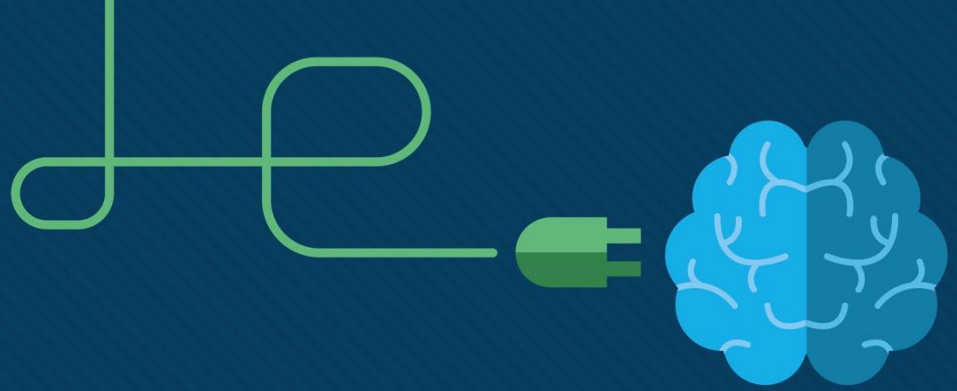


Módulo 14: Camada de Transporte

Versão original: Cisco Network Academy
Versão modificada: Eduardo Costa

Introdução às redes v7.0 (ITN)

Objetivos do módulo

Título do módulo: Camada de transporte

Objetivo do módulo: comparar as operações dos protocolos da camada de transporte no suporte à comunicação extremo a extremo.

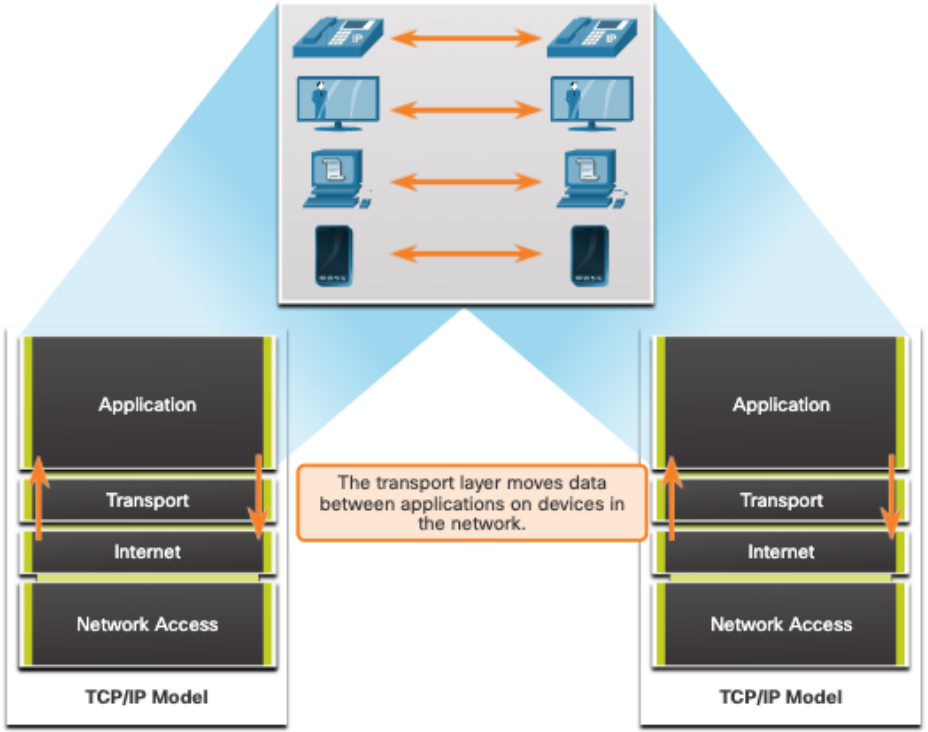
Título do Tópico	Objetivo do Tópico
Transporte de dados	Explicar a função da camada de transporte na gestão do transporte de dados na comunicação extremo a extremo.
Visão Geral do TCP	Explicar as características do TCP.
Visão Geral do UDP	Explicar as características da UDP.
Números de porto	Explicar como TCP e UDP usam os números de porto.
Processo de comunicação TCP	Explicar como os processos de estabelecimento e encerramento de sessão TCP tornam a comunicação confiável.
Confiabilidade e controle de fluxo	Explicar como as unidades de dados de protocolo TCP são transmitidas e confirmadas para garantir a entrega.
Comunicação UDP	Comparar as operações de protocolos de camada de transporte no suporte da comunicação extremo a extremo.

14.1 - Transporte de dados

Propósito de camada de transporte

A camada de transporte é:

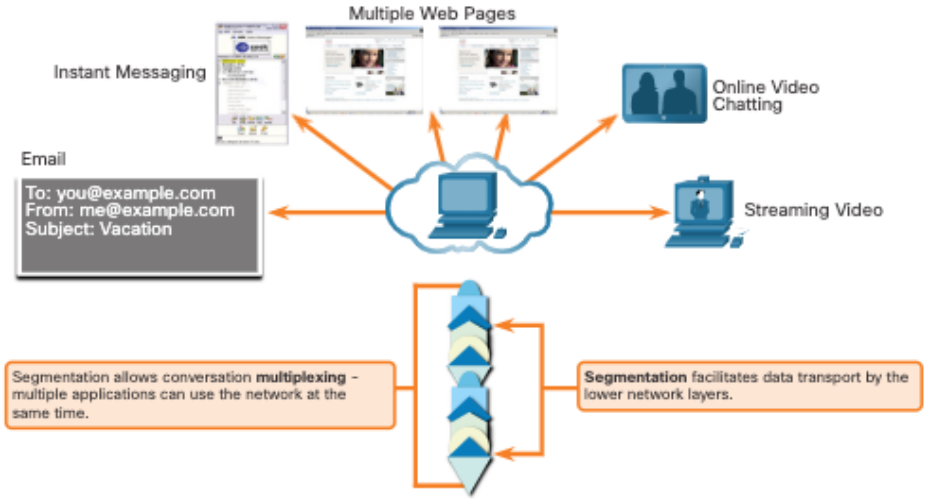
- Responsável pela comunicação lógica entre aplicações executados em hosts diferentes.
- A ligação entre a camada de aplicação e as camadas inferiores responsáveis pela transmissão da rede.



Responsabilidades da camada de transporte

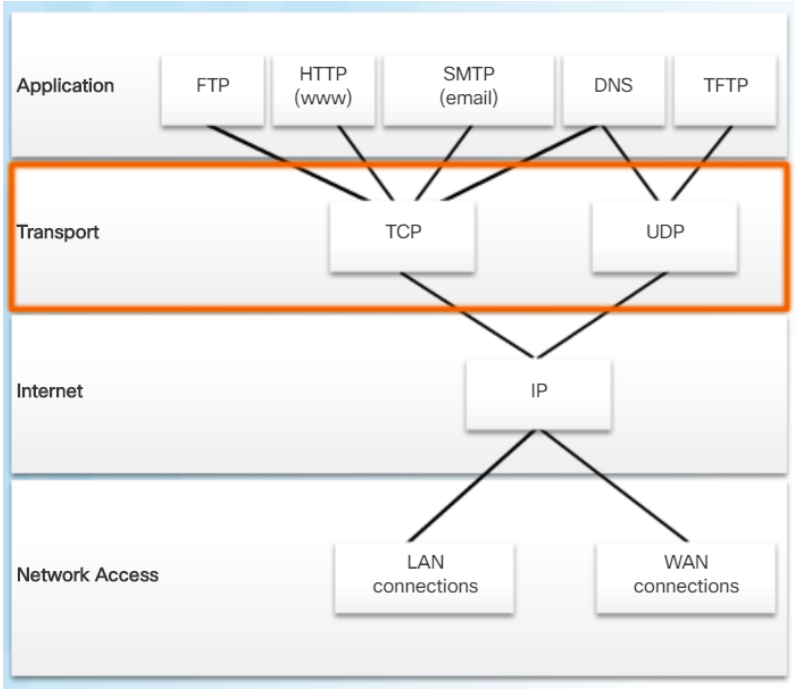
A camada de transporte tem as seguintes responsabilidades:

- Rastrear (Tracking) conversas individuais
- Segmentar dados e remontar os segmentos
- Adicionar informações de cabeçalho
- Identificar, separar e gerir várias conversas
- Usa segmentação e multiplexação para permitir que diferentes conversas de comunicação sejam intercaladas na mesma rede



Protocolos de camada de transporte

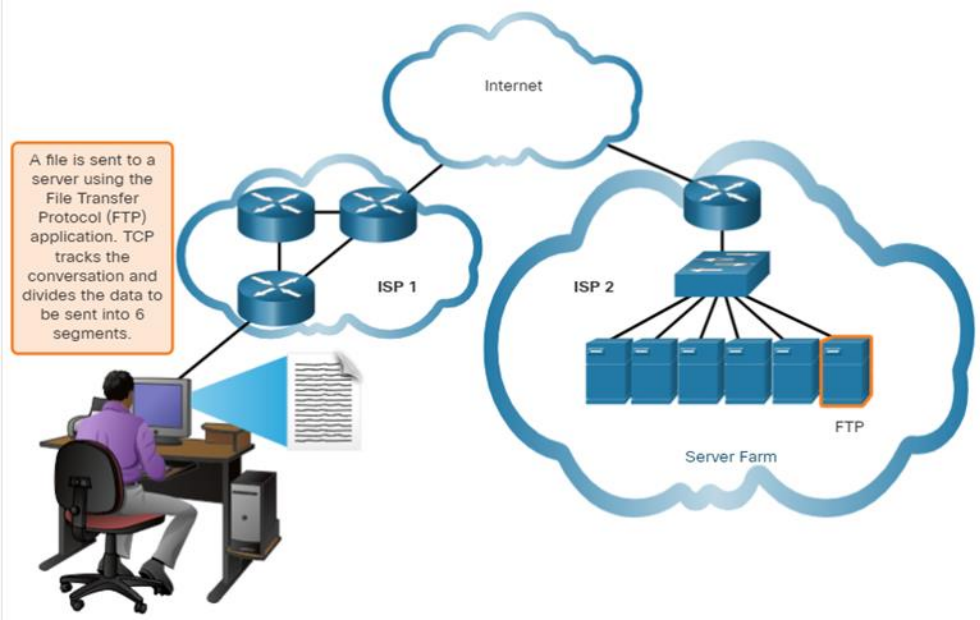
- O IP não especifica como ocorre a entrega ou o transporte de pacotes.
- Os protocolos da camada de transporte especificam como transferir mensagens entre hosts e são responsáveis pela gestão dos requisitos de fiabilidade de uma conversa.
- A camada de transporte inclui os protocolos TCP e UDP.



TCP (Transmission Control Protocol)

O TCP fornece fiabilidade e controle de fluxo. O funcionamento básico do TCP:

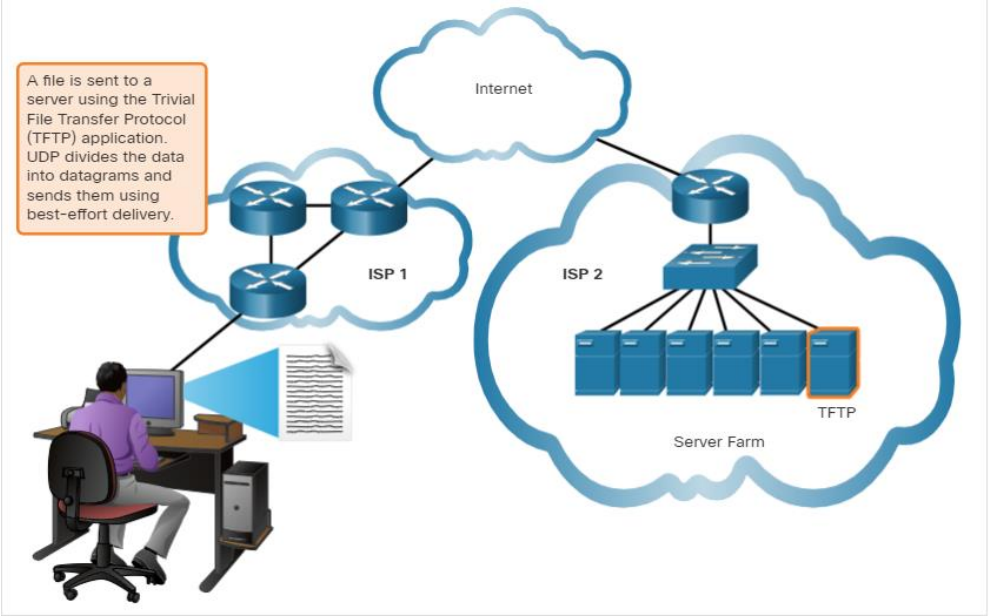
- Numera e rastreia os segmentos de dados transmitidos para um host específico a partir de uma aplicação específica
- Confirma os dados recebidos
- Retransmite quaisquer dados não confirmados após um certo período de tempo
- Ordena os dados que podem chegar pela ordem errada
- Envia dados a uma taxa eficiente que seja aceitável pelo receptor



UDP (User Datagram Protocol)

O UDP fornece as funções básicas para entrega dos datagramas entre as aplicações apropriadas, com muito pouca sobrecarga e verificação de dados.

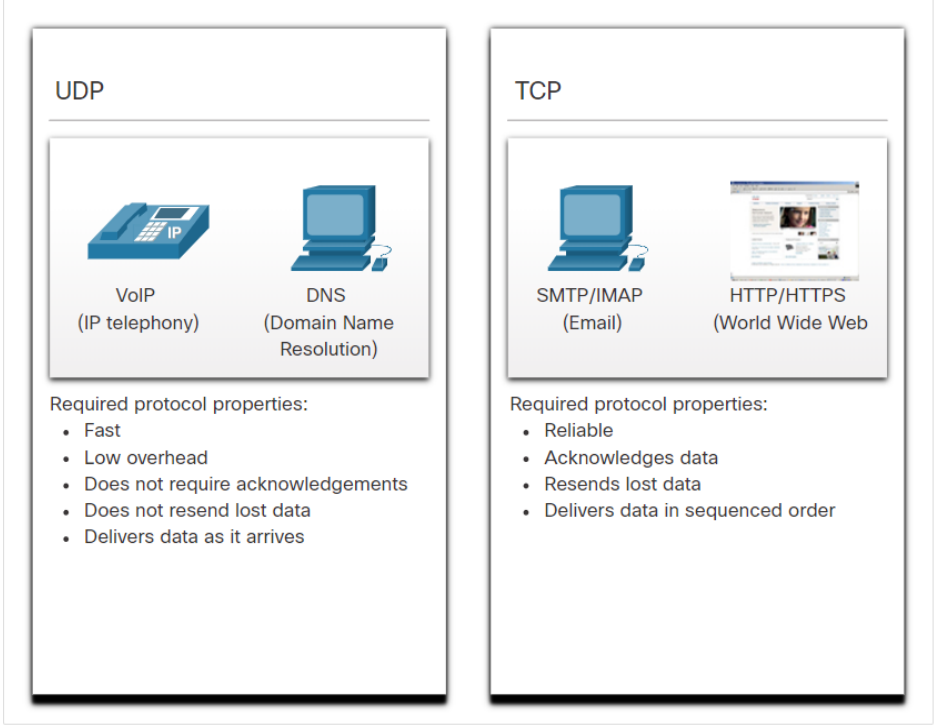
- UDP é um protocolo sem ligação (connectionless).
- O UDP é conhecido como um protocolo de entrega de melhor esforço porque não há confirmação de que os dados são recebidos no destino.



O protocolo de camada de transporte certo para a aplicação certa

O UDP também é usado por aplicações de solicitação e resposta (request-and-reply) onde os dados são mínimos, e a retransmissão pode ser feita rapidamente.

O TCP é usado como protocolo de transporte se for importante que todos os dados cheguem e que possam ser processados em sua sequência correta.



14.2 Visão geral do TCP

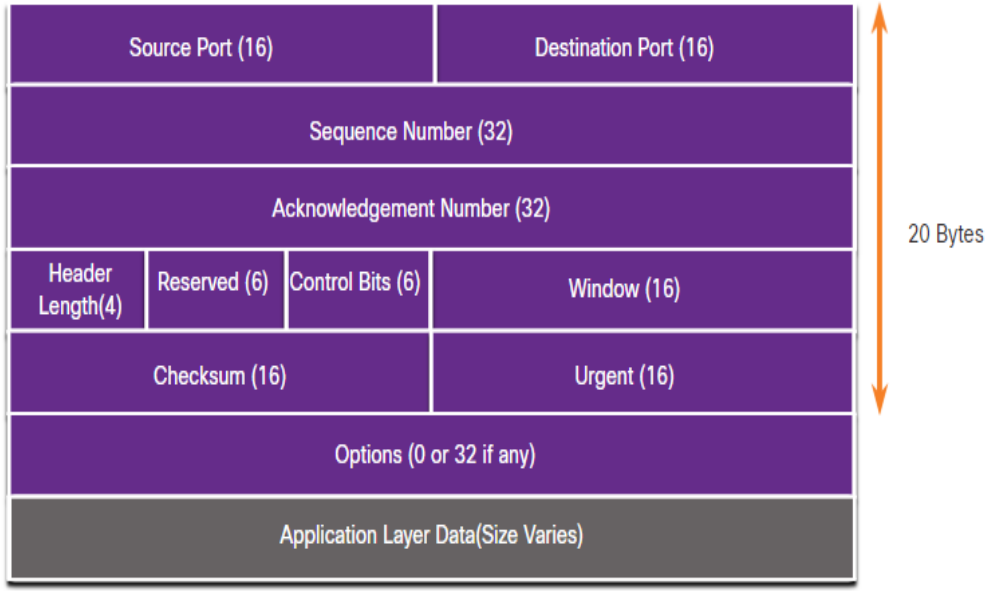
Características do TCP

- **Estabelece uma sessão -** O TCP é um protocolo orientado à ligação que negocia e estabelece uma ligação (ou sessão) permanente entre os dispositivos de origem e de destino antes de encaminhar qualquer tráfego.
- **Garante a entrega fiável -** Por várias razões, é possível que um segmento seja corrompido ou perdido completamente, pois é transmitido pela rede. O TCP garante que cada segmento enviado pela fonte chegue ao destino.
- **Fornece entrega na mesma ordem -** Como as redes podem fornecer várias rotas que podem ter taxas de transmissão diferentes, os dados podem chegar fora de ordem.
- **Suporta o controlo de fluxo -** os hosts de rede têm recursos limitados (ou seja, memória e poder de processamento). Quando percebe que esses recursos estão sobrecarregados, o TCP pode requisitar que a aplicação emissora reduza a taxa de fluxo de dados.

Cabeçalho do TCP

TCP é um protocolo stateful, o que significa que ele controla o estado da sessão de comunicação.

O TCP regista que informações foram enviadas e quais foram confirmadas.

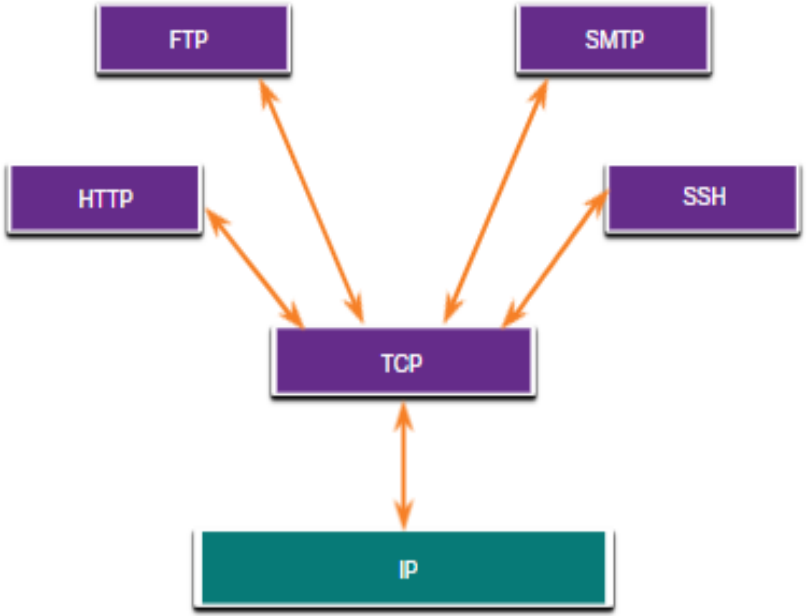


Campos de Cabeçalho TCP

Campo de cabeçalho TCP	Descrição
Porto de origem	Um campo de 16 bits usado para identificar a aplicação de origem por número de porto.
Porto de destino	Um campo de 16 bits usado para identificar a aplicação de destino por número de porto.
Número de Sequência	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 qual o próximo byte esperado da origem.
Tamanho do cabeçalho	Um campo de 4 bits conhecido como “offset de dados” que indica o comprimento do cabeçalho de segmento TCP.
Reservado	Um campo de 6 bits que é 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.
Tamanho da janela	Um campo de 16 bits usado para indicar o número de bytes que podem ser aceitos ao mesmo tempo.
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.

Aplicações que usam TCP

O TCP lida com todas as tarefas associadas à divisão do fluxo de dados em segmentos, fornecendo fiabilidade, controlando o fluxo de dados e reordenando segmentos.



14.3 - Visão geral do UDP

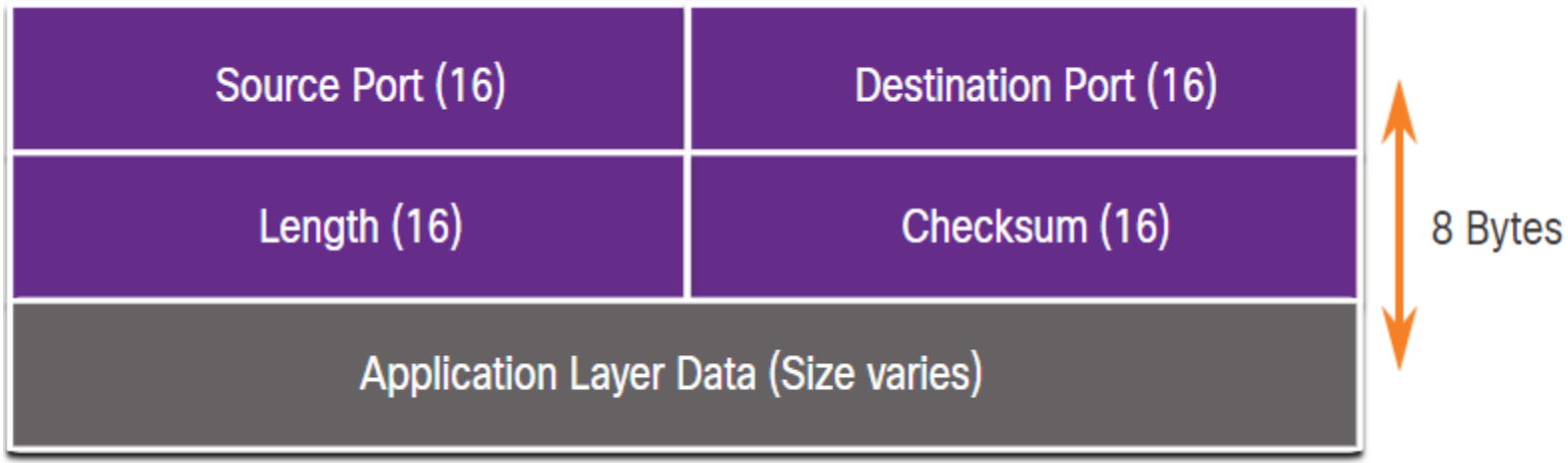
Características do UDP

As características do UDP incluem o seguinte:

- Os dados são reagrupados na ordem em que são recebidos.
- Quaisquer segmentos perdidos não são reenviados.
- Não há estabelecimento de sessão.
- O emissor não é informado sobre a disponibilidade do recurso.

Cabeçalho do UDP

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).



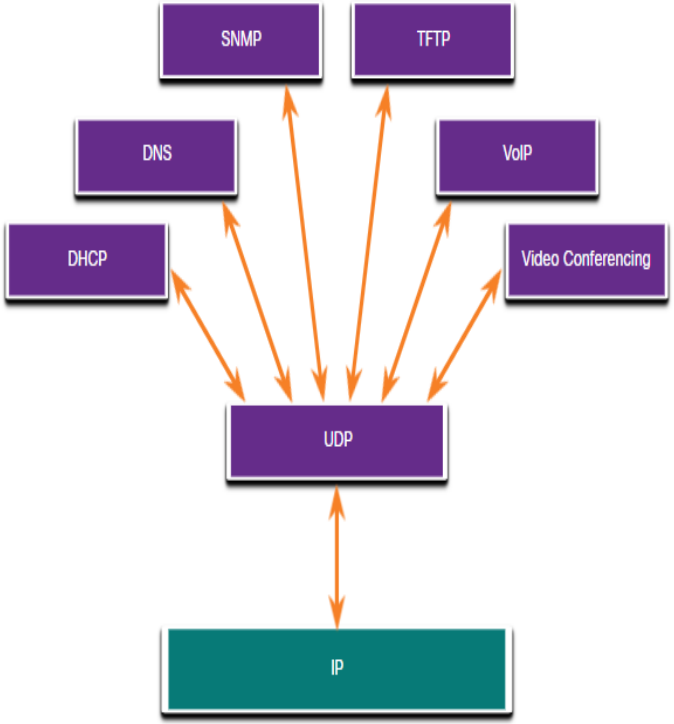
Campos do Cabeçalho UDP

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

Campo de Cabeçalho UDP	Descrição
Porto de origem	Um campo de 16 bits usado para identificar a aplicação de origem por número de porto.
Porto de destino	Um campo de 16 bits usado para identificar a aplicação de destino pelo número da porto.
Duração	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.

Aplicações que usam UDP

- Aplicações de vídeo ao vivo e multimídia - Essas aplicações podem tolerar a perda de alguns dados, mas exigem pouco ou nenhum atraso. Os exemplos incluem VoIP e transmissão de vídeo ao vivo.
- Aplicações de solicitação e resposta simples - Aplicações com transações simples em que um host envia uma solicitação e pode ou não receber uma resposta. Os exemplos incluem DNS e DHCP.
- Aplicações que lidam elas mesmas com a fiabilidade - Comunicações unidirecionais onde o controle de fluxo, detecção de erros, confirmações, e recuperação de erros não são necessárias ou podem ser executadas pela aplicação. Os exemplos incluem SNMP e TFTP.



14.4 Números de Porto

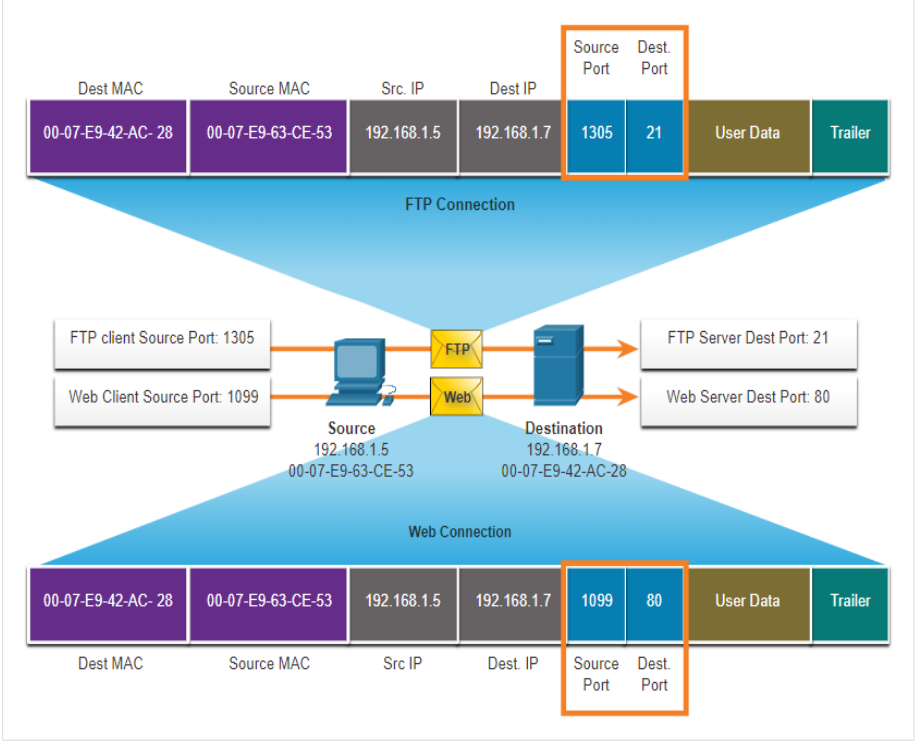
Várias comunicações separadas

Os protocolos de camada de transporte TCP e UDP usam números de porto para gerir várias conversas simultâneas.

O número da porto de origem está associado à aplicação de origem no host local, enquanto o número da porto de destino está associado à aplicação de destino no host remoto.

Pares de soquetes (Sockets Pairs)

- Os números dos portos origem e destino são colocadas no segmento.
- Os segmentos são encapsulados num pacote IP.
- A combinação do endereço IP de origem e o número de porto de origem, ou do endereço IP de destino e o número de porto de destino é conhecido como um socket.
- Os sockets permitem que vários processos em execução num cliente se diferenciem uns dos outros, e várias conexões com um processo no servidor sejam diferentes umas das outras.



Grupos de Números de Porto

Grupo de Portos	Intervalo de números	Descrição
Portos bem conhecidas	**0 a 1023**	• Números de porto reservados para serviços e aplicações comuns ou populares, como navegadores web, clientes de email e clientes de acesso remoto. •Portos bem conhecidos associados a aplicações comuns nos servidores, permitem que os clientes identifiquem facilmente o serviço associado necessário.
Portos registados	**1.024 a 49.151**	•Estes números de porto são atribuídos pela IANA a uma entidade solicitante para uso com processos ou aplicações específicas. •Estes processos são principalmente aplicações que o utilizador optou por instalar , e não aplicações comuns que receberiam um número de porto bem conhecido. •Por exemplo, a Cisco registou o porto 1812 para o processo de autenticação do servidor RADIUS.
Portos dinâmicos e/ou **privados**	**49.152 a 65.535**	•Estes portos também são conhecidos como *portos efêmeros*. •O sistema operativo do cliente geralmente atribui números de porto dinamicamente quando uma conexão a um serviço é iniciada. •O porto dinâmico é usado para identificar a aplicação cliente durante a comunicação.

Grupos de Números de Porto (Cont.)

Números de Portos Bem Conhecidos

Número do Porto	Protocolo	Aplicação
20	TCP	File Transfer Protocol (FTP) - Dados
21	TCP	Protocolo de transferência de arquivos (FTP) - Controle
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Protocolo SMTP
53	UDP, TCP	Protocolo DNS
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Servidor
68	UDP	Protocolo de configuração dinâmica de host - cliente
69	UDP	Protocolo de Transferência Trivial de Arquivo (TFTP)
80	TCP	Protocolo HTTP
110	TCP	Protocolo POP3 (Post Office Protocol - Protocolo dos Correios)
143	TCP	Protocolo IMAP
161	UDP	Protocolo de Gerenciamento Simples de Rede (SNMP)
443	TCP	HTTPS (Secure Hypertext Transfer Protocol - Protocolo de Transferência de Hipertexto Seguro)

O Comando netstat

Conexões TCP desconhecidas podem ser uma grade ameaça de segurança. O Netstat é uma ferramenta importante para verificar conexões.

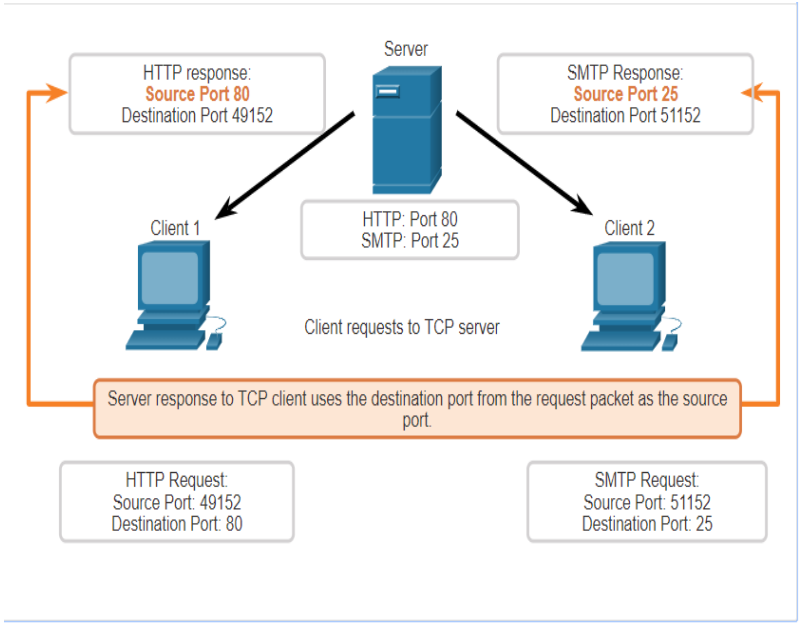
```
C:\> netstat
Conexões Ativas
Endereço Local Proto Estado do Endereço Estrangeiro
TCP 192.168.1.124:3126 192.168.0.2:netbios-ssn ESTABLISHED
TCP 192.168.1.124:3158 207.138.126.152:http ESTABLISHED
TCP 192.168.1.124:3159 207.138.126.169:http ESTABLISHED
TCP 192.168.1.124:3160 207.138.126.169:http ESTABLISHED
TCP 192.168.1.124:3161 sc.msn.com:http ESTABLISHED
TCP 192.168.1.124:3166 www.cisco.com:http ESTABLISHED
```

14.5 - Processo de comunicação TCP

Processo de servidor TCP

Cada processo de uma aplicação em execução num servidor está configurado para usar um número de porto.

- Um servidor individual não pode ter dois serviços atribuídos ao mesmo número de porta dentro dos mesmos serviços da camada de transporte.
- Uma aplicação ativa num servidor, atribuída a um porto específico é considerada aberta, o que significa que a camada de transporte aceita e processa os segmentos endereçados a esse porto.
- Qualquer solicitação de cliente que chega endereçada ao socket correto é aceita e os dados são transmitidos à aplicação do servidor.

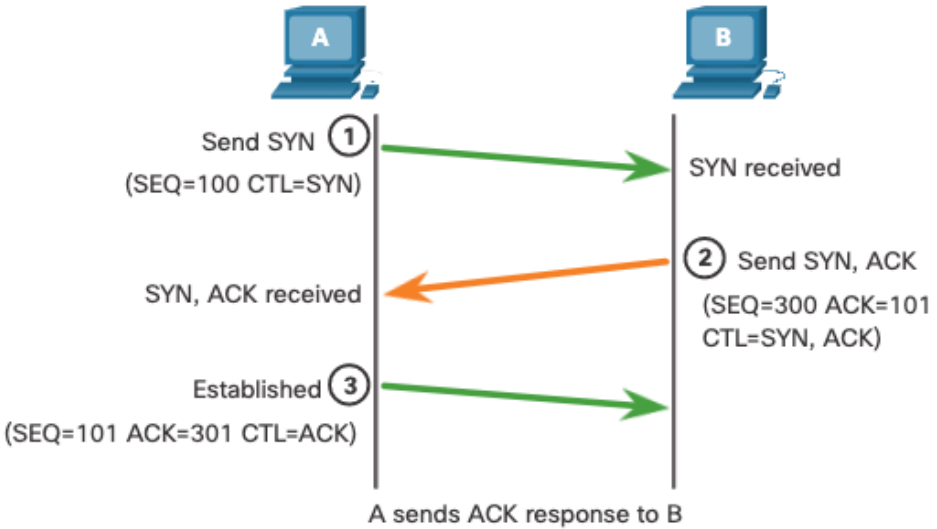


Estabelecimento da ligação TCP

Etapa 1: O cliente iniciador solicita uma sessão de comunicação cliente-servidor com o servidor.

Etapa 2: O servidor confirma a sessão de comunicação cliente-servidor e solicita uma sessão de comunicação de servidor-cliente.

Etapa 3: O cliente iniciador confirma a sessão de comunicação de servidor-cliente.



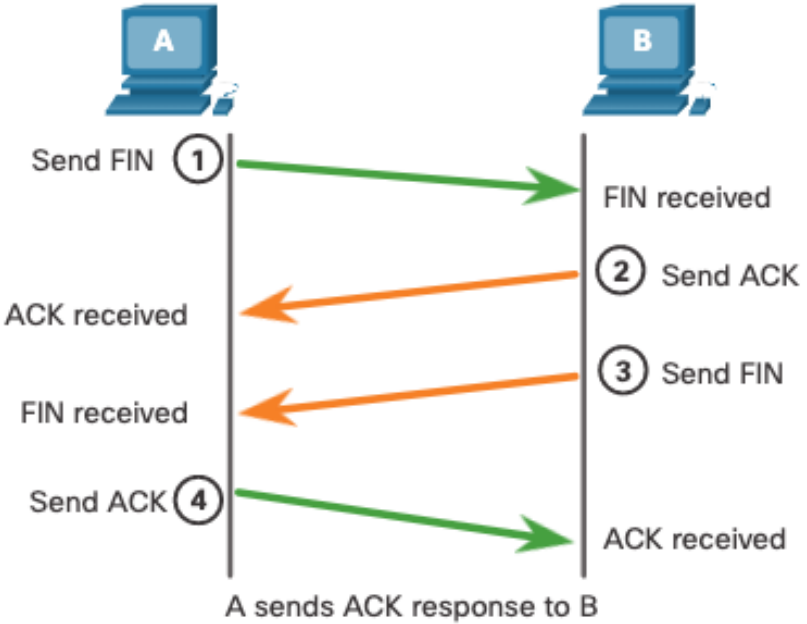
Término da sessão TCP

Etapa 1: Quando o cliente não tem mais dados para enviar no fluxo, ele envia um segmento com o sinalizador FIN ativo.

Etapa 2: O servidor envia um ACK para confirmar o recebimento do FIN para encerrar a sessão do cliente para o servidor.

Etapa 3: O servidor envia um FIN ao cliente para finalizar a sessão servidor para cliente.

Etapa 4: O cliente responde com um ACK para confirmar o FIN do servidor.



Análise do handshake triplo do TCP

As funções do handshake triplo são estas:

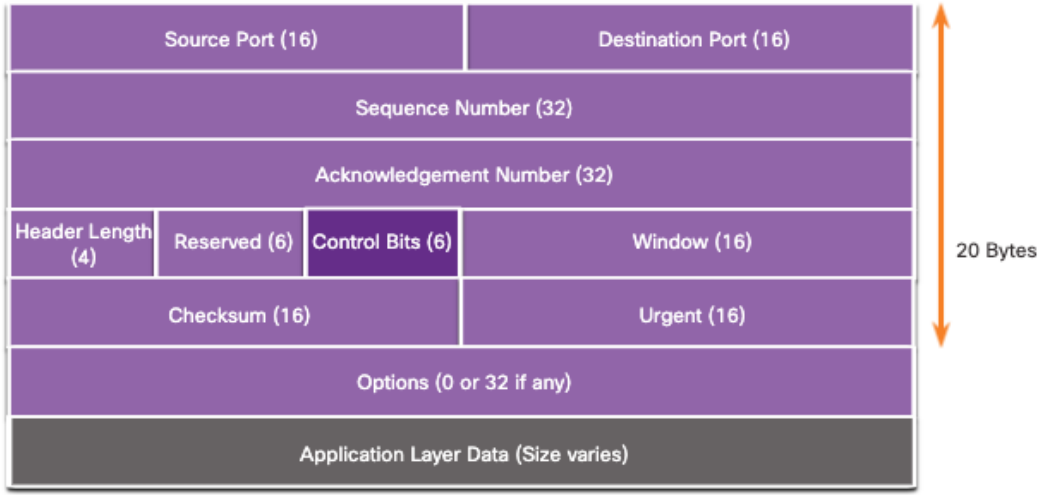
- Determina que o dispositivo de destino está presente na rede.
- Verifica se o dispositivo de destino possui um serviço ativo e está aceitando solicitações no número de porto de destino que o cliente inicial pretende usar.
- Informa o dispositivo de destino que o cliente de origem pretende estabelecer uma sessão de comunicação nesse número de porto.

Após a conclusão da comunicação, as sessões são fechadas e a ligação é terminada. Os mecanismos de ligação e sessão ativam a função de fiabilidade do TCP.

Análise do handshake triplo do TCP

Os seis sinalizadores de bit de controle são os seguintes:

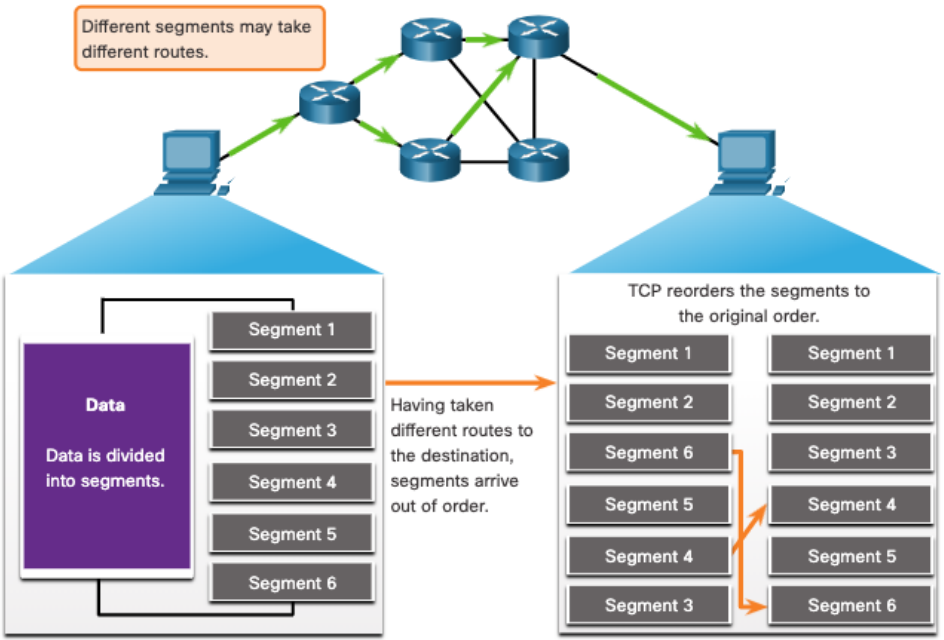
- **URG** - Campo indicador de urgência
- **ACK** - Indicador de confirmação usado no estabelecimento de ligação e término de sessão
- **PSH** - Função Push
- **RST** - Redefine a ligação quando ocorrer um erro ou tempo limite
- **SYN** - Sincronizar números de sequência usados no estabelecimento da ligação
- **FIN** - Não há mais dados do remetente e é usado no término da sessão



14.6 - Fiabilidade e controlo de fluxo

Fiabilidade do TCP – entrega ordenada e garantida

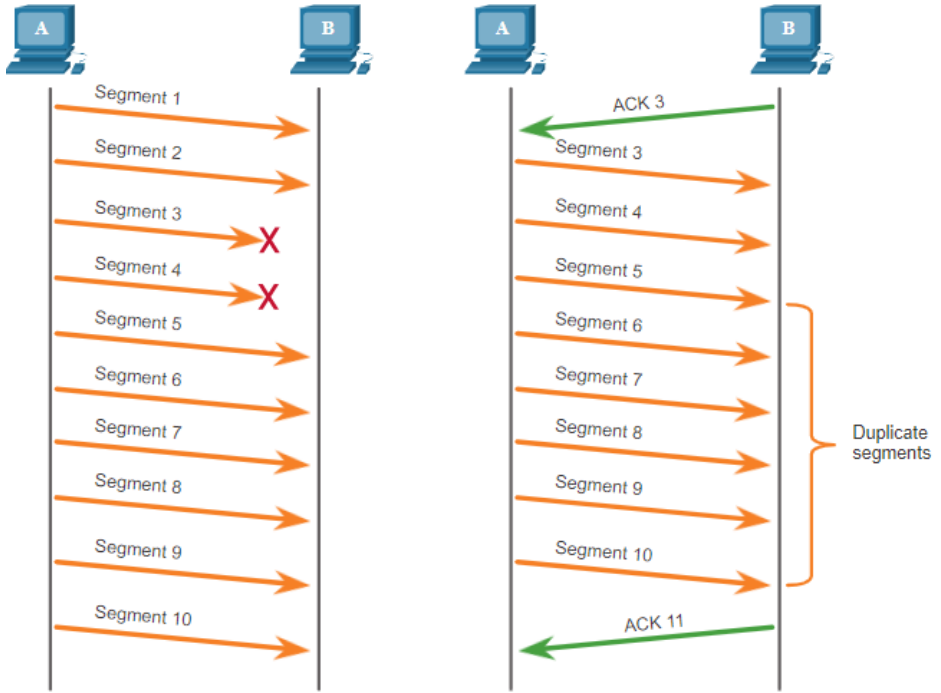
- O TCP também pode ajudar a manter o fluxo de pacotes para que os dispositivos não fiquem sobrecarregados.
- Pode haver momentos em que os segmentos TCP não cheguem ao destino ou fora de ordem.
- Todos os dados devem ser recebidos e os dados nesses segmentos devem ser remontados pela ordem original.
- Os números de sequência são atribuídos no cabeçalho de cada pacote para alcançar esse objetivo.



Fiabilidade TCP - Perda e retransmissão de dados

Não importa o quão bem projetada é uma rede é, a perda de dados ocorre ocasionalmente.

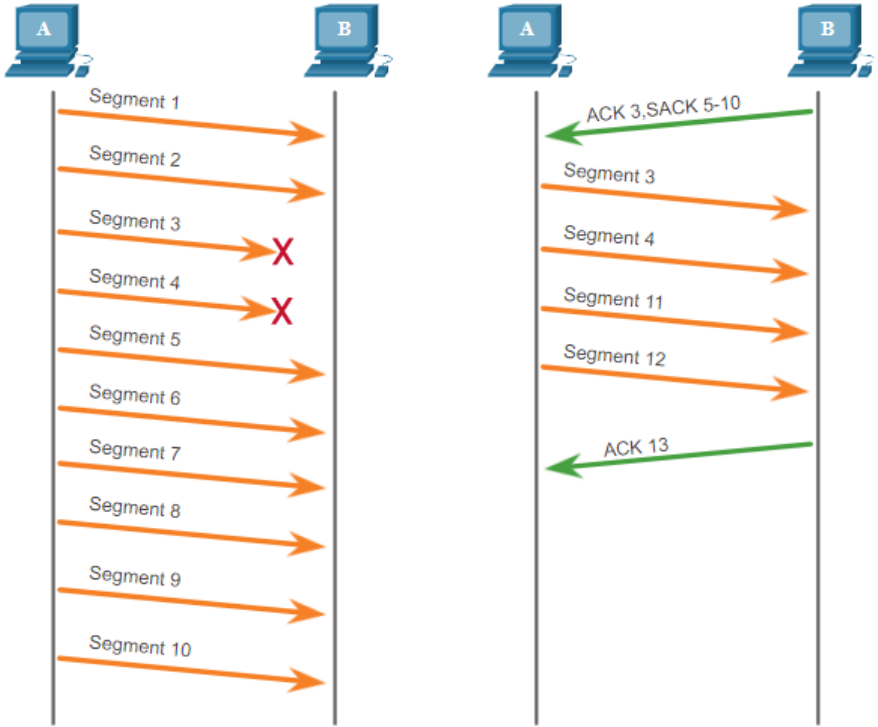
O TCP fornece métodos de gestão dessas perdas de segmento. Entre esses métodos há um mecanismo que retransmite segmentos dos dados não confirmados.



Fiabilidade TCP — Perda e Retransmissão de Dados (Cont.)

Hoje em dia, os sistemas operativos de host utilizam uma característica TCP opcional chamada confirmação seletiva (SACK), negociada durante o handshake triplo.

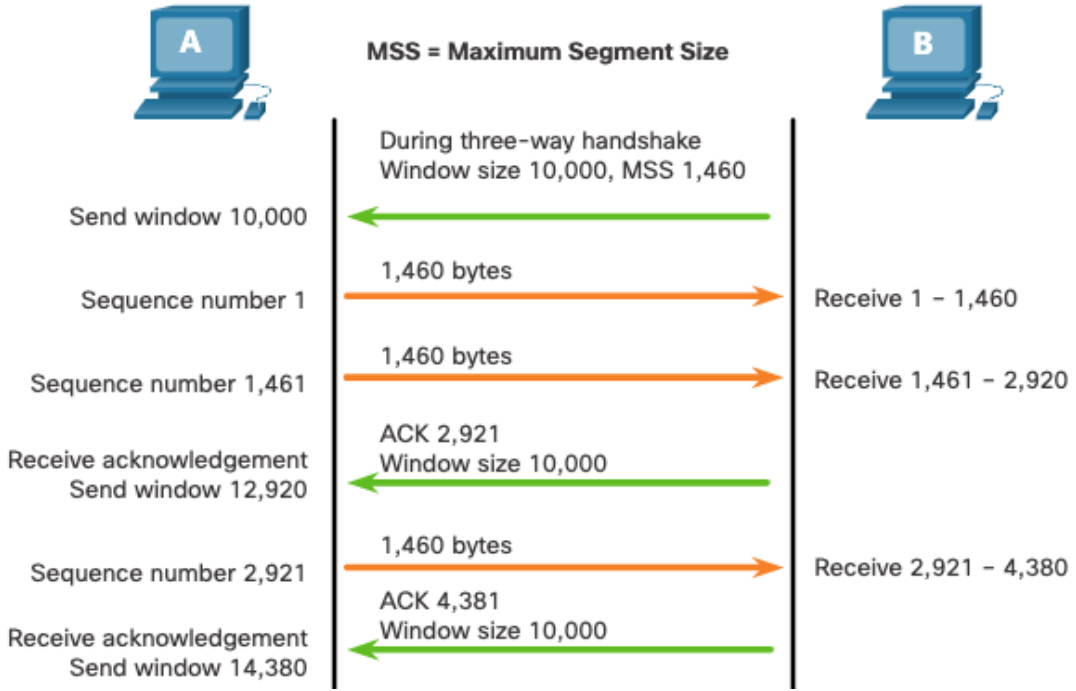
Se ambos os hosts suportarem SACK, o receptor pode confirmar explicitamente que segmentos (bytes) foram recebidos, incluindo quaisquer segmentos descontínuos.



Controle de Fluxo TCP- Tamanho da Janela e Confirmações

O TCP também fornece mecanismos para o controlo de fluxo da seguinte maneira:

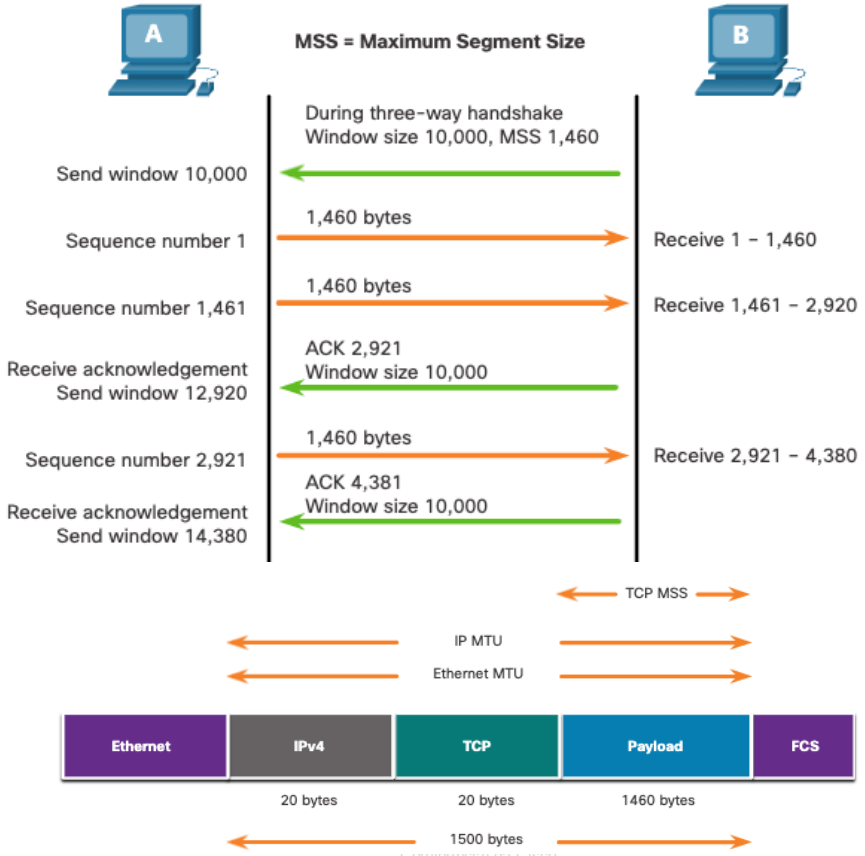
- Controlo de fluxo é a quantidade de dados que o destino pode receber e processar de forma fiável.
- O controlo de fluxo ajuda a manter a fiabilidade da transmissão TCP definindo a taxa de fluxo de dados entre a origem e o destino numa determinada sessão.



Controle de Fluxo no TCP - Tamanho Máximo do Segmento

Tamanho Máximo do Segmento (Maximum Segment Size - MSS) é a quantidade máxima de dados que o dispositivo de destino pode receber.

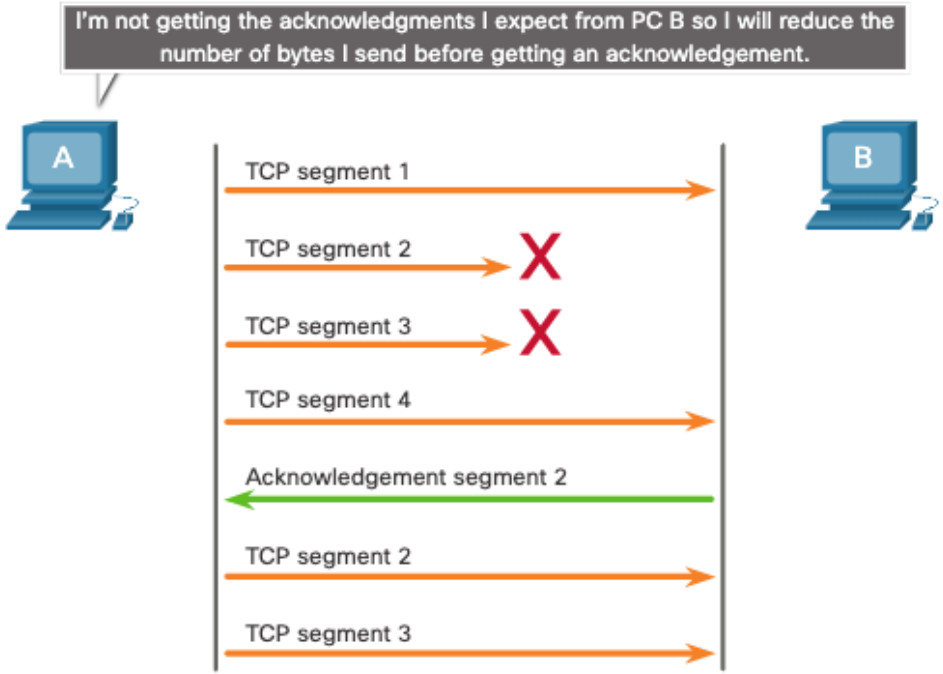
- Um MSS comum é 1.460 bytes, quando se usa IPv4.
- Um host determina o valor do seu campo MSS subtraindo os cabeçalhos IP e TCP da MTU (Ethernet Maximum Transmission Unit), que é de 1500 bytes por defeito.
- 1500 menos 40 (20 bytes para o cabeçalho IPv4 e 20 bytes para o cabeçalho TCP) deixa 1460 bytes.



Controle de fluxo de TCP - Prevenção de congestionamento

Quando ocorrem congestionamentos numa rede, isso resulta em pacotes eliminados pelo router sobrecarregado.

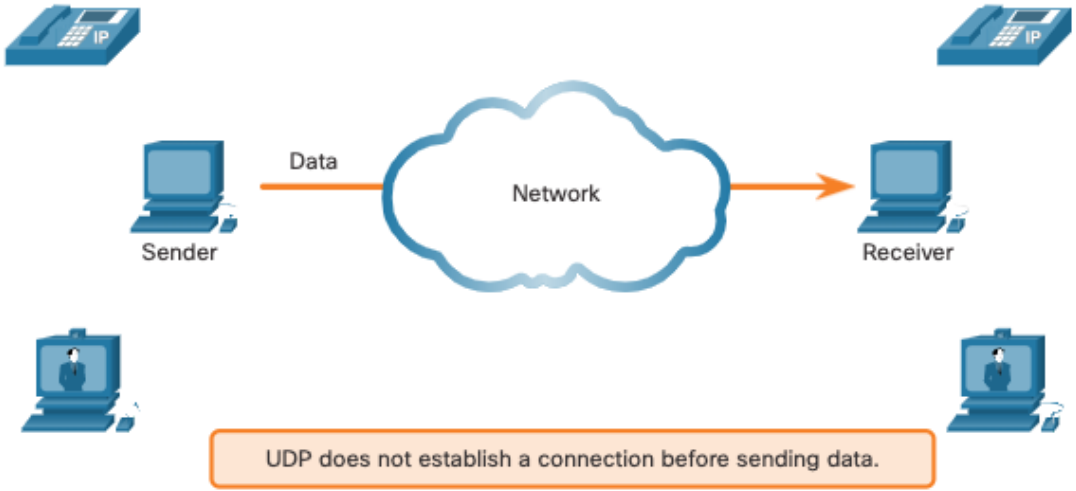
Para evitar e controlar o congestionamento, o TCP utiliza vários mecanismos de manuseamento da congestão, temporizadores e algoritmos.



14.7 - Comunicação UDP

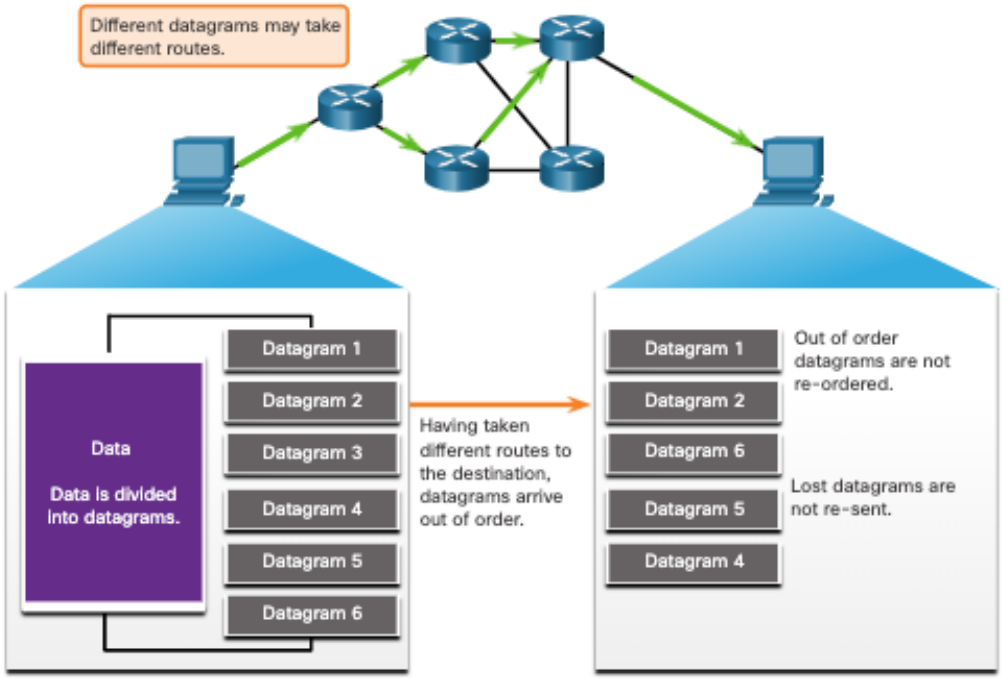
Baixa sobrecarga do UDP versus fiabilidade

O UDP não estabelece uma ligação. O UDP fornece transporte de dados com baixa sobrecarga, porque tem um cabeçalho de datagrama pequeno e nenhum tráfego de gestão de rede.



Reagrupamento de datagrama UDP

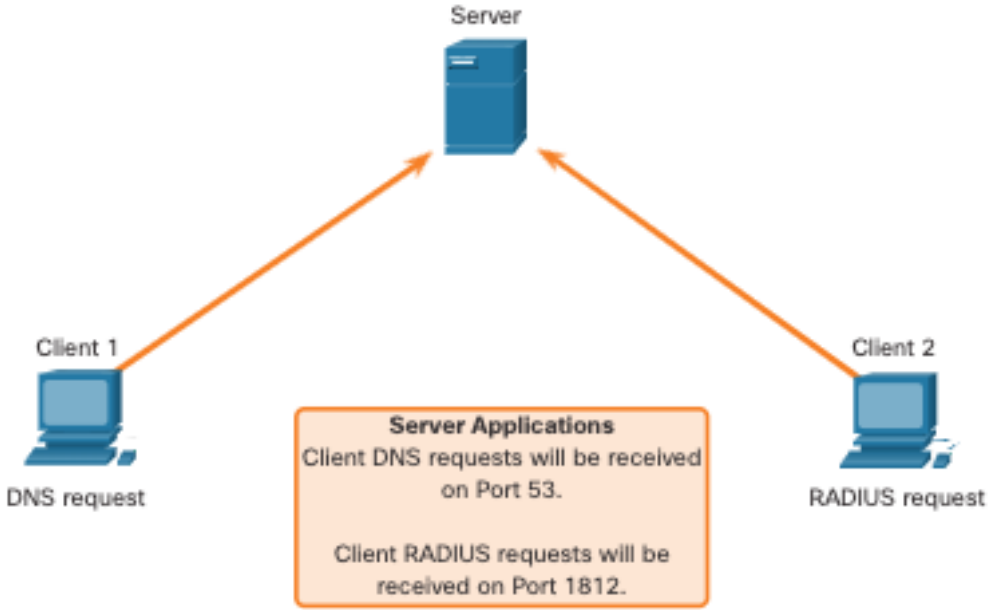
- O UDP não rastreia os números de sequência da mesma maneira que o TCP.
- O UDP não tem maneira de reordenar os datagramas na sua ordem de transmissão original.
- O UDP simplesmente remonta os dados na ordem em que foram recebidos e encaminha-os para a aplicação.



Solicitações e processos de servidor UDP

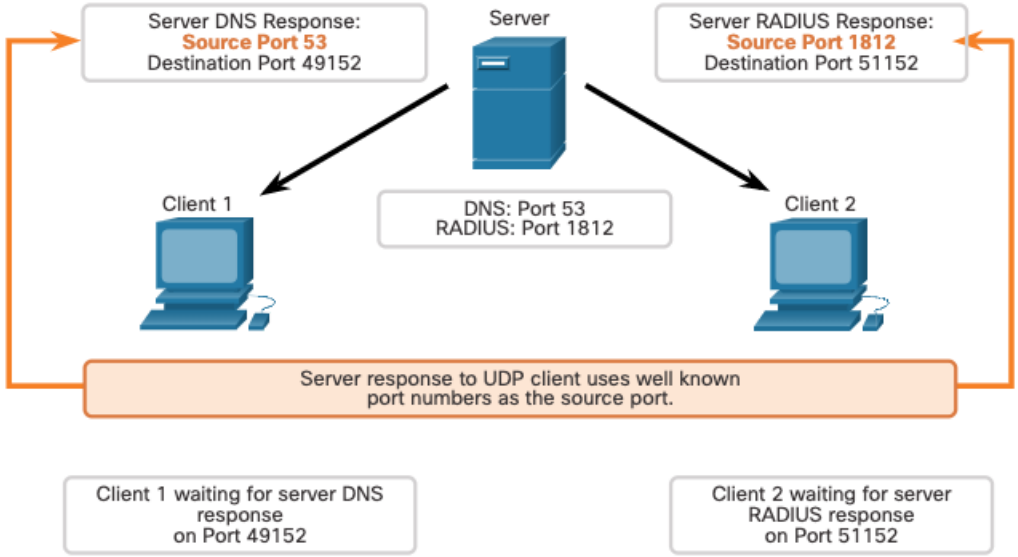
As aplicações de servidor baseadas em UDP recebem números de porto conhecidos ou registados.

Quando o UDP recebe um datagrama destinado a um destes portos, ele encaminha os dados à aplicação apropriada com base em seu número de porto.



Processos de cliente UDP

- O processo no cliente UDP seleciona dinamicamente um número de porto a partir de uma faixa de números de portos e usa-o como porto de origem para a conversa.
- A porta de destino será geralmente o número de porto bem conhecido ou registado atribuído ao processo no servidor.
- Depois do cliente ter selecionado os portos de origem e de destino, o mesmo par de portos é usado no cabeçalho de todos os datagramas na transação.



14.8 - Sumário

O que aprendi neste módulo?

- A camada de transporte é a ligação entre a camada de aplicação e as camadas inferiores responsáveis pela transmissão na rede.
- A camada de transporte inclui o TCP e o UDP.
- O TCP estabelece sessões, garante fiabilidade, fornece entrega ordenada e oferece suporte ao controlo de fluxo.
- O UDP é um protocolo simples que fornece as funções básicas da camada de transporte.
- O UDP reconstrói os dados na ordem em que são recebidos, os segmentos perdidos não são reenviados, não faz nenhum estabelecimento de sessão e o UPD não informa o remetente da disponibilidade de recursos.
- Os protocolos de camada de transporte TCP e UDP usam números de porto para gerir várias conversas simultâneas.
- Cada processo de aplicação em execução num servidor está configurado para usar um número de porto.
- O número da porto é atribuído automaticamente ou configurado manualmente por um administrador do sistema.
- 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.

O que eu aprendi neste módulo (Cont.)?

- Os números de sequência são atribuídos no cabeçalho de cada pacote.
- O controlo de fluxo ajuda a manter a fiabilidade da transmissão TCP, ajustando a taxa de fluxo de dados entre a origem e o destino.
- A origem pode transmitir 1.460 bytes de dados dentro de cada segmento TCP. Este é o MSS típico que um dispositivo de destino pode receber.
- 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.
- Para evitar e controlar o congestionamento, o TCP emprega vários mecanismos de manipulação de congestionamento.