chamado de Pesquisa ICANN pode ser usado para obter o registro de registro uma URL. Outros serviços WHOIS são mantidos por registros regionais de internet, como RIPE e APNIC.



# NAT

10.3.1

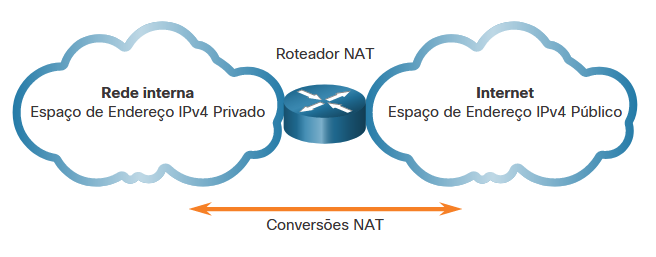
## Espaço de endereço particular IPv4

Não há endereços IPv4 públicos o suficiente para designar um endereço exclusivo para cada dispositivo conectado à Internet. As redes são implementadas geralmente usando endereços IPv4 privados, conforme definido na RFC 1918. O intervalo de endereços incluído no RFC 1918 está incluído na tabela a seguir. É muito provável que o computador que você usa para este curso esteja atribuído a um endereço privado.

| **Classe** | **Intervalo de Endereço Interno RFC 1918** | **Prefixo** |
| --- | --- | --- |
| A | 10.0.0.0 - 10.255.255.255 | 10.0.0.0/8 |
| B | 172.16.0.0 - 172.31.255.255 | 172.16.0.0/12 |
| C | 192.168.0.0 - 192.168.255.255 | 192.168.0.0/16 |

Esses endereços privados são usados em uma organização ou local para permitir que os dispositivos se comuniquem localmente. Entretanto, como esses endereços não identificam nenhuma empresa ou organização, os endereços IPv4 privados não podem ser roteados pela Internet. Para permitir que um dispositivo com IPv4 privado acesse dispositivos e recursos de fora da rede local, o endereço privado deve primeiro ser convertido a um endereço público.

Como mostrado na Figura, o NAT fornece a conversão de endereços particulares para endereços públicos. Isso permite a um dispositivo com endereço IPv4 privado acessar recursos fora de sua rede privada, como aqueles encontrados na Internet. O NAT combinado com o endereço IPv4 privado tem sido o método principal para preservar endereços IPv4 públicos. Um único IPv4 público pode ser compartilhado por centenas, mesmo milhares de dispositivos, cada um configurado com um IPv4 privado original.



Sem o NAT, o esgotamento do espaço de endereços IPv4 ocorreria bem antes do ano 2000. No entanto, o NAT tem limitações e desvantagens, que serão exploradas mais adiante neste módulo. A solução para a redução do espaço de endereços IPv4 e limitações do NAT é a eventual transição para IPv6.

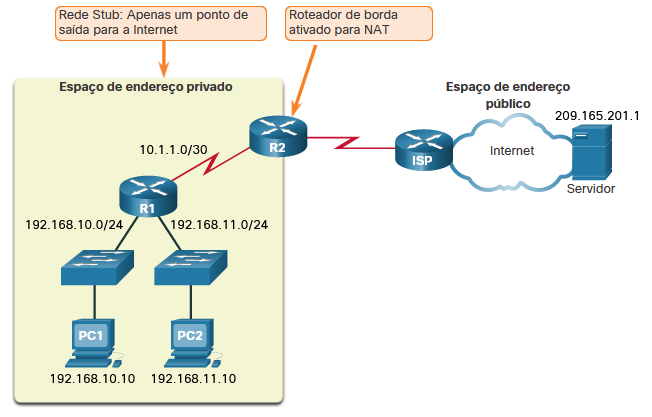
10.3.2

**O que é o NAT?**

O NAT tem várias utilidades, mas seu principal uso é conservar endereços IPv4 públicos. Ele faz isso permitindo que as redes usem endereços IPv4 privados internamente e fornecendo conversão para um endereço público somente quando necessário. O NAT tem um benefício percebido de adicionar um certo grau de privacidade e segurança a uma rede, porque oculta endereços IPv4 internos de redes externas.

Os roteadores ativados para NAT podem ser configurados com um ou mais endereços IPv4 públicos válidos. Esses endereços públicos são conhecidos como o pool de NATs. Quando um dispositivo interno enviar o tráfego para fora da rede, o roteador ativado para NAT converterá o IPv4 interno do dispositivo a um endereço público do pool de NATs. Para dispositivos externos, todo o tráfego que entra e sai da rede parece ter um endereço IPv4 público do pool de endereços fornecido.

Um dispositivo ativado para NAT geralmente opera na fronteira de uma rede stub. Uma rede stub é uma ou mais redes com uma única conexão com a rede vizinha, uma entrada e uma saída da rede. No exemplo da figura, o R2 é um roteador de borda. Como visto do ISP, o R2 forma uma rede stub.



Quando um dispositivo dentro da rede stub quer se comunicar com um dispositivo fora de sua rede, o pacote é encaminhado para o roteador de borda. O roteador de borda realiza o processo de NAT, convertendo o endereço privado interno do dispositivo a um endereço público, externo e roteável.

**Observação:** A conexão com o ISP pode usar um endereço privado ou um endereço público que é compartilhado entre os clientes. Neste módulo, um endereço público é exibido.

10.3.4

**Tradução de Endereço de Porta**

A conversão do PAT, também conhecida como sobrecarga de NAT, mapeia os endereços IPv4 privados para um único endereço IPv4 público ou para alguns endereços. É isso que a maioria dos roteadores domésticos faz. O ISP atribui um endereço ao roteador e, ainda assim, vários membros da família podem acessar, simultaneamente, a Internet. Esta é a forma mais comum de NAT para a casa e para a empresa.

Com o PAT, vários endereços podem ser mapeados para um ou para alguns endereços, pois cada endereço privado é também seguido por um número de porta. Quando um dispositivo inicia uma sessão TCP/IP, ele gera um valor de porta de origem TCP ou UDP ou um ID de consulta especialmente atribuído para ICMP, para identificar, de forma exclusiva, a sessão. Quando o roteador de NAT recebe um pacote do cliente, usa seu número de porta origem para identificar excepcionalmente a conversão do NAT específico.

O PAT garante que os dispositivos utilizem um número de porta diferente do TCP para cada sessão com um Servidor na Internet. Quando uma resposta volta do Servidor, o número de porta origem, que se torna o número de porta destino na viagem de ida e volta, determina a que dispositivos o roteador encaminha os pacotes. O processo de PAT também valida que os pacotes de entrada tenham sido solicitados, adicionando portanto um nível de segurança à sessão.

Clique em Reproduzir na figura para visualizar uma animação do processo PAT. O PAT usa números de portas origem exclusivos no endereço IP global interno para distinguir entre conversões.

Como o R2 processa cada pacote, ele usa um número de porta (1331 e 1555, neste exemplo) para identificar o dispositivo que originou o pacote. O endereço origem (SA) é o endereço local interno com número de porta TCP/UDP designado adicionado. O endereço de destino (DA) é o endereço global externo com o número da porta de serviço adicionado. Neste exemplo, a porta de serviço é 80, que é HTTP.

Para o endereço origem, o R2 converte o endereço local interno a um endereço global interno com o número de porta adicionado. O endereço de destino não é alterado, mas agora é referido como o endereço IPv4 global externo. Quando o Servidor web responde, o caminho é invertido.

# Serviços de transferência e compartilhamento de arquivos

10.4.1

## FTP e TFTP

**File Transfer Protocol (FTP)**

O protocolo FTP é outro protocolo da camada de aplicação comumente utilizado. O FTP foi desenvolvido para possibilitar transferências de arquivos entre um cliente e um servidor. Um cliente FTP é uma aplicação executada em um computador que é usado para enviar e receber arquivos de um servidor FTP.

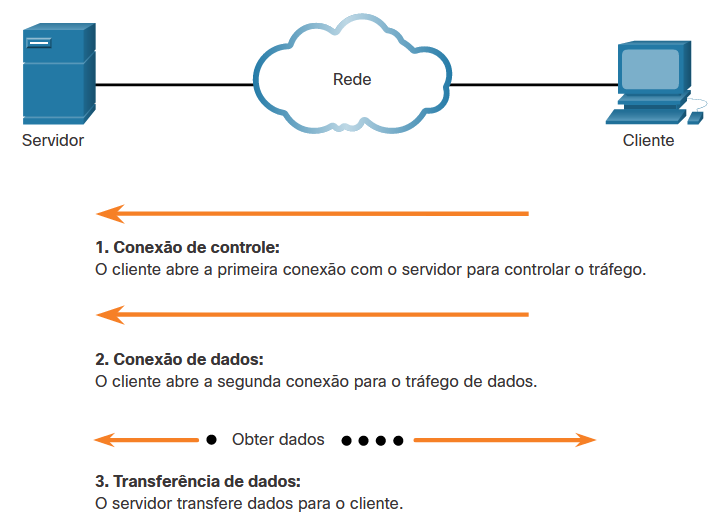
Como a figura ilustra, para transferir dados com sucesso, o FTP precisa de duas conexões entre o cliente e servidor, uma para comandos e respostas, outra para a transferência real de arquivos:

1. O cliente estabelece a primeira conexão com o servidor para controlar o tráfego usando a porta TCP 21, que consiste em comandos do cliente e respostas do servidor.

2. O cliente estabelece a segunda conexão com o servidor para transferência de dados propriamente dita, usando a porta TCP 20. Essa conexão é criada toda vez que houver dados a serem transferidos.

A transferência de dados pode acontecer em ambas as direções. O cliente pode baixar dados do servidor ou o cliente pode fazer upload (enviar) de dados para o servidor.

O FTP não foi projetado para ser um protocolo de camada de aplicativo seguro. Por esse motivo, o SSH File Transfer Protocol, que é uma forma segura de FTP que usa o protocolo Secure Shell para fornecer um canal seguro, é a implementação preferencial de transferência de arquivos.



Com base nos comandos enviados pela conexão de controle, os dados podem ser baixados do servidor ou carregados do cliente.

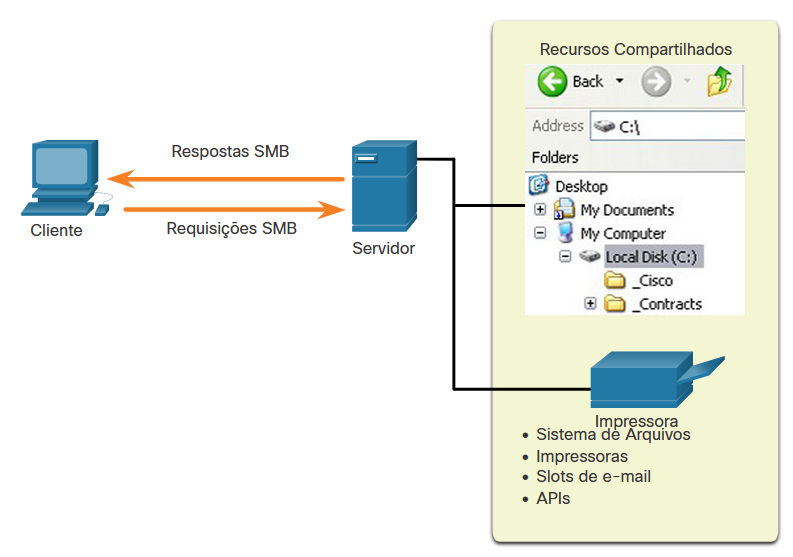
**Protocolo de Transferência Trivial de Arquivo (TFTP)**

TFTP é um protocolo de transferência de arquivos simplificado que usa o conhecido número de porta UDP 69. Ele não tem muitos dos recursos do FTP, como as operações de gerenciamento de arquivos de listagem, exclusão ou renomeação de arquivos. Devido à sua simplicidade, o TFTP tem uma sobrecarga de rede muito baixa e é popular para aplicativos de transferência de arquivos não críticos. No entanto, é fundamentalmente inseguro, porque não tem recursos de login ou controle de acesso. Por esta razão, o TFTP precisa ser implementado com cuidado, e somente quando absolutamente necessário.

10.4.2

**SMB**

O Server Message Block (SMB) é um protocolo de compartilhamento de arquivo cliente / servidor que descreve a estrutura de recursos de rede compartilhados, como diretórios, arquivos, impressoras e portas seriais, conforme mostrado na figura. É um protocolo de requisição/resposta. Todas as mensagens SMB têm um formato em comum. Esse formato utiliza um cabeçalho com tamanho fixo seguido por um parâmetro de tamanho variável e componente de dados.

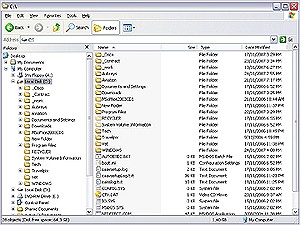


SMB é um cliente / servidor, protocolo de solicitação-resposta. Os servidores podem disponibilizar seus próprios recursos para os clientes na rede.

As mensagens SMB podem iniciar, autenticar e encerrar sessões, controlar o acesso a arquivos e impressoras e permitir que um aplicativo envie ou receba mensagens de ou para outro dispositivo.

O compartilhamento de arquivos SMB e os serviços de impressão se tornaram o sustento da rede da Microsoft, conforme mostrado abaixo.

A segunda figura mostra um arquivo de cópia que ocorre entre dois computadores Windows formam um sistema de arquivos para o outro através da rede.



Captura de dadosCopiar arquivo

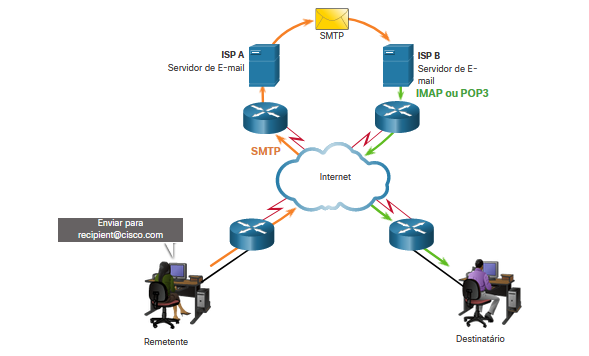
Um arquivo pode ser copiado de um computador para outro com o Windows Explorer usando o protocolo SMB.

# E-mail

10.5.1

## Protocolos de E-mail

Um dos serviços básicos oferecidos por um ISP é a hospedagem de e-mails. Para ser executado em um computador ou outro dispositivo final, o e-mail precisa de várias aplicações e serviços, como mostra a figura. O e-mail é um método de armazenar, de enviar e de recuperar mensagens eletrônicas em uma rede. Mensagens de e-mail são armazenadas nos bancos de dados em servidores de e-mail.



Os clientes de e-mail se comunicam com os servidores de e-mail para enviar e receber e-mails. Os servidores de e-mail se comunicam com outros servidores de e-mail para transportar mensagens de um domínio para outro. Um cliente de e-mail não se comunica diretamente com outro para enviar e-mails. Em vez de isso, os clientes confiam nos servidores para transportar mensagens.

O e-mail suporta três protocolos separados para a operação: SMTP, POP e IMAP. O processo da camada de aplicação que envia e-mail usa o SMTP. Um cliente recupera e-mails usando um dos dois protocolos da camada de aplicação: POP ou IMAP.

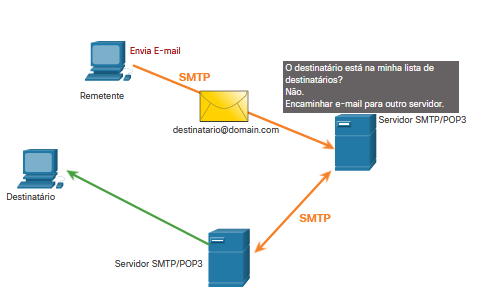
10.5.2

**SMTP**

Os formatos de mensagens SMTP exigem um cabeçalho de mensagem e um corpo de mensagem. Enquanto o corpo da mensagem pode conter qualquer valor de texto, o cabeçalho da mensagem deve ter um endereço de e-mail de destinatário devidamente formatado e um endereço de remetente.

Quando um cliente envia e-mail, o processo de SMTP do cliente se conecta com um processo SMTP do servidor na porta muito conhecida 25. Depois que a conexão é feita, o cliente tenta enviar o e-mail para o servidor através da conexão. Quando o servidor recebe a mensagem, ele a coloca em uma conta local, se o destinatário for local, ou encaminha para outro servidor de e-mail para entrega, como mostra a figura.

O servidor de e-mail destino pode não estar on-line ou pode estar ocupado quando mensagens de e-mail forem enviadas. Portanto, o SMTP armazena mensagens a serem enviadas mais tarde. Periodicamente, o servidor verifica se há mensagens na fila e tenta enviá-las novamente. Se a mensagem ainda não for entregue após um período pré-determinado de expiração, ela é devolvida ao remetente como não entregue.



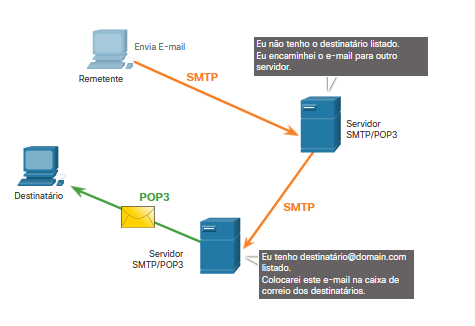
10.5.3

**POP3**

O POP3 é usado por um aplicativo para recuperar e-mails de um servidor de e-mail. Com o POP3, o e-mail é baixado do servidor para o cliente e, em seguida, excluído do servidor, conforme mostrado na figura.

O servidor inicia o serviço POP3 ouvindo passivamente na porta TCP 110 as solicitações de conexão do cliente. Quando um cliente deseja utilizar o serviço, ele envia uma requisição para estabelecer uma conexão TCP com o servidor. Quando a conexão é estabelecida, o servidor POP3 envia uma saudação. O cliente e o servidor POP3 trocam comandos e respostas até que a conexão seja fechada ou abortada.

Com o POP3, as mensagens de e-mail são baixadas para o cliente e removidas do servidor, portanto, não há um local centralizado onde as mensagens de e-mail são mantidas. Como o POP3 não armazena mensagens, ele é indesejável para uma pequena empresa que precisa de uma solução de backup centralizada.

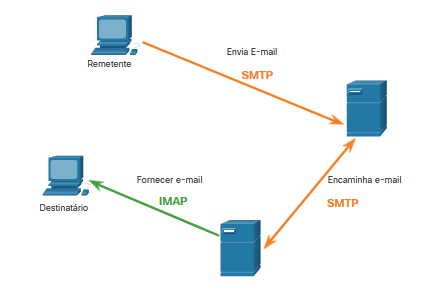


10.5.4

**IMAP**

IMAP é outro protocolo que descreve um método para recuperar mensagens de e-mail, conforme mostrado na figura. Ao contrário do POP3, quando o usuário se conecta a um servidor compatível com IMAP, as cópias das mensagens são baixadas para o aplicativo cliente. As mensagens originais são mantidas no servidor até que sejam excluídas manualmente. Os usuários exibem cópias das mensagens em seu software cliente de e-mail.

Os usuários podem criar uma hierarquia de arquivos no servidor para organizar e armazenar o e-mail. A estrutura de arquivos é duplicada no cliente de e-mail também. Quando um usuário decide excluir uma mensagem, o servidor sincroniza essa ação e exclui a mensagem do servidor.



# HTTP

10.6.1

## Protocolo HTTP e HTML

Existem protocolos específicos da camada de aplicativo que são projetados para usos comuns, como navegação na Web e e-mail. O primeiro tópico lhe deu uma visão geral desses protocolos. Este tópico entra em mais detalhes.

Quando um endereço da Web ou URL (URL) é digitado em um navegador da Web, ele estabelece uma conexão com o serviço da Web. O serviço Web está em execução no servidor que está a utilizar o protocolo HTTP. URLs e URIs (Uniform Resource Identifiers) são os nomes que a maioria das pessoas associa aos endereços da Web.

Para entender melhor como o navegador e o servidor da web interagem, examine como uma página da web é aberta em um navegador. Neste exemplo, use a URL <http://www.cisco.com/index.html>.

**Etapa 1**

O navegador interpreta como três partes da URL:

* http (o protocolo ou esquema)
* [www.cisco.com](http://www.cisco.com) (o nome do servidor)
* index.html (o nome do arquivo específico solicitado)

**Etapa 2**

O navegador então verifica com um servidor de nomes para converter [www.cisco.com](http://www.cisco.com) em um endereço IP numérico, usado para conectar-se ao servidor. O cliente inicia uma solicitação HTTP para um servidor enviando uma solicitação GET para o servidor e solicita o arquivo index.html.

**Etapa 3**

Em resposta à solicitação, o servidor envia o código HTML para esta página da Web para o navegador.

**Etapa 4**

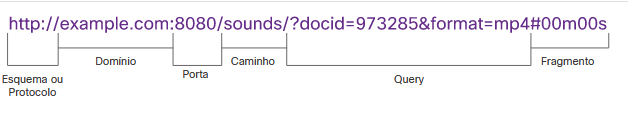
O navegador decifra o código HTML e formata a página da janela do navegador.

10.6.2

**O URL HTTP**

URLs HTTP também podem especificar a porta no servidor que deve manipular os métodos HTTP. Além disso, ele pode especificar uma seqüência de caracteres de consulta e fragmento. A cadeia de consulta normalmente contém informações que não são tratadas pelo processo do servidor HTTP propriamente dito, mas são tratadas por outro processo que está em execução no servidor. As cadeias de caracteres de consulta são precedidas por um “?” caractere e normalmente consistem em uma série de pares de nome e valor. Um fragmento é precedido por um caractere “#”. Refere-se a uma parte subordinada do recurso que é solicitado na URL. Por exemplo, um fragmento pode se referir a uma âncora nomeada em um documento HTML. O URL acessará o documento e, em seguida, moverá para a parte do documento especificada pelo fragmento se existir um link de âncora nomeado correspondente no documento. Uma URL HTTP que inclui essas partes é mostrada na figura.

A figura mostra um u r l h t t p://exemplo dot com dois pontos 80 barra para frente soa barra? doc I d é igual a 9 7 3 2 8 5 formato e comercial igual a m p 4 libra sinal 0 m 0 0 s. O h t p dois-pontos barra para frente é o esquema ou protocolo. Exemplo dot com é o domínio. 80 é o porto. sounds é o caminho. A área da marca de perguntas para logo antes do sinal libra é a consulta e o resto é um fragmento. Este U R L diz para usar H T T P para acessar o servidor em example.com usando a porta 8080. A partir do diretório de sons, retorne o documento com o id de 973285 com formato de mp4 (um arquivo de som mp4) na posição 00 minutos e 00 segundos (o início do arquivo de som).



**Este URL diz para usar HTTP para acessar o servidor em example.com usando a porta 8080. A partir do diretório de sons, retorne o documento com o id de 973285 com formato de mp4 (um arquivo de som mp4) na posição 00 minutos e 00 segundos (o início do arquivo de som).**

## Operação HTTP

A figura mostra um cliente executando uma solicitação HTTP para um servidor HTTP. O arquivo solicitado é um nome de domínio totalmente qualificado. A solicitação usa um Get para recuperar a página da Web. O campo URL é mostrado no computador cliente como uma solicitação <http://www.cisco.com.>



Servidor HTTPClienteURL (Localizador Uniforme de Recursos)Requisição HTTPArquivo solicitadoHost : www.cisco.com  
GET /index.html HTTP/1.1Nome de domínio totalmente qualificado

HTTP é um protocolo de solicitação/resposta que usa a porta TCP 80, embora outras portas possam ser usadas. Quando um cliente, normalmente um navegador da Web, envia uma solicitação para um servidor web, ele usará um dos seis métodos especificados pelo protocolo HTTP.

* **GET** - Uma solicitação de dados do cliente. Um cliente (navegador da web) envia a mensagem GET ao servidor da web para solicitar páginas HTML, conforme mostrado na figura.
* **POST** - Envia dados a serem processados por um recurso.
* **PUT** - Carrega recursos ou conteúdo para o servidor da web, como uma imagem.
* **DELETE** - Exclui o recurso especificado.
* **OPTIONS** - Retorna os métodos HTTP que o servidor suporta.
* **CONNECT** - Solicita que um servidor proxy HTTP encaminha a sessão HTTP TCP para o destino desejado.

Embora o HTTP seja notavelmente flexível, não é um protocolo seguro. As mensagens de solicitação enviam informações ao servidor em texto sem formatação que podem ser interceptadas e lidas. As respostas do servidor, normalmente páginas HTML, também não são criptografadas.

10.6.4

## Códigos de status HTTP

As respostas do servidor HTTP são identificadas com vários códigos de status que informam o aplicativo host do resultado das solicitações do cliente para o servidor. Os códigos são organizados em cinco grupos. Os códigos são numéricos, com o primeiro número no código indicando o tipo de mensagem. Os cinco grupos de códigos de status são:

* **1xx** - Informativo
* **2xx** - Sucesso
* **3xx** - Redirecionamento
* **4xx** - Erro do cliente
* **5xx** - Erro do Servidor

Uma explicação de alguns códigos de status comuns é mostrada na figura. Um excelente recurso para detalhes sobre códigos de status específicos pode ser encontrado pesquisando por “rest api tutorial” e “códigos de status HTTP”. Os códigos de status HTTP são mostrados no tráfego cliente/servidor HTTP e são úteis para investigações de segurança cibernética.

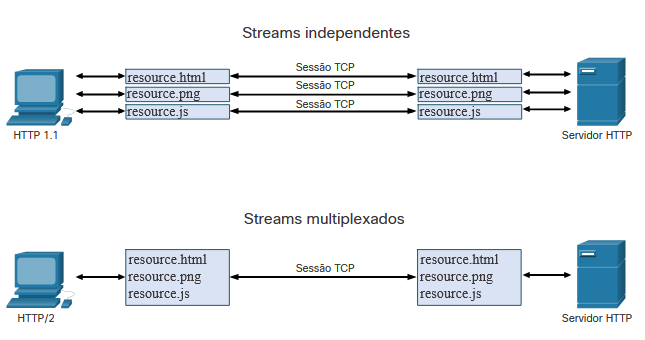
| **Código** | **Status** | **Significado** |
| --- | --- | --- |
| 1xx - Informativo |  |  |
| 100 | Continuar | O cliente deve continuar com a solicitação. O servidor verificou que a solicitação pode ser atendida. |
| 2xx - Sucesso |  |  |
| 200 | OK | A solicitação foi concluída com sucesso. |
| 202 | Aceito | A solicitação foi aceita para processamento, mas o processamento não foi concluído. |
| 4xx — Erro do cliente |  |  |
| 403 | Proibido | A solicitação é entendida pelo servidor, mas o recurso não será atendido. Isso ocorre possivelmente porque o solicitante não está autorizado a exibir o recurso. |
| 404 | Não encontrada | O servidor não conseguiu localizar o recurso solicitado. Isso pode ser causado por um URL desatualizado ou incorreto. |

10.6.5

## HTTP/2

HTTP/2 é uma revisão importante para a especificação do protocolo HTTP. O objetivo do HTTP/2 é melhorar o desempenho HTTP abordando problemas de latência que existiam na versão HTTP 1.1 do protocolo. HTTP/2 usa o mesmo formato de cabeçalho que HTTP 1.1 e usa os mesmos códigos de status. No entanto, há muitos recursos importantes para HTTP/2 que um analista de segurança cibernética deve estar ciente.

A figura mostra a diferença entre fluxos independentes e fluxos multiplexados na transferência de informações usando HTTP.



* **Multiplexação** — servidores HTTP e clientes realizam conversas chamadas de fluxos para cada transação. Por exemplo, um cliente se conectará a um servidor HTTP, solicitará recursos desse servidor e receberá os recursos solicitados. Com HTTP 1.1, apenas um fluxo era suportado por vez. Com HTTP/2, um cliente e um servidor podem ter vários fluxos em execução entre eles ao mesmo tempo na mesma conexão TCP, como mostrado na figura. Isso fornece eficiência muito aprimorada para o protocolo.
* **Servidor PUSH** - Servidores HTTP são capazes de enviar conteúdo que ainda não foi solicitado ao cliente. O servidor antecipa o conteúdo que é provável que o cliente solicite. O cliente armazena este conteúdo em cache para uso futuro.
* **Um protocolo binário** — Em HTTP 1.1, comandos, como solicitações de cliente para servidor, são feitos em formato de texto. HTTP/2 mudou para o uso de comandos binários. Isso supera alguns problemas complicados com a versão anterior, reduz a sobrecarga de solicitação e resposta e reduz a latência e melhora a taxa de transferência.
* **Compactação de cabeçalho** — Os cabeçalhos de solicitação e resposta HTTP são compactados para reduzir ainda mais a quantidade de largura de banda exigida pelos fluxos HTTP/2.

10.6.6

**Protegendo HTTP — HTTPS**

Para comunicação segura na Internet, é usado o protocolo HTTP Secure (HTTPS). HTTPS usa a porta TCP 443. O HTTPS utiliza autenticação e criptografia para proteger dados durante o trajeto entre o cliente e o servidor. HTTPS usa o mesmo processo de resposta do servidor de solicitação do cliente que o HTTP, mas o fluxo de dados é criptografado com Secure Socket Layer (SSL) ou Transport Layer Security (TLS), antes de ser transportado pela rede. Embora SSL seja o antecessor do TLS, ambos os protocolos são frequentemente referidos como SSL.

HTTPS/2 é especificado para usar HTTPS sobre TLS com a extensão Application-Layer Protocol Negociation (ALPN) para TLS 1.2 ou mais recente. O padrão HTTP/2 não especifica criptografia, no entanto, todos os principais aplicativos de software cliente exigem isso. Portanto, pode-se supor que HTTP/2 é, de fato, criptografado.

Uma grande quantidade de informações confidenciais, como senhas, informações de cartão de crédito e informações médicas, são transmitidas pela Internet usando HTTPS.

# Resumo dos serviços de rede

10.7.1

## O que aprendi neste módulo?

**DHCP**

O protocolo DHCP (Dynamic Host Configuration Protocol) para IPv4 automatiza a atribuição de endereços IPv4. Isso é conhecido como endereçamento dinâmico e é a alternativa ao endereçamento estático. Em redes maiores, ou onde a população de usuários muda com frequência, o endereçamento dinâmico costuma ser o método preferido para atribuições de endereços. Muitas redes usam ambos os métodos. DHCP é usado para hosts de uso geral, como dispositivos finais de usuário. O endereçamento estático é usado para dispositivos de rede, como roteadores de gateway, comutadores, servidores e impressoras.

Quando um dispositivo IPv4 configurado com DHCP é inicializado ou se conecta à rede, o cliente transmite uma mensagem de descoberta de DHCP (DHCPDISCOVER) para identificar quaisquer servidores DCHP que estejam disponíveis na rede. Um servidor DHCP responde com uma mensagem de oferta DCHP (DHCPOFFER), que oferece uma concessão ao cliente. A mensagem de oferta contém o endereço IPv4 e a máscara de sub-rede a serem atribuídos, o endereço IPv4 do servidor DNS e o endereço IPv4 do gateway padrão. O cliente pode receber várias mensagens de DHCPOFFER se houver mais de um servidor DHCP na rede local. Deve-se escolher entre eles e enviar uma mensagem DCHPREQUEST que identifica o servidor explícito e a oferta de aluguel que o cliente está aceitando. Se o endereço IPv4 ainda estiver disponível, o servidor retornará uma mensagem DHCPACK. Se a oferta não for mais válida, ela retornará uma mensagem DCHPNACK. O formato de mensagem DHCPv4 é usado para todas as transações de DHCPv4. As mensagens DHCPv4 são encapsuladas no protocolo de transporte UDP.

**Visão geral do DNS**

O Sistema de Nomes de Domínio (DNS) foi desenvolvido para fornecer um meio confiável de gerenciar e fornecer nomes de domínio e seus endereços IP associados. O sistema DNS consiste em uma hierarquia global de servidores distribuídos que contêm bancos de dados de nomes para mapeamentos de endereços IP. Os analistas de segurança cibernética devem ter um conhecimento completo do DNS porque uma análise recente das ameaças à segurança da rede descobriu que mais de 90% do software malicioso usado para atacar as redes usa o sistema DNS para realizar campanhas de ataque.

A seguir estão as etapas envolvidas na resolução de DNS:

* O usuário digita um FQDN em um campo de endereço do navegador.
* Uma consulta DNS é enviada ao servidor DNS designado.
* O servidor DNS corresponde ao FQDN com seu endereço IP.
* A resposta da consulta DNS é enviada de volta ao cliente com o endereço IP do FDQN.
* O computador cliente usa o endereço IP para enviar solicitações ao servidor.

O DNS usa a porta UDP 53 para consultas e respostas DNS. O servidor DNS armazena diferentes tipos de RRs usados para resolver nomes. Esses registros contêm o nome, endereço e tipo de registro. O DNS usa o mesmo formato de mensagem entre servidores, consistindo em uma pergunta, resposta, autoridade e informações adicionais para todos os tipos de consultas de clientes e respostas de servidores, mensagens de erro e transferência de informações de registros de recursos. O DNS dinâmico (DDNS) permite que um usuário ou organização registre um endereço IP com um nome de domínio como no DNS. No entanto, quando o endereço IP do mapeamento muda, o novo mapeamento pode ser propagado por todo o DNS quase que instantaneamente. DDNS pode ser abusado por atores de ameaça de várias maneiras e URLs que usam DDNS devem ser suspeitos. WHOIS é um protocolo baseado em TCP usado para identificar proprietários de domínios da Internet por meio do sistema DNS. O WHOIS tem limitações, e os hackers têm maneiras de esconder suas identidades.

**NAT**

O NAT fornece a tradução de endereços privados para endereços públicos. Isso permite que dispositivos com endereços IPv4 privados acessem recursos fora de sua rede privada, como aqueles encontrados na Internet. O NAT ajuda a conservar endereços IPv4 públicos. Os roteadores ativados para NAT podem ser configurados com um ou mais endereços IPv4 públicos válidos. Esses endereços são conhecidos como pool NAT. Um dispositivo ativado para NAT geralmente opera na fronteira de uma rede stub. Quando um dispositivo dentro da rede stub quer se comunicar com um dispositivo fora de sua rede, o pacote é encaminhado para o roteador de borda. O roteador de borda executa o processo NAT, traduzindo o endereço privado interno do dispositivo para o endereço público externo roteável. A conversão do PAT, também conhecida como sobrecarga de NAT, mapeia os endereços IPv4 privados para um único endereço IPv4 público ou para alguns endereços.

**Serviços de transferência e compartilhamento de arquivos**

O protocolo de transferência de arquivos (FTP) é outro protocolo de camada de aplicativo comumente usado. Ele foi desenvolvido para permitir a transferência de arquivos entre um cliente e um servidor. Para transferir arquivos com êxito, o FTP requer duas conexões entre o cliente e o servidor: uma para comandos e respostas e outra para a transferência de arquivos propriamente dita. SSH File Transfer Protocol é uma forma segura de FTP que usa Secure Shell para fornecer um canal seguro. O Trivial File Transfer Protocol (TFTP) é um protocolo simplificado de transferência de arquivos que usa a porta UDP número 69. O TFTP é fundamentalmente inseguro. O Server Message Block (SMB) é um protocolo de compartilhamento de arquivos cliente / servidor que descreve a estrutura de recursos de rede compartilhados, como diretórios, arquivos, impressoras e portas seriais. O compartilhamento de arquivos SMB e os serviços de impressão se tornaram a base da rede da Microsoft.

**E-mail**

Os clientes de e-mail se comunicam com os servidores de e-mail para enviar e receber e-mails. Os servidores de correio se comunicam com outros servidores de correio para transportar mensagens de um domínio para outro. O e-mail suporta três protocolos separados para operação: SMTP, POP e IMAP. O processo da camada de aplicativo que envia mensagens de um cliente para um servidor de e-mail usa SMTP. Um cliente recupera e-mails de um servidor de email usando POP3 ou IMAP.

**HTTP**

Navegadores e servidores web interagem usando as seguintes etapas:

1. O navegador interpreta as três partes do URL.
2. O navegador verifica com um servidor de nomes para converter um endereço em um endereço IP numérico. O cliente inicia uma solicitação HTTP para um servidor enviando uma solicitação GET para o servidor.
3. Em resposta à solicitação, o servidor envia o html dessa página da web para o navegador.
4. O navegador decifra o HTML e renderiza a página para a janela do navegador.

HTTP URLs também pode especificar a porta no servidor que deve lidar com os métodos HTTP. Além disso, ele pode especificar uma seqüência de caracteres de consulta e fragmento. HTTP é um protocolo de solicitação/resposta que usa a porta TCP 80, embora outras portas possam ser usadas. Quando um cliente envia uma solicitação para um servidor web, ele usará um dos seis métodos especificados pelo protocolo HTTP: GET, POST, PUT, DELETE, OPTIONS e CONNECT. HTTP é flexível, mas não seguro. As respostas do servidor HTTP são identificadas com códigos de status organizados em cinco grupos de códigos: 1xx, 2xx, 3xx, 4xx e 5xx. HTTP/2 é uma grande revisão para a especificação do protocolo HTTP que é projetado para melhorar o desempenho HTTP, abordando problemas de latência. Para uma comunicação segura pela Internet, é usado HTTP Secure (HTTPS). HTTPS usa autenticação e criptografia para proteger os dados enquanto eles trafegam entre o cliente e o servidor.

Qual mensagem um host IPv4 usa para responder quando recebe uma mensagem DHCPOFFER de um servidor DHCP?

DHCPREQUEST

Tópico 10.1.0 - Quando o cliente recebe o DHCPOFFER do servidor, ele envia de volta uma mensagem de broadcast DHCPREQUEST. Ao receber a mensagem DHCPREQUEST, o servidor responde com uma mensagem DHCPACK unicast.

Em uma rede doméstica, qual dispositivo mais provavelmente fornecerá o endereçamento IP dinâmico aos clientes na rede doméstica?

Um roteador doméstico

Tópico 10.1.0 - Em uma rede doméstica, um roteador doméstico geralmente serve como servidor DHCP. O roteador doméstico é responsável por atribuir endereços IP dinamicamente a clientes na rede doméstica. Os ISPs também usam o DHCP, mas normalmente atribuem um endereço IP à interface de Internet do roteador doméstico, e não aos clientes na rede doméstica. As empresas costumam ter um servidor de arquivos ou outro servidor dedicado para fornecer serviços DHCP à rede. Por fim, um servidor DNS é responsável por encontrar o endereço IP de uma URL, e não por fornecer endereçamento dinâmico aos clientes da rede.

Qual protocolo automatiza a atribuição de endereços IP em uma rede e qual número de porta ele usa? (Escolha duas.)

67 , DHCP

Tópico 10.1.0 - O DNS usa a porta 53 e traduz URLs em endereços IP. O SMB fornece acesso compartilhado a arquivos e impressoras e usa a porta 445. A porta 80 é usada por HTTP. HTTP é um protocolo usado para se comunicar entre um navegador web e um servidor.

Um site específico não parece estar respondendo em um computador com Windows 7. Qual comando o técnico pode usar para mostrar quaisquer entradas DNS armazenadas em cache para esta página da Web?

Ipconfig/ displaydns

Tópico 10.2.0 -

Que tipo de servidor usaria IMAP?

e-mail

Tópico 10.5.0 - SMTP, IMAP e POP são três protocolos de camada de aplicativo para aplicações de e-mail.

Qual é o benefício de usar o DDNS?

O procedor DDNS detecta uma alteração no endereço IP do cliente e atualiza imediatamente a alteração de mapeamento

Tópico 10.2.0 - DNS dinâmico (DDNS) permite que um usuário ou organização registre um endereço IP com um nome de domínio como no DNS. No entanto, quando o endereço IP do mapeamento muda, o novo mapeamento pode ser propagado através do DNS quase instantaneamente.

Qual protocolo de camada de aplicativo descreve os serviços que são usados para compartilhamento de arquivos em redes Microsoft?

SMB

Tópico 10.4.0 - Compartilhamento de arquivos SMB e serviços de impressão são usados para compartilhamento de arquivos na rede Microsoft.

Qual protocolo da camada de aplicação usa mensagens do tipo GET, PUT e POST?

HTTP

Tópico 10.6.0 - O comando GET é uma solicitação do cliente para dados de um servidor web. Um comando PUT carrega recursos e conteúdo, como imagens, para um servidor web. Um comando POST carrega arquivos de dados para um servidor web.

Qual protocolo permite que o e-mail seja baixado de um servidor de e-mail para um cliente e, em seguida, exclui o e-mail do servidor?

POP3

Tópico 10.5.0 -

Com o POP, o e-mail é baixado do servidor para o cliente e, em seguida, excluído do servidor.

SMTP é usado para enviar ou encaminhar e-mail.

Ao contrário do POP, quando um usuário se conecta via IMAP, cópias das mensagens são baixadas para o aplicativo cliente e as mensagens originais são mantidas no servidor até que sejam excluídas manualmente.

HTTP é usado para dados de tráfego da web e é considerado inseguro.

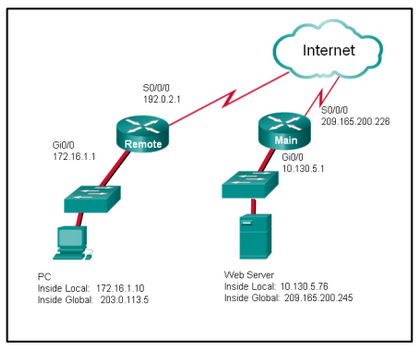
Qual site é considerado seguro porque criptografa a comunicação entre o site e os visitantes?

https://www.ourblogs.info/

Tópico 10.6.0 - Referência do currículo: Module 1.1

Uma URL típica é do protocolo de formato://hostname\_or\_address[:porta]/. O protocolo HTTPS significa Hypertext Transfer Protocol sobre SSL (Secure Socket Layer). Usando este protocolo, os dados transferidos entre o site e o usuário são criptografados. O formato ht& #8203; tps://websiteé usado por servidores web para transferir e exibir conteúdo de forma segura. HTTP e FTP não fornecem criptografia durante as transferências de dados.

From left to right, PC is connected to the router Remote through a switch, Remote is connected to the Internet cloud, the cloud is connected to the router Main, and Main is connected to a web server through a switch. The PC has a label: PC: Inside local: 172.16.1.10 Inside global: 203.0.113.5 Main has two labels: Label 1 - Gi0/0, 172.16.1.1 Label 2 - S0/0/0, 192.0.2.1 Main has two labels: Label 1: S0/0/0, 209.165.200.226 Label 2: Gi0/0, 10.130.5.1 The web server has a label: Web server: Inside local: 10.130.5.76 Inside global: 209.165.200.245



Consulte a figura. O NAT é configurado em Remoto e Principal. O PC está enviando uma solicitação ao Servidor Web. Qual endereço IPv4 é o endereço IP de origem do pacote entre o Principal e o servidor da Web?

203.0.113.5

Tópico 10.3.0 - Como o pacote está entre o principal e o servidor da web, o endereço IP de origem é o endereço global interno do PC, 203.0.113.5.

Qual instrução melhor descreve a operação do protocolo de transferência de arquivos?

Um servidor FTP usa um numero de porta de origem 21 e um numero de porta de destino gerado aleatoriamente durante o estabelecimento do tráfego de controle com um cliente FTP

Tópico 10.4.0 - Ao usar o File Transfer Protocol, um cliente FTP usa um número de porta de origem gerado aleatoriamente, mas visa um número de porta de destino 20 ou 21 no servidor FTP. Os números da porta de destino dependem se é a primeira conexão para o tráfego de controle na porta 21 ou a segunda conexão para o tráfego de dados na porta 20.

Na tradução de NAT para hosts internos, qual endereço seria usado por usuários externos para alcançar hosts internos?

Dentro global

Tópico 10.3.0 - Da perspectiva de um dispositivo NAT, endereços globais internos são usados por usuários externos para alcançar hosts internos. Dentro dos endereços locais são os endereços atribuídos aos hosts internos. Endereços globais externos são os endereços de destinos na rede externa. Endereços locais externos são os endereços privados reais dos hosts de destino atrás de outros dispositivos NAT.

Qual é um exemplo de um domínio de nível superior?

.com

Tópico 10.2.0 - Domínios de nível superior representam um país ou tipo de organização, como .com ou .edu.