



Módulo 10: Serviços de rede



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do módulo

Título do módulo: Serviços de rede

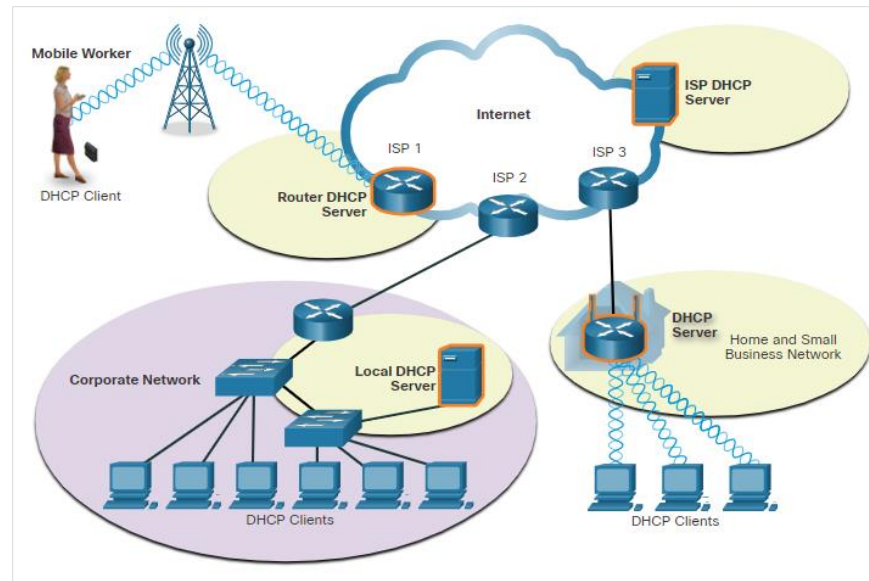
Objetivo do módulo: Explicar como os serviços de rede habilitam a funcionalidade da rede.

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.

10.1 DHCP

Dynamic Host Configuration Protocol

- Dois tipos de endereçamento:
 - **Dinâmico** - o protocolo DHCP (Dynamic Host Configuration Protocol) para serviço IPv4 automatiza a atribuição de endereços IPv4, máscaras de sub-rede, gateways e outros parâmetros de rede IPv4.
 - **Estático** - O administrador da rede insere manualmente as informações do endereço IP nos hosts.
- Quando um host se conecta à rede, o servidor DHCP escolhe um endereço de um intervalo configurado de endereços denominado pool e o atribui ao host.
- O DHCP pode alocar endereços IP por um período de tempo configurável, chamado período de concessão.

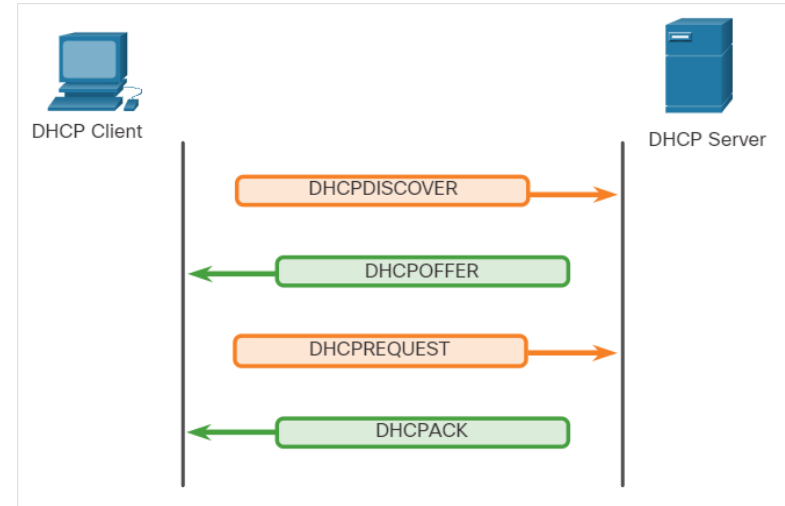


Redes médias a grandes — o servidor DHCP é um servidor local baseado em PC

Rede doméstica - o servidor DHCP está no roteador local conectando a rede doméstica ao ISP.

Operação do DHCP

- A operação DHCP inclui: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK e DHCPNAK.
- Quando o dispositivo configurado com DHCP se conecta à rede, o cliente transmite uma mensagem **DHCPDISCOVER** para identificar quaisquer servidores DHCP disponíveis na rede.
- Um servidor DHCP responde com uma mensagem **DHCPOFFER**, que oferece uma concessão ao cliente.
- O cliente envia uma mensagem **DHCPREQUEST** que identifica o servidor explícito e a oferta de aluguel que o cliente está aceitando.
- Se o endereço IPv4 solicitado pelo cliente, ou oferecido pelo servidor, ainda estiver disponível, o servidor retornará a mensagem **DHCPACK**. Se a oferta não for mais válida, o servidor selecionado responde com uma mensagem **DHCPNAK**. Se uma mensagem **DHCPNAK** for retornada, o processo de seleção começará novamente com uma nova mensagem **DHCPDISCOVER** sendo transmitida.



Formato de Mensagem DHCP

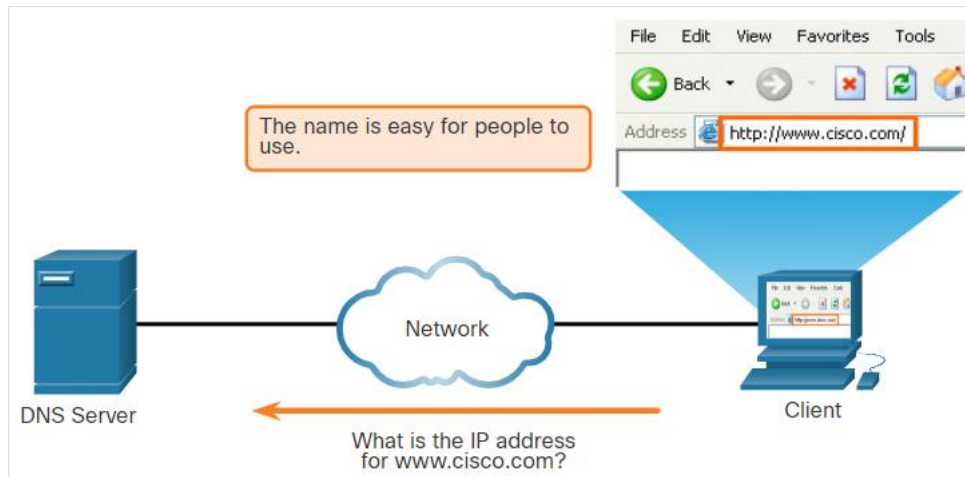
- O formato de mensagem DHCPv4 é usado para todas as transações de DHCPv4.
- As mensagens DHCPv4 são encapsuladas no protocolo de transporte UDP.
- A tabela abaixo lista os campos cobertos na estrutura da mensagem DHCPv4.

Campos na estrutura da mensagem DHCPv4		
Código de operação (OP)	Segundos	Endereço IP do gateway
Tipo de Hardware	Flags	Endereço de Hardware do Cliente .
Comprimento do endereço de hardware	Endereço IP do cliente	Nome do servidor
Saltos	Seu endereço IP	Nome do arquivo de inicialização
Identificador de transação	Endereço IP do servidor	Opções DHCP

10.2 DNS

Visão geral do DNS

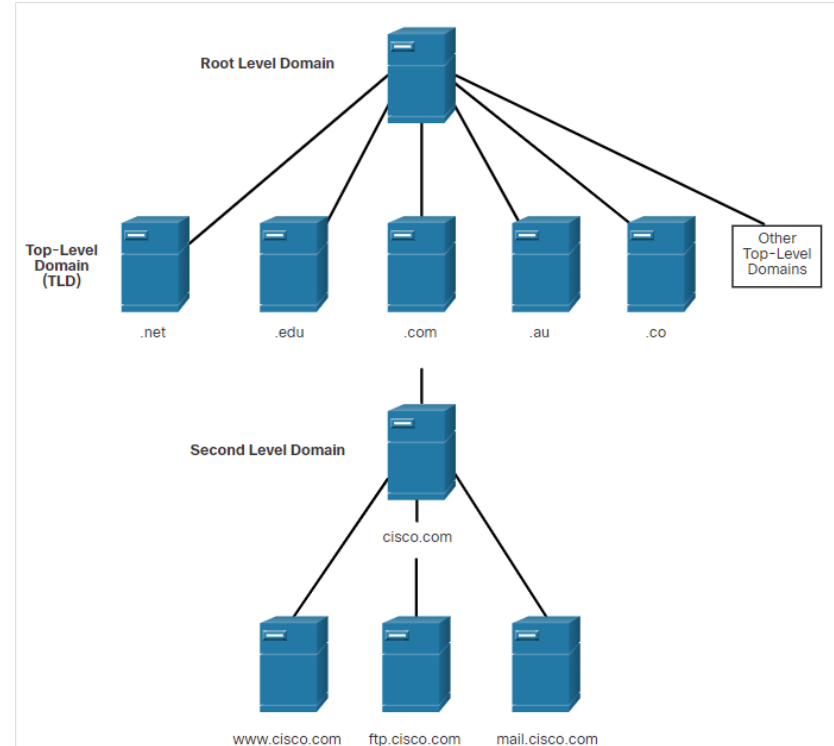
- O Sistema de Nomes de Domínio (DNS) fornece nomes de domínio e seus endereços IP associados.
- O sistema DNS consiste em uma hierarquia global de servidores distribuídos que contêm bancos de dados de nomes para mapeamentos de endereços IP.
- O computador cliente na figura enviará uma solicitação ao servidor DNS para obter o endereço IP de www.cisco.com para que ele possa endereçar pacotes para esse servidor.
- O tráfego DNS mal-intencionado pode ser detectado por meio da análise de protocolo e da inspeção de informações de monitoramento de DNS.



DNS resolve nomes para endereços IP

A Hierarquia de Domínio DNS

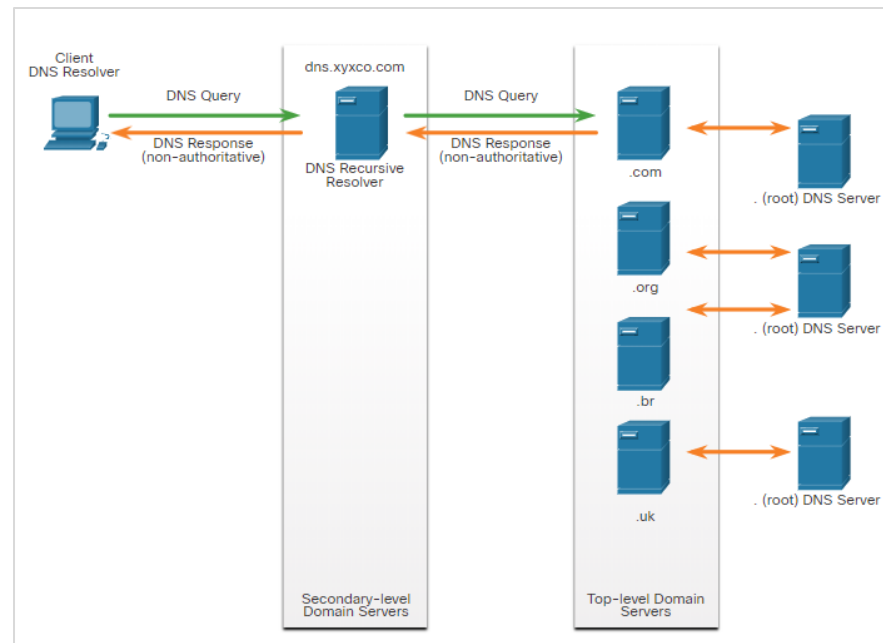
- O DNS consiste em uma hierarquia de domínios genéricos de nível superior e vários domínios de nível de país.
- Os domínios de segundo nível são representados por um nome de domínio seguido por um domínio de nível superior.
- Os subdomínios são encontrados no próximo nível da hierarquia DNS e representam alguma divisão do domínio de segundo nível.
- Domínio de quarto nível pode representar um host em um subdomínio.
- Os domínios de nível superior representam o tipo de organização ou país de origem.
Exemplos: **(.org)** - uma organização sem fins lucrativos, **(.au)** - Austrália.



Hierarquia DNS

O Processo de Pesquisa de DNS

- Para resolver um nome para um endereço IP, o resolvidor, primeiro verificará seu cache DNS local. Se o mapeamento não for encontrado, uma consulta será emitida para o servidor DNS.
- 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**.
- Os servidores DNS de cache podem resolver consultas recursivas sem encaminhar as consultas para servidores de nível superior.



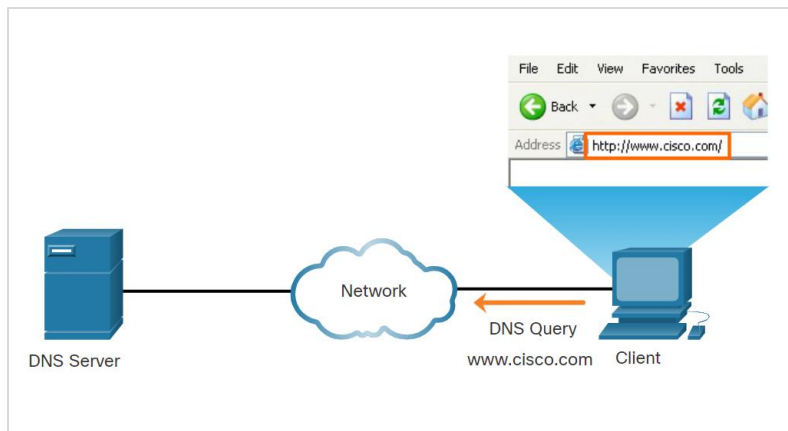
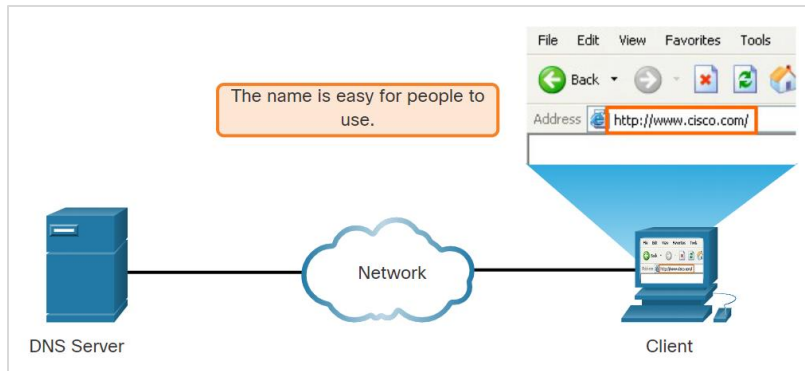
- Se um servidor exigir dados para uma zona, ele solicitará uma transferência desses dados de um servidor autoritário para essa zona. O processo de transferência de dados DNS entre servidores é conhecido como transferência de zona.

O Processo de Pesquisa de DNS (Cont.)

Etapas envolvidas na resolução de DNS:

Etapa 1 - O usuário digita um FQDN no campo Endereço do aplicativo do navegador.

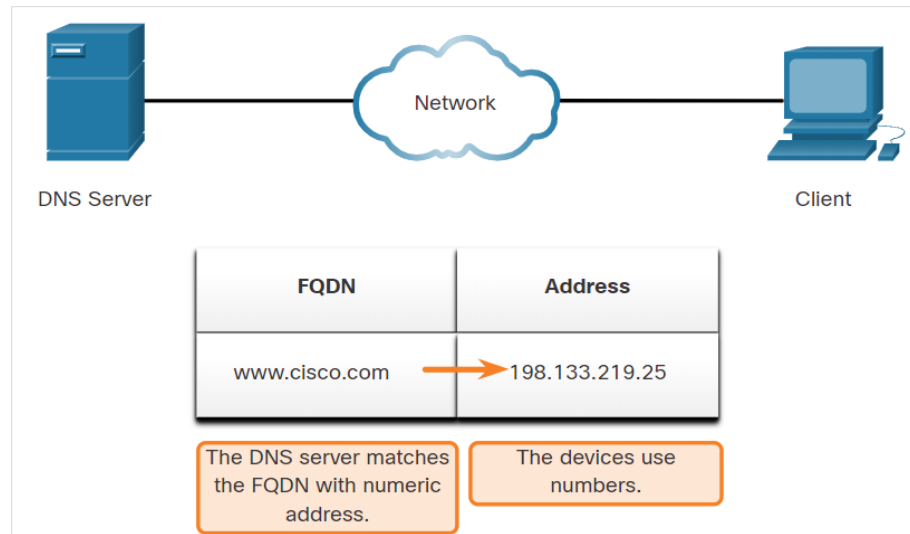
Etapa 2 - Uma consulta DNS é enviada ao servidor DNS designado para o computador cliente.



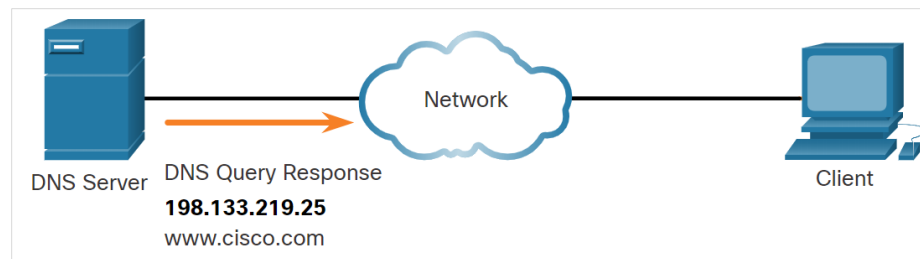
O Processo de Pesquisa de DNS (Cont.)

Etapas envolvidas na resolução de DNS:

Etapa 3 - O servidor DNS combina o FQDN com seu endereço IP.



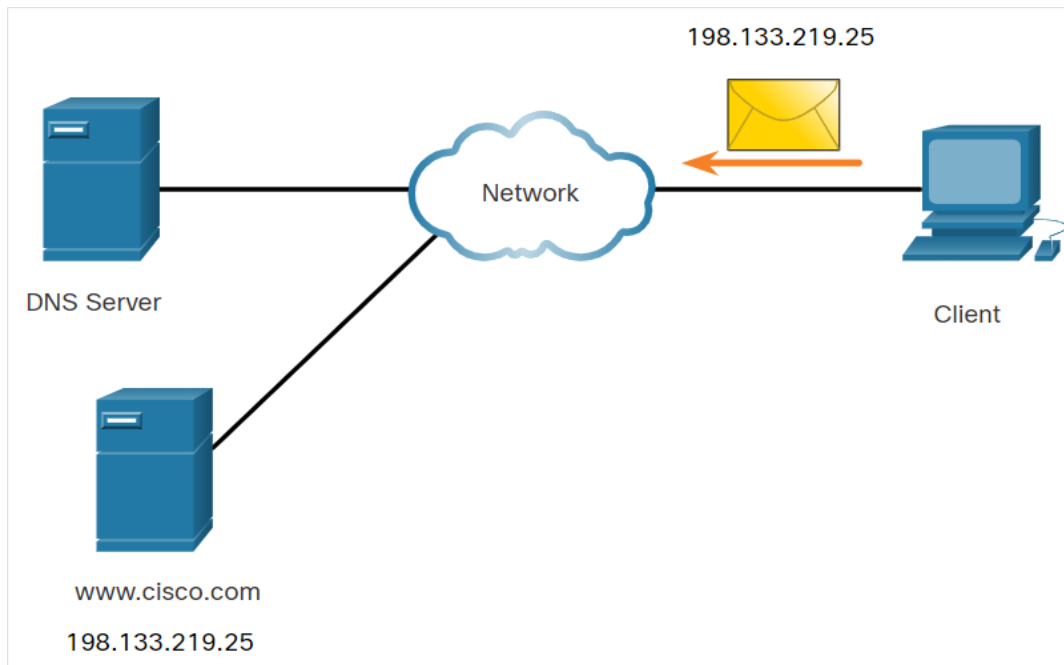
Etapa 4 - A resposta da consulta DNS é enviada de volta ao cliente com o endereço IP do FQDN.



O Processo de Pesquisa de DNS (Cont.)

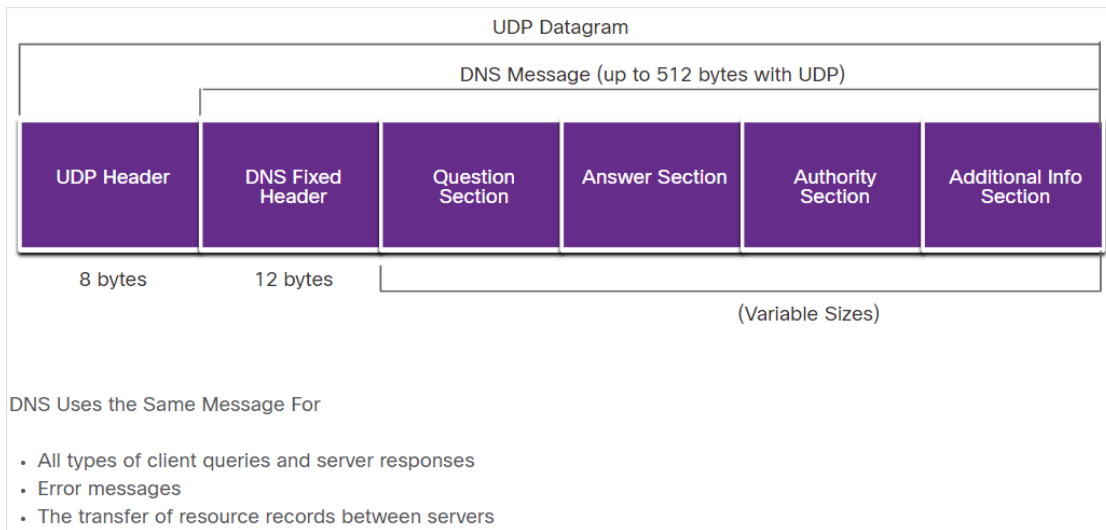
Etapas envolvidas na resolução de DNS:

Etapa 5 - O servidor DNS combina o FQDN com seu endereço IP.



Formato de Mensagem DNS

- O DNS usa a porta UDP 53 para consultas e respostas DNS.
- Se uma resposta DNS exceder 512 bytes, DNS dinâmico (DDNS) é usado.
- As comunicações do protocolo DNS usam um único formato denominado **mensagem**.
- O DNS usa o mesmo formato de mensagem para todos os tipos de consultas do cliente e resposta do servidor, mensagens de erro e transferência de informações de registro de recursos.



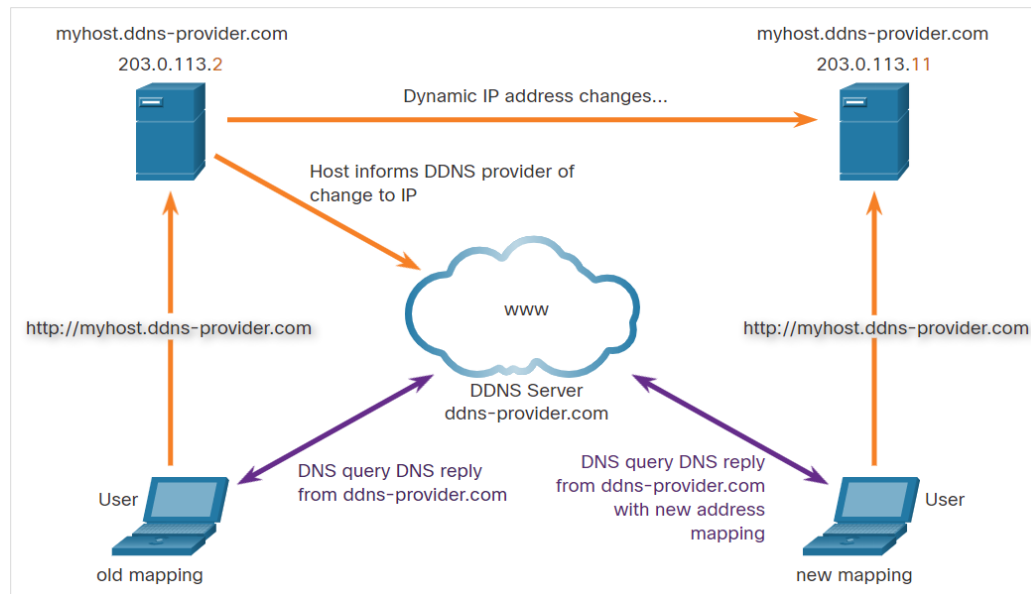
Formato de mensagem DNS (cont.)

Seções do formato de mensagem DNS:

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

DNS dinâmico

- O DNS dinâmico (DDNS) permite que um usuário ou organização registre um endereço IP com um nome de domínio como no DNS.
- O subdomínio é mapeado para o endereço IP do servidor do usuário ou conexão de roteador doméstico para a Internet.
- Quando uma alteração é detectada, o fornecedor DDNS é imediatamente informado da alteração e o mapeamento entre o subdomínio do utilizador e o endereço IP da Internet é imediatamente actualizado.



- O serviço do fornecedor DDNS fornece esse endereço IP para o servidor DNS de segundo nível do resolvidor. Este servidor DNS, na organização ou no ISP, fornece o endereço IP DDNS para o resolvidor.

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.
- O aplicativo WHOIS usa uma consulta, na forma de um FQDN.
- O WHOIS é um ponto de partida para identificar locais potencialmente perigosos da Internet que possam ter sido alcançados através da rede.
- O ICANN Lookup, uma ferramenta WHOIS baseada na Internet, é usado para obter o registro de um URL.

The screenshot shows the ICANN Lookup website. At the top, there is a navigation bar with language options: 简体中文, English, Français, Русский, Español, العربية, and Portuguese. Below this is a header with the ICANN LOOKUP logo and links for ABOUT WHOIS, POLICIES, GET INVOLVED, WHOIS COMPLAINTS, and KNOWLEDGE CENTER. The main section is titled "Domain Name Registration Data Lookup". It features a text input field labeled "Enter a domain name" with a placeholder "Enter a domain". To the right of the input field is a link for "Frequently Asked Questions (FAQ)" and a blue "Lookup" button. Below the input field, there is a disclaimer: "By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the Domain Name Registration Data Lookup Terms of Use." The bottom section is titled "About ICANN's Domain Name Registration Data Lookup" and contains text explaining the tool's purpose and a link to the terms of use. Below that is a section titled "DOMAIN NAME REGISTRATION DATA LOOKUP TERMS OF USE" with detailed text about the tool's functionality and data handling.

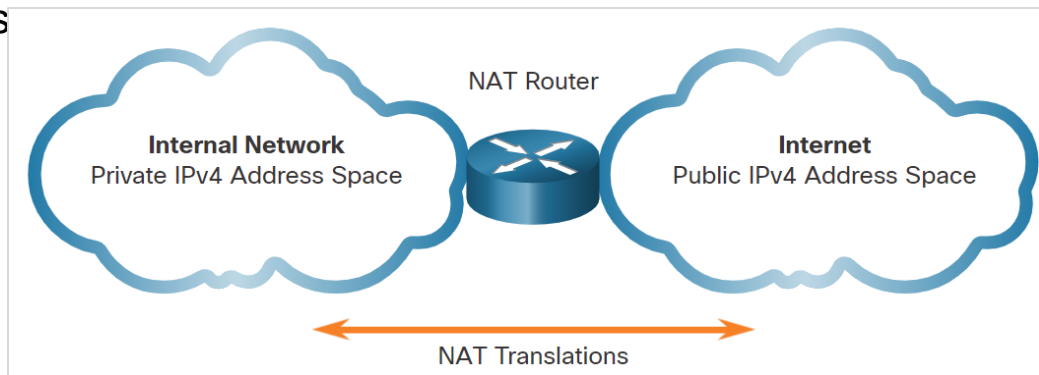
Laboratório - Usando o Wireshark para Examinar uma Captura UDP DNS

- Nesse laboratório, você completará os seguintes objetivos:
 - Comunique-se com um servidor DNS enviando uma consulta DNS usando o protocolo de transporte UDP.
 - Use o Wireshark para examinar a consulta DNS e as trocas de resposta com o mesmo servidor.

10.3 NAT

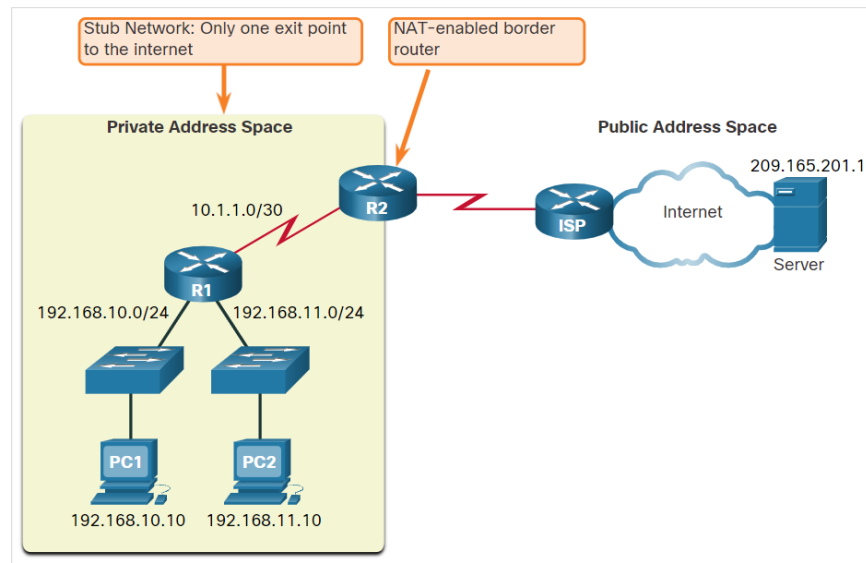
Espaço de endereço particular IPv4

- Para permitir que um dispositivo com endereço IPv4 privado acesse dispositivos e recursos fora da rede local, o endereço privado deve ser traduzido para um endereço público.
- O NAT fornece a tradução de endereços privados para endereços públicos.
- Um único endereço IPv4 público pode ser compartilhado por milhares de dispositivos, cada um configurado com um endereço IPv4 privado exclusivo.
- A solução para a redução do espaço de endereços IPv4 e limitações do NAT é a eventual transição para IPv6.



O que é o NAT?

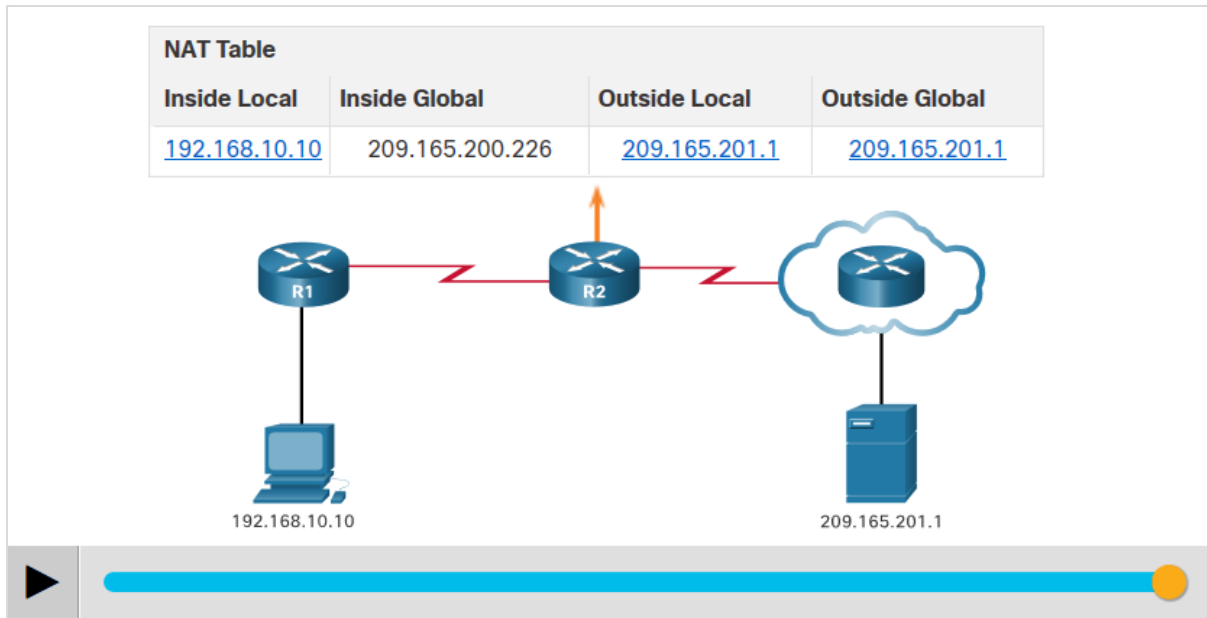
- O NAT é usado para conservar endereços IPv4 públicos.
- Os roteadores habilitados para NAT podem ser configurados com um ou mais endereços IPv4 públicos válidos, conhecidos como **pool NAT**.
- Um dispositivo ativado para NAT geralmente opera na fronteira de uma rede stub.
- Quando um dispositivo dentro da rede stub deseja se comunicar com um dispositivo fora de sua rede, o pacote é encaminhado para o roteador de fronteira e o roteador executa o processo NAT.



Nota: 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.

Como o NAT funciona?

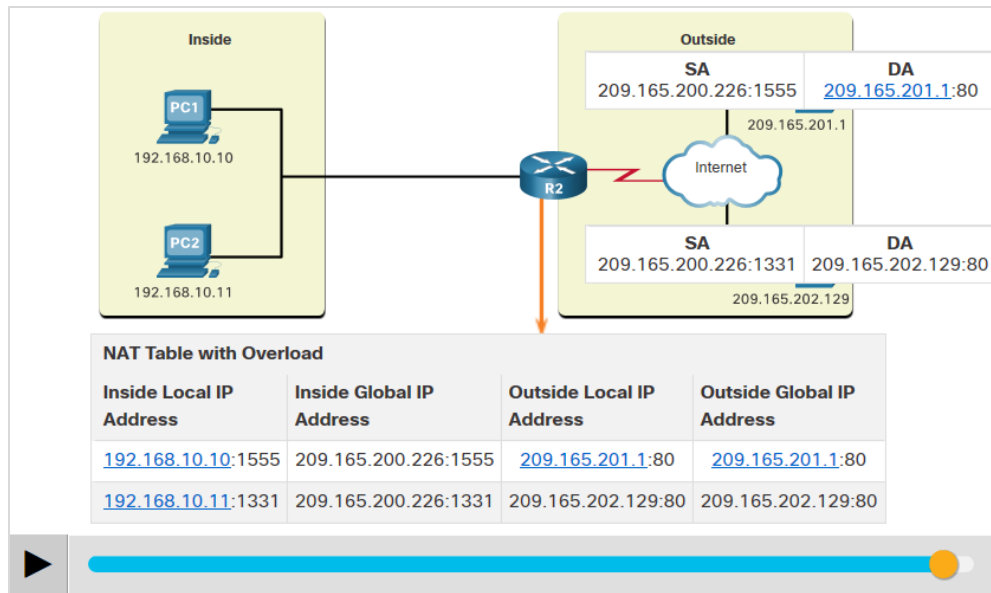
- Neste exemplo, o PC1 com endereços privados 192.168.10.10 deseja se comunicar com um Servidor web externo com endereço público 209.165.201.1.
- Clique no botão Reproduzir na figura para visualizar uma animação.



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.
- 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.
- O PAT garante que os dispositivos utilizem um número de porta diferente do TCP para cada sessão com um Servidor na Internet.
- O PAT usa números de portas origem exclusivos no endereço IP global interno para distinguir entre conversões.

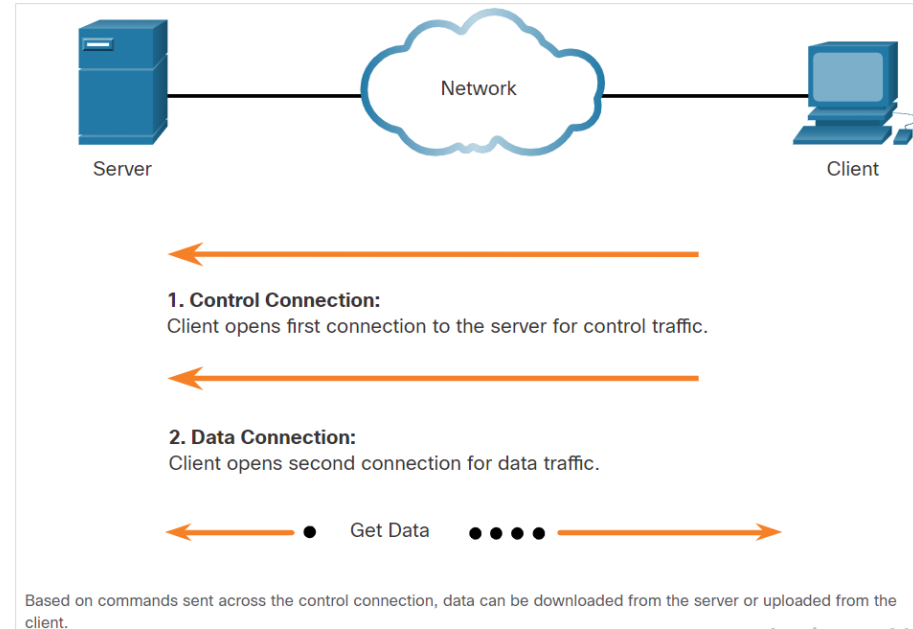
Clique em Reproduzir na figura para visualizar uma animação do processo PAT.



10.4 Serviços de transferência e compartilhamento de arquivos

FTP e TFTP

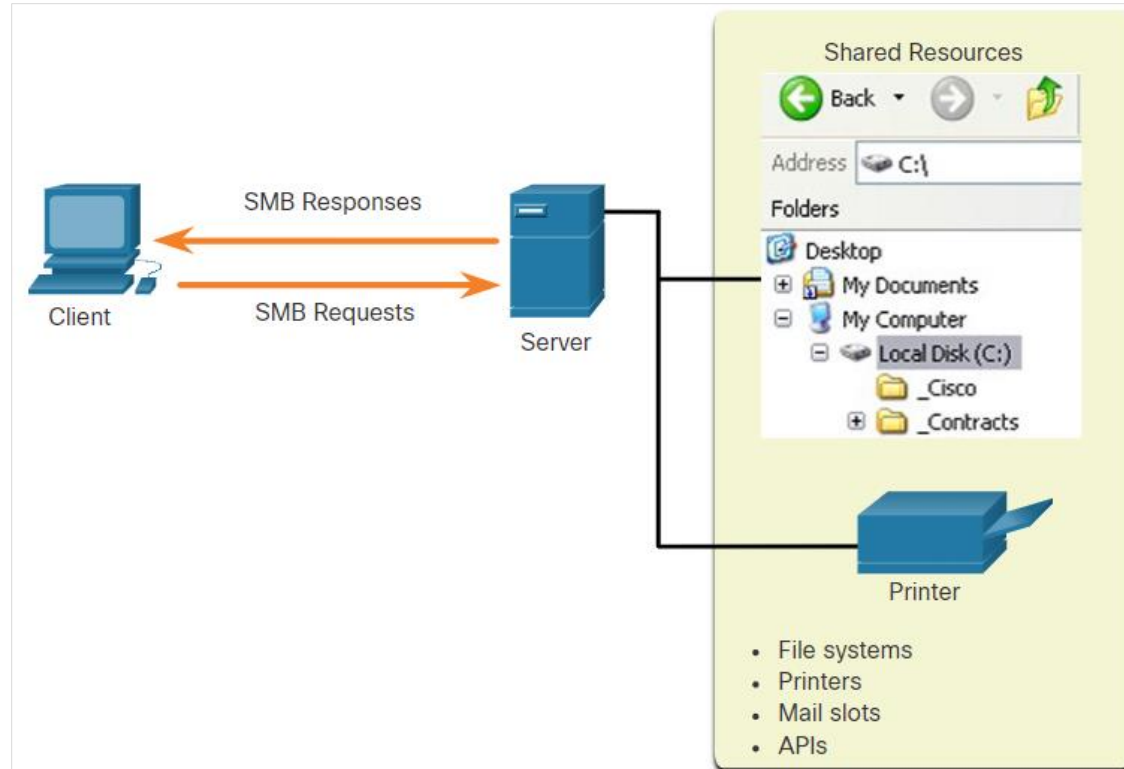
- O FTP permite a transferência de dados entre um cliente e um servidor.
- Um cliente FTP é executado em um computador e é usado para enviar e receber dados de um servidor FTP.
- Conexões FTP entre o cliente e o servidor:
 - **Conexão de controle:** O cliente abre a primeira conexão com o servidor para controlar o tráfego.
 - **Conexão de dados:** O cliente abre a segunda conexão com o servidor para tráfego de dados.
- O Protocolo de Transferência de Ficheiros Trivial (TFTP) é um protocolo de transferência de ficheiros simplificado que utiliza o conhecido número de porta UDP 69.



Serviços de transferência e compartilhamento de arquivos

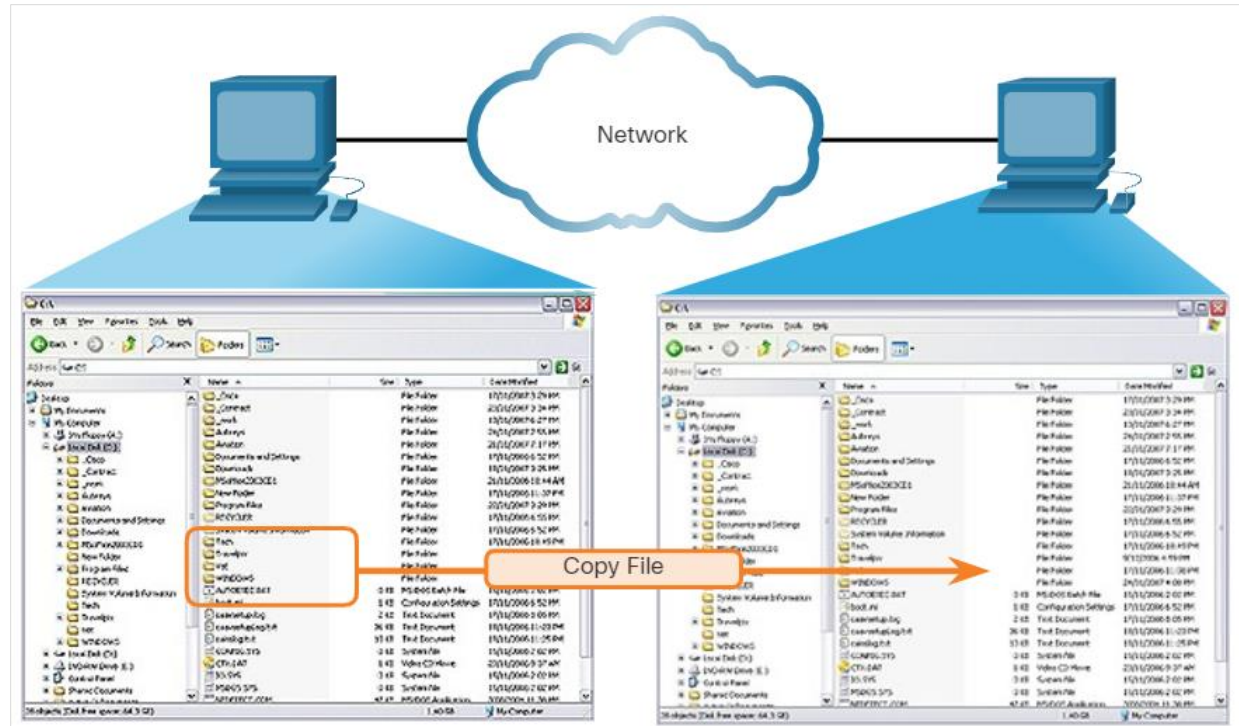
SMB

- O Server Message Block (SMB) é um protocolo de compartilhamento de arquivo cliente / servidor que descreve a estrutura de recursos de rede compartilhados.
- SMB é um cliente / servidor, protocolo de solicitação-resposta.
- Os servidores podem disponibilizar seus próprios recursos para os clientes na rede.



Serviços de transferência e compartilhamento de arquivos SMB (Cont.)

- 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 a base da rede da Microsoft.
- Um arquivo pode ser copiado de um computador para outro com o Windows Explorer usando o protocolo SMB.



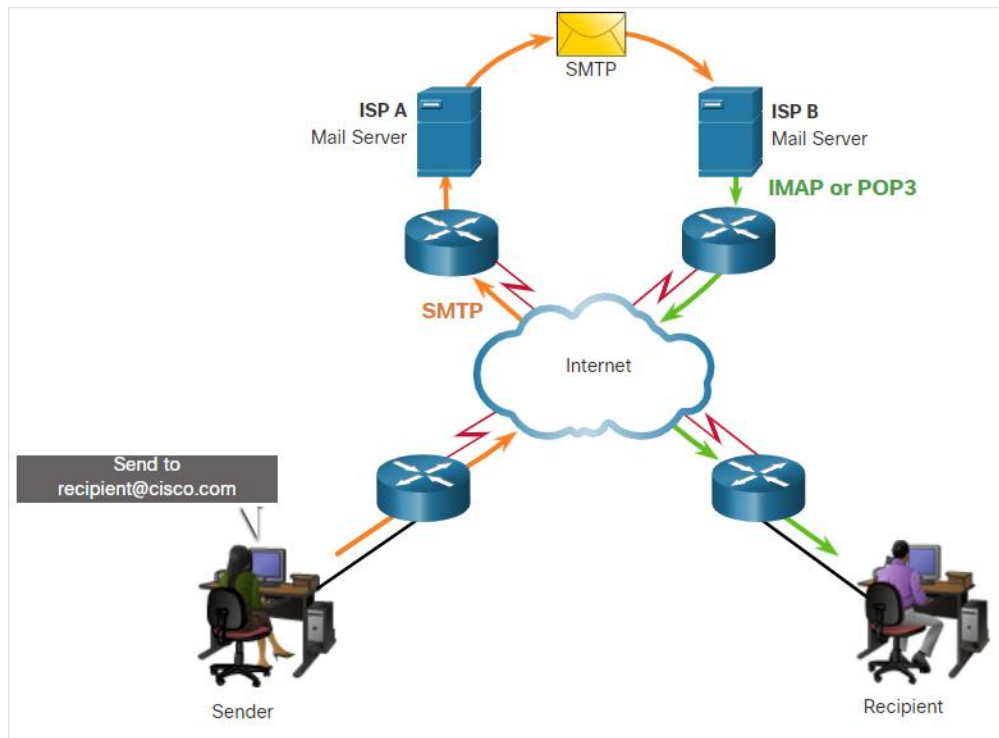
Laboratório - Usando o Wireshark para Examinar Capturas FTP e TFTP

- Neste laboratório, você completará os seguintes objetivos:
 - Identificar os Campos do Cabeçalho e a Operação TCP Usando uma Captura de Sessão FTP do Wireshark
 - Identificar os Campos do Cabeçalho e a Operação UDP Usando uma Captura de Sessão TFTP do Wireshark

10.5 E-mail

Protocolos de email

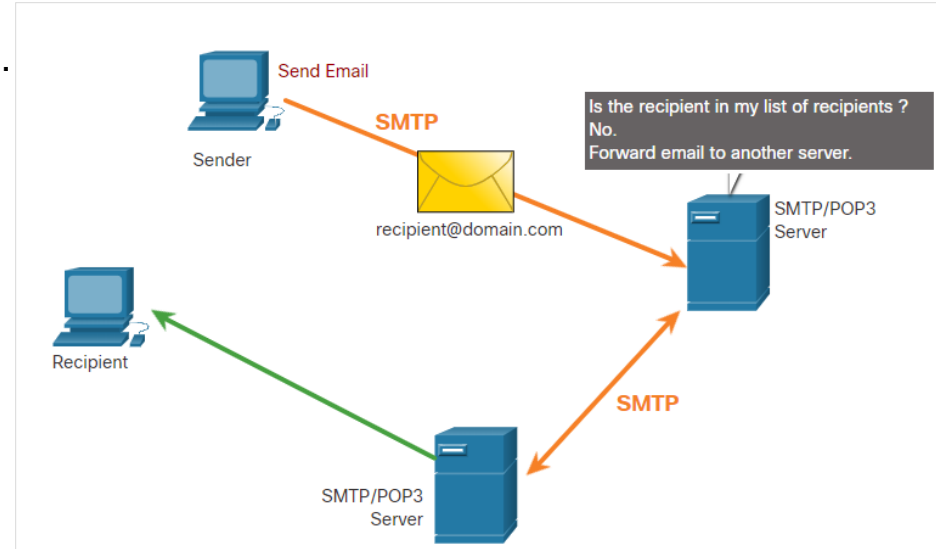
- O e-mail é um método de armazenar, de enviar e de recuperar mensagens eletrônicas em uma rede.
- Os clientes de e-mail se comunicam com os servidores de e-mail para enviar e receber e-mails.
- O e-mail suporta três protocolos separados para a operação: SMTP, POP e IMAP.
- Um cliente recupera e-mails usando um dos dois protocolos da camada de aplicação: POP ou IMAP.



E-mail

SMTP

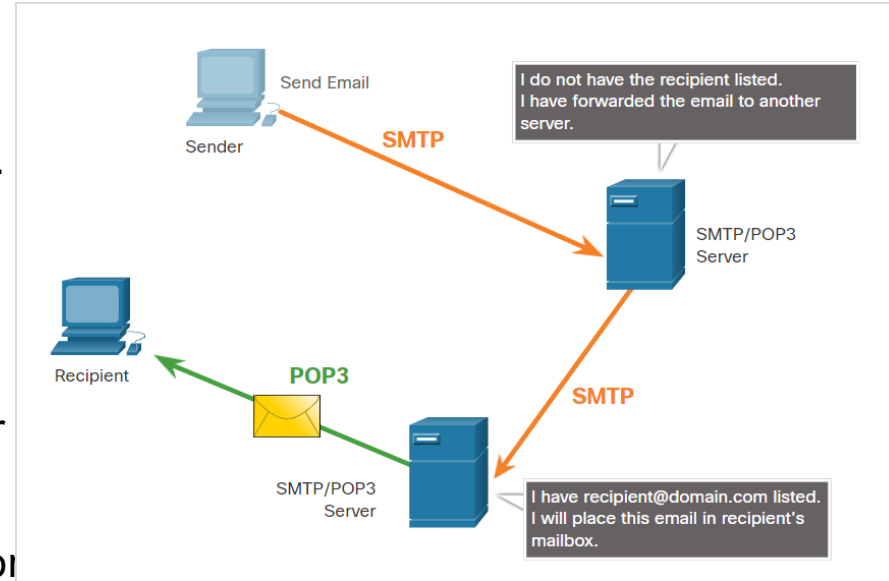
- Os formatos de mensagens SMTP exigem um cabeçalho de mensagem e um corpo de mensagem.
- Quando um cliente envia um e-mail, o processo SMTP do cliente se conecta a um processo SMTP do servidor em uma porta 25 bem conhecida.
- Quando o servidor recebe a mensagem, ele a coloca em uma conta local, se o destinatário for local, ou encaminha a mensagem para outro servidor de correio para entrega.
- 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.



E-mail

POP3

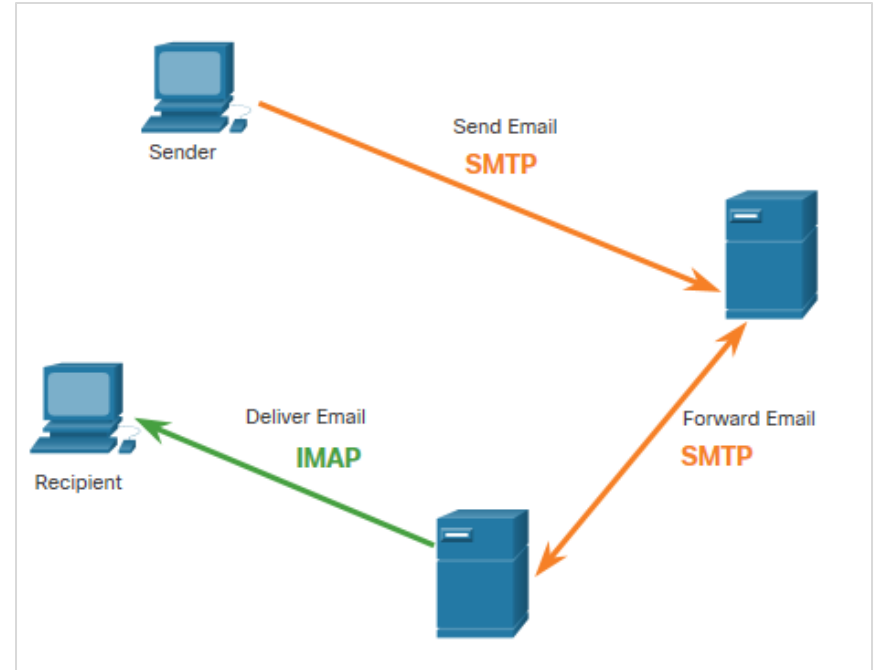
- POP3 é usado por um aplicativo para recuperar um e-mail de um servidor de e-mail.
- Com o POP3, as mensagens de email são baixadas para o cliente e removidas do servidor.
- O servidor inicia o serviço POP3 ouvindo passivamente na porta TCP 110 as solicitações de conexão do cliente.
- O cliente envia uma solicitação para estabelecer uma conexão TCP com o servidor.
- Assim que a conexão for estabelecida, o servidor POP3 enviará uma saudação. O cliente e o servidor POP3 trocam comandos e respostas até que a conexão seja fechada ou abortada.



E-mail

IMAP

- IMAP é o protocolo que descreve um método para recuperar mensagens de e-mail.
- Quando o usuário se conecta a um servidor compatível com IMAP, cópias das mensagens são baixadas para o aplicativo cliente. As mensagens originais são mantidas no servidor até serem 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.
- Quando um usuário decide excluir uma mensagem, o servidor sincroniza essa ação e exclui a mensagem do servidor.



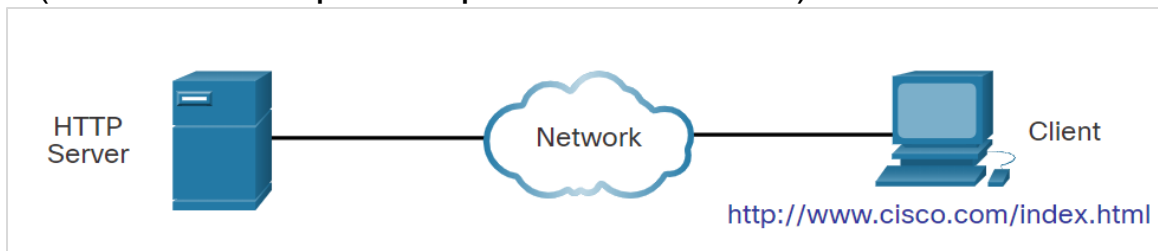
10.6 HTTP

Protocolo HTTP e HTML

- Quando um endereço da web ou Uniform Resource Locator (URL) é digitado em um navegador da web, o navegador da web estabelece uma conexão com o serviço da web que está usando o protocolo HTTP.
- Vamos dar uma olhada em como uma página da web é aberta em um navegador.
Exemplo: <http://www.cisco.com/index.html>

Etapas 1: o navegador interpreta as três partes do URL:

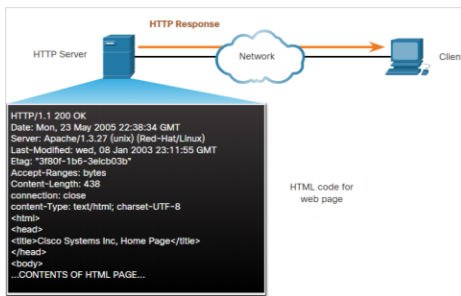
- http (o protocolo ou esquema)
- www.cisco.com (o nome do servidor)
- index.html (o nome do arquivo específico solicitado)



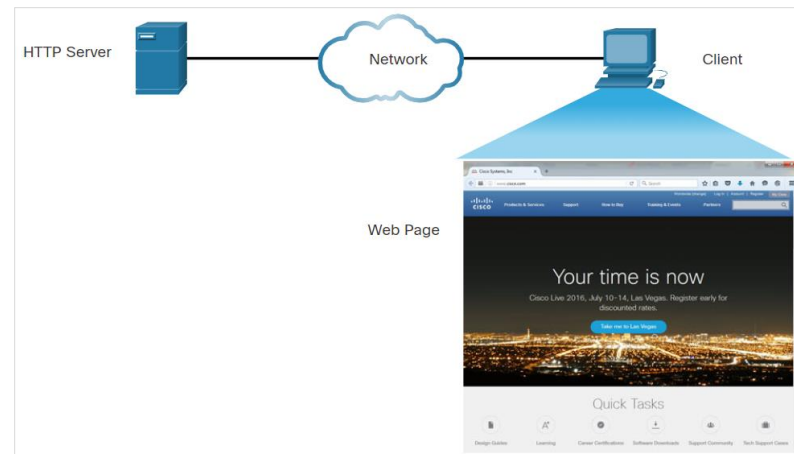
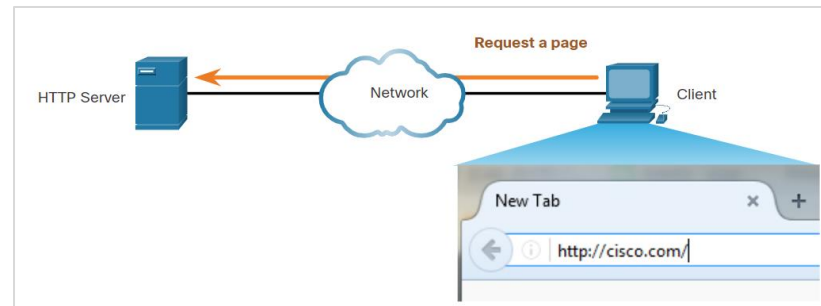
HTTP

Hypertext Transfer Protocol e Hypertext Markup Language (Cont.)

- **Etapa 2:** O cliente inicia uma solicitação HTTP a um servidor enviando uma solicitação GET ao servidor e solicita o arquivo index.html.
- **Etapa 3:** Em resposta à solicitação, o servidor envia ao navegador o código HTML dessa página da web.

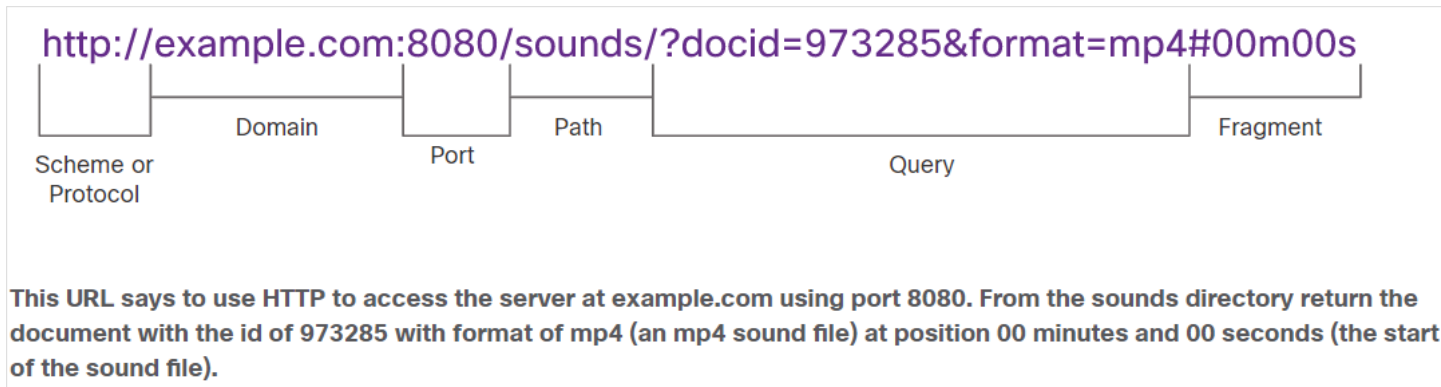


- **Etapa 4:** O navegador decifra o código HTML e formata a página para a janela do navegador.



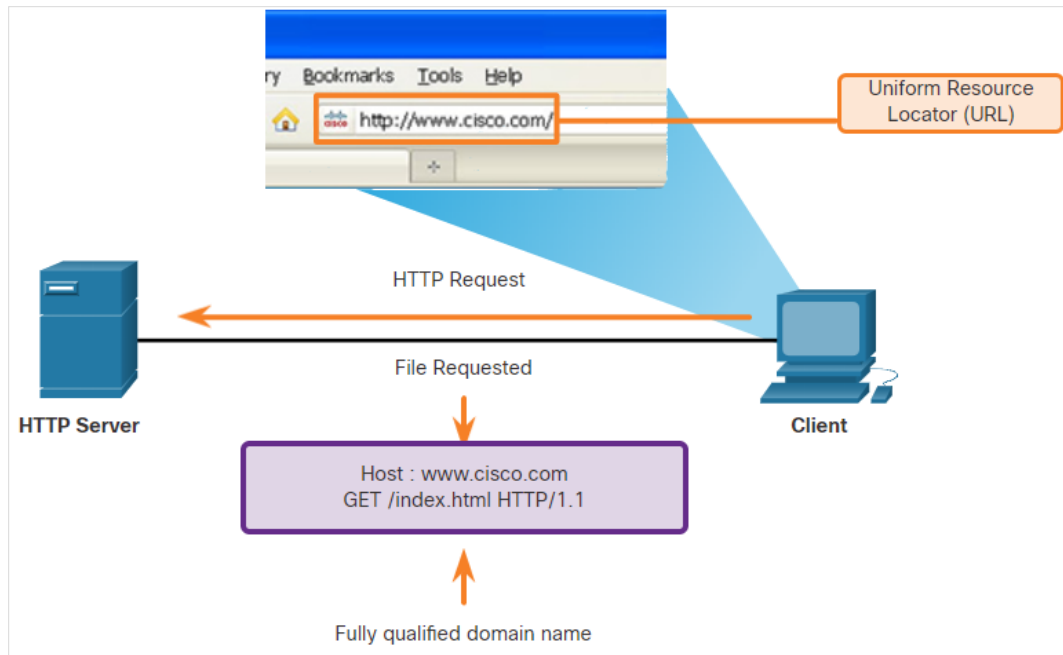
O URL HTTP

- URLs HTTP podem especificar a porta no servidor que deve manipular os métodos HTTP.
- Ele pode especificar uma seqüência de caracteres de consulta e fragmento.
- 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.
- As partes de uma URL HTTP são mostradas na figura abaixo:



Operação HTTP

- HTTP é um protocolo de solicitação/resposta que usa a porta TCP 80. Ele é flexível, mas não um protocolo seguro.
- Quando um cliente envia uma solicitação para um servidor web, ele usará um dos seis métodos especificados por HTTP:
 - GET
 - POST
 - PUT
 - DELETE
 - OPTIONS



Códigos de status HTTP

- Os códigos de status HTTP 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 de cliente e **5xx**- Erro de servidor
- A tabela abaixo explica alguns códigos de status comuns:

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.

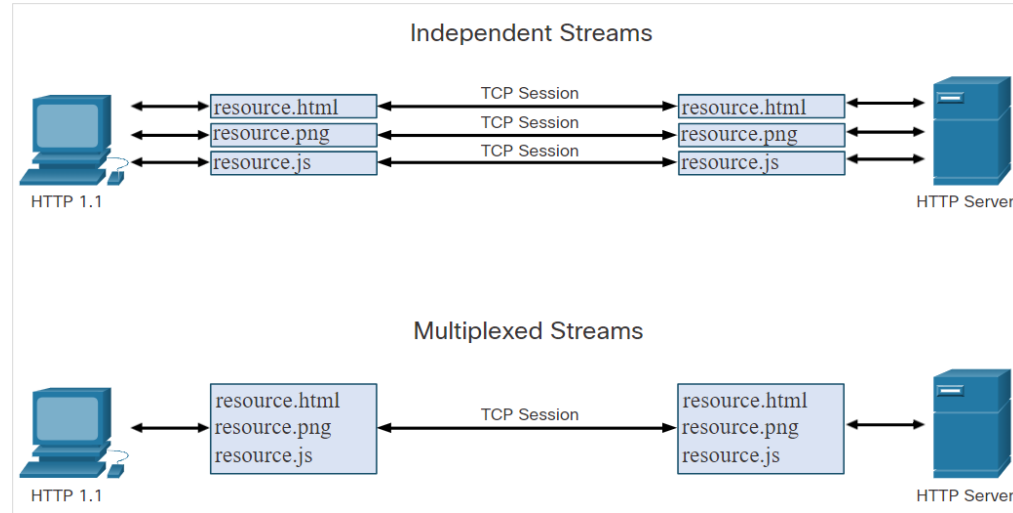
Códigos de Status HTTP (Cont.)

Código	Status	Significado
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.

HTTP

HTTP/2

- 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.
- Alguns recursos importantes do HTTP/2 que um analista de segurança cibernética deve estar ciente:
 - Multiplexação
 - PUSH do servidor
 - Um protocolo binário
 - Compressão de cabeçalho



Protegendo HTTP — HTTPS

- Para comunicação segura na Internet, é usado o protocolo HTTP Secure (HTTPS).
- HTTPS usa autenticação e criptografia para proteger os dados enquanto eles trafegam 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.
- HTTPS/2 é especificado para usar HTTPS sobre TLS com a extensão Application-Layer Protocol Negotiation (ALPN) para TLS 1.2 ou mais recente.
- Informações confidenciais são transmitidas pela Internet usando HTTPS.

Laboratório - Usando Wireshark para examinar tráfego HTTP e HTTPS

- Neste laboratório, você completará os seguintes objetivos:
 - Capturar e visualizar tráfego HTTP
 - Capture e veja o tráfego HTTPS

10.7 Resumo dos serviços de rede

O que aprendi neste módulo?

- 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.
- A operação DHCP inclui: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK e DHCPNAK.
- O DNS resolve nomes para endereços IP. Há cinco etapas envolvidas na resolução de DNS.
- O NAT fornece a tradução de endereços privados para endereços públicos. Um dispositivo ativado para NAT geralmente opera na fronteira de uma rede stub.
- 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.
- O FTP foi desenvolvido para permitir a transferência de arquivos entre um cliente e um servidor. O Protocolo de Transferência de Ficheiros Trivial (TFTP) é um protocolo de transferência de ficheiros simplificado que utiliza a porta UDP número 69.

O que eu aprendi neste módulo? (Continuação)

- Os clientes de e-mail se comunicam com os servidores de e-mail para enviar e receber e-mails.
- O e-mail suporta três protocolos separados para operação: SMTP, POP e IMAP.
- Os navegadores da Web e os servidores da Web interagem usando as quatro etapas.
- HTTP é um protocolo de solicitação / resposta que usa a porta TCP 80.
- 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.
- Códigos de status HTTP: 1xx, 2xx, 3xx, 4xx e 5xx.
- 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.

