



Cisco Networking Academy CCNA - Módulo II

Claurem P. C. Marques



Cisco Certified Academy Instructor



Platin – www.adetec.org.br/platin

Capítulo 10 – TCP/IP Intermediário

10.1 Operação do TCP

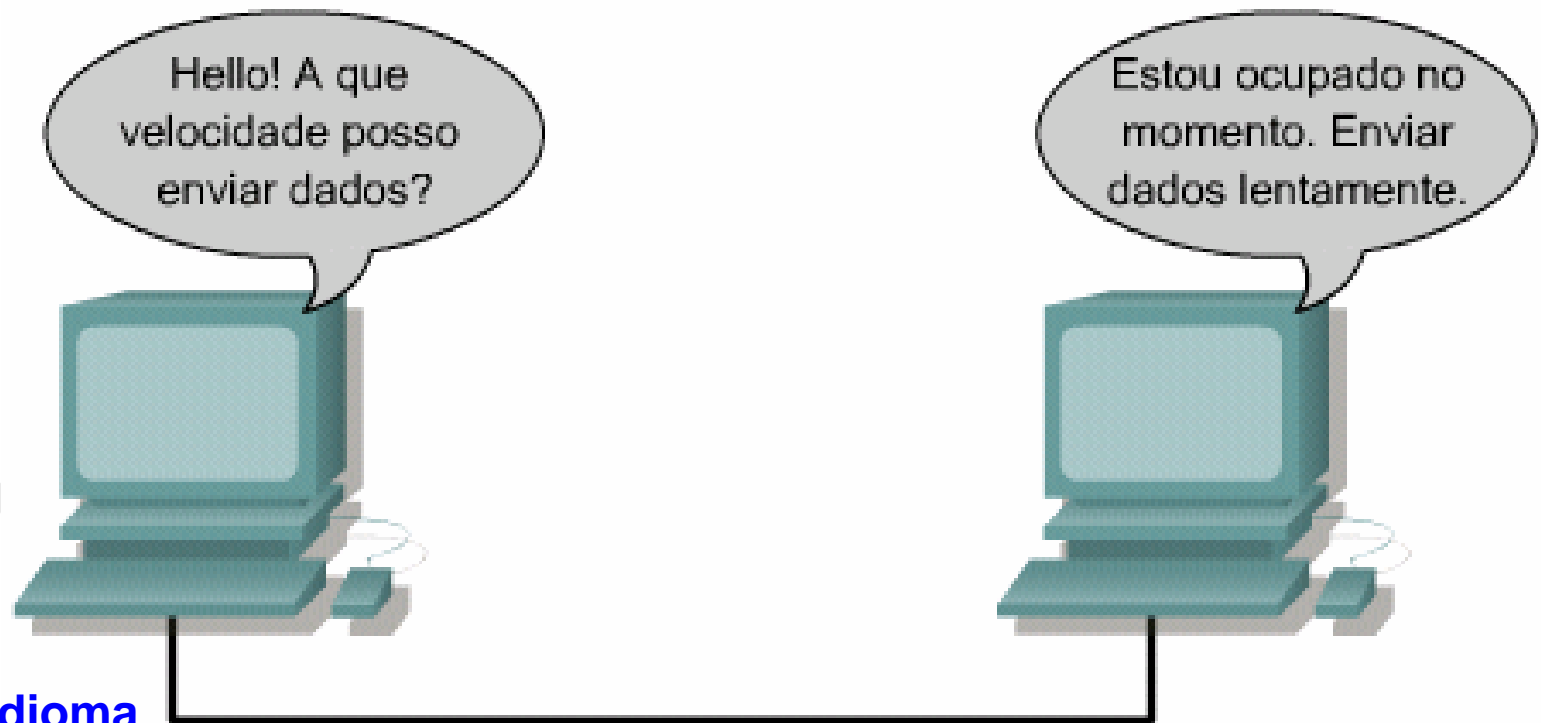
- [10.1.1](#) Operação do TCP
- [10.1.2](#) Sincronização ou handshake triplo
- [10.1.3](#) Ataques de recusa de serviço
- [10.1.4](#) Janelamento e tamanho da janela
- [10.1.5](#) Números de seqüência
- [10.1.6](#) Confirmações Positivas
- [10.1.7](#) Operação do UDP

10.2 Visão geral das portas da camada de transporte

- [10.2.1](#) Várias conversas entre hosts
- [10.2.2](#) Portas para serviços
- [10.2.3](#) Portas para clientes
- [10.2.4](#) Numeração das portas e números de portas conhecidos
- [10.2.5](#) Exemplo de várias sessões entre hosts
- [10.2.6](#) Comparação entre endereços MAC, endereços IP e números de portas

Operação do TCP

- **Confiabilidade**
- **Controle de Fluxo**

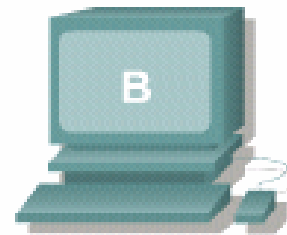
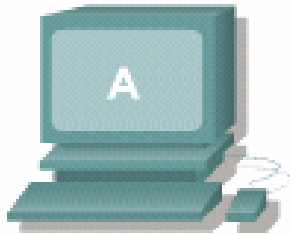


Sincronização ou Handshake Triplo

0	4	10	16	24	31
Porta Origem			Porta Destino		
Número de Seqüência					
Número de Confirmação					
Hlen	Reservado	(Bits de Controle	Janela		
Checksum			Ponteiro de Urgência		
Opções (Se houver)				Enchimento	
Dados					
...					

O formato do campo de um segmento TCP contém um cabeçalho TCP seguido de dados. Os segmentos são usados para estabelecer conexões, assim como para conduzir dados e confirmações.

Sincronização ou Handshake Triplo



O TCP é um
protocolo
Orientado a
Conexão

1 Enviar SYN(seq=100
ctl=SYN)

SYN recebido

SYN recebido

2 Enviar SYN,
ACK(seq=300ack=
101ctl=syn,ack)

3 Estabelecido(seq=101
ack=301ctl=ack)

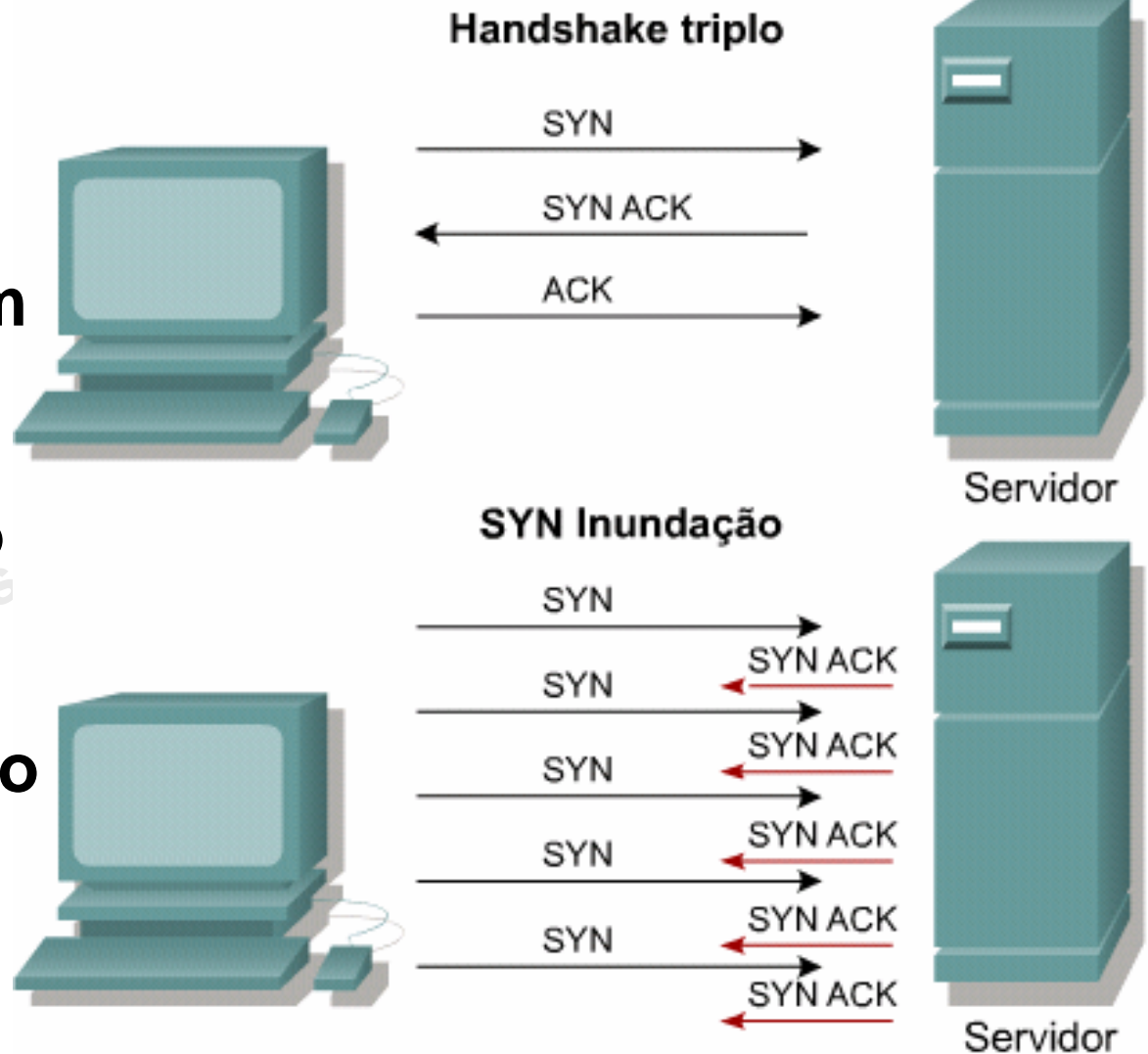
Este host inicia uma conexão, ao enviar um pacote SYN, indicando seu número de sequência inicial x com um determinado bit no cabeçalho definido para indicar um pedido de conexão

Este host recebe o pacote, registra o número de sequência de x, responde com uma confirmação de x+1 e inclui seu próprio número de sequência inicial de y.

Este host responde com um (ACK) simples de y+1, indicando que recebeu o ACK anterior, que finaliza o processo de conexão.

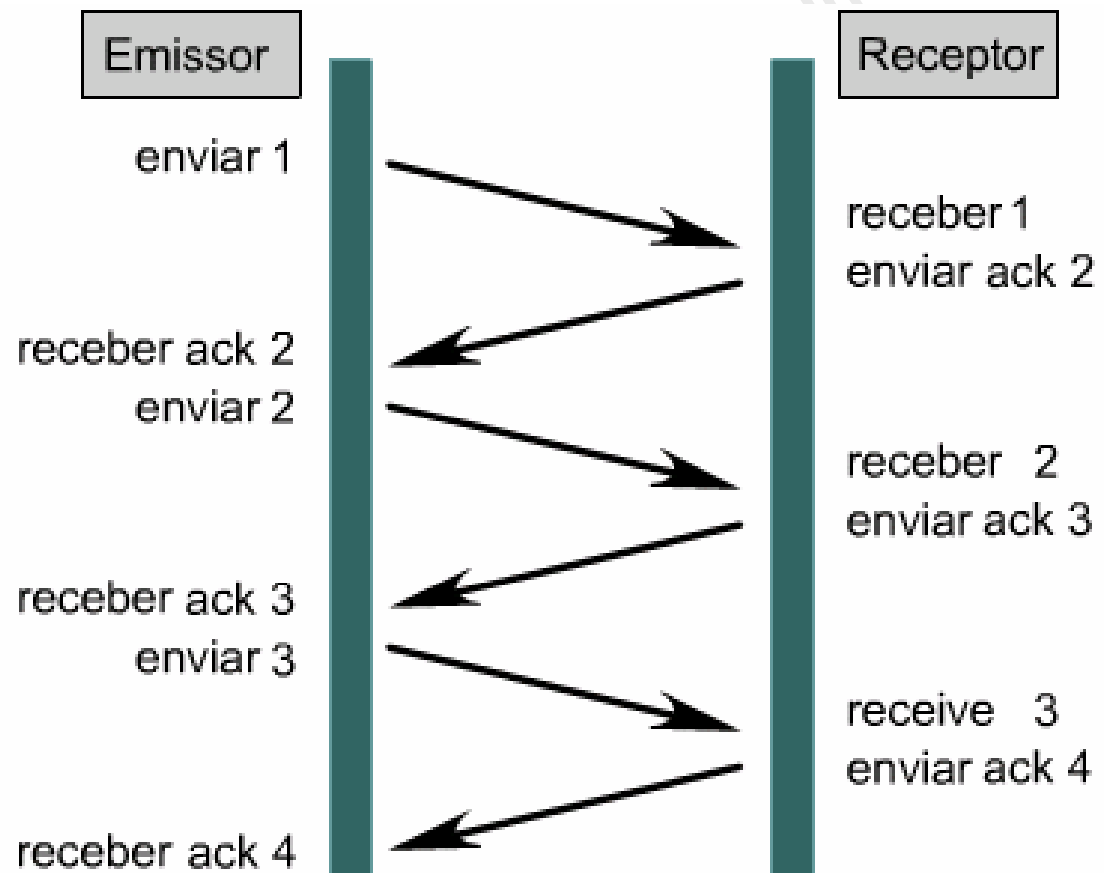
Ataques de Recusa de Serviço

- O **hacker** inicia uma sincronização, mas falsifica o endereço IP de origem
- Os **hackers** inundam o host atacado com essas solicitações SYN falsas, fazendo com que esse host use todos os seus recursos de conexão para responder e esperar pelas conexões falsas



Janelamento e Tamanho da Janela

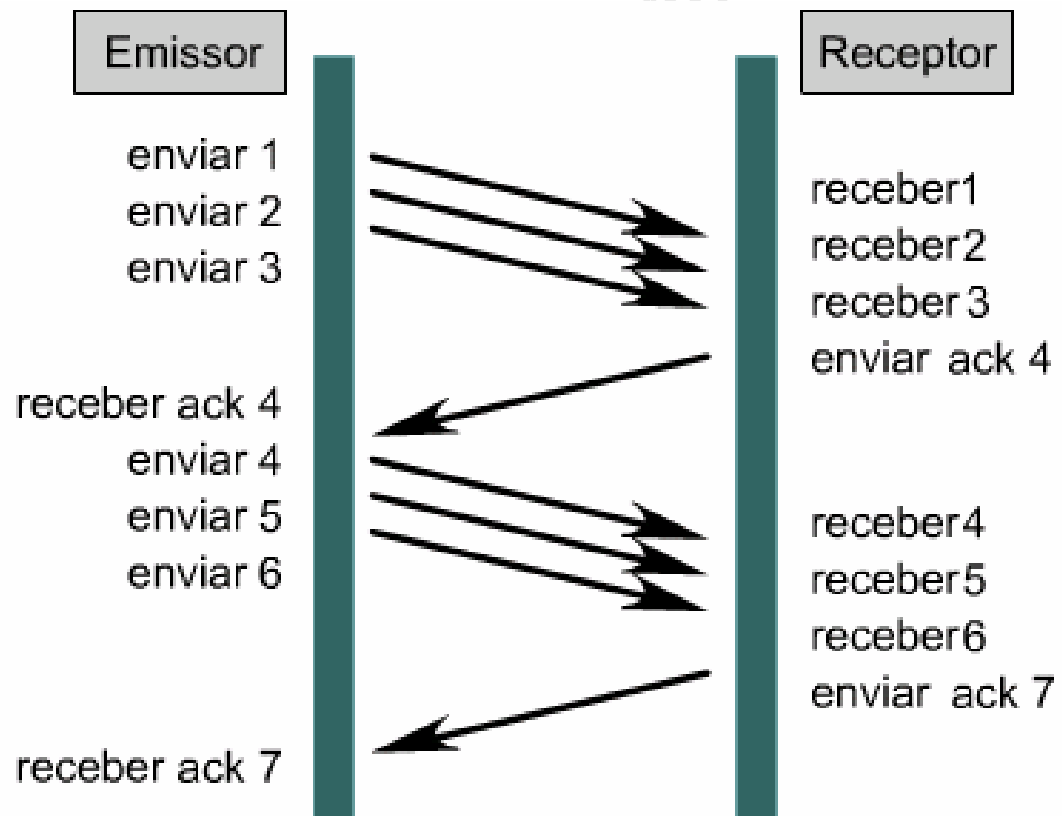
- **Tamanho da janela = 1**
- **Se o tamanho da janela for 1, cada byte precisa ser confirmado antes do próximo byte ser enviado**



Isto foi simplificado para o exemplo. Tamanho da janela real é muito maior, tipicamente milhares de bytes.

Janelamento e Tamanho da Janela

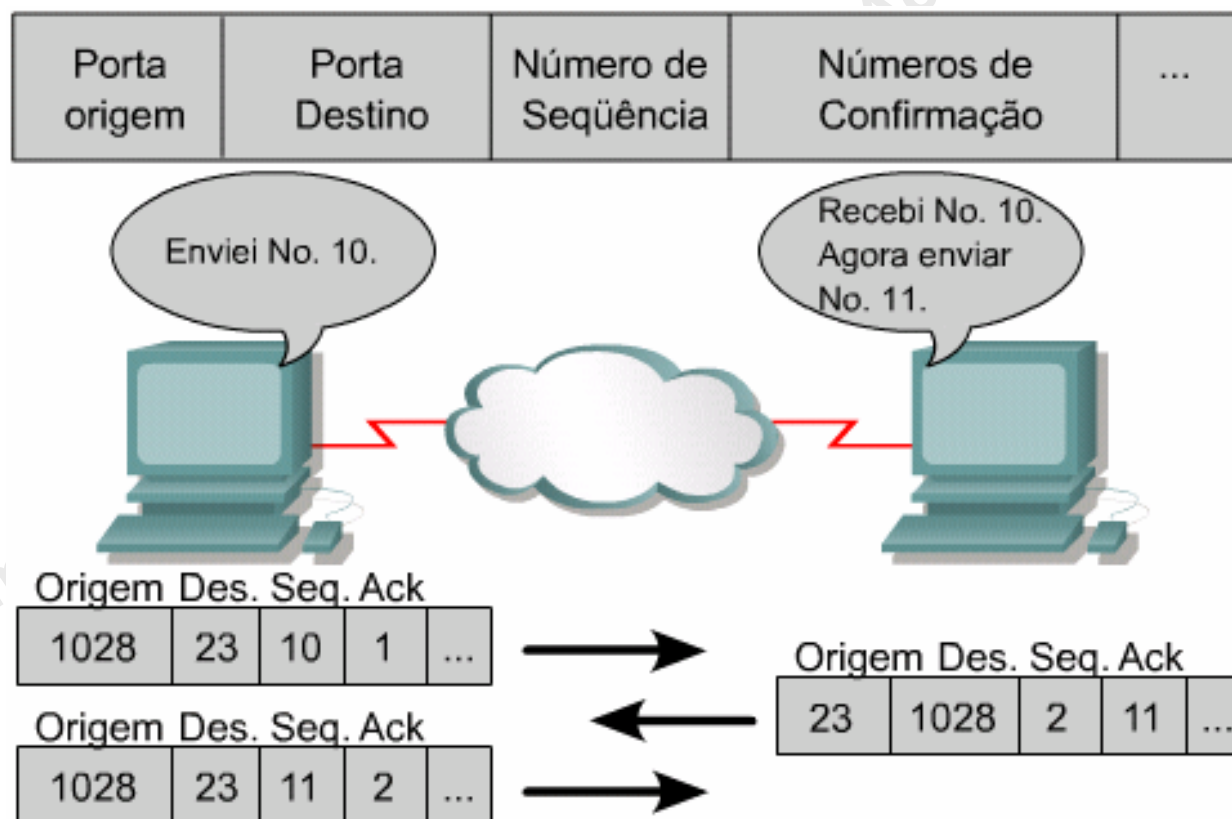
- O TCP utiliza o janelamento para determinar dinamicamente o tamanho da transmissão antes que seja recebida uma confirmação
- Há um aumento na confiabilidade



Isto foi simplificado para o exemplo. Tamanho da janela real é muito maior, tipicamente milhares de bytes.

Números de Seqüência

- Os segmentos de dados que estão sendo transmitidos precisam ser remontados no destino



Formato de Segmento TCP

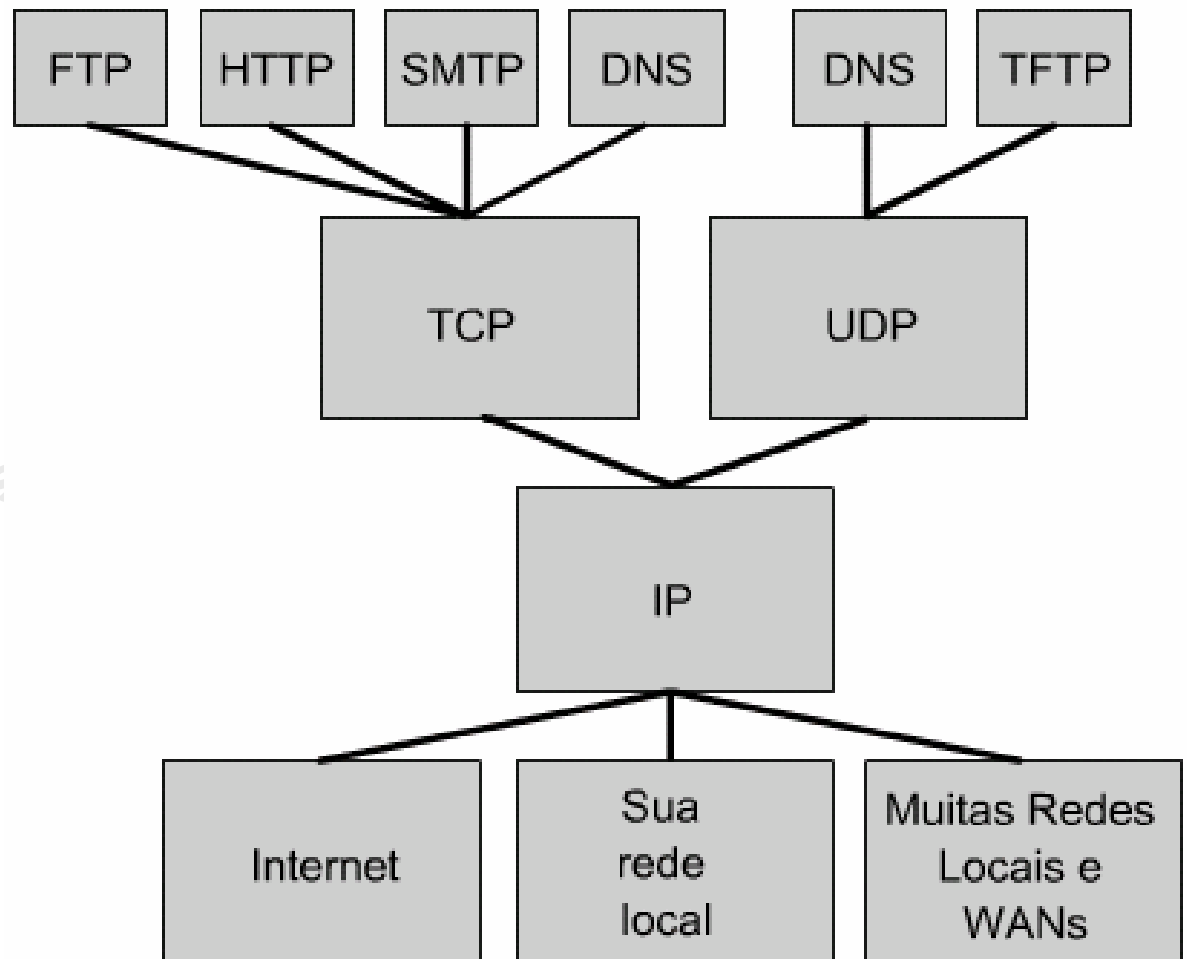
- **Números de seqüência também funcionam como números de referência, para que o receptor saiba se recebeu todos os dados**

0	4	10	16	24	31
Porta origem			Porta Destino		
Número de Seqüência					
Acknowledgment Number					
Hlen	Reserved	Code Bits	Window		
Checksum			Urgent Pointer		
Options (If Any)				Padding	
Data					
...					

O formato do campo de um segmento TCP contém um cabeçalho TCP seguido de dados. Os segmentos são usados para estabelecer conexões, assim como para conduzir dados e confirmações.

Protocolo TCP

- O **TCP** deve ser usado quando os aplicativos precisam garantir que um pacote chegue intacto, em seqüência e não duplicado



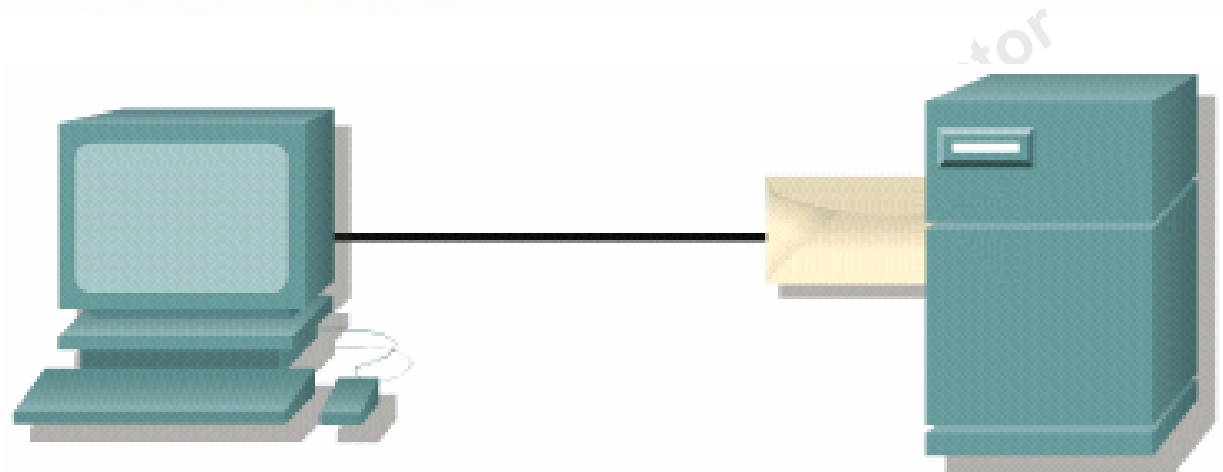
Operação do UDP

- **UDP não usa janelamento nem confirmações, isso é função dos protocolos das camadas superiores**
- **Não há troca de informações nem de dados**

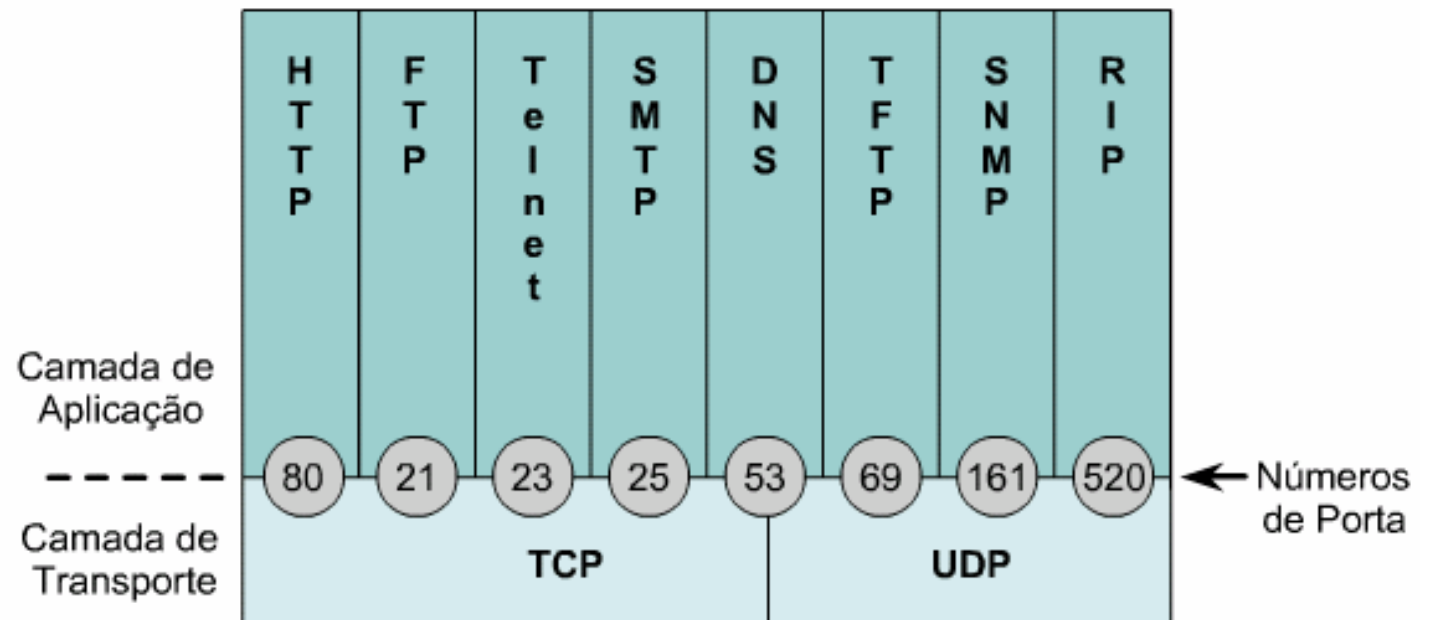
# of Bits	16	16	16	16	16
	Porta origem	Porta Destino	Comprimento	Check Sum	Dados

Os segmentos UDP não contêm campos de sequência ou de confirmação.

Várias conversas entre hosts

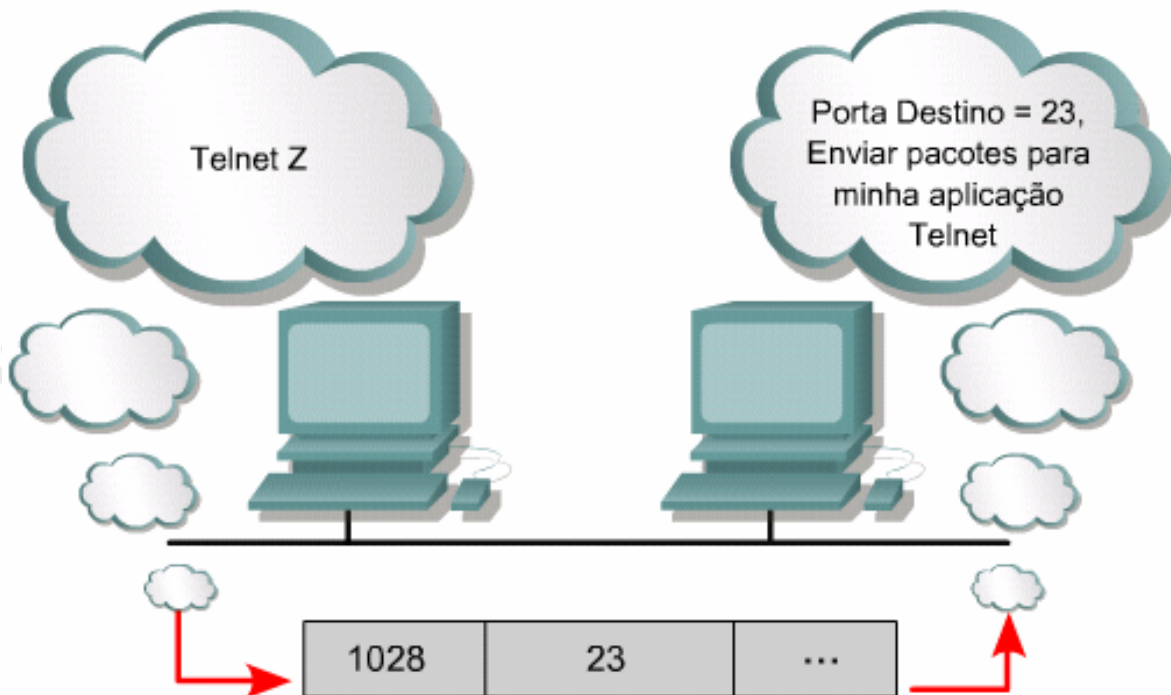


SMTP (e-mail) e WWW



Número da Porta Telnet

Porta Origem	Porta Destino	...
--------------	---------------	-----



Portas para Serviços

- Essas portas conhecidas definem os aplicativos que são executados acima dos protocolos da camada de transporte

Decimal	Palavra-chave	Descrição
69	FTP	Protocolo de Transferência de Arquivos Trivial
75		Qualquer serviço privado de discagem de saída
77		Qualquer serviço RJE privado
79	FINGER	Finger
80	HTTP	Protocolo de Transferência de Hiper-texto
95	SUPDUP	Protocolo SUPDUP
101	HOSTNAME	Servidor de nomes de host NIC
102	ISO-TSAP	ISO-TSAP
110	POP3	Protocolo de correio para clientes receberem correspondência armazenadas no servidor de email
113	AUTH	Serviço de Autenticação
117	UUCP-PATH	Serviço de Rota UUCP
123	NTP	Protocolo de Horário para Redes (Network Time Protocol)
133-159		Não assinalado
160-223		Reservado
224-241		Não assinalado
242-255		Não assinalado

Portas para Clientes

- As portas de destino são definidas usando-se as portas conhecidas

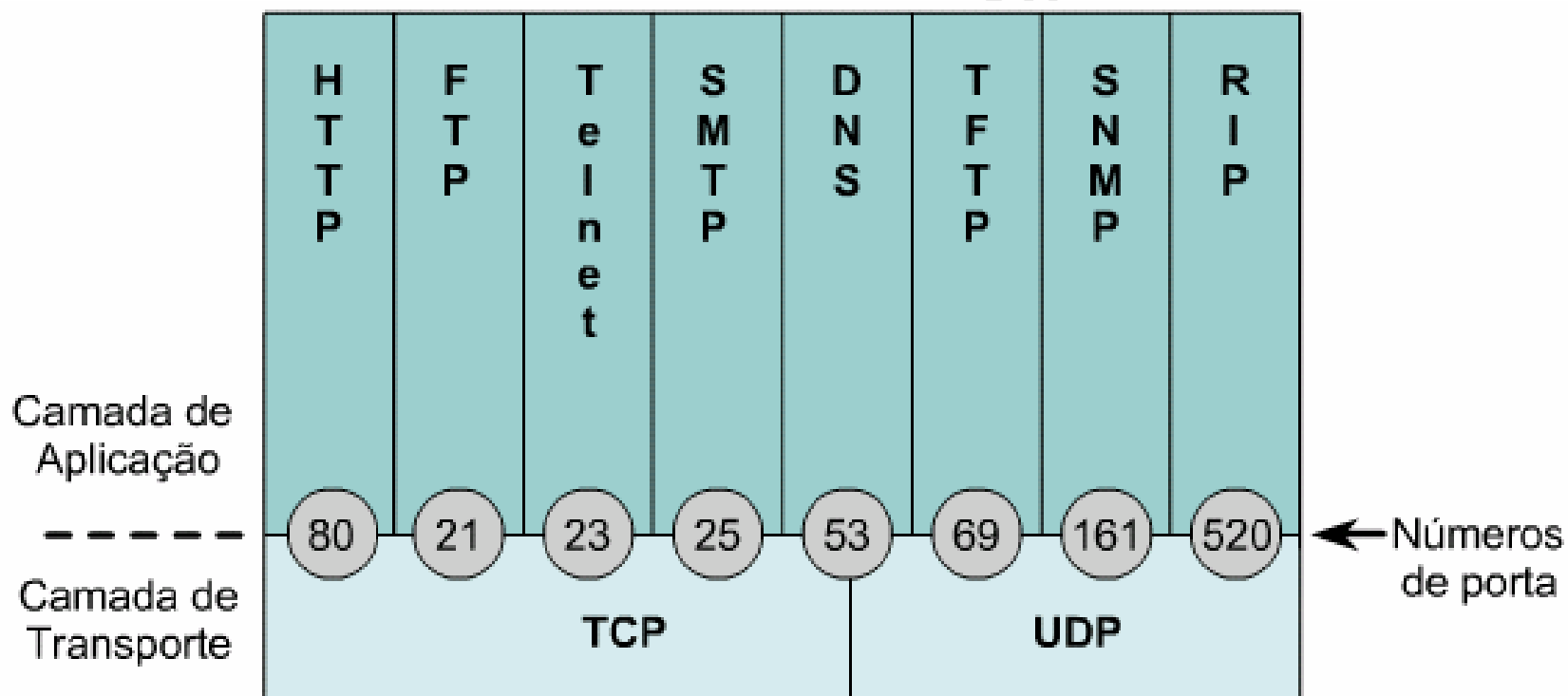
# of Bits	16	16	16	16	16
	Porta origem	Porta Destino	Comprimento	Check Sum	Dados

No sequence or acknowledgment fields.

0	4	10	16	24	31
Porta origem			Porta Destino		
Número de Seqüência					
Número de Reconhecimento					
Hlen	Reservado	Bits de Código	Janela		
Checksum			Ponteiro de Urgência		
Opções (se houver)				enchimento	
Dados					
...					

O formato dos campos em um segmento TCP contém um cabeçalho TCP seguido de dados. Os segmentos são usados para estabelecer conexões, assim como para conduzir dados e confirmações.

- Os números de portas são divididos em portas conhecidas, portas registradas e portas dinâmicas ou privadas



- **As primeiras 1023 portas são portas conhecidas. Como o nome indica, essas portas são usadas para serviços de rede conhecidos, tais como FTP, Telnet ou DNS**
- **As portas registradas variam de 1024 a 49151**
- **As portas entre 49152 e 65535 são definidas como portas dinâmicas ou privadas**

Exemplo de várias sessões entre hosts

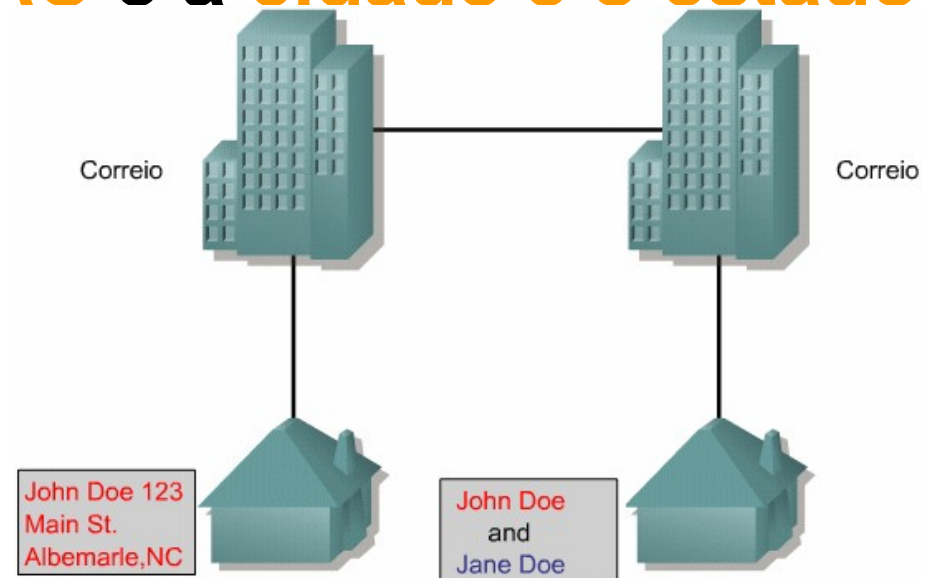
Números de Porta e soquetes

- Números de portas são usados para rastrear várias sessões que podem ocorrer entre hosts.
- Um número de porta e o endereço de rede combinam-se para formar um soquete.

- **Um par de soquetes, um em cada host, forma uma conexão exclusiva**

Comparação entre endereços MAC, endereços IP e números de portas

- O endereço de uma carta consiste em um nome, logradouro, cidade e estado. Essas informações podem ser comparadas à porta, ao endereço MAC e ao endereço IP usados para os dados de rede. O **nome no envelope seria equivalente ao número de porta**, o **logradouro seria o MAC** e a **cidade e o estado seriam o endereço IP**



Resumo



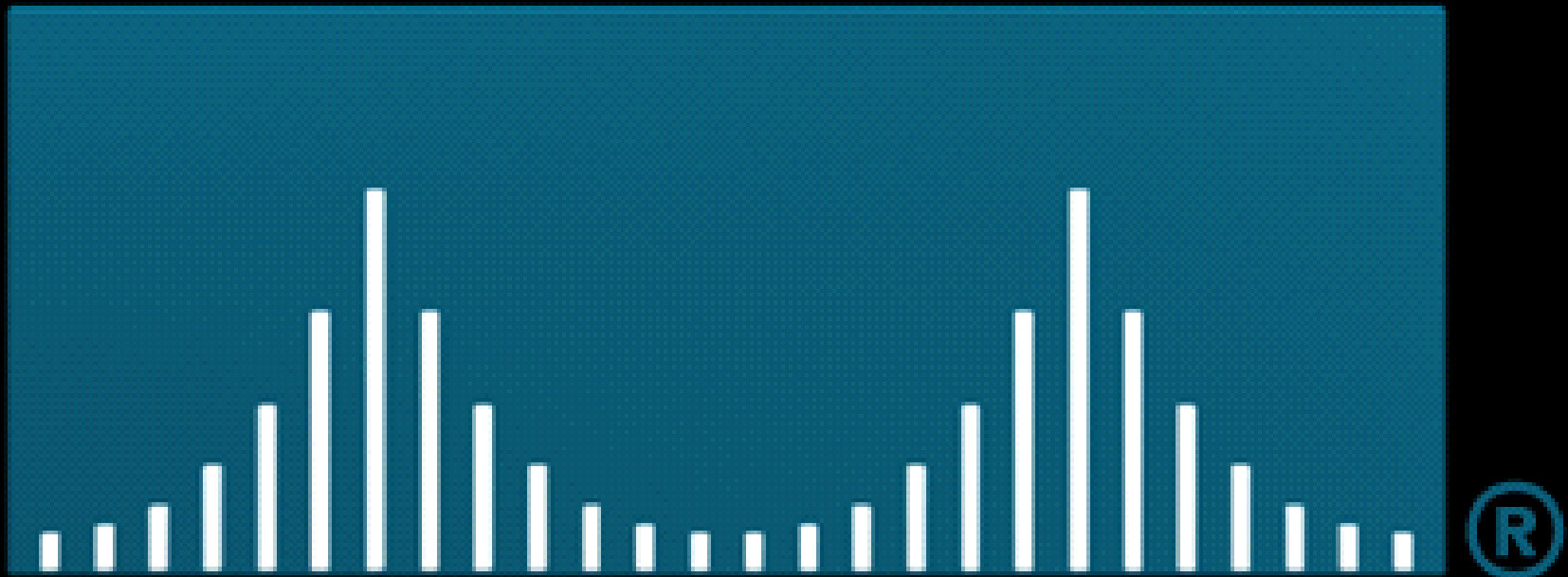
- **Descrição da operação do TCP;**
- **Processo de sincronização (handshake triplo);**
- **Ataques de recusa de serviço;**
- **Janelamento e tamanho da janela;**
- **Números de seqüência;**
- **ACK positiva;**
- **Operação do UDP;**

Resumo



- **Várias conversas entre hosts;**
- **Portas para serviços;**
- **Portas para clientes;**
- **Numeração de portas e portas conhecidas;**
- **Exemplo de várias sessões entre hosts;**
- **Comparação entre endereços MAC, endereços IP e números de portas.**

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATIONSM

This document was created with Win2PDF available at <http://www.daneprairie.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.