2023

Introdução às redes

Módulo 10 – Camada de aplicação

Índice

10 - Camada de aplicação

10.0 - O que vou aprender neste módulo?

10.1 - Aplicação, Apresentação e Sessão

- 15.1.1 - Camada de Aplicação
- 15.1.2 - Camada de Apresentação e de Sessão
- 15.1.3 - Protocolos TCP/IP da Camada de Aplicação

10.2 - Ponto a ponto

- 15.2.1 - Modelo Cliente-Servidor
- 15.2.2 - Redes Ponto a ponto
- 15.2.3 - Aplicações Peer-to-Peer
- 15.2.4 - Aplicações P2P Comuns

10.3 - Protocolos de E-mail e Web

- 15.3.1 - HTTP e HTML
- 15.3.2 - HTTP e HTTPS
- 15.3.3 - Protocolos de E-mail
- 15.3.4 - SMTP, POP e IMAP

10.4 - Serviços de Endereçamento IP

- 10.4.1 - Serviço de Nomes de Domínio (DNS)
- 10.4.2 - Formato de Mensagem DNS
- 10.4.3 - Hierarquia DNS
- 10.4.4 - O Comando nslookup
- 10.4.5 - Verificador de Sintaxe - O Comando nslookup
- 10.4.6 - Protocolo de Configuração Dinâmica de Host (DHCP)
- 10.4.7 - Operação do DHCP
- 15.4.8 - Laboratório - Observe a resolução DNS

10.5 - Serviços de Compartilhamento de Arquivos

- 10.5.1 - Protocolo FTP
- 10.5.2 - Protocolo SMB

10.6 - O que eu aprendi neste módulo?

Camada de aplicação

10.0. - O que vou aprender neste módulo?

Título do módulo: Camada de aplicação

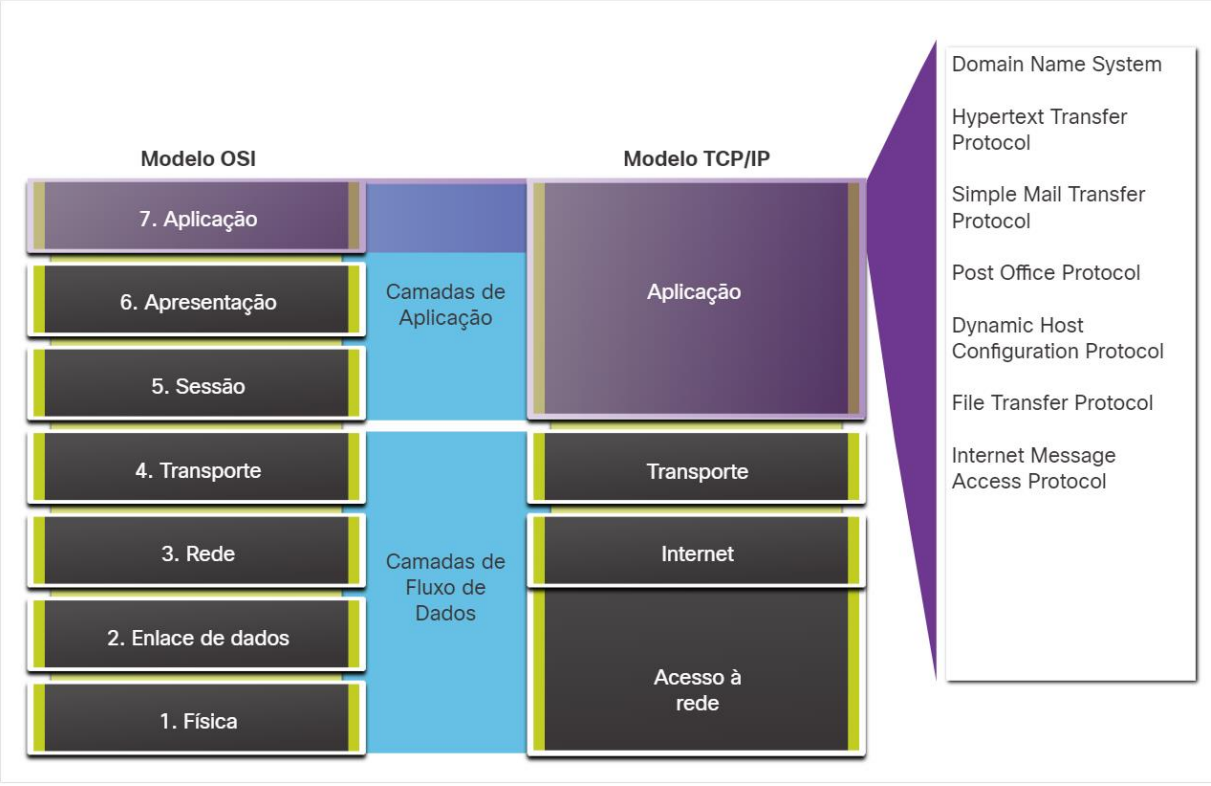
Objetivo do módulo: Explicar a operação de protocolos da camada de aplicação para dar suporte às aplicações do usuário final.

Título do Tópico	Objetivo do Tópico
Aplicação, Apresentação e Sessão	Explicar como as funções da camada de aplicação, camada de apresentação, e camada de sessão trabalham em conjunto para fornecer serviços de rede para o usuário final aplicativos empresariais.
Ponto a ponto	Explicar como os aplicativos de usuário final operam em uma rede ponto a ponto.
Protocolos de e-mail e Web	Explicar como os protocolos Web e de e-mail operam.
Serviços de endereçamento IP	Explicar como DHCP e DNS funcionam.
Serviços de compartilhamento de arquivos	Explicar como os protocolos de transferência de arquivos operam.

10.1 Aplicação, Apresentação e Sessão

10.1.1 Camada de Aplicação

Nos modelos OSI e TCP / IP, a camada de aplicativo é a camada mais próxima do usuário final. Conforme mostrado na figura, é a camada que fornece a interface entre os aplicativos usados para se comunicar e a rede subjacente pela qual as mensagens são transmitidas. Os protocolos da camada de aplicação são utilizados para troca de dados entre programas executados nos hosts de origem e destino.



Com base no modelo TCP / IP, as três camadas superiores do modelo OSI (aplicativo, apresentação e sessão) definem funções da camada de aplicativo TCP / IP.

Há muitos protocolos da camada de aplicação e outros novos estão em constante desenvolvimento. Alguns dos protocolos da camada de aplicação mais conhecidos incluem o HTTP (Hypertext Transfer Protocol), o FTP (File Transfer Protocol), o TFTP (Trivial File Transfer Protocol), o IMAP (Internet Message Access Protocol) e o DNS (Domain Name Service).

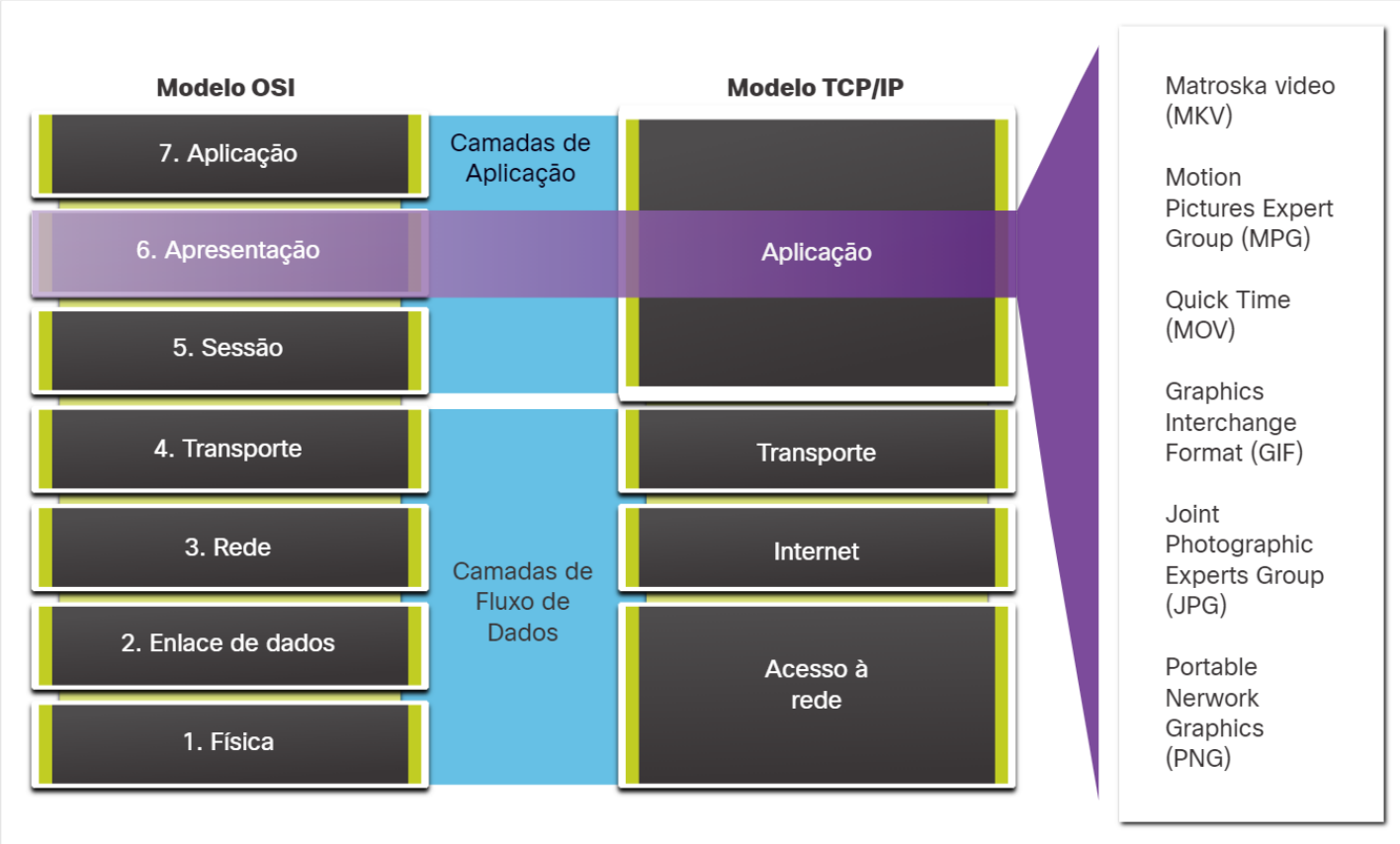
10.1.2 Camada de Apresentação e de Sessão

Camada de apresentação

A camada de apresentação tem três funções principais:

- Formatar ou apresentar dados no dispositivo de origem em um formato compatível para recebimento pelo dispositivo de destino.
- Comprimir dados de uma maneira que possa ser descompactada pelo dispositivo de destino.
- Criptografar dados para transmissão e descriptografar dados após o recebimento.

Conforme mostra a figura, a camada de apresentação formata dados para a camada de aplicação e define padrões para formatos de arquivo. Alguns padrões bem conhecidos para vídeo incluem Matroska Video (MKV), Motion Picture Experts Group (MPG) e QuickTime Video (MOV). Alguns formatos conhecidos de imagem gráfica são o formato Graphics Interchange Format (GIF), o Joint Photographic Experts Group (JPG) e o formato Portable Network Graphics (PNG).



Camada de sessão

Como o nome sugere, as funções na camada de sessão criam e mantêm diálogos entre as aplicações origem e destino. A camada de sessão processa a troca de informações para iniciar diálogos, mantê-los ativos e reiniciar sessões interrompidas ou ociosas por um longo período.

10.1.3 Protocolos TCP/IP da Camada de Aplicação

Os protocolos de aplicativos TCP / IP especificam o formato e as informações de controle necessárias para muitas funções comuns de comunicação da Internet. Os protocolos da camada de aplicação são utilizados pelos dispositivos de origem e destino durante uma sessão de comunicação. Para que as comunicações sejam bem-sucedidas, os protocolos da camada de aplicativo implementados no host de origem e destino devem ser compatíveis.

Sistema de Nomes

DNS - Sistema de Nomes de Domínio (ou Serviço)

- TCP, cliente UDP 53
- Converte nomes de domínio, como cisco.com, em endereços IP.

Configuração do host

BOOTP - Protocolo de Bootstrap

- Cliente UDP 68, servidor 67
- Permite que uma estação de trabalho sem disco descubra seu próprio endereço IP, o endereço IP de um servidor BOOTP na rede e um arquivo a ser carregado na memória para inicializar a máquina
- O BOOTP está sendo substituído pelo DHCP

DHCP - Protocolo de configuração de host dinâmico

- Cliente UDP 68, servidor 67
- Atribui dinamicamente endereços IP para serem reutilizados quando não forem mais

Email

SMTP - Protocolo Simples de Transferência de Correio

- TCP 25
- Permite que os clientes enviem e-mail para um servidor de e-mail
- Permite que servidores enviem e-mail para outros servidores
- **POP3 - Protocolo da agência postal**
- TCP 110
- Permite que os clientes recuperem e-mails de um servidor de e-mail
- Transfere o e-mail para a aplicação de correio local do cliente
- **IMAP - Protocolo de Acesso à Mensagem na Internet**
- TCP 143
- Permite que os clientes acessem e-mails armazenados em um servidor de e-mail
- Mantém o e-mail no servidor

Transferência de arquivo

FTP - Protocolo de Transferência de Arquivos

- TCP 20 a 21
- Define as regras que permitem que um usuário em um host acesse e transfira arquivos de e para outro host em uma rede
- O FTP é um protocolo de entrega de arquivos confiável, orientado à conexão e reconhecido

TFTP - Protocolo de Transferência de Arquivos Trivial

- Cliente* UDP 69
- 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

HTTP - Protocolo de transferência de hipertexto

- TCP 80, 8080
- Um conjunto de regras para a troca de texto, imagens gráficas, som, vídeo e outros arquivos multimídia na World Wide Web

HTTPS - HTTP seguro

- TCP, UDP 443
- O navegador usa criptografia para proteger conversações HTTP
- Autentica o site ao qual você conecta o seu navegador

10.2 Ponto a ponto

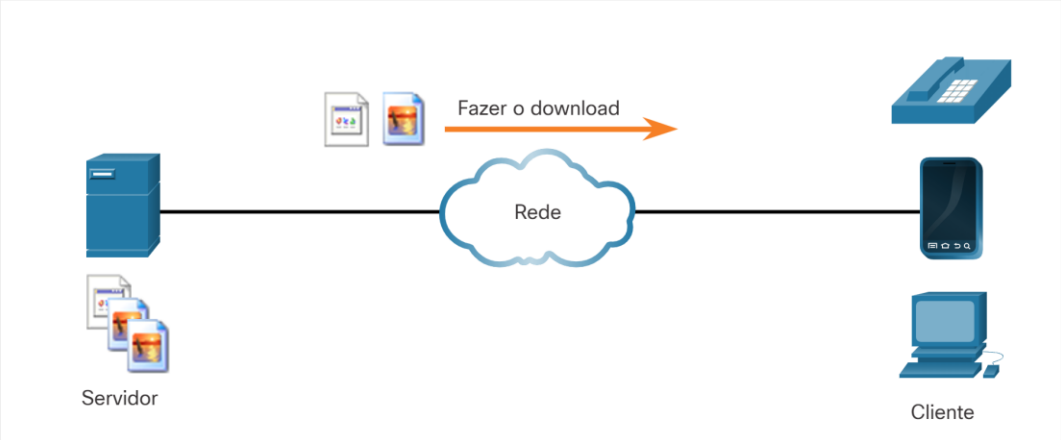
10.2.1 Modelo Cliente-Servidor

No tópico anterior, você aprendeu que os protocolos de camada de aplicativo TCP/IP implementados no host de origem e de destino devem ser compatíveis. Neste tópico, você aprenderá sobre o modelo cliente/servidor e os processos utilizados, que estão na camada de aplicação. O mesmo se aplica a uma rede ponto a ponto. No modelo cliente / servidor, o dispositivo que solicita as informações é chamado de cliente e o dispositivo que responde à solicitação é chamado de servidor. O cliente é uma combinação de hardware/software que as pessoas usam para acessar diretamente os recursos armazenados no servidor.

Considera-se que os processos de cliente e servidor estão na camada de aplicação. O cliente começa a troca ao requisitar dados do servidor, que responde enviando uma ou mais sequências de dados ao cliente. Os protocolos da camada de aplicação descrevem o formato das requisições e respostas entre clientes e servidores. Além da transferência real de dados, essa troca de informações também pode exigir informações de autenticação de usuário e identificação de um arquivo de dados a ser transferido.

Um exemplo de rede cliente / servidor é usar o serviço de e-mail de um ISP para enviar, receber e armazenar e-mail. O cliente de e-mail em um computador doméstico emite uma solicitação ao servidor de e-mail do ISP para qualquer e-mail não lido. O servidor responde enviando o e-mail requisitado ao cliente. A transferência de dados de um cliente para um servidor é chamada de upload e os dados de um servidor para um cliente como um download.

Conforme mostrado na figura, os arquivos são baixados do servidor para o cliente.



10.2.2 Redes Ponto a ponto

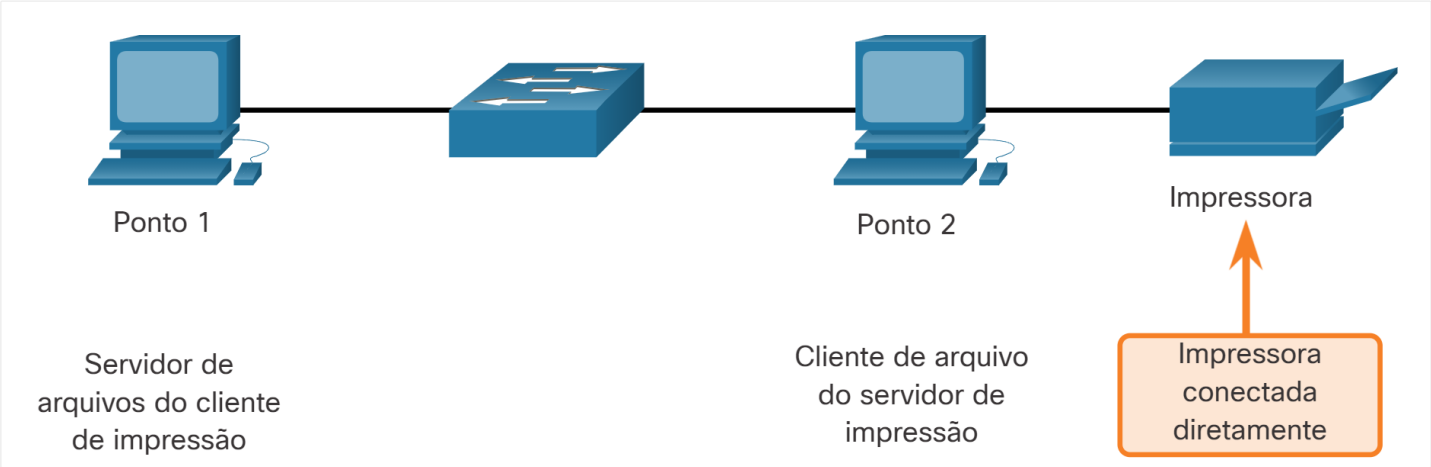
No modelo de rede ponto a ponto (P2P), os dados são acessados de um dispositivo sem usar um servidor exclusivo.

O modelo de rede P2P inclui duas partes: redes P2P e aplicações P2P. As duas partes têm características semelhantes, mas, na prática, funcionam de maneira bastante diferente.

Em uma rede P2P, dois ou mais computadores são conectados via rede e podem compartilhar recursos (como impressoras e arquivos) sem ter um servidor exclusivo. Cada dispositivo final conectado (conhecido como peer) pode funcionar como cliente ou servidor. Um computador pode assumir o papel de servidor para uma transação ao mesmo tempo em que é o cliente de outra. As funções de cliente e servidor são definidas de acordo com a requisição.

Além de compartilhar arquivos, uma rede como essa permitiria aos usuários ativar jogos em rede ou compartilhar uma conexão com a Internet.

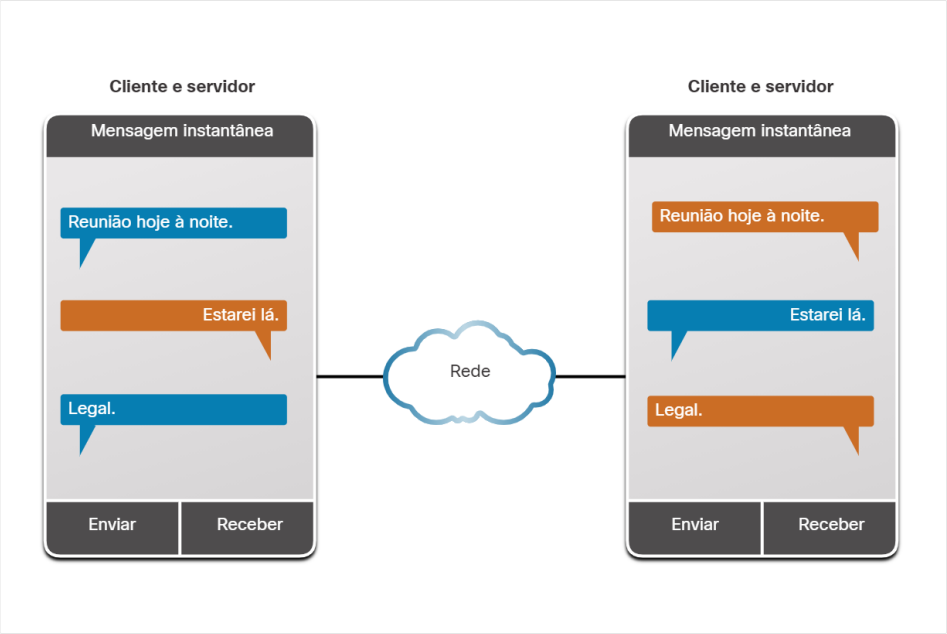
Em uma comunicação peer-to-peer, ambos os dispositivos são considerados iguais no processo de comunicação. O ponto 1 tem arquivos compartilhados com o ponto 2 e pode acessar a impressora compartilhada diretamente conectada ao ponto 2 para imprimir arquivos. O ponto 2 está compartilhando a impressora conectada diretamente com o Peer 1 ao acessar os arquivos compartilhados no Peer 1, como mostrado na figura.



10.2.3 Aplicações Peer-to-Peer

Um aplicação P2P permite que um dispositivo atue como cliente e servidor na mesma comunicação, como mostra a figura. Nesse modelo, todo cliente é um servidor e todo servidor é um cliente. Aplicações P2P exigem que cada dispositivo final forneça uma interface de usuário e execute um serviço em segundo plano.

Algumas aplicações P2P utilizam um sistema híbrido no qual o compartilhamento de recursos é descentralizado, mas os índices que apontam para as localizações de recursos são armazenados em um diretório centralizado. Em um sistema híbrido, cada peer acessa um servidor de índice para obter a localização de um recurso armazenado em outro peer.



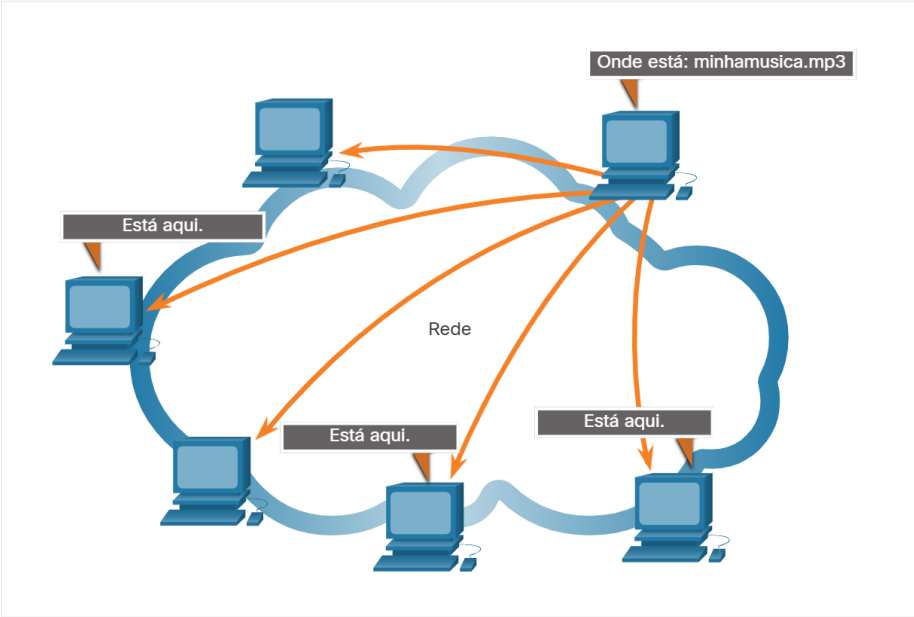
Ambos os clientes iniciam e recebem mensagens simultaneamente.

10.2.4 Aplicações P2P Comuns

Com aplicativos P2P, cada computador na rede que está executando o aplicativo pode atuar como um cliente ou servidor para os outros computadores na rede que também estão executando o aplicativo. As redes P2P comuns incluem o seguinte:

- ☐ BitTorrent
- ☐ Direct Connect
- ☐ eDonkey
- ☐ Freenet

Algumas aplicações P2P usam o protocolo Gnutella, que permite que os usuários compartilhem arquivos completos com outros usuários. Conforme mostrado na figura, o software cliente compatível com Gnutella permite que os usuários se conectem aos serviços Gnutella pela Internet e localizem e acessem recursos compartilhados por outros colegas Gnutella. Muitos aplicativos cliente Gnutella estão disponíveis, incluindo µTorrent, BitComet, DC++, Deluge e emule.



Muitas aplicações P2P permitem que os usuários compartilhem trechos de vários arquivos entre si ao mesmo tempo. Os clientes usam um arquivo torrent para localizar outros usuários com as peças de que precisam, para que possam se conectar diretamente a eles. Este arquivo também contém informações sobre os computadores rastreadores que controlam quais usuários possuem partes específicas de determinados arquivos. Os clientes solicitam peças de vários usuários ao mesmo tempo. Isso é conhecido como enxame e a tecnologia é chamada BitTorrent. BitTorrent tem seu próprio cliente. Mas existem muitos outros clientes BitTorrent, incluindo uTorrent, Deluge e qBittorrent.

> **Observação:** Qualquer tipo de arquivo pode ser compartilhado entre usuários. Muitos desses arquivos são protegidos por direitos autorais, o que significa que apenas o autor tem o direito de distribuí-lo. É ilegal baixar ou distribuir arquivos protegidos por direitos autorais, sem a permissão do detentor desses direitos. A violação dos direitos autorais pode resultar em ações criminais e cíveis.

10.3 Protocolos de E-mail e Web

10.3.1 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.

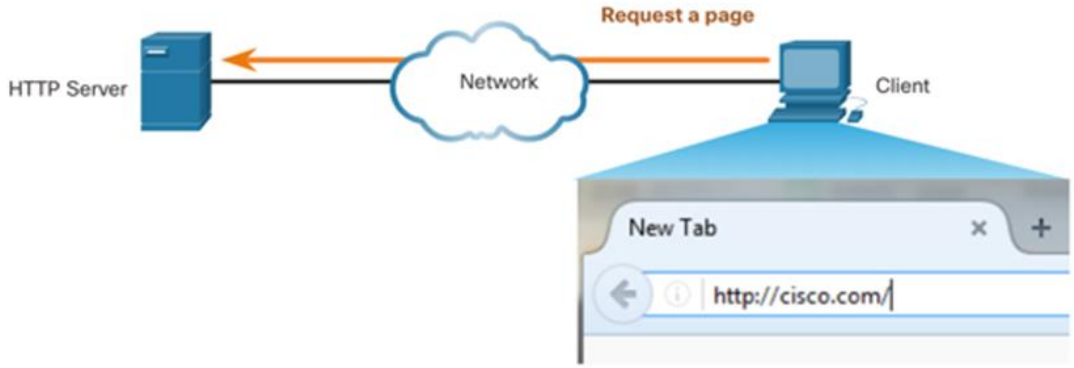
Etapa 1

O navegador interpreta como três partes da URL:

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

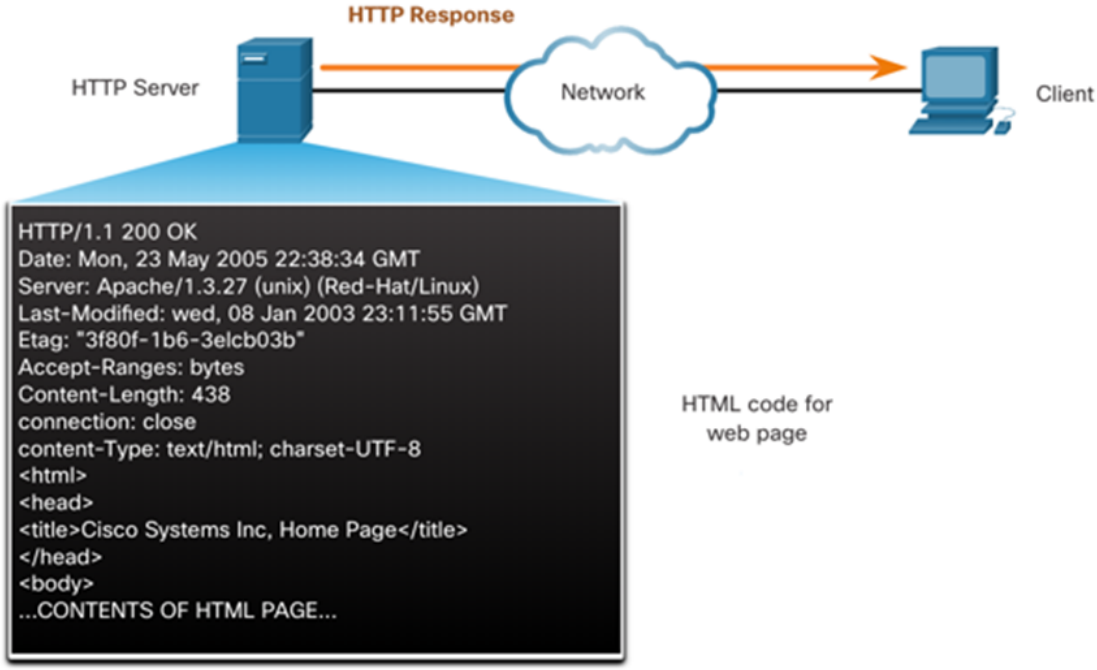
Etapa 2

O navegador então verifica com um servidor de nomes para converter www.cisco.com 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.



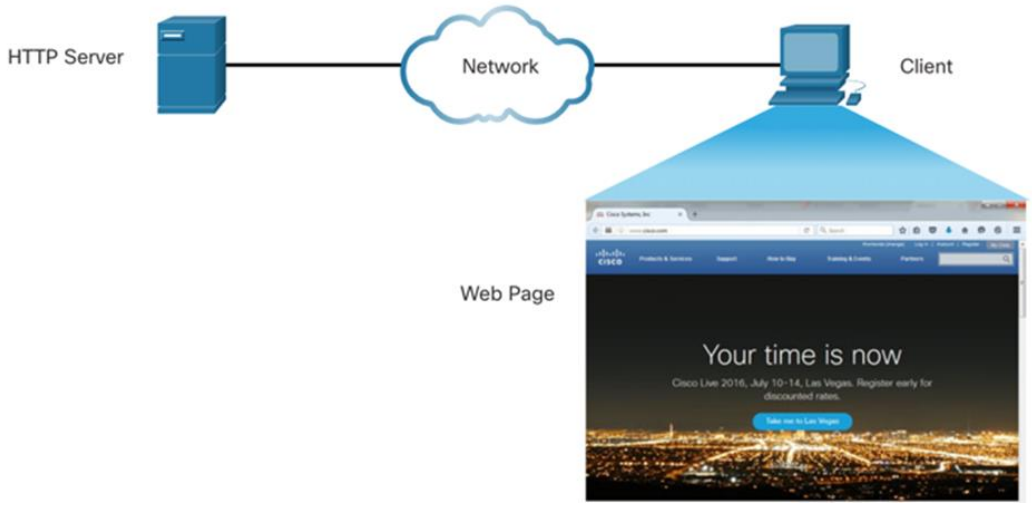
Etapa 3

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.

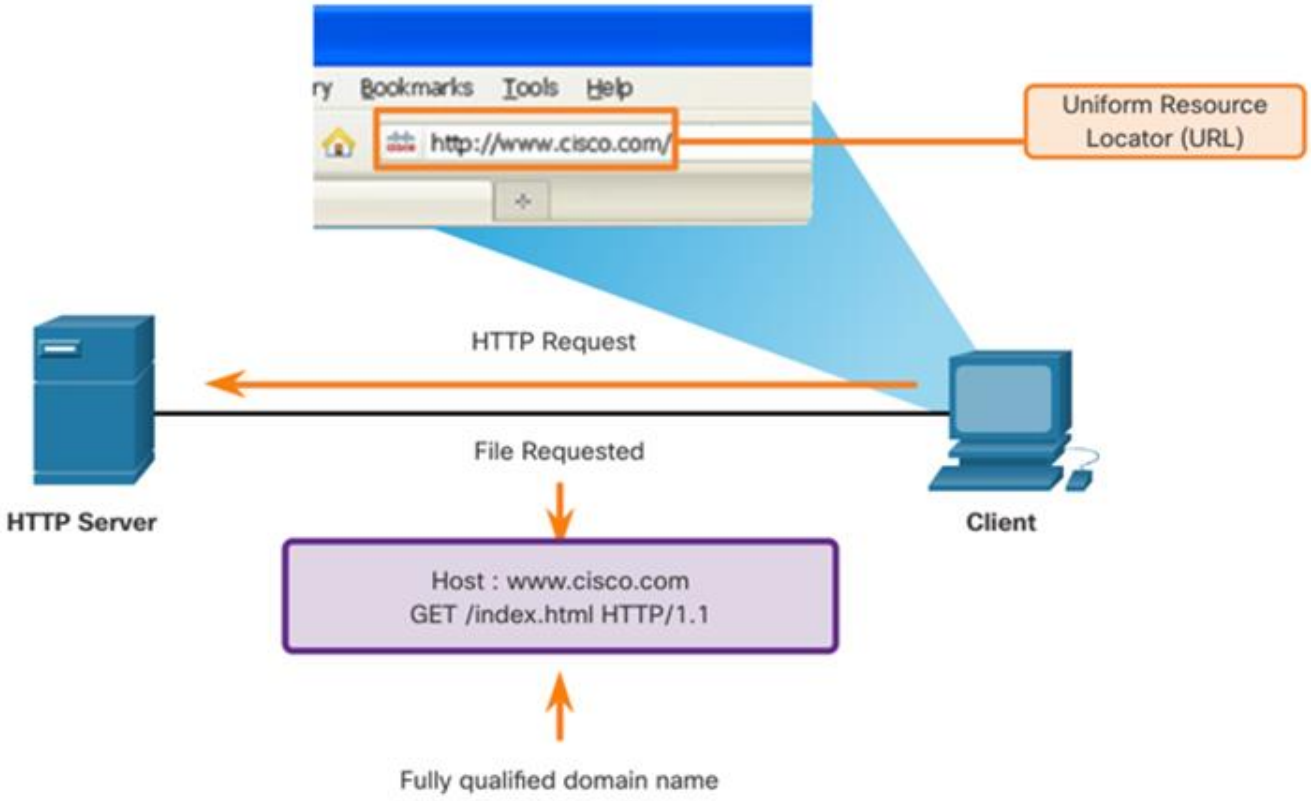


10.3.2 HTTP e HTTPS

O HTTP especifica um protocolo de requisição/resposta. Quando um cliente, normalmente um navegador Web, envia uma requisição a um servidor Web, é o HTTP quem especifica os tipos de mensagem usados nessa conversação. Os três tipos de mensagens comuns são GET (veja a figura), POST e PUT:

- **GET** - Esta é uma solicitação de dados do cliente. Um cliente (navegador Web) envia a mensagem GET ao servidor Web para requisitar páginas HTML.
- **POST** - Isso carrega arquivos de dados no servidor da web, como dados do formulário.
- **PUT** - Isso carrega recursos ou conteúdo para o servidor da web, como uma imagem.

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.

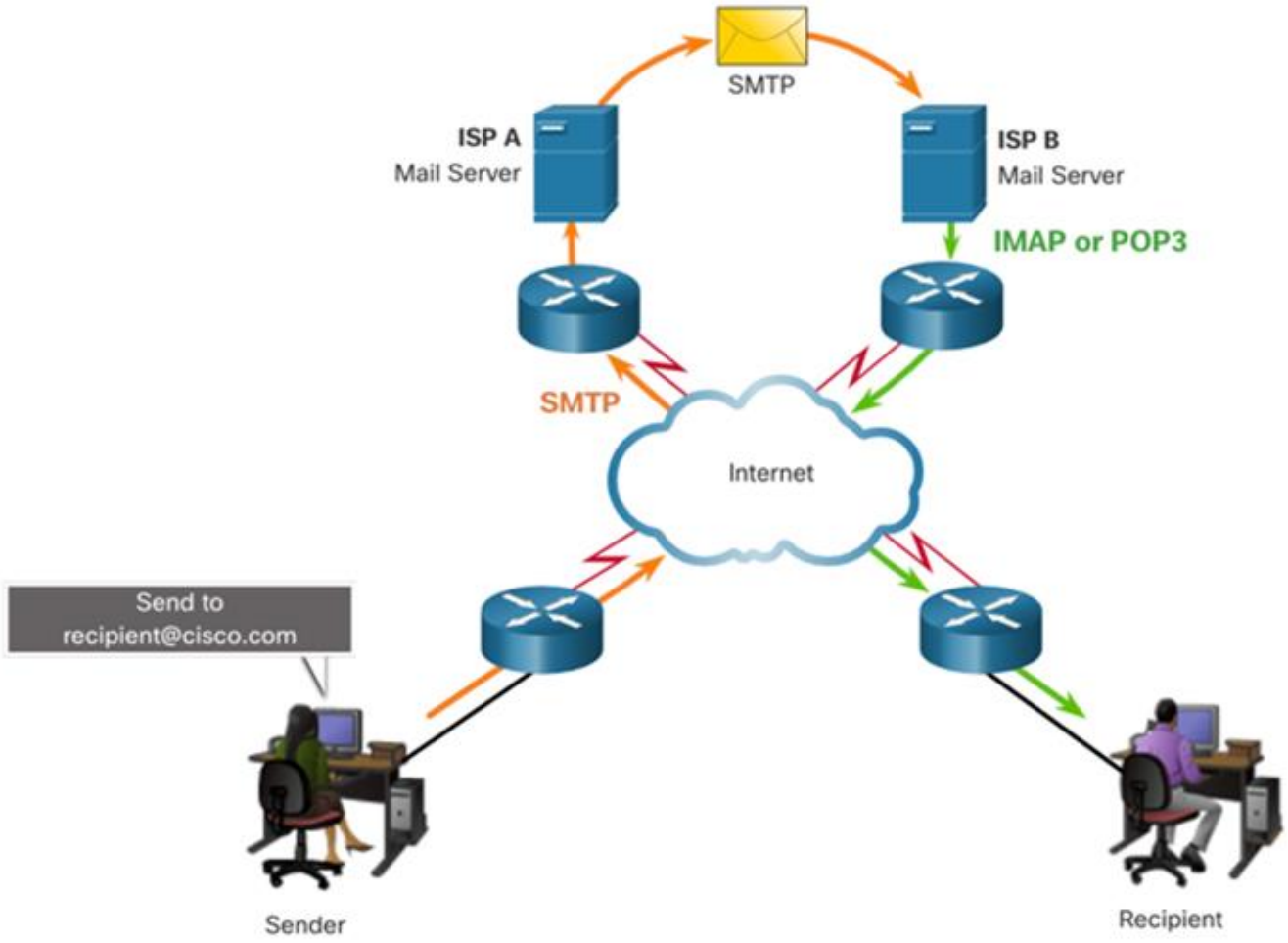


Embora o HTTP seja notavelmente flexível, não é um protocolo seguro. As mensagens de solicitação enviam informações ao servidor em texto sem formatação que podem ser interceptadas e lidas. As respostas do servidor, normalmente páginas HTML, também não são criptografadas.

Para comunicação segura na Internet, é usado o protocolo HTTP Secure (HTTPS). O HTTPS utiliza autenticação e criptografia para proteger dados durante o trajeto entre o cliente e o servidor. O HTTPS usa o mesmo processo de requisição do cliente, resposta do servidor do HTTP, mas o fluxo de dados é criptografado com SSL antes de ser transportado através da rede.

10.3.3 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 e encaminhar, 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.

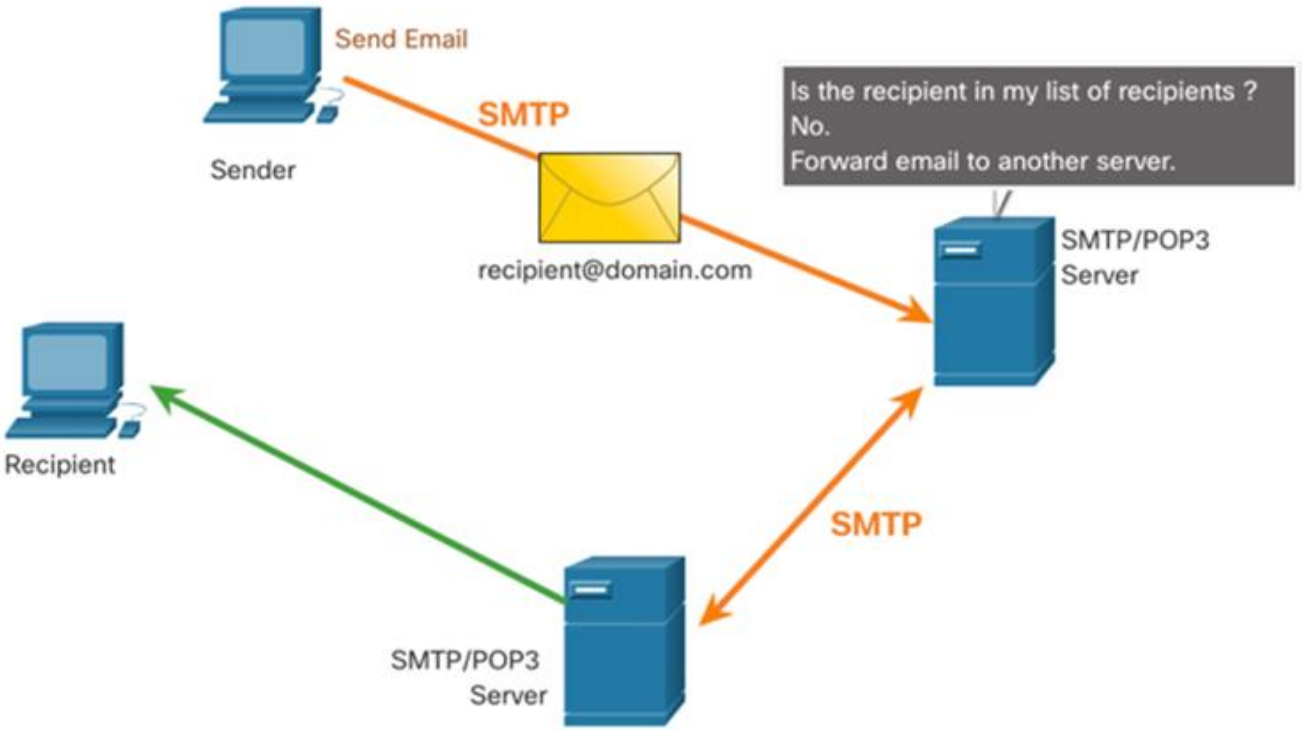
10.3.4 SMTP, POP e IMAP

SMTP

Os formatos de mensagens SMTP exigem um cabeçalho de mensagem e um corpo de mensagem. Embora o corpo da mensagem possa conter qualquer quantidade de texto, o cabeçalho da mensagem deve ter um endereço de e-mail do destinatário formatado corretamente e um endereço do 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 a mensagem para outro servidor de correio para entrega.

O servidor de e-mail de destino pode não estar on-line ou estar ocupado quando as mensagens de e-mail são 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.



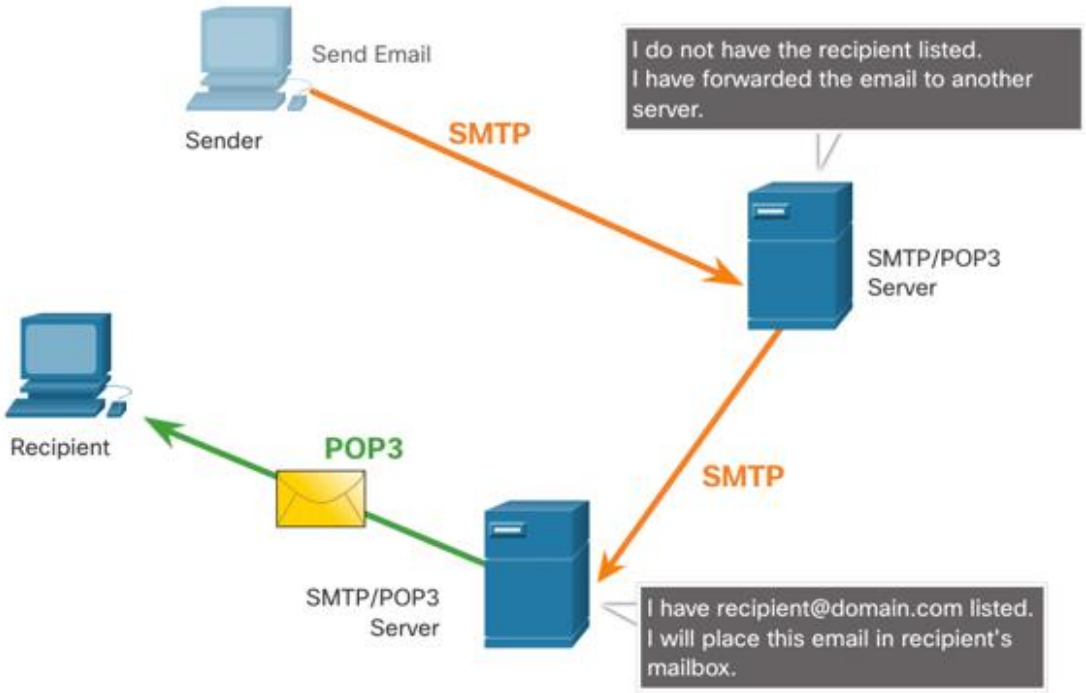
POP

O POP é usado por uma aplicação para recuperar e-mails de um servidor de e-mail. Com o POP, o e-mail será transferido do servidor ao cliente e excluído do servidor. Esta é a operação padrão do POP.

O servidor inicia o serviço POP ao escutar de forma passiva a porta TCP 110 por requisições de conexão dos clientes. Quando um cliente deseja fazer uso do serviço, ele envia uma solicitação para estabelecer uma conexão TCP com o servidor, conforme mostrado na figura. Quando a conexão é estabelecida, o servidor POP envia uma saudação. O cliente e o servidor POP trocam comandos e respostas até que a conexão seja encerrada ou cancelada.

Com o POP, 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 sejam mantidas. Como o POP não armazena mensagens, não é recomendado para pequenas empresas que precisam de uma solução de backup centralizada.

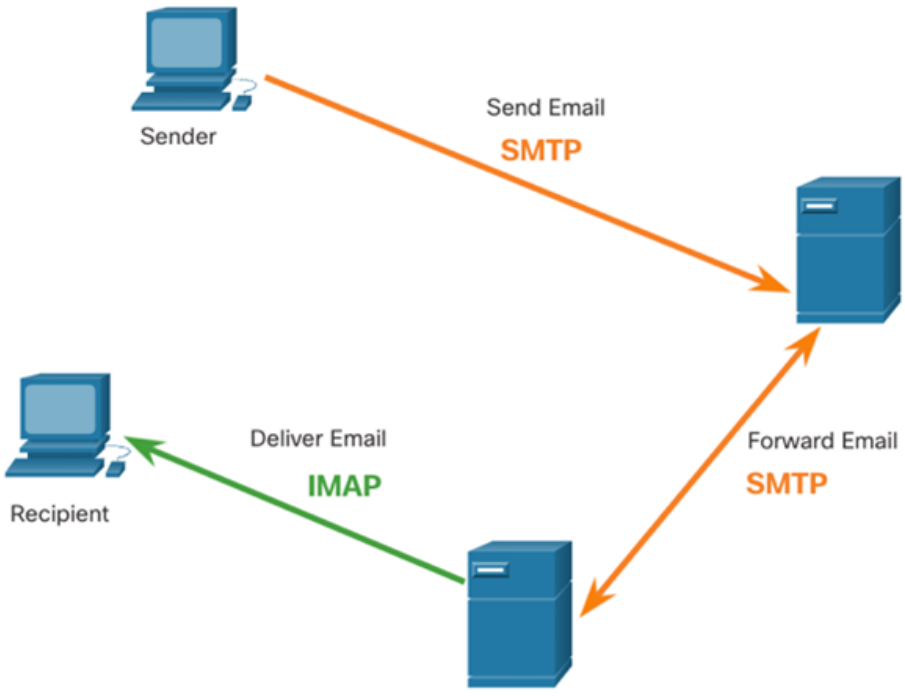
POP3 é a versão mais usada.



IMAP

O IMAP é outro protocolo que descreve um método para recuperar mensagens de e-mail. Ao contrário do POP, quando o usuário se conecta a um servidor compatível com IMAP, as cópias das mensagens são baixadas para o aplicativo cliente, conforme mostrado na figura. 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.



10.4 Serviços de Endereçamento IP

10.4.1 Serviço de Nomes de Domínio (DNS)

Existem outros protocolos específicos da camada de aplicativo que foram projetados para facilitar a obtenção de endereços para dispositivos de rede. Esses serviços são essenciais porque seria muito demorado lembrar endereços IP em vez de URLs ou configurar manualmente todos os dispositivos em uma rede média a grande. O primeiro tópico neste módulo lhe deu uma visão geral desses protocolos. Este tópico entra em mais detalhes sobre os serviços de endereçamento IP, DNS e DHCP.

Em redes de dados, os dispositivos são rotulados com endereços IP numéricos para enviar e receber dados pelas redes. Os nomes de domínio foram criados para converter o endereço numérico em um nome simples e reconhecível.

Na internet, nomes de domínio totalmente qualificados (FQDNs), como (http://www.cisco.com), são muito mais fáceis de lembrar do que 198.133.219.25, que é o endereço numérico real para este servidor. Se a Cisco decidir alterar o endereço numérico de www.cisco.com, ele será transparente ao usuário, porque o nome de domínio permanecerá o mesmo. O novo endereço é simplesmente vinculado ao nome de domínio atual e a conectividade é mantida.

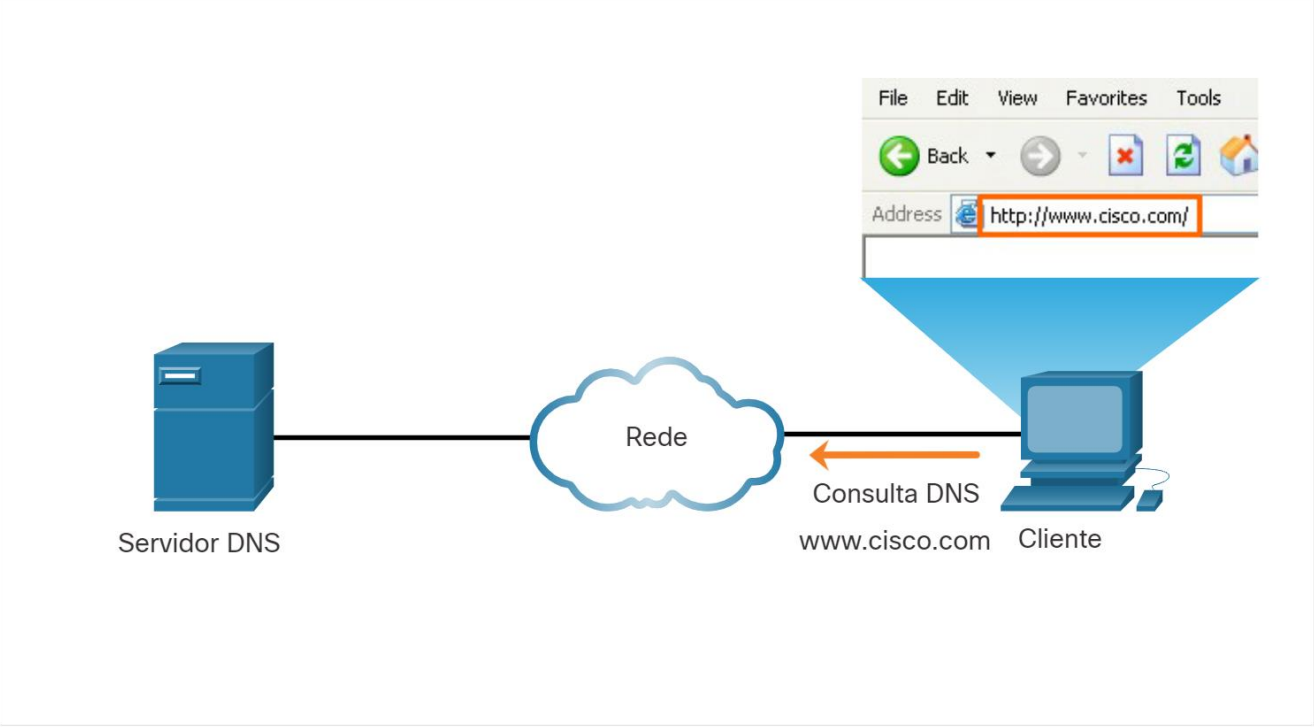
O protocolo DNS define um serviço automatizado que compara nomes de recursos com o endereço de rede numérico requisitado. Ele inclui o formato para consultas, respostas e dados. As comunicações do protocolo DNS utilizam um único formato, chamado de mensagem. Este formato de mensagem é utilizado para todos os tipos de consultas de cliente e respostas de servidor, mensagens de erro e transferência de informações de registro de recursos entre servidores.

Etapa 1

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

Etapa 2

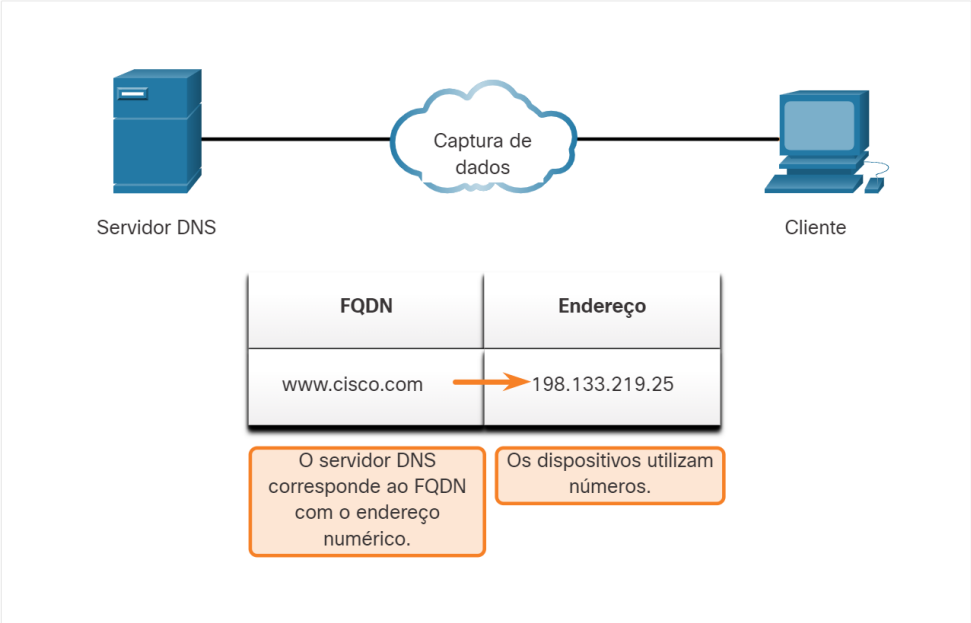
Uma consulta DNS é enviada para o servidor DNS designado para o computador cliente.



O servidor DNS corresponde ao FQDN com seu endereço IP.

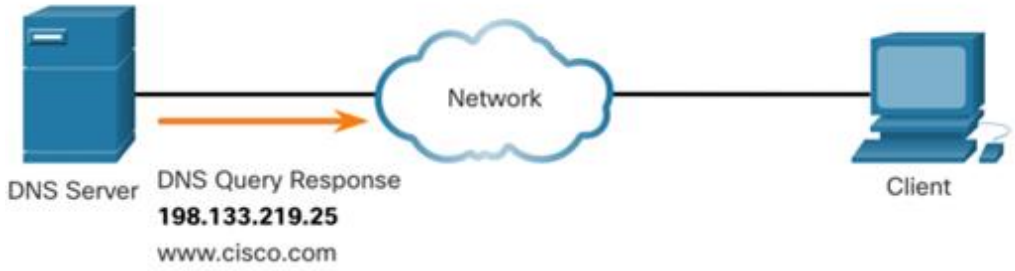
Etapa 3

O servidor DNS corresponde ao FQDN com seu endereço IP.



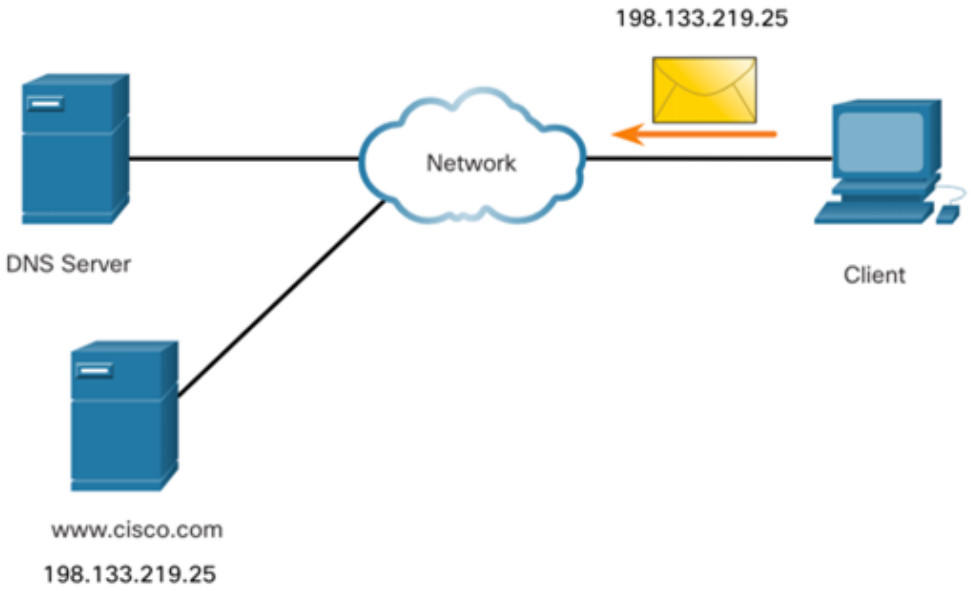
Etapa 4

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.



10.4.2 Formato de Mensagem DNS

O servidor DNS armazena diferentes tipos de registros de recursos usados \u200b\u200bpara resolver nomes. Esses registros contêm o nome, endereço e tipo de registro. Alguns desses tipos de registro são os seguintes:

- **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 primeiro examina seus próprios registros para resolver o nome. Se não conseguir resolver o nome usando seus registros armazenados, ele entrará em contato com outros servidores para resolver o nome. 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 eficiente de DNS nos PCs com Windows também armazena nomes resolvidos anteriormente na memória. O comando **ipconfig /displaydns** exibe todas as entradas DNS em cache.

Conforme mostrado na tabela, 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 cliente e respostas de servidor, mensagens de erro e transferência de informações de registro de recursos.

Seçãode mensagens DNS	Descrição
Pergunta	A pergunta para o servidor de nomes
Atender	Registros de recursos respondendo a pergunta
Autoridade	Registros de recursos apontando para uma autoridade
Adicional	Registros de recursos com informações adicionais

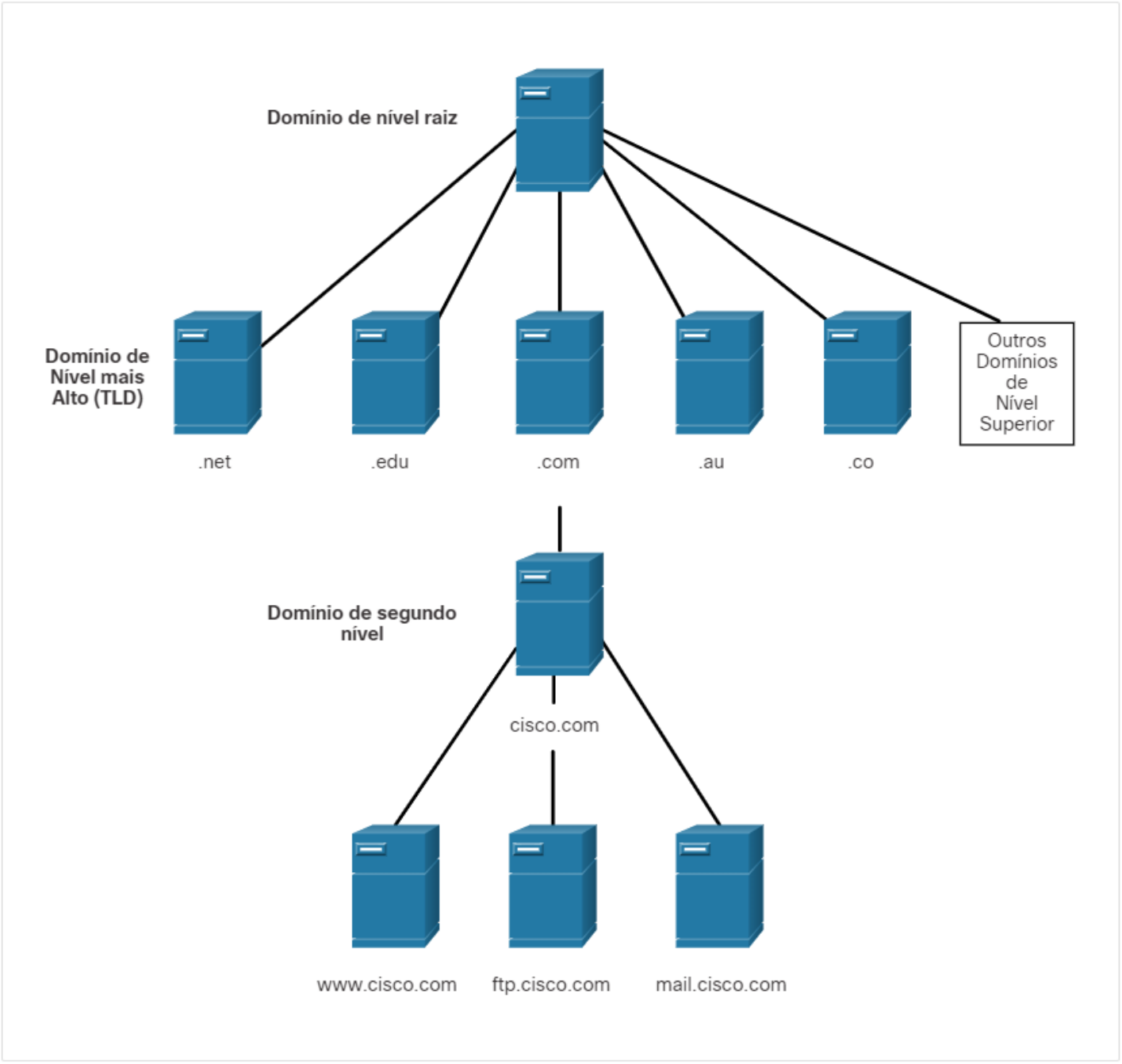
10.4.3 Hierarquia DNS

O protocolo DNS usa um sistema hierárquico para criar um banco de dados para fornecer resolução de nomes, conforme mostrado na figura. O DNS usa os nomes de domínio para formar a hierarquia.

A estrutura de nomenclatura é dividida em zonas pequenas, gerenciáveis. Cada servidor DNS mantém um arquivo de banco de dados específico e só é responsável por gerenciar os mapeamentos de nome para IP para essa pequena parte da estrutura DNS. Quando um servidor DNS recebe uma requisição para a conversão de um nome que não faça parte da sua zona DNS, o servidor DNS a encaminha para outro servidor DNS na zona apropriada para a tradução. O DNS é escalável porque a resolução do nome do host está espalhada por vários servidores.

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

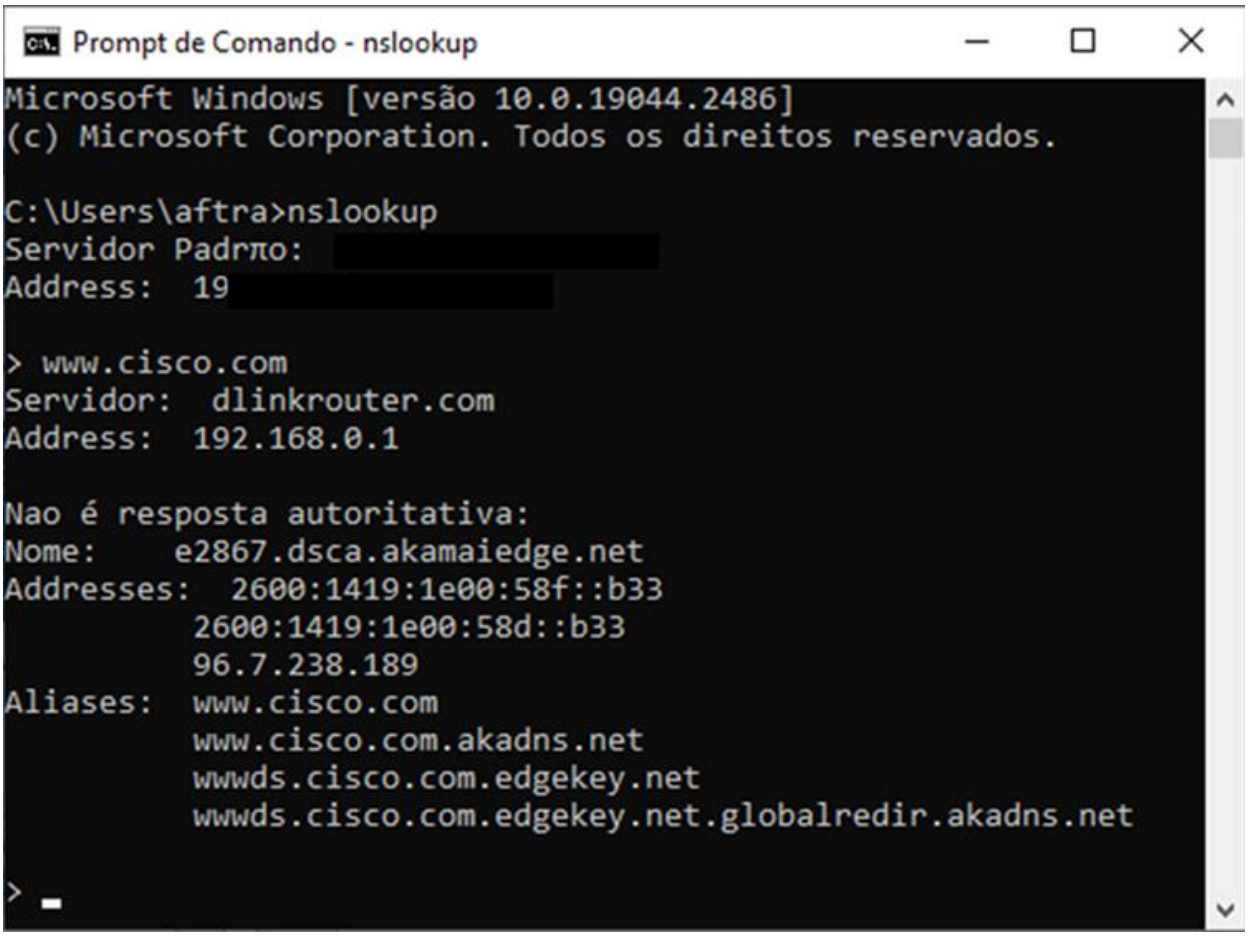


10.4.4 O Comando nslookup

Ao configurar um dispositivo de rede, um ou mais endereços de servidor DNS são fornecidos para que o cliente DNS possa usá-los na resolução de nomes. Normalmente, o ISP fornece os endereços a serem usados nos servidores DNS. Quando um aplicativo de usuário solicita a conexão a um dispositivo remoto por nome, o cliente DNS solicitante consulta o servidor de nomes para resolver o nome para um endereço numérico.

Os sistemas operacionais de computador também têm um utilitário chamado Nslookup que permite ao usuário consultar manualmente os servidores de nomes para resolver um determinado nome de host. Este utilitário também pode ser usado para corrigir problemas de resolução de nomes e verificar o status atual dos servidores de nomes.

Nesta figura, quando o comando **nslookup** é emitido, o servidor DNS padrão configurado para o seu host é exibido. O nome de um host ou domínio pode ser inserido no **nslookup** prompt. O utilitário Nslookup tem muitas opções disponíveis para testes e verificações extensivas do processo DNS.



10.4.6 Protocolo de Configuração Dinâmica de Host (DHCP)

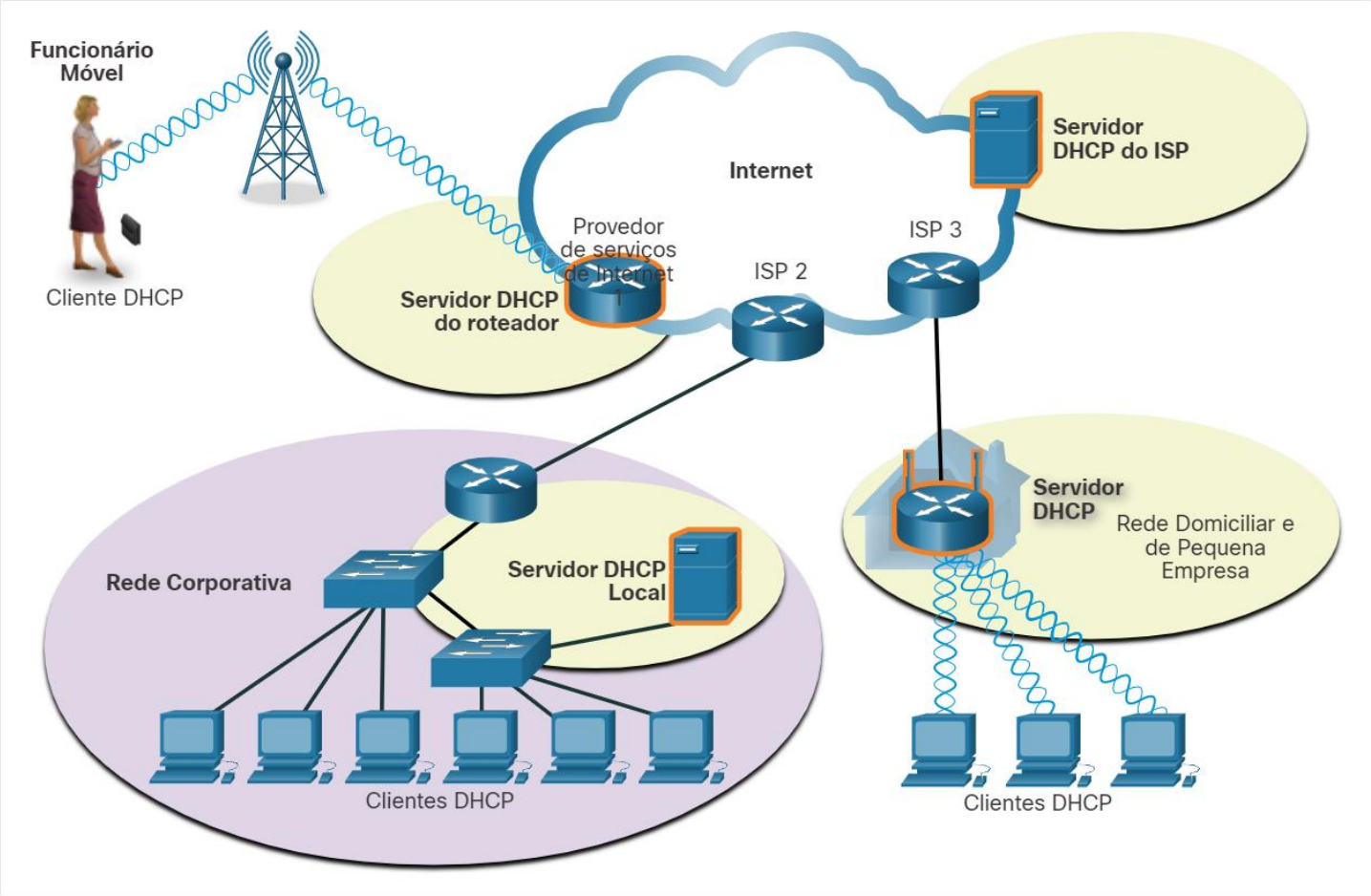
O serviço DHCP para IPv4 torna automática a atribuição de endereços IPv4, máscaras de sub-rede, gateways e outros parâmetros de rede IPv4. Isso é conhecido como o endereçamento dinâmico. A alternativa para o endereçamento dinâmico é o endereçamento estático. Ao usar o endereçamento estático, o administrador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

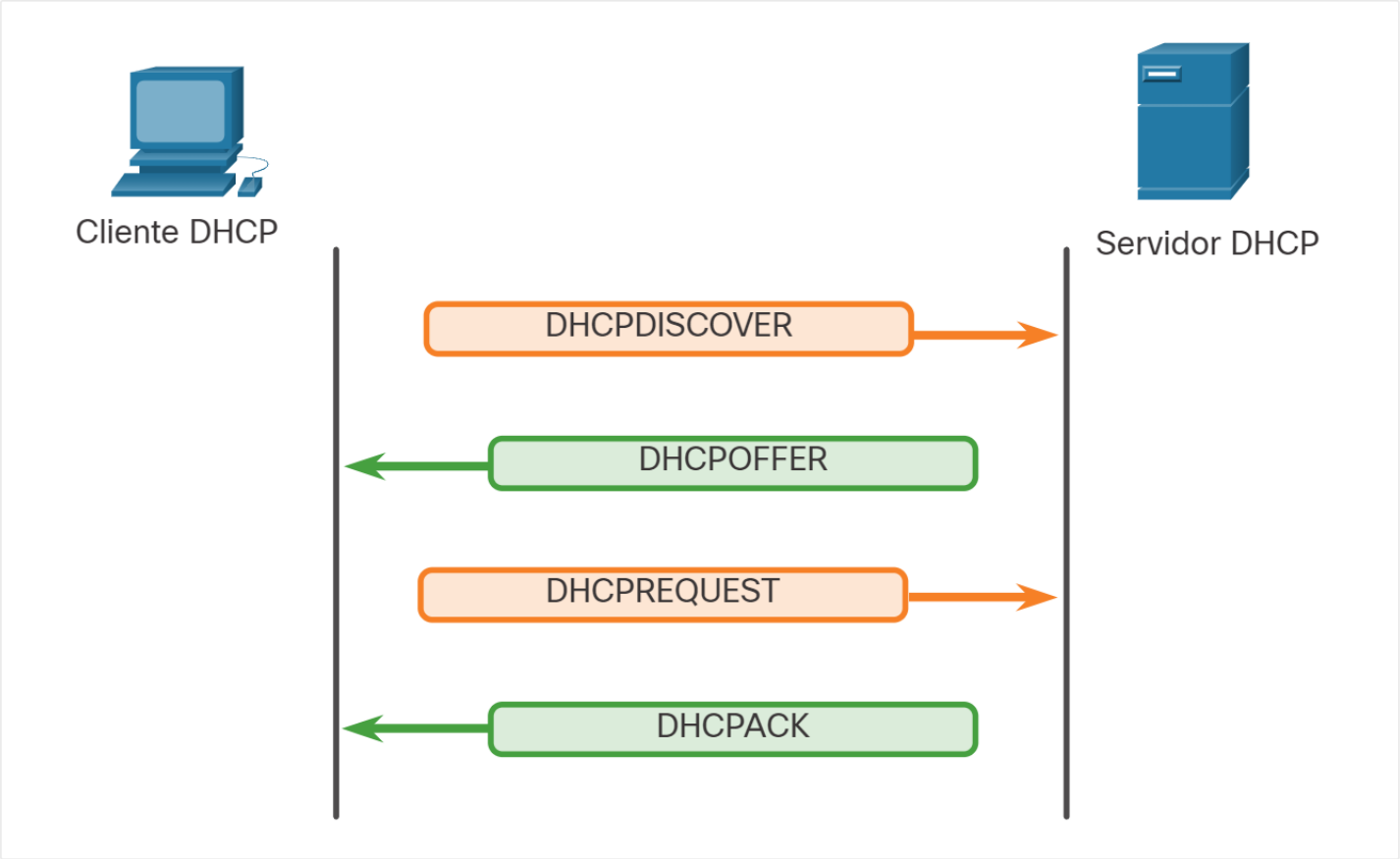


Muitas redes utilizam DHCP e endereçamento estático. O DHCP é usado para hosts de uso geral, como dispositivos de usuário final. O endereçamento estático é usado para dispositivos de rede, como roteadores de gateway, comutadores, servidores e impressoras.

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.

10.4.7 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.

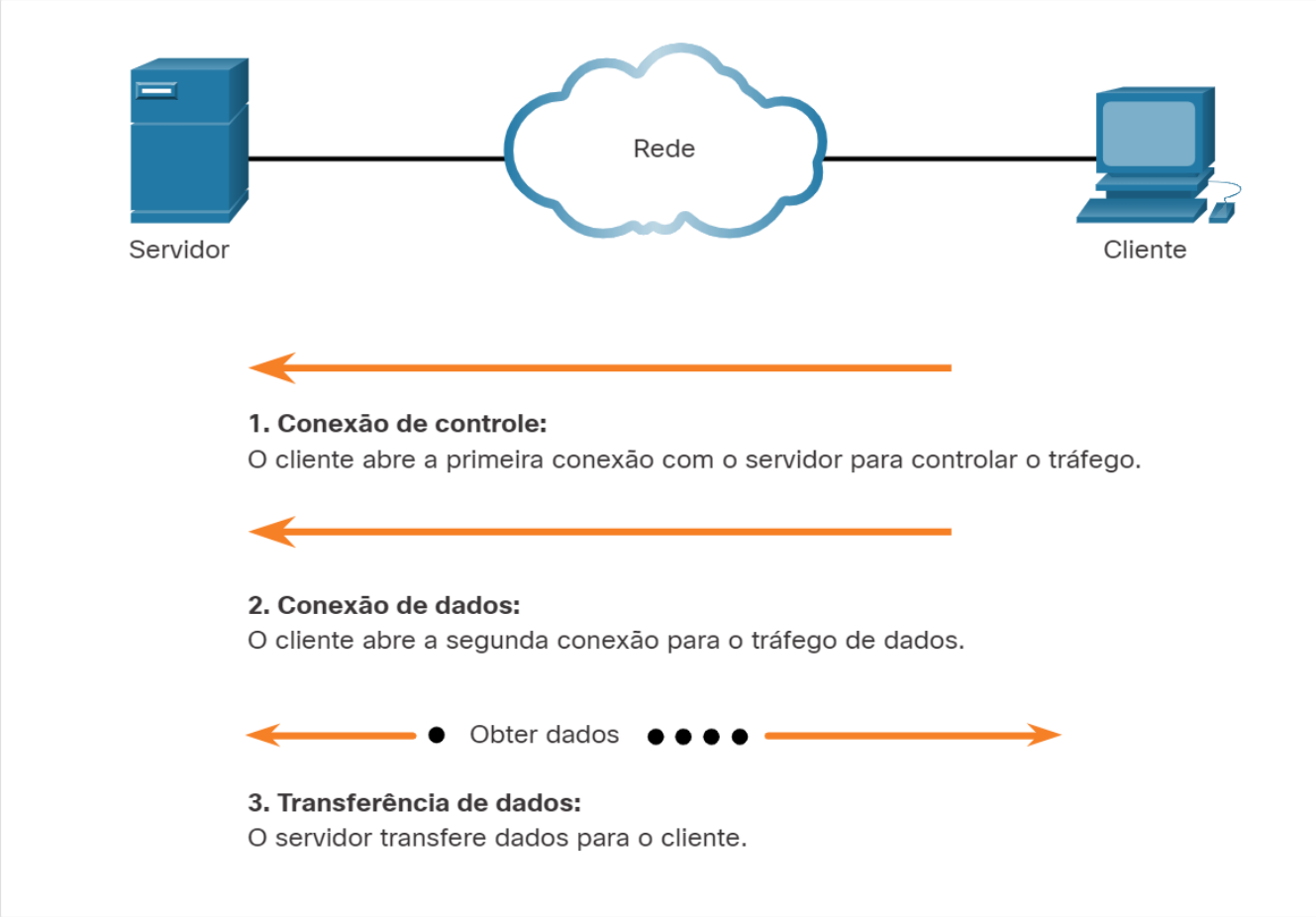
O DHCPv6 possui um conjunto de mensagens semelhantes às do DHCPv4. As mensagens DHCPv6 são SOLICIT, ADVERTISE, INFORMATION REQUEST, e REPLY.

10.5 Serviços de Compartilhamento de Arquivos

10.5.1 Protocolo FTP

Como você aprendeu em tópicos anteriores, no modelo cliente/servidor, o cliente pode carregar dados para um servidor e baixar dados de um servidor, se ambos os dispositivos estiverem usando um protocolo de transferência de arquivos (FTP). Como HTTP, e-mail e protocolos de endereçamento, FTP é comumente usado protocolo de camada de aplicativo. Este tópico aborda o FTP com mais detalhes.

O FTP foi desenvolvido para possibilitar transferências de arquivos entre um cliente e um servidor. Um cliente FTP é um aplicativo que é executado em um computador que está sendo usado para enviar e receber dados de um servidor FTP.



O cliente estabelece a primeira conexão com o servidor para o tráfego de controle usando a porta TCP 21. O tráfego consiste em comandos do cliente e respostas do servidor.

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.

10.5.2 Protocolo SMB

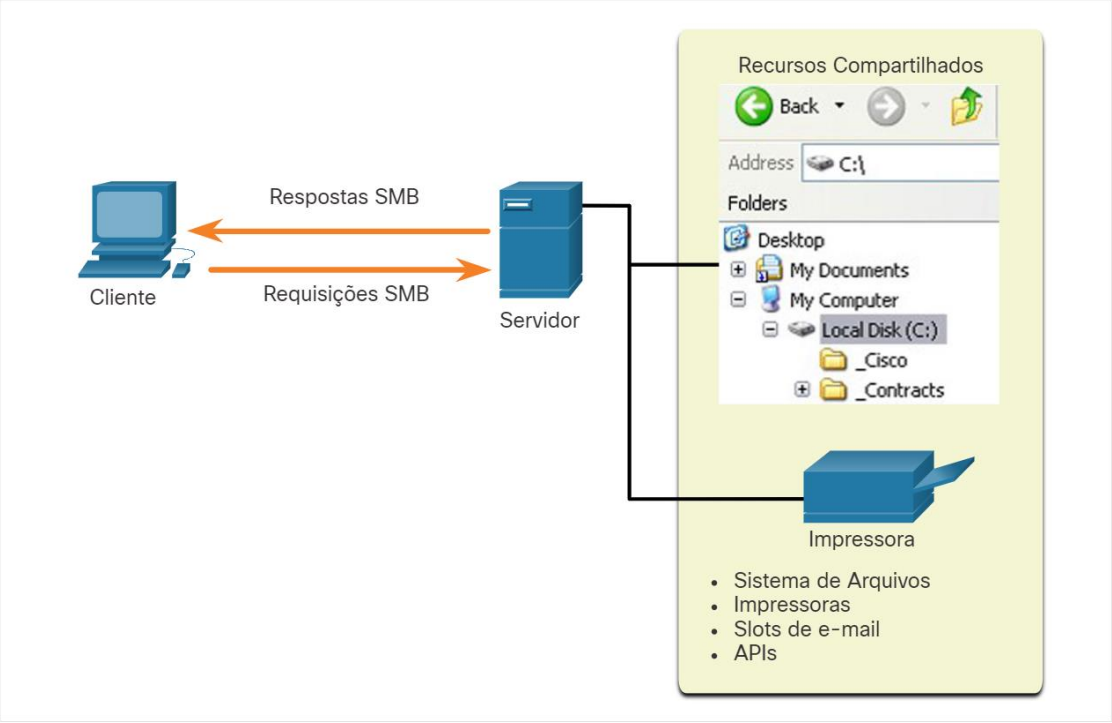
O Server Message Block (SMB) é um protocolo de compartilhamento de arquivos cliente/servidor, que descreve a estrutura de recursos de rede compartilhados, como diretórios, arquivos, impressoras e portas seriais. É um protocolo de requisição/resposta. Todas as mensagens SMB têm um formato em comum. Esse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

Aqui estão três funções de mensagens SMB:

- Iniciar, autenticar e encerrar sessões.Iniciar, autenticar e encerrar sessões.
- Arquivo de controle e acesso à impressora.
- Permitir que um aplicativo envie ou receba mensagens para ou de outro dispositivo.

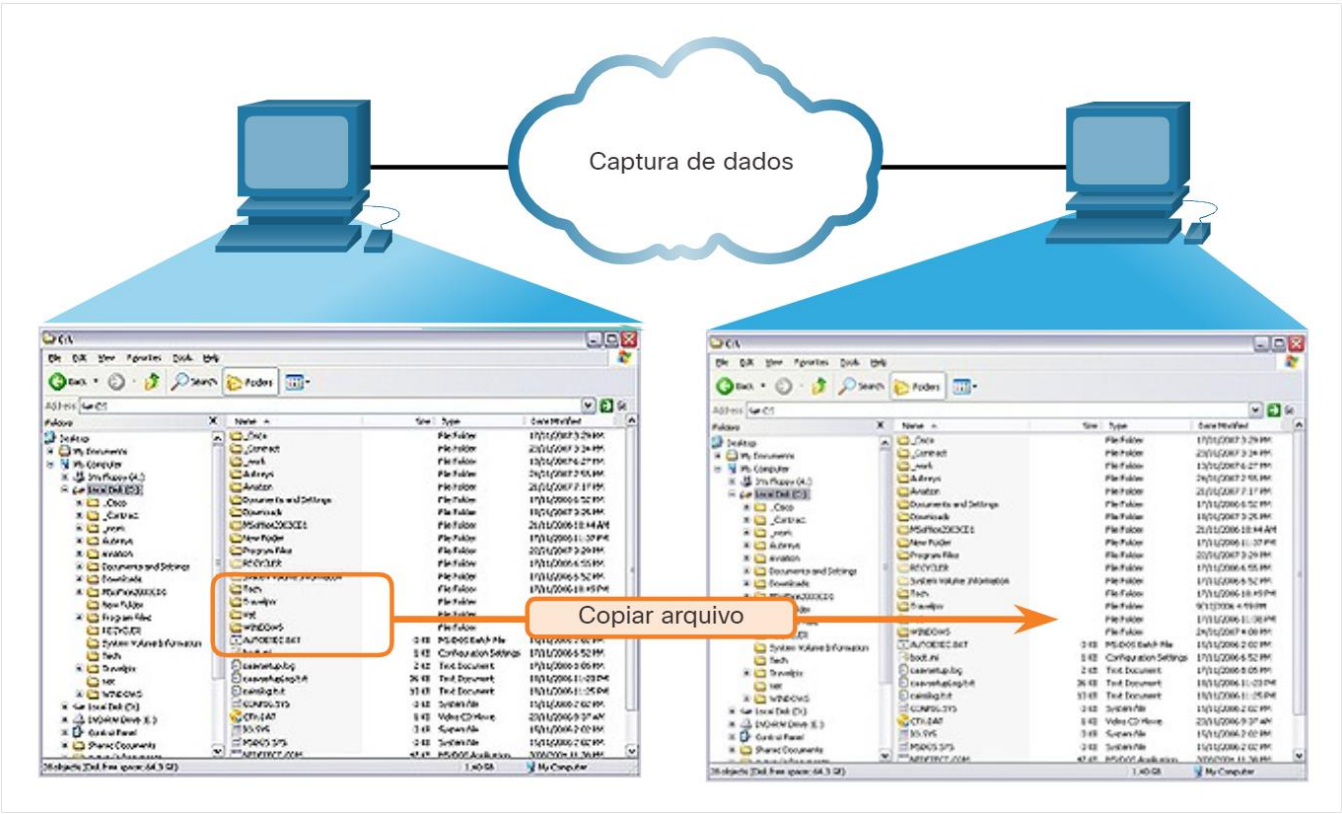
Os serviços de compartilhamento de arquivos e impressão do SMB se tornaram o sustentáculo das redes Microsoft. Com a introdução da série de software Windows 2000, a Microsoft mudou a estrutura subjacente para uso do SMB. Nas versões anteriores de produtos Microsoft, os serviços SMB utilizavam um protocolo não TCP/IP para implementar a

resolução de nomes. A partir do Windows 2000, todos os produtos Microsoft subsequentes usam a nomeação DNS, que permite que os protocolos TCP / IP suportem diretamente o compartilhamento de recursos SMB, conforme mostrado na figura.



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

O processo de troca de arquivos SMB entre PCs com Windows é mostrado na próxima figura.



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

Diferentemente do compartilhamento de arquivos permitido pelo FTP, os clientes estabelecem uma conexão de longo prazo com os servidores. Depois que a conexão é estabelecida, o usuário do cliente pode acessar os recursos no servidor como se o recurso fosse local para o host do cliente.

Os sistemas operacionais LINUX e UNIX também fornecem um método de compartilhamento de recursos com redes Microsoft usando uma versão do SMB chamada SAMBA. Os sistemas operacionais Apple Macintosh também oferecem suporte ao compartilhamento de recursos usando o protocolo SMB.

10.6 - O que eu aprendi neste módulo?

Aplicação, Apresentação e Sessão

Nos modelos OSI e TCP / IP, a camada de aplicativo é a camada mais próxima do usuário final. Os protocolos da camada de aplicação são utilizados para troca de dados entre programas executados nos hosts de origem e destino. A camada de apresentação tem três funções principais: formatação ou apresentação de dados no dispositivo de origem em um formulário compatível para recebimento pelo dispositivo de destino, compactação de dados de uma maneira que pode ser descompactado pelo dispositivo de destino e criptografar dados para transmissão e descriptografia de dados após o recebimento . A camada de sessão cria e mantém diálogos entre as aplicações origem e destino. A camada de sessão processa a troca de informações para iniciar diálogos, mantê-los ativos e reiniciar sessões interrompidas ou ociosas por um longo período. Os protocolos da camada de aplicativos TCP / IP especificam o formato e as informações de controle necessárias para muitas funções comuns de comunicação da Internet. Esses protocolos são usados pelos dispositivos de origem e de destino durante uma sessão. Os protocolos implementados no host de origem e de destino devem ser compatíveis.

Ponto a Ponto

No modelo cliente / servidor, o dispositivo que solicita as informações é chamado de cliente e o dispositivo que responde à solicitação é chamado de servidor. O cliente começa a troca ao requisitar dados do servidor, que responde enviando uma ou mais sequências de dados ao cliente. Em uma rede P2P, dois ou mais computadores estão conectados via rede e podem compartilhar recursos sem ter um servidor dedicado. Todos os pares podem funcionar como servidor e cliente. Um computador pode assumir o papel de servidor para uma transação ao mesmo tempo em que é o cliente de outra. Aplicações P2P exigem que cada dispositivo final forneça uma interface de usuário e execute um serviço em segundo plano. Algumas aplicações P2P utilizam um sistema híbrido no qual o compartilhamento de recursos é descentralizado, mas os índices que apontam para as localizações de recursos são armazenados em um diretório centralizado. Muitos aplicativos P2P permitem que os usuários compartilhem partes de arquivos ao mesmo tempo. Clientes usam um arquivo pequeno chamado torrent para localizar outros usuários que possuam as partes dos arquivos de que precisam para que possam se conectar diretamente com eles. Este arquivo também contém informações sobre os computadores rastreadores que controlam quais usuários têm quais partes de quais arquivos.

Protocolos da Web e de email

Quando um endereço ou URL da Web é digitado em um navegador, ele estabelece uma conexão com o serviço da Web. O serviço Web está em execução no servidor que está a utilizar o protocolo HTTP. O HTTP especifica um protocolo de requisição/resposta. Quando um cliente, normalmente um navegador Web, envia uma requisição a um servidor Web, é o HTTP quem especifica os tipos de mensagem usados nessa conversação. Os três tipos de mensagens comuns são GET, POST e PUT. Para comunicação segura na Internet, o HTTPS usa o mesmo processo de resposta do servidor de solicitações do cliente que o HTTP, mas o fluxo de dados é criptografado com SSL antes de ser transportado pela rede. O e-mail suporta três protocolos separados para operação: SMTP, POP e IMAP. O processo da camada de aplicação que envia e-mail usa o SMTP. Um cliente recupera e-mails usando POP ou IMAP. 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. O POP é usado por uma aplicação para recuperar e-mails de um servidor de e-mail. Com o POP, o e-mail será transferido do servidor ao cliente e excluído do servidor. Com o IMAP, diferentemente do POP, quando o usuário se conecta a um servidor compatível com IMAP, as cópias das mensagens são baixadas no aplicativo cliente. As mensagens originais são mantidas no servidor até que sejam excluídas manualmente.

Serviços de endereçamento IP

O protocolo DNS corresponde aos nomes dos recursos com o endereço de rede numérico necessário. As comunicações do protocolo DNS usam um formato de mensagem para todos os tipos de consultas de clientes e respostas do servidor, mensagens de erro e a transferência de informações do registro de recursos entre servidores. O DNS usa nomes de domínio para formar uma hierarquia. Cada servidor DNS mantém um arquivo de banco de dados específico e só é responsável por gerenciar os mapeamentos de nome para IP para essa pequena parte da estrutura DNS. Os SOs de computador usam o Nslookup para permitir que o usuário consulte manualmente os servidores de nomes para resolver um determinado nome de host. O serviço DHCP para IPv4 automatiza a atribuição de endereços IPv4, máscaras de sub-rede, gateways e outros parâmetros de rede IPv4. O DHCPv6 fornece serviços semelhantes para clientes IPv6, exceto que ele não fornece um endereço de gateway padrão. Quando um dispositivo configurado para DHCP IPv4 é inicializado ou conectado 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 DHCPv6 possui um conjunto de mensagens semelhantes às do DHCPv4. As mensagens DHCPv6 são SOLICIT, ADVERTISE, INFORMATION REQUEST, e REPLY.

Serviços de compartilhamento de arquivos

Um cliente FTP é um aplicativo que é executado em um computador que está sendo usado para enviar e receber dados de um servidor FTP. O cliente estabelece a primeira conexão com o servidor para o tráfego de controle usando a porta TCP 21. O cliente estabelece a segunda conexão com o servidor para transferência de dados propriamente dita, usando a porta TCP 20. O cliente pode baixar dados do servidor ou o cliente pode fazer upload (enviar) de dados para o servidor. Aqui estão três funções de mensagens SMB: 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. Diferentemente do compartilhamento de arquivos permitido pelo FTP, os clientes estabelecem uma conexão de longo prazo com os servidores. Após a conexão ser estabelecida, o usuário do cliente pode acessar os recursos no servidor como se o recurso fosse local ao host do cliente.