GET básico de redes

Definições

Coleção interligada de computadores autônomos com capacidade de comunicação.

A interligação é concretizada por meios físicos de transmissão, como cabos e ondas de rádio.

A comunicação é a troca de informações organizada de acordo com a geografia e a natureza dos dados.

A comunicação não é indispensável para o funcionamento de cada computador, ou seja, cada computador é autônomo.

Tipos de Redes

LAN

MAN

WAN

Topologias

FÍSICA:

Arranjo físico de equipamentos, considerando os meios de propagação.

Anel, barramento, estrela, malha...

LÓGICA:

Arranjo lógico de equipamentos, considerando protocolos de comunicação e hierarquias

Ethernet, Token Ring, Arcnet...

Modelo TCP/IP

Modelo OSI


Aplicação 7
Apresentação 6
Sessão 5
Transporte 4
Rede 3
Enlace 2
Física 1

Modelo OSI

- Trabalha com os bits 0 e 1
- Define taxa de transferência, tensões e características do meio
- Controla o acesso ao meio
- Faz controle básico mas não trata erros de transmissão

Modelo OSI

- Trabalha com endereço MAC
- Controlar o fluxo
- Estabelece protocolo de comunicação entre sistemas diretamente conectados. Ex: PPP, NetBios
- Detecta e pode corrigir erros da camada 1

Modelo OSI

- Responsável pelo endereçamento dos pacotes
- Converte endereço IP em endereço MAC
- Determina o roteamento dos pacotes

Modelo OSI

- Prepara os dados vindos da camada de sessão em pacotes e envia para a camada de rede
- No caso dos pacotes vindos da camada de rede, remonta o dado e envia para a camada de sessão
- Controla o fluxo, a ordenação dos pacotes e o controle de erros
- Pode trabalhar de forma orientada à conexão ou não. Ex: TCP, UDP, ICMP

Modelo OSI

- Permite que aplicações em maquinas diferentes estabeleçam comunicação
- Define a forma de transmissão dos dados
- Marca os dados de forma que seja possível tratar alguns erros

Modelo OSI

- Faz a compressão dos dados vindos da camada de aplicação
- Nesta camada, é possível criptografar os dados

Modelo OSI

- Identifica e estabelece quais aplicações devem ser usadas, assim como seus protocolos.
- Exemplos de protocolos: HTTP, SMTP, POP3, IMAP, FTP, SSH, Telnet, DNS, Torrent

Ethernet

Conjunto de tecnologias de camada física com um protocolo de controle de acesso ao meio

Compatível entre implementações distintas

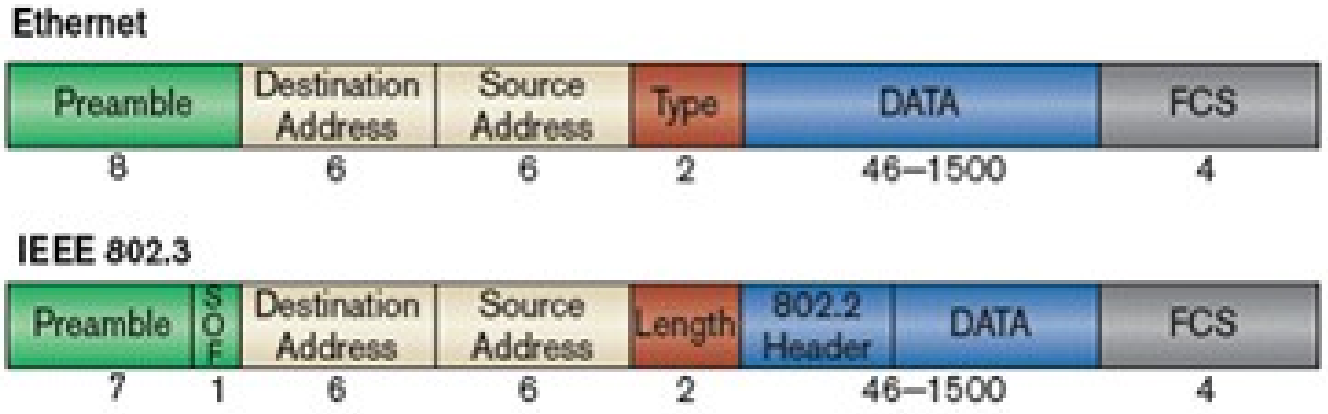
Tecnologia barata e escalável para LANs

Quadro Ethernet

Permite envio de dados de camadas superiores com informações de controle

Previne corrupção de dados através de um tipo de verificação, o Frame Check Sequence (FCS)

Permite a comunicação entre dispositivos que compartilham o acesso ao mesmo meio



Quadro Ethernet

Preâmbulo (Preamble):

Sequência alternada de 1 e 0 no início de cada pacote. Usa um campo de sincronização SFD para indica que a porção contendo dados da mensagem irá na sequência. Esse campo só foi necessário nos enlaces assíncronos (10Mb/s). Nos enlaces atuais ele não existe.

Destination Address:

Endereço MAC do destinatário

Source Address:

Endereço MAC do remetente

Quadro Ethernet

Type/Length:

Indica o tamanho em Bytes do campo de dados

Data:

Dados que deverão ser passados a próxima camada. Deve ter tamanho mínino de 46 bytes e máximo de 1500 bytes

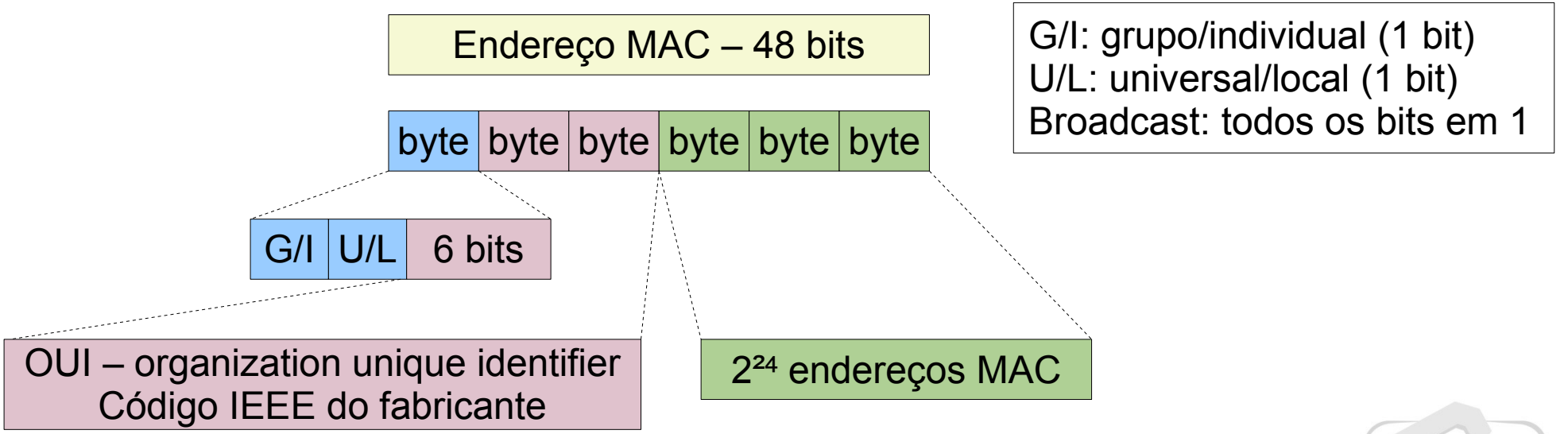
FCS – Frame Check Sequence:

Contem o Cyclic Redundancy Check (CRC). Faz checagem baseada em algorítimos matemáticos para verificação da integridade dos quadros transmitidos. Identifica quadros corrompidos, porém não os corrige.

Endereçamento Ethernet

Cada dispositivo deve ter um endereço único formado por 48bits exibido em hexadecimal

A primeira metade do endereço (24 bits) identifica o fabricante e a segunda metade (24 bits) identifica de forma única o dispositivo



CSMA/CD

“Carrier Sense Multiple Access with Collision Detection”

Algoritmo para prevenir, detectar e tratar colisões em redes Ethernet

Colisões ocorrem quando duas estações disputam o acesso ao meio simultaneamente

Cabeamento Ethernet

Alguns exemplos:

Cabo UTP (Unshielded Twisted Pair, ou par trançado não blindado) – 10BaseT, 100BaseT

Cabo STP (Shielded Twisted Pair, ou par trançado blindado) – 10BaseT, 100BaseT

Coaxial fino (Thin Ethernet – 10Base2) – operam com apenas 10 Mbit/s – CONECTOR BNC

Coaxial grosso (Thick Ethernet – 10Base5) – operam com apenas 10 Mbit/s – CONECTOR AUI

Cabeamento Ethernet

Categoria 1:

Refere-se ao cabo telefônico UTP tradicional que pode transportar voz, mas não dados. A maioria dos cabos telefônicos anteriores a 1983 era de cabos pertencentes à Categoria 1

Categoria 2:

Esta categoria certifica o cabo UTP para transmissões de dados de até 4 Mbps (megabits por segundo). Contém quatro pares trançados

Categoria 3:

Esta categoria certifica o cabo UTP para transmissões de dados de até 10 Mbps. Contém quatro pares trançados com cerca de nove torções por metro

Cabeamento Ethernet

Categoria 4:

Esta categoria certifica o cabo UTP para transmissões de dados de até 16 Mbps. Contém quatro pares trançados

Categoria 5:

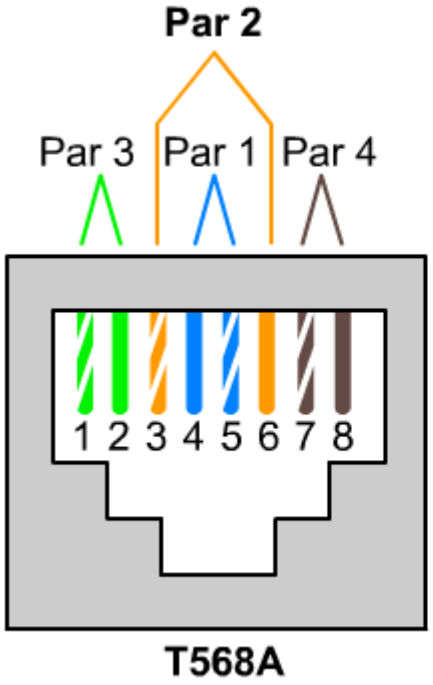
Esta categoria certifica o cabo UTP para transmissões de dados de até 100 Mbps. Contém quatro pares trançados de fio de cobre

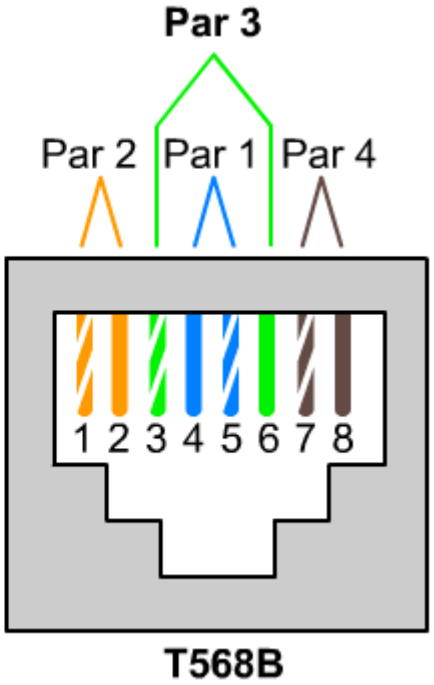
Categoria 5e e 6:

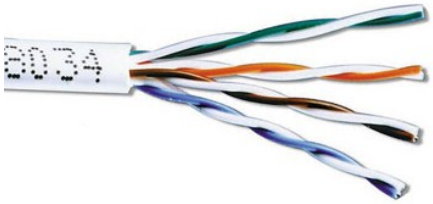
Esta categoria certifica o cabo UTP para transmissões de dados em Gigabit Ethernet. Contém quatro pares trançados de fio de cobre

Cabeamento Ethernet

Dividido nos padrões EIA/TIA T568A e T568B







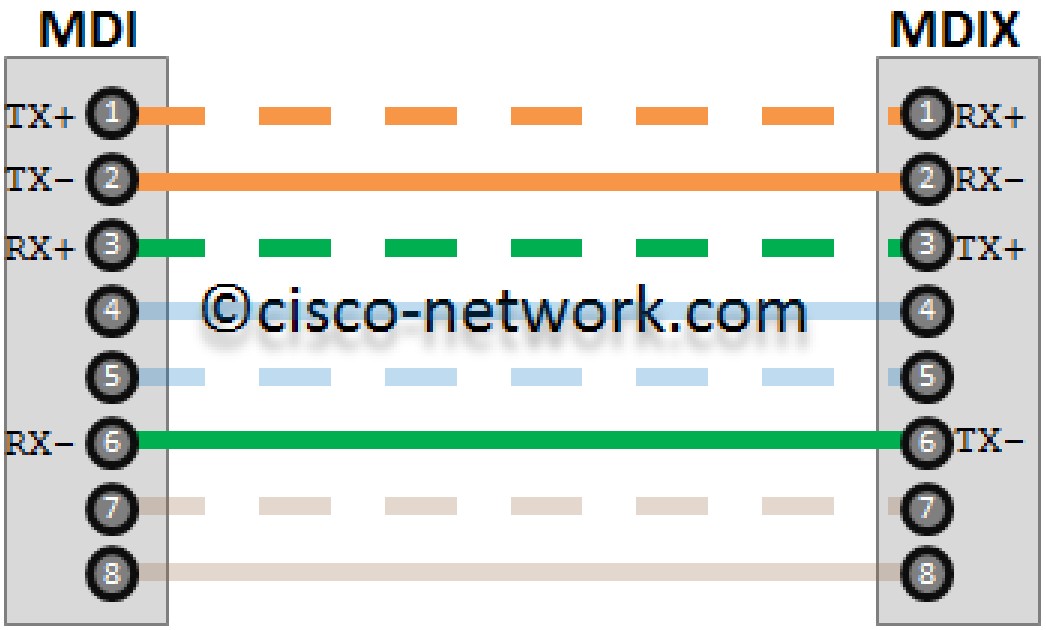
Dispositivos MDI/MDI-X

MDI:

Placas de rede, roteadores...

MDI-X:

Hubs, switchs...



Periféricos de Rede

NIC – Network Interface Card

- É a famosa placa de rede
- Atua na camada 2

Repetidor

- Amplifica/regenera o sinal
- Em linhas gerais, todo dispositivo de rede funciona como repetidor
- Atua na camada 1

HUB

- Replica os sinais para todas as suas portas
- Trabalha da mesma forma que o repetidor
- Atua na camada 1

Periféricos de Rede

Bridge

- Conecta duas redes, não necessariamente do mesmo protocolo
- Trabalham apenas com redirecionamento de pacotes
- Atua na camada 2

Switch

- Ao contrário do hub, envia os pacotes apenas para a porta de destino
- Seu funcionamento é semelhante ao de uma bridge
- Atua na camada 2

Roteador

- Trabalha com endereçamento lógico
- Define as rotas que os pacotes devem seguir
- Atua na camada 3

Dominio de Colisão x Broadcast

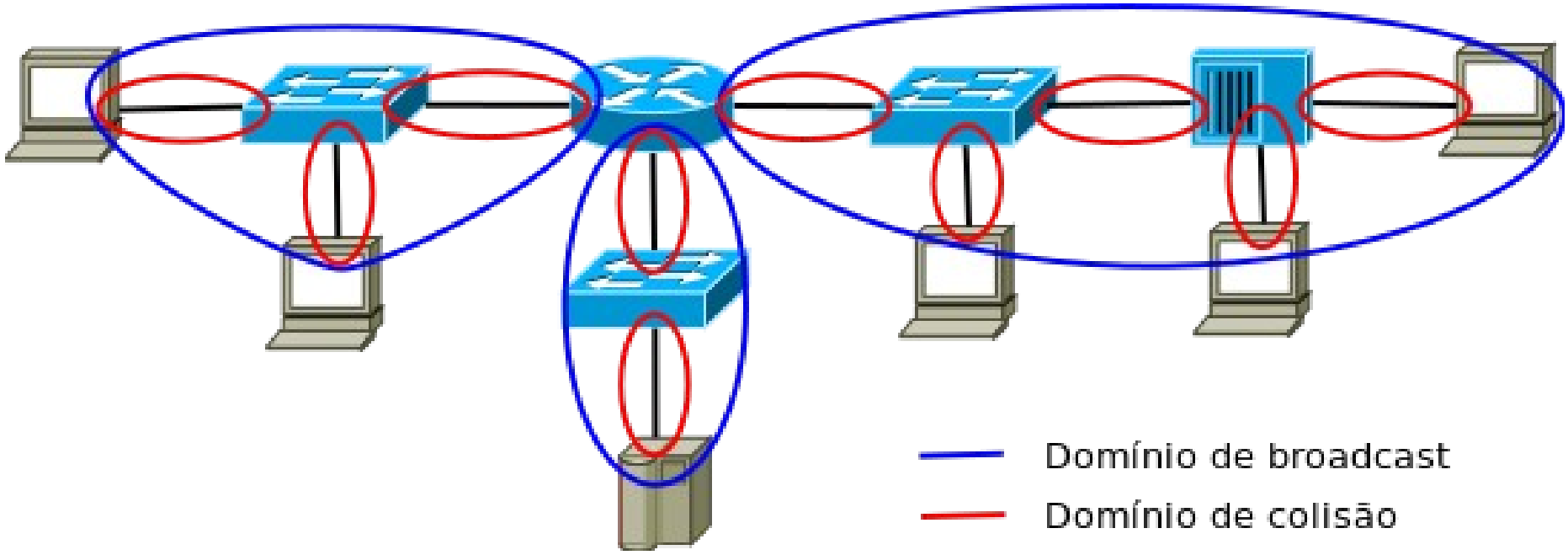
Dominio de Broadcast:

Um domínio de broadcast é um segmento lógico de uma rede de computadores em que um computador ou qualquer outro dispositivo conectado à rede é capaz de se comunicar com outro sem a necessidade de utilizar um dispositivo de roteamento

Dominio de Colisão:

Área lógica onde os pacotes podem colidir uns contra os outros, em particular no protocolo Ethernet

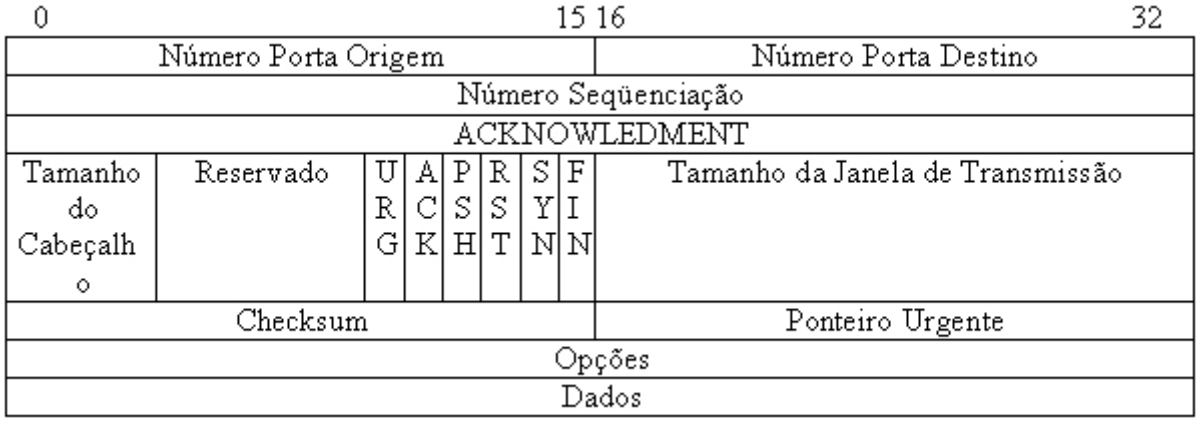
Dominio de Colisão x Broadcast



Protocolos

TCP – Transmission Control Protocol

- Atua na camada 4, porém, em alguns casos atua também na camada 5
- Orientado à conexão
- Controla o fluxo e o congestionamento

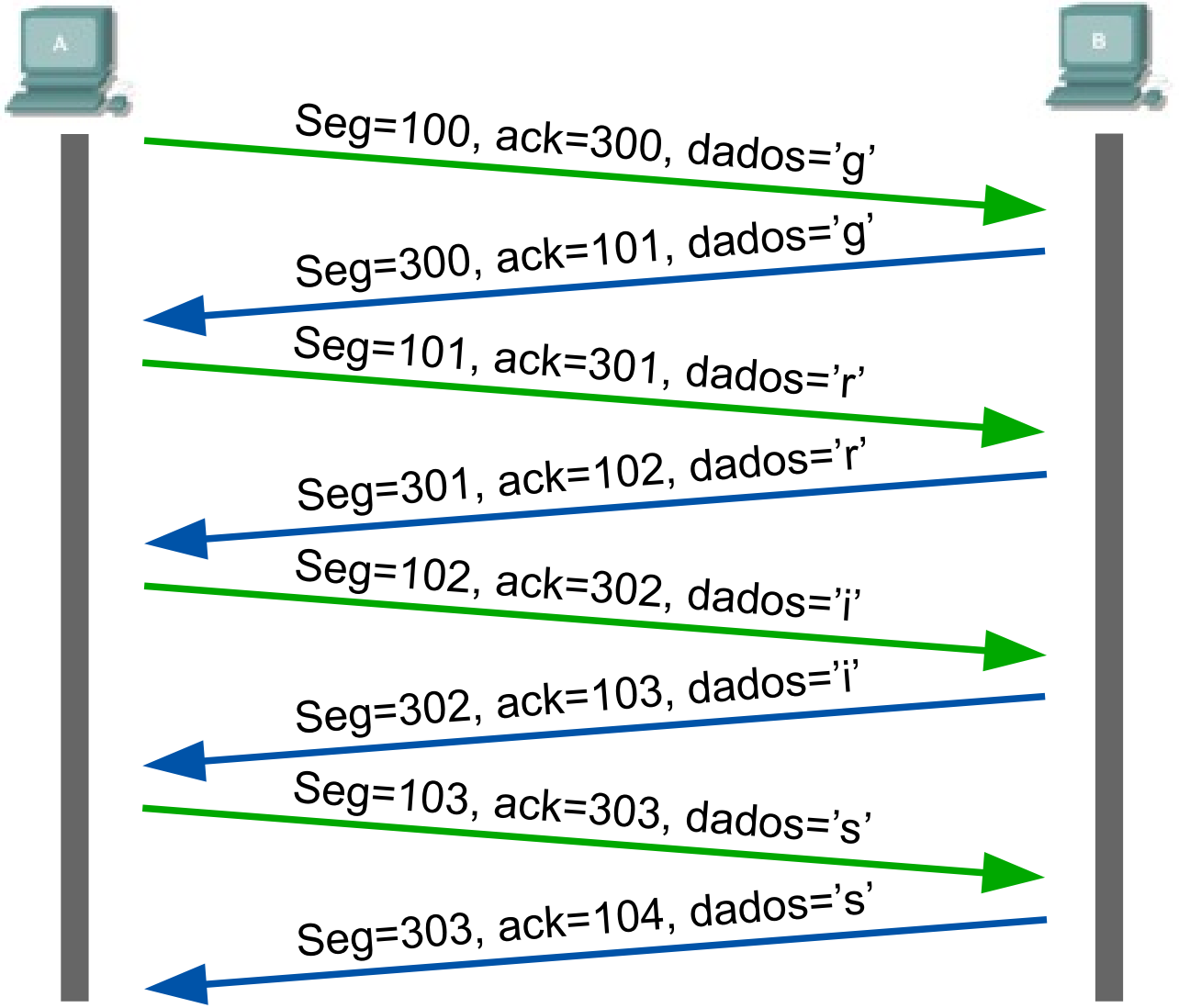


TCP – Comportamento

- Utiliza a ideia de janela deslizante com tamanho variável
- O sequence number indica o numero do pacote enviado
- O acknowledgement (ACK) indica o próximo byte esperado
- Toda vez que um pacote chega ao seu destino um ACK é enviado como resposta
- O tamanho da janela é aumentado à medida que são recebidos ACKs
- As retransmissões são baseadas em timeout

TCP – Sequenciamento

- Os dados enviados são repetidos (ou ecoados) nas respostas ACK

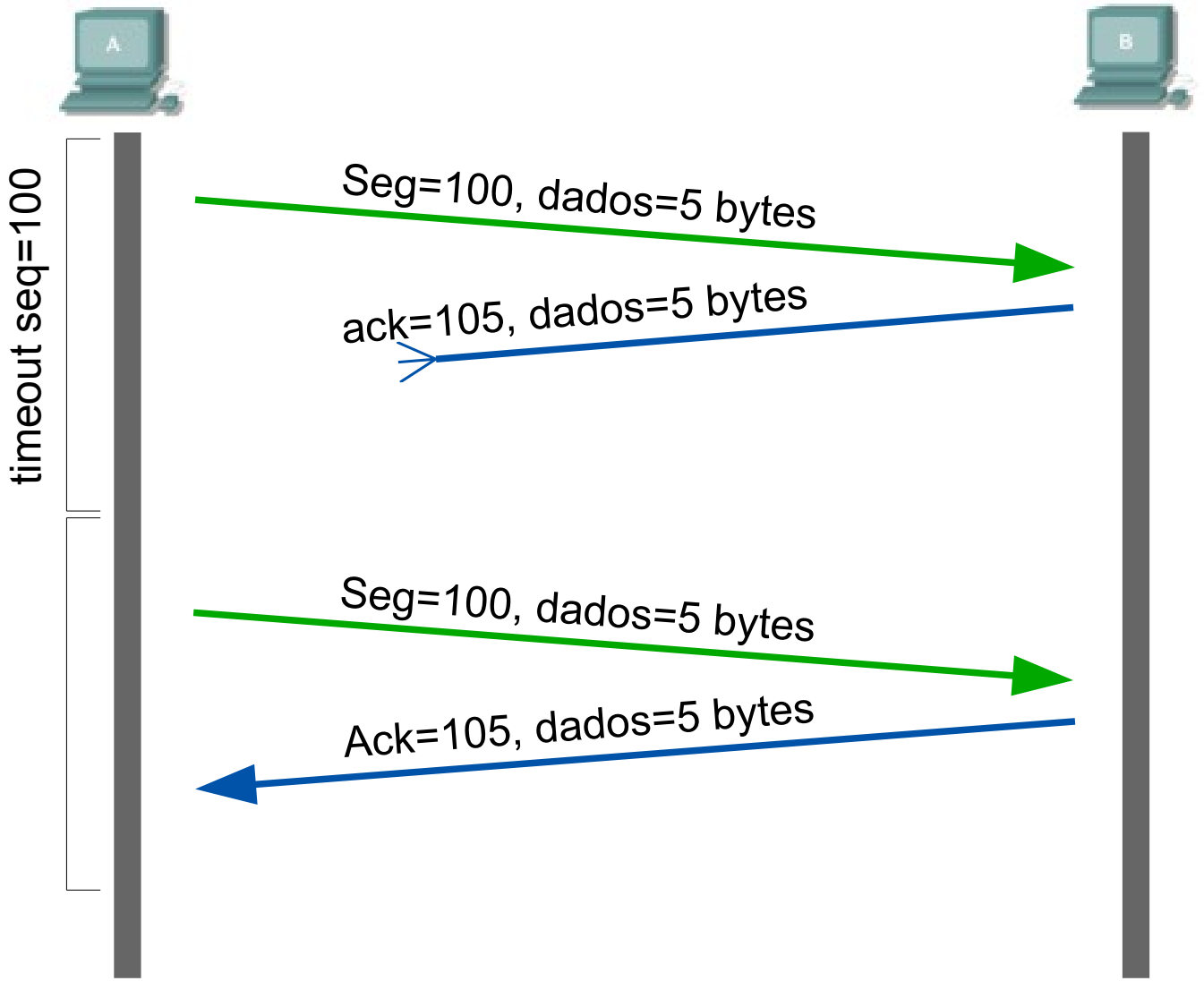


TCP – Funcionamento

- Um timeout é iniciado toda vez que um segmento é transmitido
- O timeout é cancelado quando o ACK correspondente é recebido
- Se um pacote é perdido mas os pacotes seguintes são recebidos, são enviados ACKs de mesmo valor (duplicados)
- O recebimento de três ACKs duplicados força a retransmissão do segmento perdido e cancela o timeout (fast retransmit)

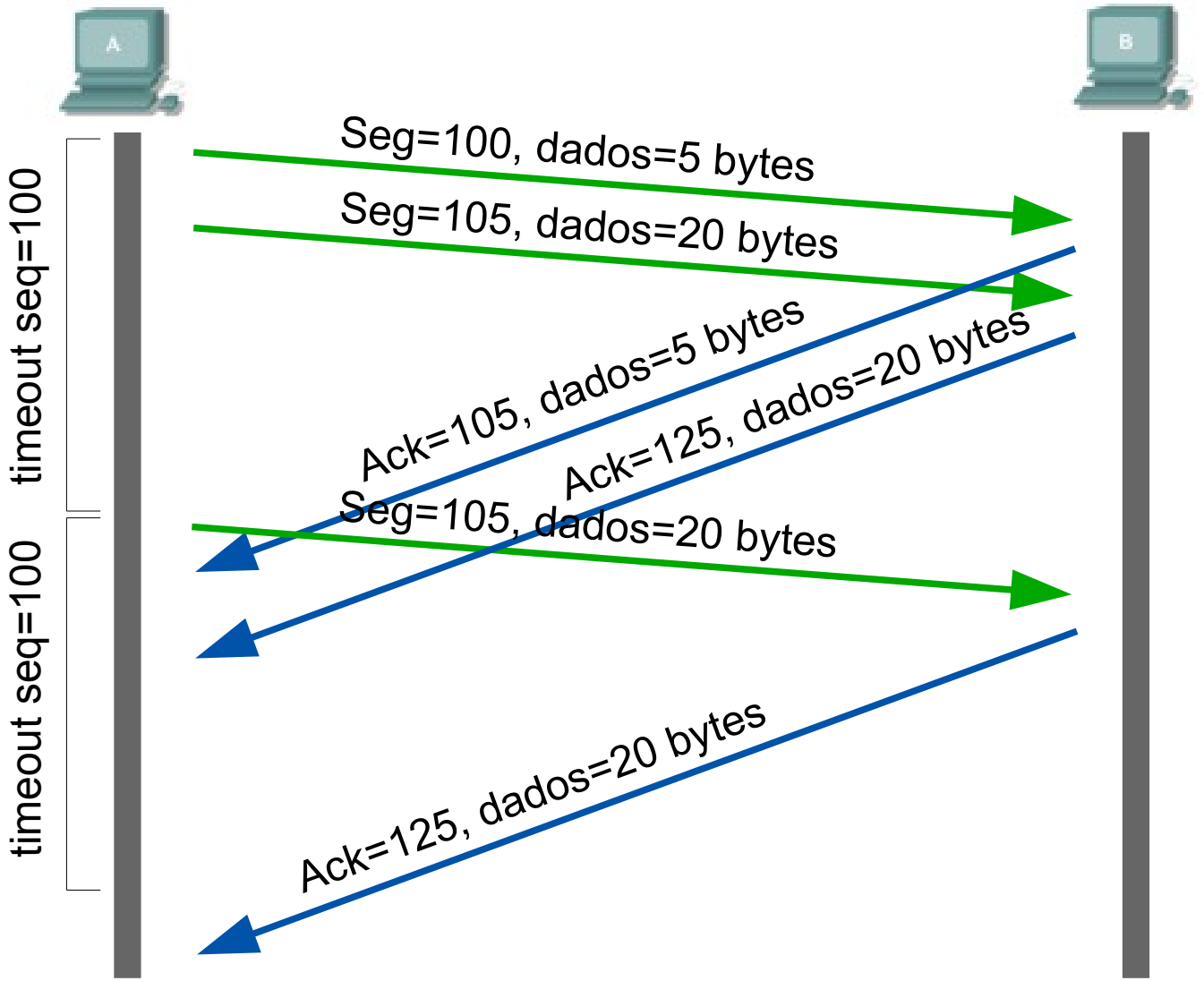
TCP – Retransmissão

- Perda do pacote e retransmissão por timeout



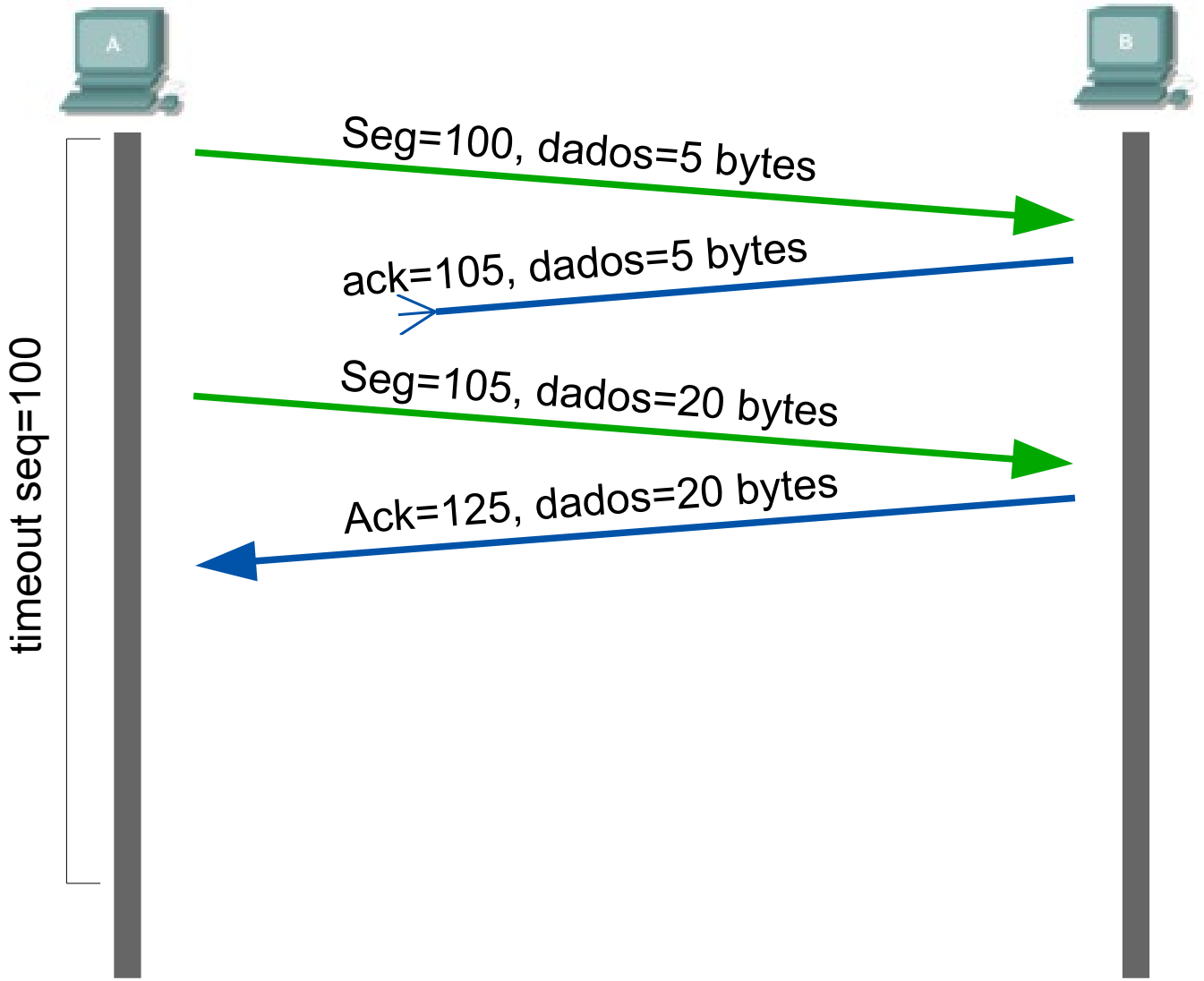
TCP – Retransmissão

- ACK duplicado e timeout “curto”



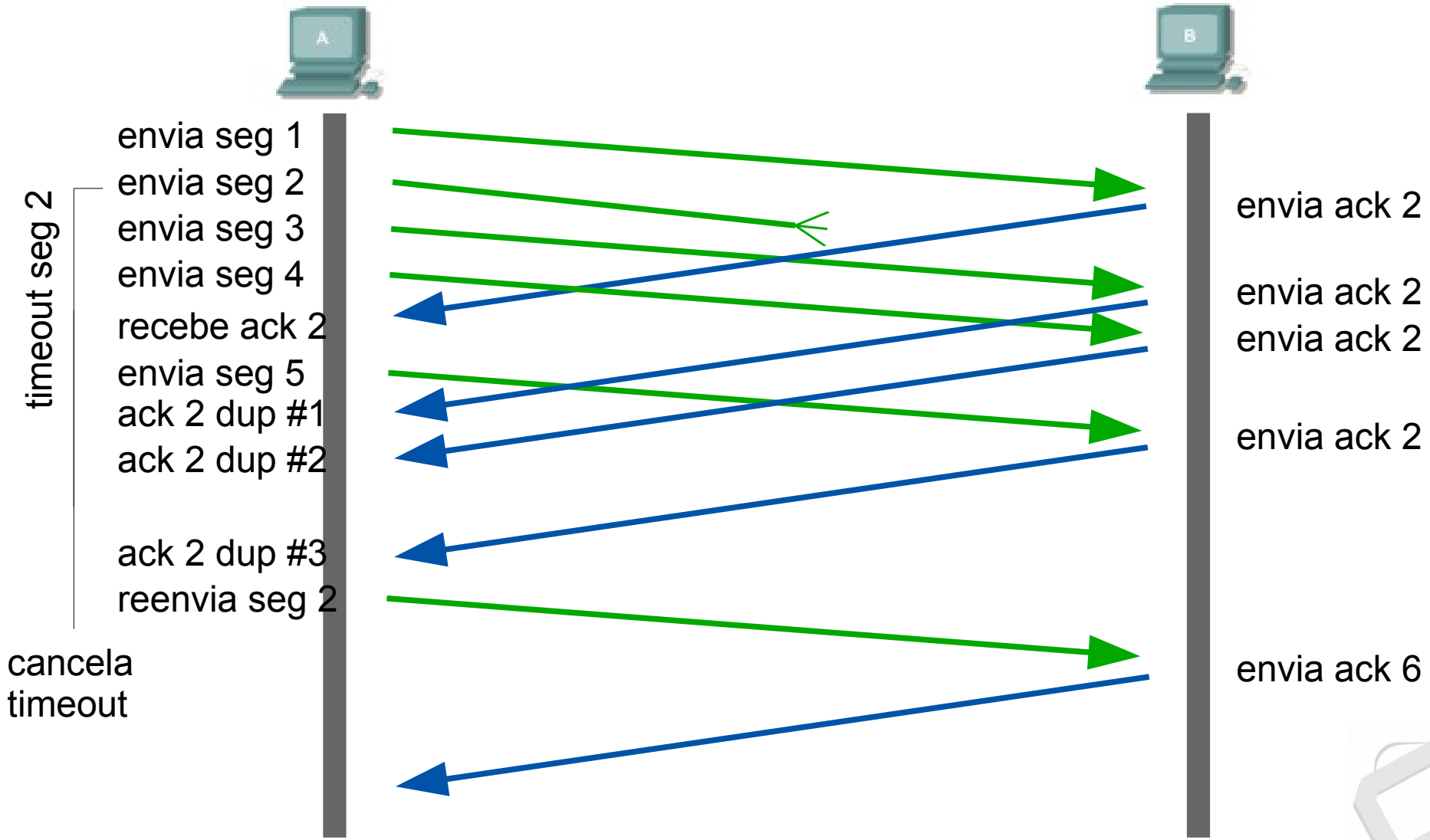
TCP – Retransmissão

- ACK cumulativo



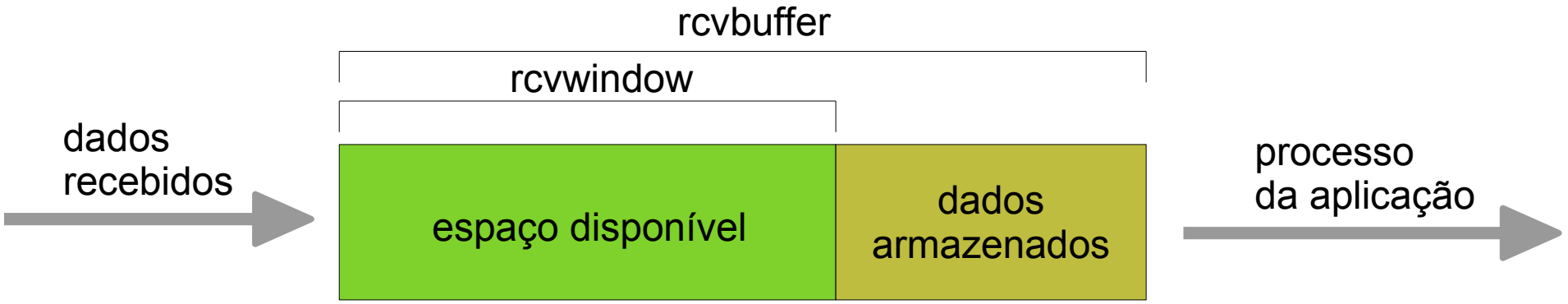
TCP – Fast Retransmit

- ACK cumulativo

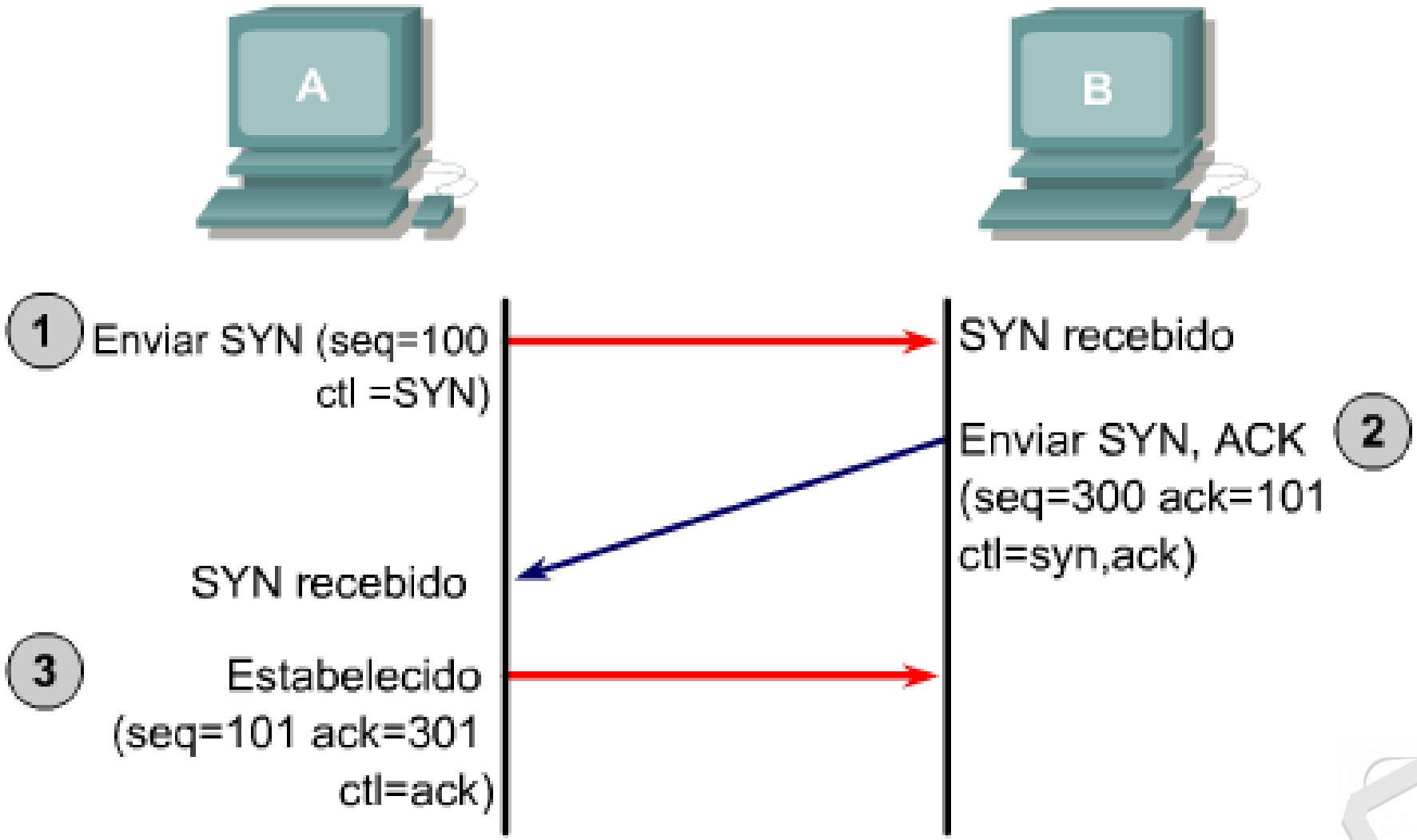


TCP – Controle de Fluxo

- O receptor TCP tem um buffer para armazenar os pacotes
- Os processos podem ser lentos para ler desse buffer
- O emissor não deve enviar dados rápido demais de modo que o buffer fique cheio

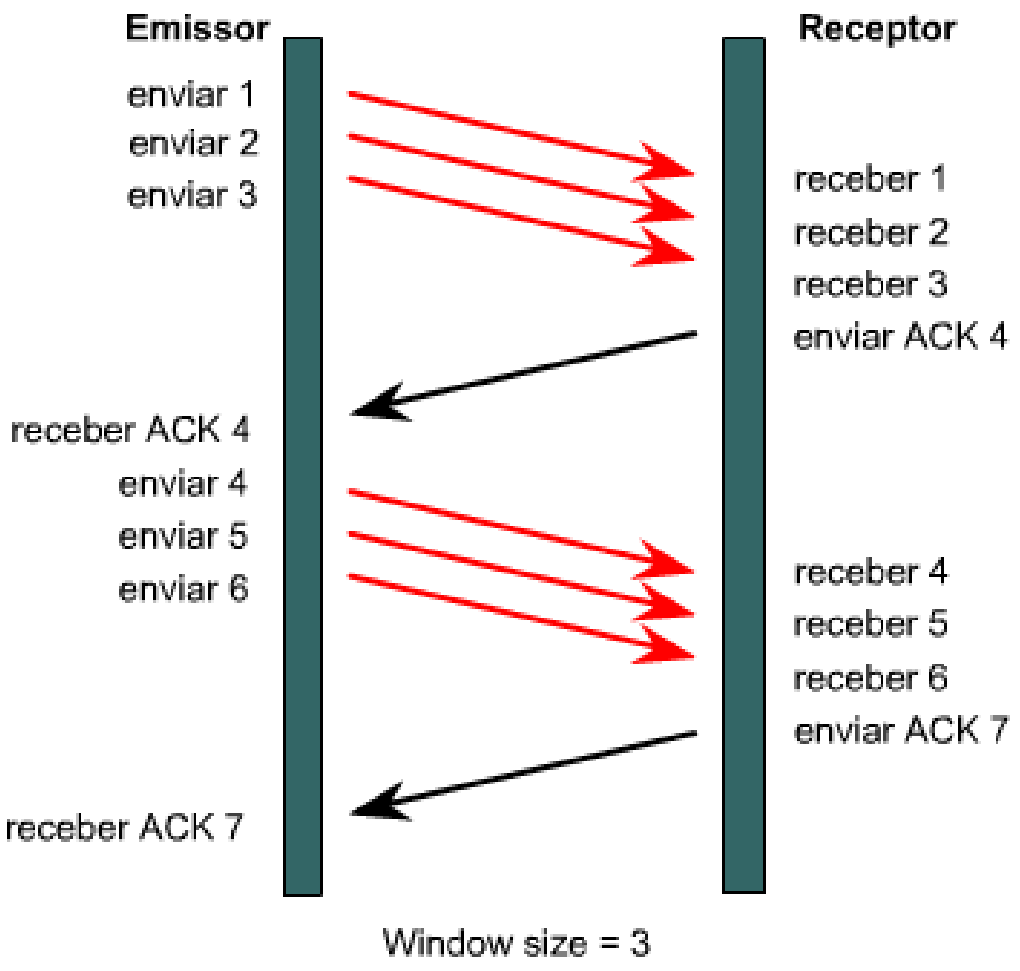


TCP – Three-way handshake



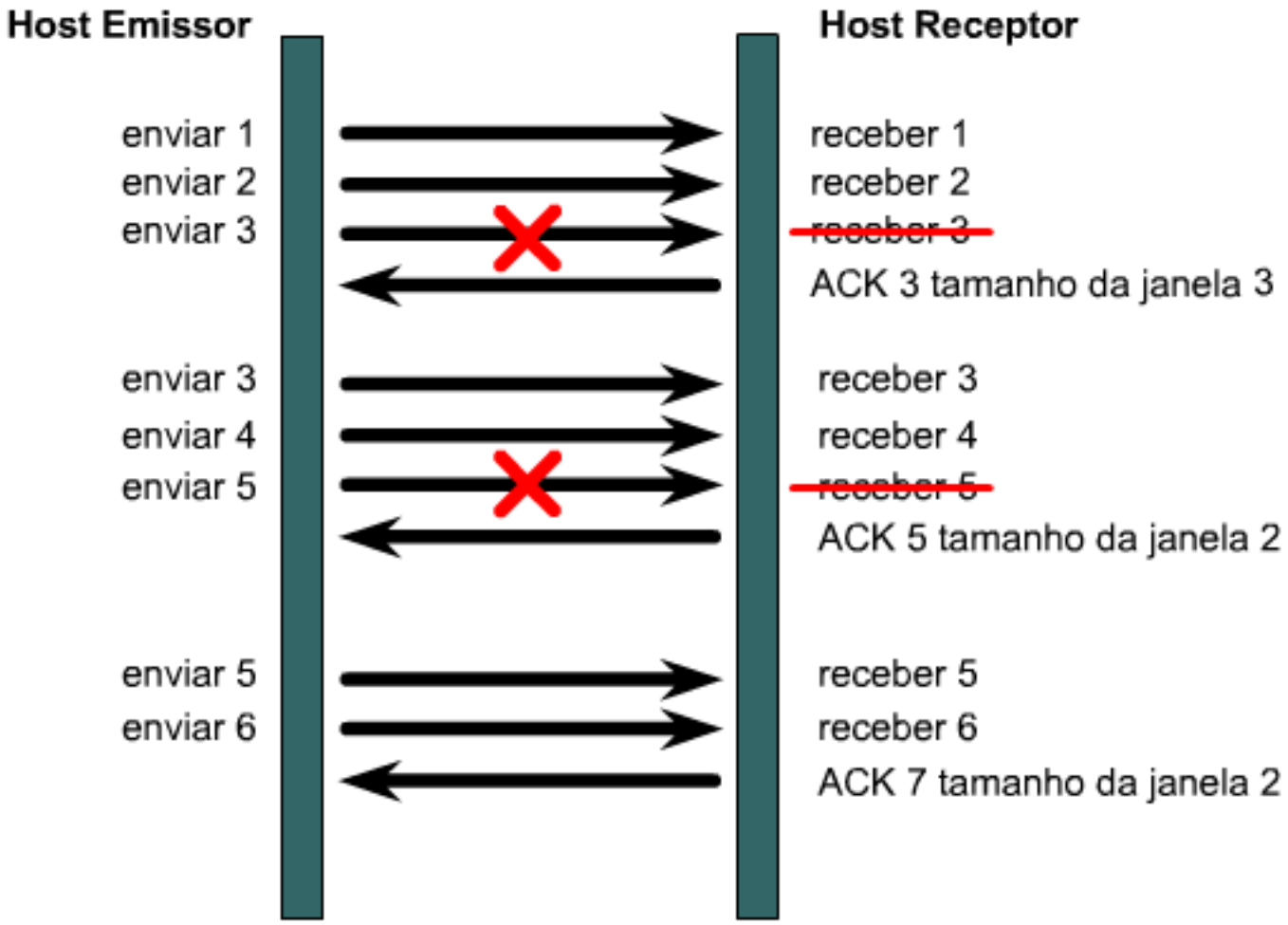
TCP – Controle de fluxo

- *Window:* número de pacotes esperado.
- É gradualmente aumentado quando possível.
- É diminuido quando a rede fica congestionada.



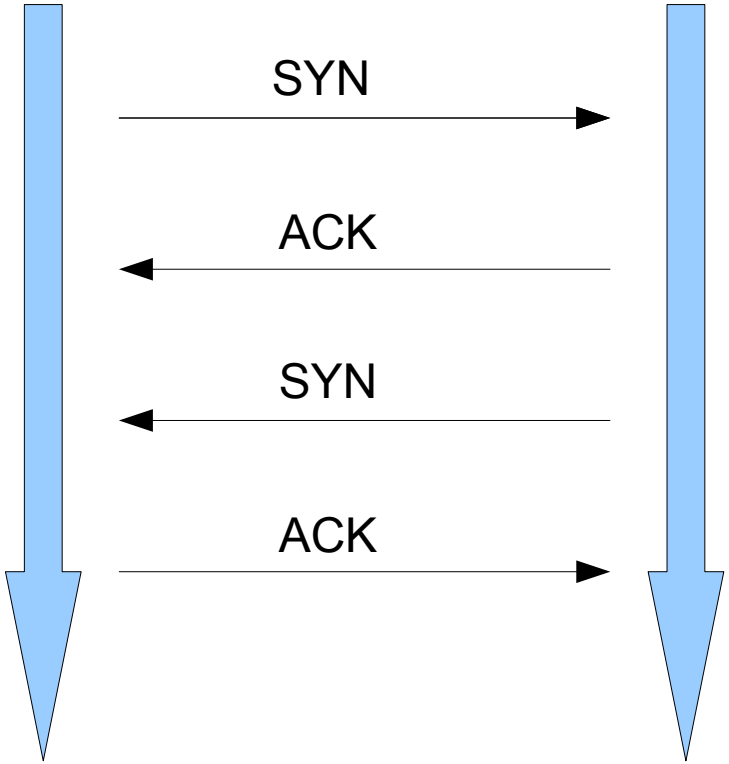
TCP – Falha no controle de fluxo

- Diminuição da janela, após repetidas falhas.
- Reenvio a partir do ponto de falha.



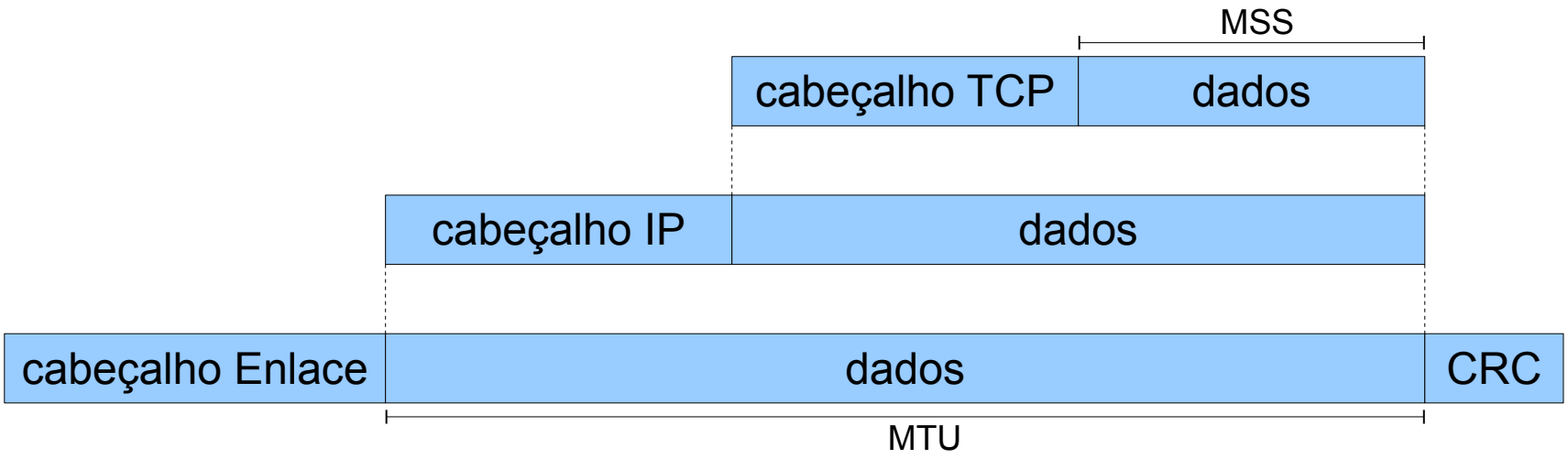
Three-way handshake is a LIE!!!

- Segundo RFC793
- Temos na verdade um 4-way handshake



TCP

- cwnd (congstion window) = quantidade de bytes que podem ser transmitidos
- threshold = controla o crescimento da janela
- MTU (maximum transmission unit) = 1500 bytes (ethernet)
- txwnd (janela de transmissão = mínimo entre rcvwnd e cwnd
- MSS (maximum segment size) = MTU – 20 bytes (cabeçalho TCP) – 20 bytes (cabeçalho IP)
- MSS mínimo = 536 bytes

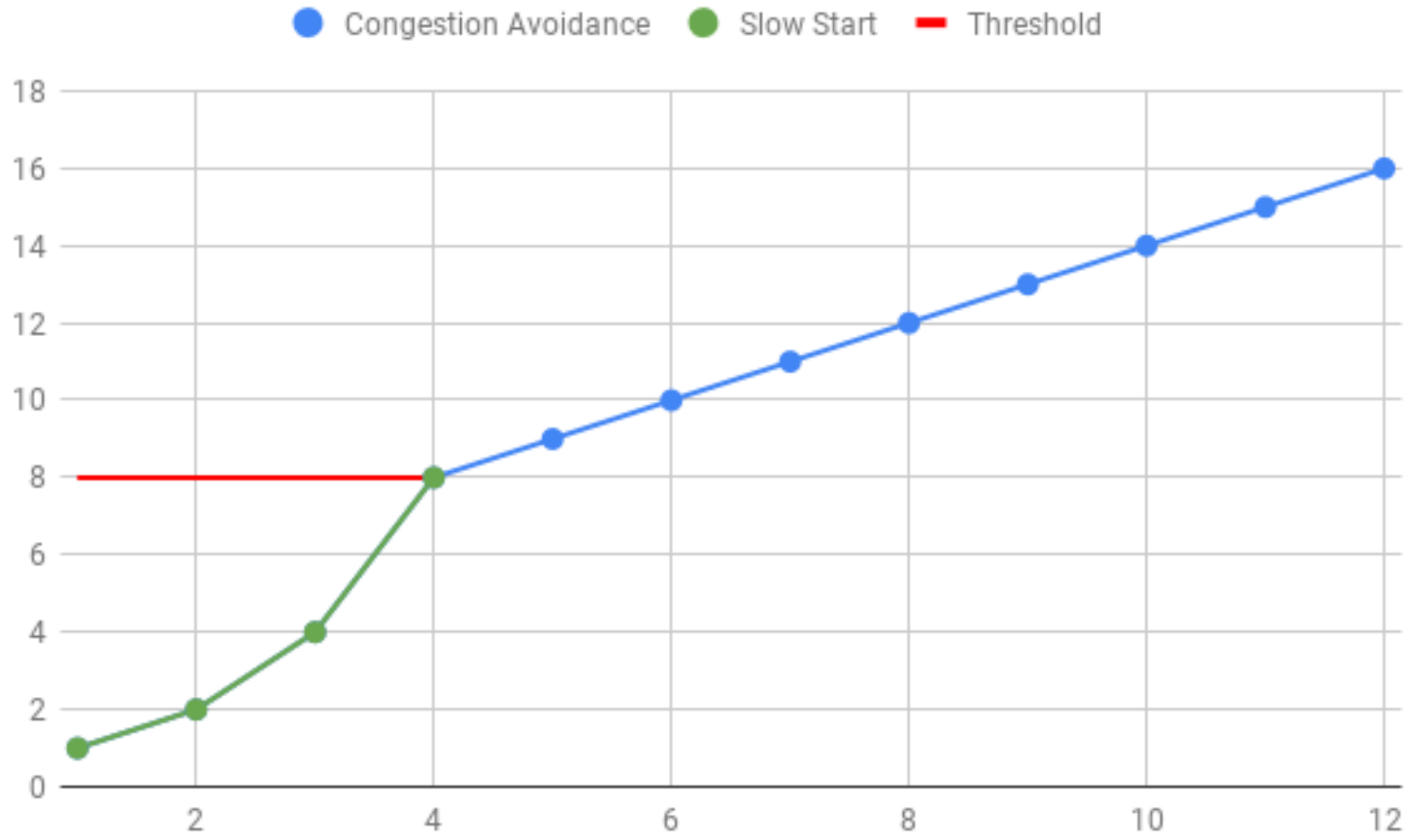


TCP

- cwnd (congstion window) = 1 byte (MSS)
- Threshold = 65535 bytes
- rcvwnd informado pela requisição SYN (abertura de conexão)
- Trata perdas (timeout ou duplicação) como congestionamento.
- Se ocorre timeout, reinicia em slow start.
- Se ocorre 3 ACKs duplicados, diminui a oferta. threshold = cwnd / 2
- Slow Start → Inicia com cwnd = 1. Enquanto cwnd < threshold, duplica cwnd a cada ACK recebido.
- Congestion Avoidande → Enquanto cwnd >= threshold, incrementa cwnd em 1 a cada ACK recebido.

TCP

Comportamento a partir de slow start até atingir congestion avoidance



TCP

Comportamento serrilhado do TCP

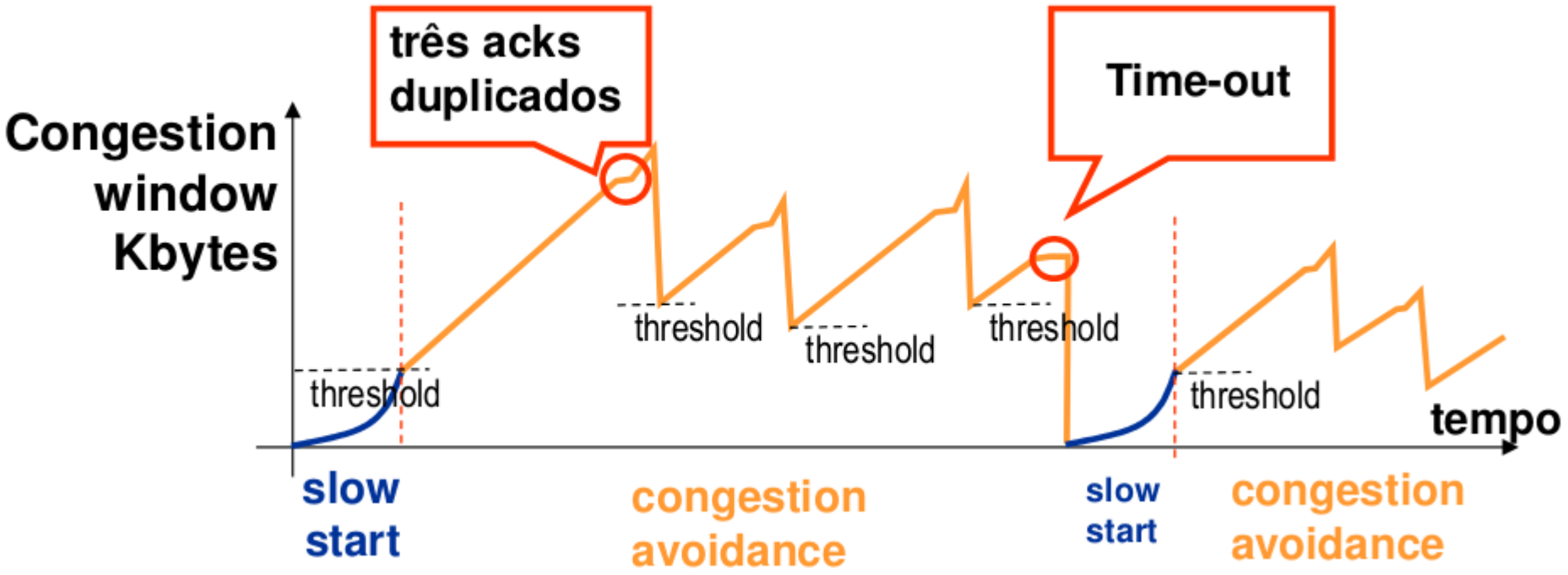
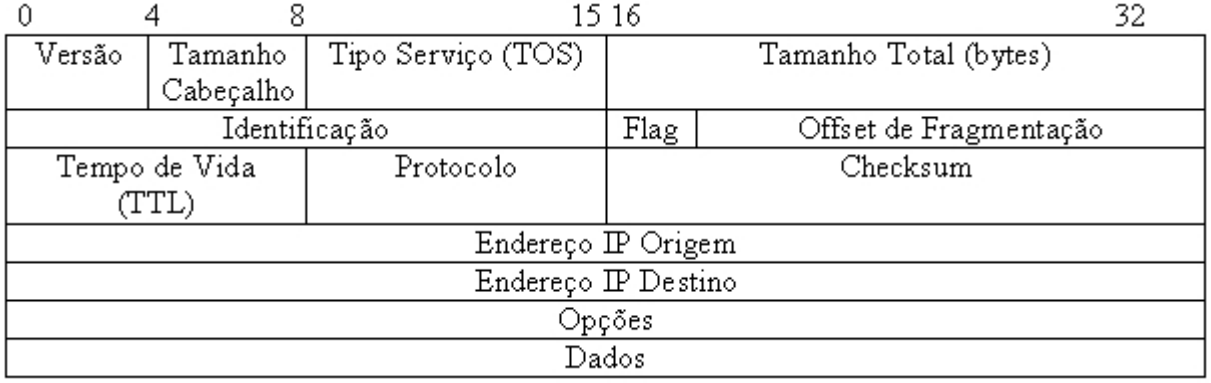


Imagem dos slides do Prof. Aguiar

Protocolos

IP – Internet Protocol

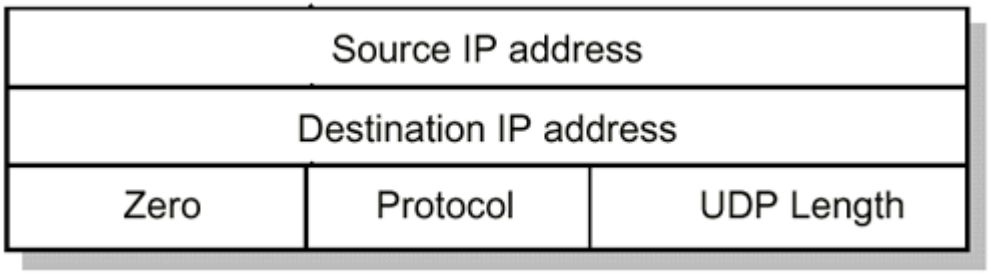
- Atua na camada 3
- Responsável pelo endereçamento dos pacotes



Protocolos

UDP – User Datagram Protocol

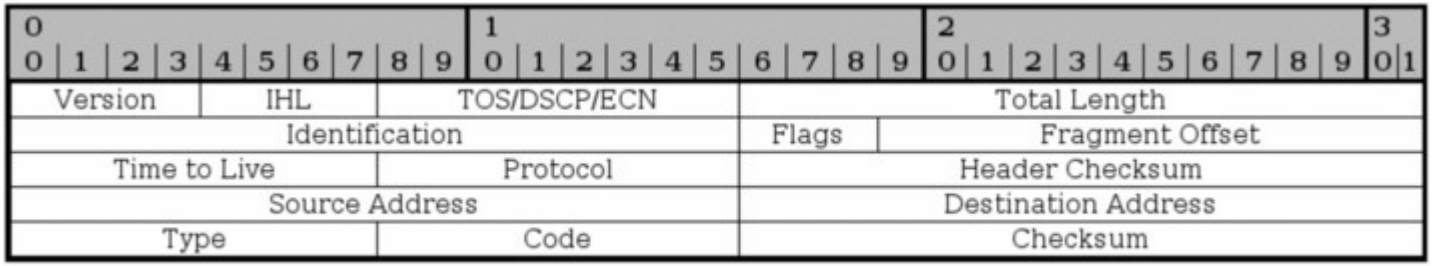
- Atua na camada 4
- Não é orientado à conexão



Protocolos

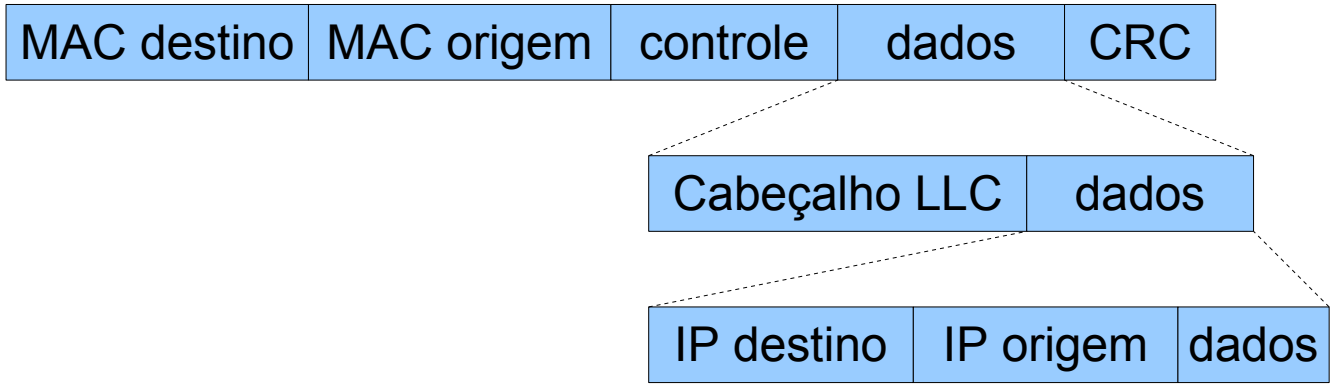
ICMP – Internet Control Message Protocol

- Atua na camada 3
- São as mensagens de controle de equipamentos de rede



Encaminhamento de Pacotes

- Dentro do mesmo domínio de rede, os pacotes são encaminhados com base no endereço MAC
- Pacotes destinados para fora do mesmo domínio de rede são encaminhados com base no IP
- A cada salto entre domínios de rede diferentes, o IP é usado para determinar o destino e o MAC para encaminhar o pacote dentro do domínio de rede
- Para determinar “o caminho correto”, o endereço MAC é alterado a cada salto



Address Resolution Protocol

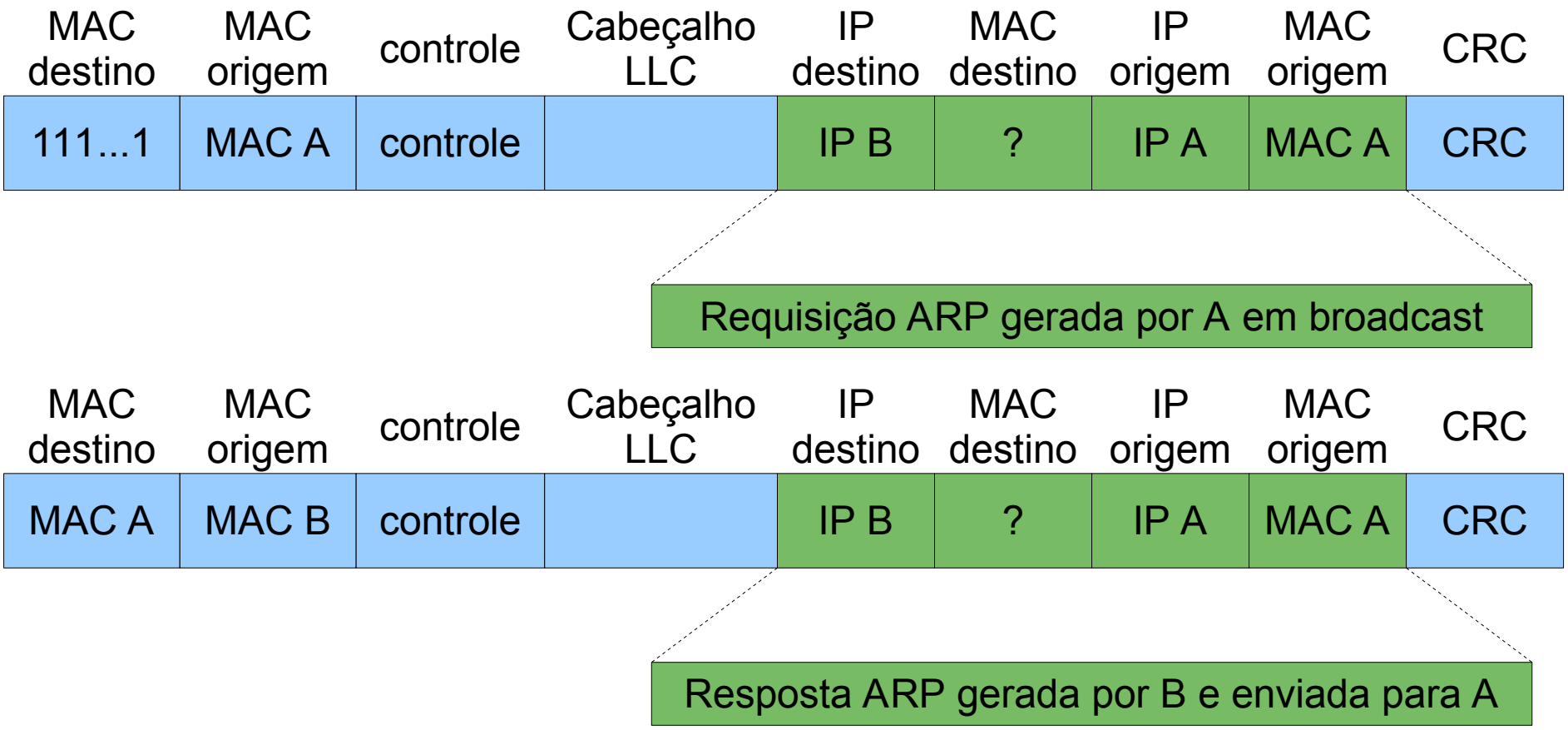
- O quê?
  - Resolução de endereços IP em endereços MAC.
  - Anunciaçã de novo endereço MAC na rede local.
- Por quê?
  - Dado um IP, como determinar o $MAC?$
  - Manutenção do $cache$ de mapeamento.
- Como?
  - Pacotes de requisição / resposta ARP.
  - Difusão local – um $broadcast$ a nível de enlace caracteriza um protocolo de enlace, não de rede.

Address Resolution Protocol

- Quando?
  - Quando o *MAC* do destinatário é desconhecido.
  - Após o vencimento do *cache*.
  - Ao iniciar a máquina.
- No *IPv6*, dá lugar ao *Neighbor Discovery Protocol*.

Address Resolution Protocol

Suponha que um host A queira saber o MAC de um host B



Ataque por *ARP Spoofing*

- O quê?
  - Alteração maldosa do *cache* de mapeamento *ARP* (às vezes chamada de *ARP cache poisoning*).
- Por quê?
  - *Passive sniffing*: fuçar o tráfego.
  - *Man-in-the-middle*: alterar o tráfego
  - *Denial of Service*: interromper o tráfego.
- Como?
  - Através de pacotes de anunciação *ARP* forjados.
  - Em geral, divulga-se o *MAC* do atacante com o *IP* do *Gateway*.

FTP, HTTP, SSH, SMTP, SQL

FTP – File Tranfer Protocol

- Transferência de arquivos numa rede
- Por padrão, usa as portas TCP/20 para transferência de dados e TCP/21 para controle

HTTP – Hypertext Transfer Protocol

- Trabalha no tratamento de requisições entre cliente e servidor, normalmente para sites
- Por padrão, usa a porta TCP/80

SSH – Secure Shell

- Acesso seguro à administração remota e tunelamento de conexões
- Por padrão, usa a porta TCP/22

FTP, HTTP, SSH, SMTP, SQL

SMTP – Simple Mail Transfer Protocol

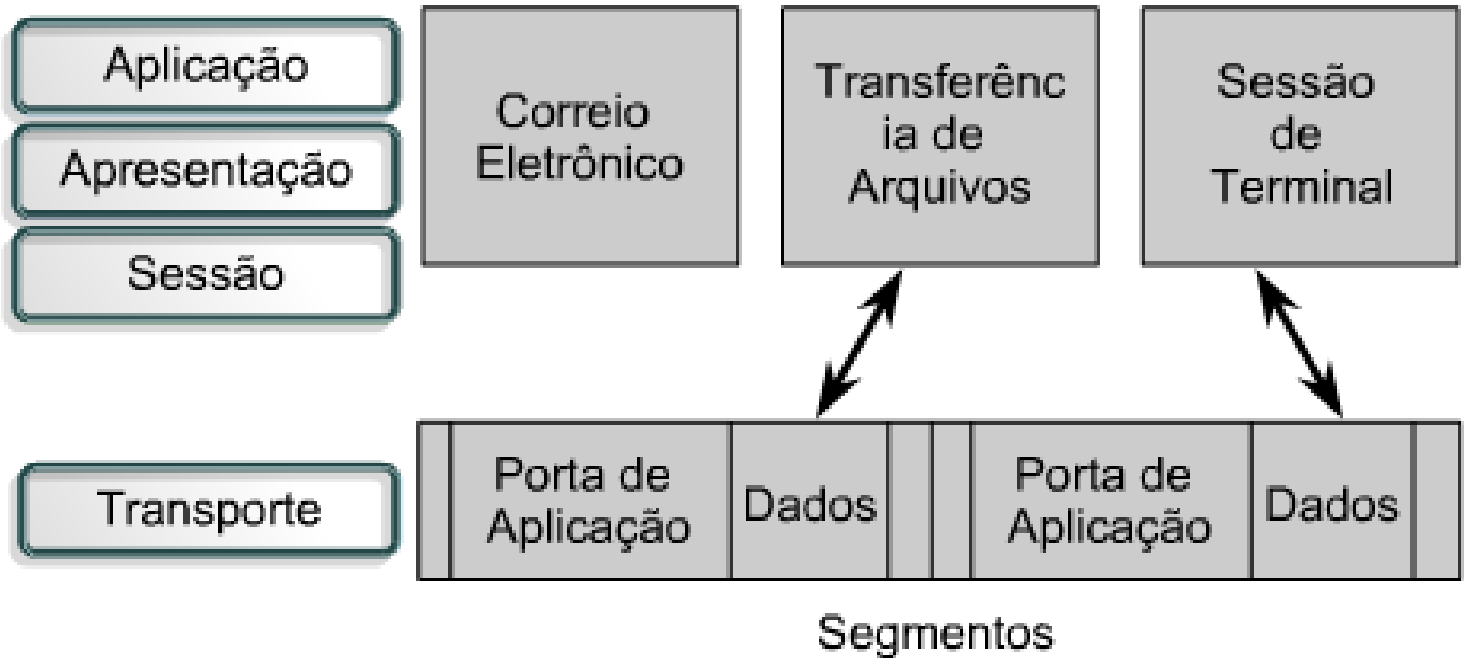
- Usado para transmissão de e-mails
- Por padrão, usa a porta TCP/25

SQL – Structured Query Language

- Linguagem de programação de banco de dados
- Por padrão, usa a porta TCP-UDP/156. Em casos específicos usa as portas TCP-UDP/3306 e TCP-UDP/5432

Sockets

- Constituem canais lógicos de comunicação.
- São caracterizados por:
  - Endereço de rede, no caso o IP.
  - Número de porta de 2^{16} bits (0 a 65535).
- Multiplexam o canal físico de comunicação.



Sockets

- Os sistema operacional determina qual processo recebe os pacotes oriundos de uma porta específica.
- Alterar esta relação requer privilégios elevados.

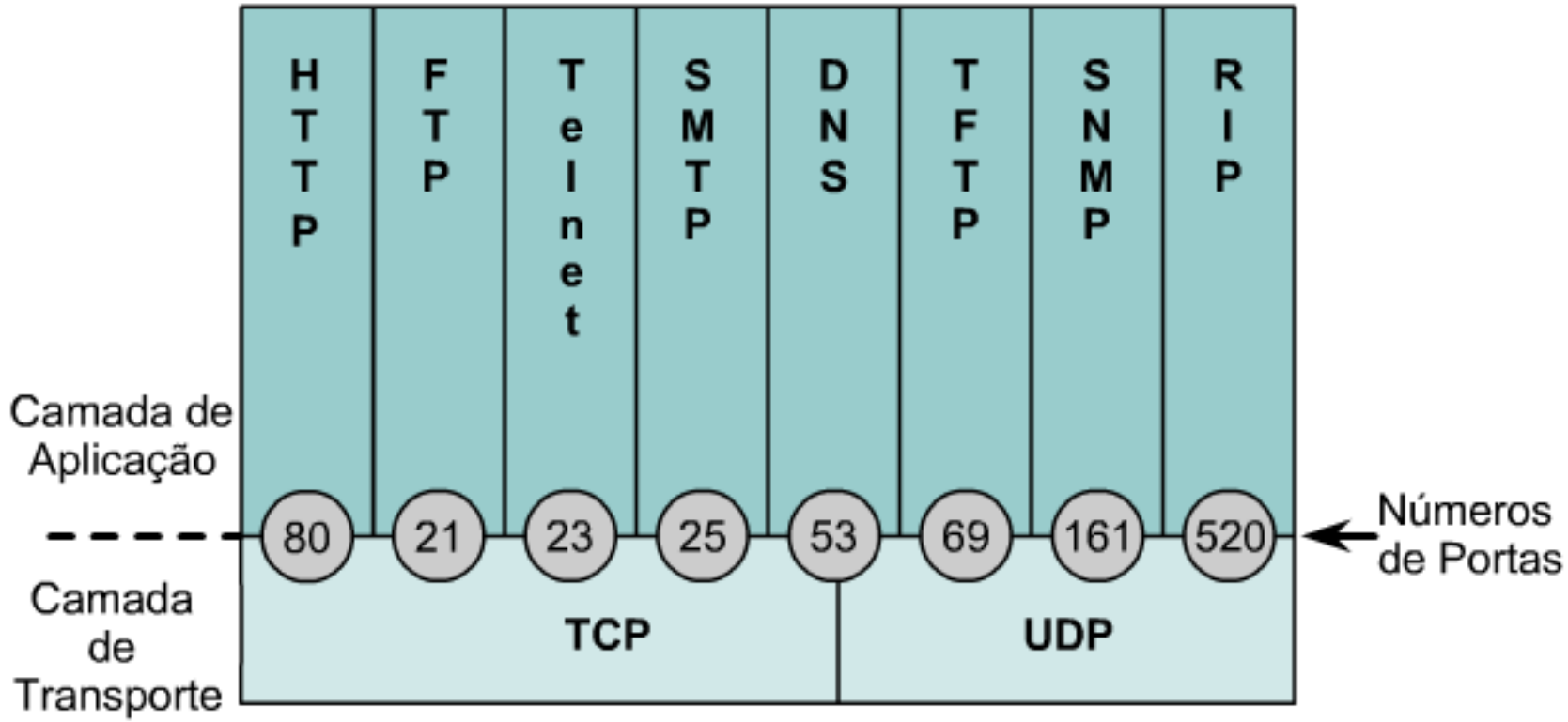
Sockets – Faixas de portas

- 0 a 1023 – Portas bem conhecidas *(well-known ports)*. Enumeram serviços oferecidos.
- 1024 a 49151 – Portas registradas. Utilizadas por aplicações comerciais.
- 49152 a 65535 – Portas privadas (ou dinâmicas). Utilizadas a esmo pelos usuários.
- O órgão que regula as faixas é o *Internet Assigned Numbers Authority (IANA).*

www.iana.org/assignments/port-numbers

Well-known sockets

- São portas padronizadas para serviços comuns.
- Processos → Serviços *(daemons)*.
- Alterar a porta padrão requer privilégios de *root*.



Visualizando portas ativas com *netstat*

- Com *netstat* descobrimos as mais variadas informações sobre o subsistema de rede.
- Sintaxe

$ netstat

-n exibe a informação em formato numérico.

-a exibe *sockets* em modo de escuta ou não.

-t exibe *sockets TCP.*

-u exibe *sockets UDP*.

-p exibe os processos ligados aos *sockets*.

Investigando portas ativas com *nmap*

- Uma das mais poderosas ferramentas para auditoria e mapeamento de redes é o *nmap*.
- Uma versão gráfica simples e útil é o *zenmap.*
- Sua sintaxe é complexa, por isso, veremos exemplos específicos.

  # nmap -A -sT -sU -t4 <localhost|ip|fqdn>
  exibe as portas TCP e UDP ativas na máquina especificada e detecta o SO.

  - Experimente estes dois:

    $ nmap -A -T4 scanme.nmap.org

    $ nmap -A -T4 playground.nmap.org

Domain Name System

- O quê?
  - Mapeamento de nomes literais em IPs.
- Por quê?
  - Quantidade imensa de máquinas na Internet.
  - Dificuldade de memorizar IPs.
  - Dinamismo de endereços.
- Como?
  - Reqisições aos servidores de nomes.
  - Banco de dados hierárquicamente distribuído.

Domain Name System

- A nomeação de máquinas numa rede segue um esquema hierárquico.
- Os nomes são agrupados em domínios, que por sua vez são agrupados em domínios superiores.
- A separação de domínios é feita por “.”.
- O domínio raiz é identificado por “.”.
- O agrupamento é mais local à esquerda e mais global à direita.

Domain Name System

- Alguns domínios de primeiro nível *(top-level domains)* são: *org, com, gov, br, etc*.
- Nomes completos são chamados de *FQDN*.
- Domínio da *UFRJ: ufrj.br*.
- Domínio do *DCC: dcc.ufrj.br*.
  - Subdomínio de *ufrj.br*.
- Em geral, a máquina que contém páginas *HTML* se chama *www*.
  - *www.dcc.ufrj.br* contém as páginas do *DCC*.
  - *www.ufrj.br* contém as páginas da *UFRJ*.

Servidores raiz no mundo

- Apontam para os servidores de nomes responsáveis pelos *top-level domains.*
- O servidor soberano sobre um domínio é chamado de *authoritative name server.*
- Uma lista dos *top-level domains* pode ser obtida em *http://www.iana.org/domains/root/db/*
- Busque por *root servers in the world* em *maps.google.com.*

Descobrindo DNS primário e secundário

- O aquivo */etc/resolv.conf* contém informações sobre servidores de nomes, domínios locais e resolução de nomes.
- Uma entrada de servidor de nomes é na forma

```
nameserver <ip_do_servidor>
```

- O primeiro registro é o DNS primário e o segundo é o DNS secundário.
- Execute

```
$ cat /etc/resolv.conf
```

Registros *DNS*

- Em servidores de nomes, registros são guardados com uma sintaxe específica:

  A↔registros comuns *IPv4*.

  AAAA↔registros comuns *IPv6*.

  CNAME↔apelidos, nomes alternativos.

  MX↔servidores de e-mail.

  NS↔servidores de nomes.

  HINFO↔informações de hardware.

  PTR↔mapeamento reverso endereço→nome.

  SOA↔autoridade sobre uma zona.

Consultas *DNS* com *dig*

- O programa *dig faz* consultas *DNS* detalhadas.
- Ele imprime informação no formato em que os registros são usualmente armazenados.
- Sintaxe:

  $ dig [opções] <nome> [tipo] [@servidor]

  tipo é um dos tipos de registros *DNS* vistos.

  @servidor é opcional e especifica o servidor utilizado para a consulta.

  [opções] pode ser uma ou mais das listadas na próxima página.

dig – opções

+*[no]short* [não]devolve apenas o *IP.*

+*[no]answer* [não]devolve a seção de resposta.

+*[no]authoritative* [não]devolve a seção de autoridade.

+*[no]question* [não]devolve a resposta.

+*[no]all* [não]devolve todas as seções.

+*[no]stats* [não]devolve tempos de resposta.

+*[no]additional* [não]devolve informações adicionais.

+*[no]trace* [não]rastreia os servidores visitados.

Consultas *DNS* com *dig*

- Consultas interessantes:

```
$ dig yahoo.com
$ dig yahoo.com NS
$ dig ssh.dcc.ufrj.br
$ dig dcc.ufrj.br NS
$ dig google.com MX
$ dig debian.org
$ dig inter.net AXFR @ns02.eusc.inter.net
$ dig @luit.iitg.ernet.in iitg.ernet.in
  axfr
```

Descobrindo e alterando o nome local

- O aquivo */etc/hostname* contém o nome do computador local em uma linha única.
- Visualizando o nome:

```
$ hostname
```

- *Visualizando o nome totalmente qualificado:*

```
$ hostname --fqdn
```

- Alterando o nome (temporariamente)*:*

```
$ sudo hostname <novo_nome>
```

- Para alterar definitivamente, edite o arquivo */etc/hostname* como *root*.

Descobrindo o nome de domínio

- O nome de de domínio constitui a parte do $FQDN$ após o primeiro ponto.
- Em geral, depende dos arquivos `/etc/hosts` e `/etc/hosts.conf`.
- Visualizando o nome:

```
$ dnsdomainname
```

- O nome de domínio não pode ser alterado através deste comando.

Dynamic Host Configuration Protocol

- Provê uma forma de configurar máquinas:
  - Fornecendo um IP dinâmico.
  - Indicando DNS primário e secundário.
  - Informando o $Gateway$ padrão.
- É largamente utilizado por provedores.
- Permite fixar IPs para máquinas chave na rede.
- Dispensa a atribuição de IPs estáticos.
- Facilita o ingresso de $notebooks$ na rede.
- Facilita a ampliação da rede local.

Network Address Translation

- Comunicação de uma rede privada com uma rede exterior.
- Toda comunicação deve partir de dentro.
- Ocultamento da estrutura interna da rede.
- Economia de endereços públicos.
- Conversõs de endereços privados↔roteador.
- Roteador possui um endereço externo público.

Endereçamento $IPv4$

- Deve ser único dentro das redes alcançáveis.
- Composto de 32 $bits$ (ou 4 $bytes$).
- Representado em 4 números decimais, em geral.
- Dividido em cinco classes: A, B, C, D e E.

Notação decimal pontuada

- Mais amigável.
- Simples e rápido de visualizar e escrever

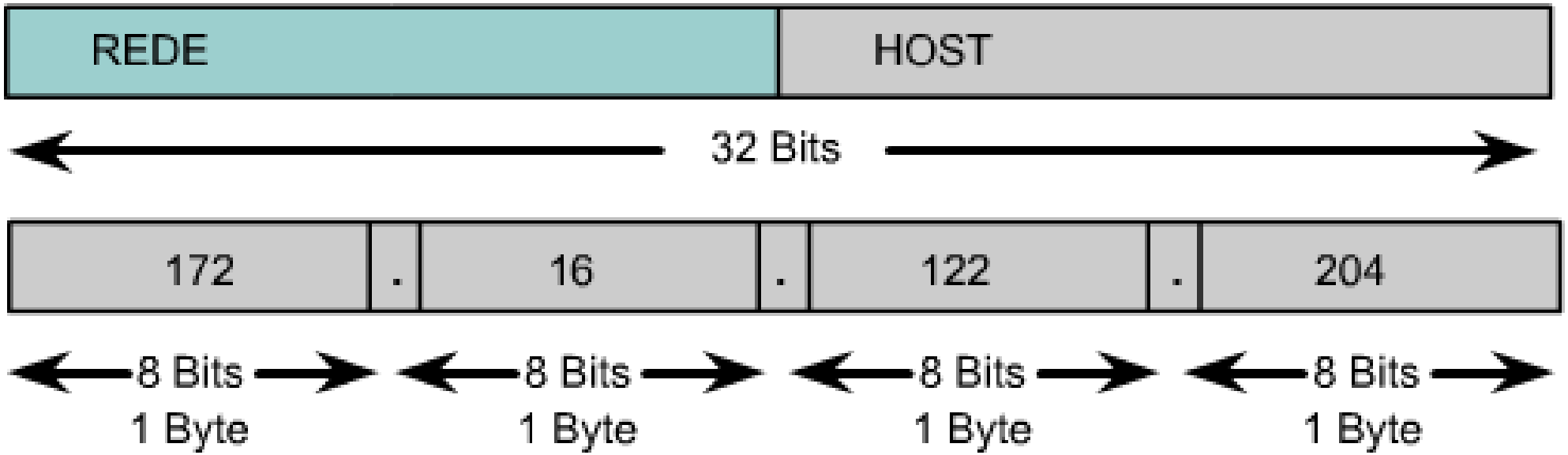
11001000110010010000001101001101

=

200.201.3.77

Estruturação de endereços IP

- A porção de rede equivale a um edifício.
- A porção de estação equivale a um apartamento.
- Há $bits$ para rede e $bits$ para estação.



Cálculo de endereços IP

- Simples conversão binário - decimal e vice-versa
- Cada 8 bits = 1 octeto

  Exemplo:

11001000.11001001.00000011.01001101

11001000 = 200

11001001 = 201

00000011 = 3

00000011 = 77

Endereço decimal = 200.201.3.77

Classes de endereços IP

- Definem redes com tamanhos diferentes.
- A classificação se baseia no primeiro octeto.
- Classes A, B e C: utilizadas normalmente
- Classe D: utilizada para $multicast.$
- Classe E: reservada para pesquisas.

Classes de endereços IP

Classe	Informações referentes ao primeiro *byte*			Número de redes por classe	Número de estações por rede
	Bits de ordem superior	**Primeiro endereço**	**Último endereço**		
A	0	0	127	126*	16M
B	10	128	191	16K	64K
C	110	192	223	2M	254
D	1110	224	239		
E	11110	240	247		

* A faixa 127.x.y.z corresponde ao *loopback*.

Administração de endereços IP

- Endereços públicos:
  - Únicos.
  - Distribuição dinâmica pelos $ISPs$.
- Endereços reservados:
  - Atribuídos pelo $IANA$ – pela $FAPERJ$, no Rio.
  - Estáticos e possuídos por instituições.
- Endereços privados.
- Endereços especiais.

Whois service directory

- O comando *whois b*usca informações sobre domínios, endereços, instituições e indivíduos.
- Um *whois* no site do *IANA: http://whois.iana.org/*
- Com ele é possível achar informações interessantes sobre máquinas na *Internet*.
- Sintaxe:

```
$ whois <endereço_ip>
```

Alguns endereços interessantes

- Experimente os endereços abaixo:

```
$ whois 146.164.0.0
$ whois 201.51.150.0
$ whois 202.12.27.0
$ whois 192.203.230.0
$ whois 192.112.36.0
$ whois 128.0.0.0
```

Endereços privados

- Não utilizados publicamente.
- Redes sem visibilidade mundial.
- Economia de endereços públicos.
- Faixas especiais nas classes A, B e C:

  10.0.0.0 a 10.255.255.255.

  172.16.0.0 a 172.31.255.255.

  192.168.0.0 a 192.168.255.255.

Endereços especiais

Primeiro octeto	**Segundo octeto**	**Terceiro octeto**	**Quarto octeto**	**Significado do endereço**
0	0	0	0	**Estação atual**
127	Qualquer seqência de *bits*			***Loopback***
Sequência de zeros		Porção de estação		**Estação na rede atual**
Porção de rede		Sequência de zeros		**Endereço da rede atual**
Porção de rede		Sequência de uns		**Difusão em rede remota**
255	255	255	255	**Difusão na rede local**

Máscaras de sub-rede

- São a base para a existência das sub-redes.
- Extendem as máscaras-padrão.
- Máscaras-padrão:
  - Classe A: 255.0.0.0.
  - Classe B: 255.255.0.0.
  - Classe C: 255.255.255.0.
- Notação com barra:
  - Indica o número de $bits$ de rede.
  - Todos estes tem o valor 1.

Sub-redes

- Multiplexam um único IP público.
- Externamente, parecem uma única rede.
- Internamente, são múltiplas redes.
- Aproveitam a amplitude de certas classes:
  - A classe A permite 16M estações em uma rede.
  - É possível criar sub-redes com menos estações.

Cálculo de Sub-redes

- Podem ser representadas pela notação decimal pontuada ou pelo numero de bits

11111111.11111111.11111111.00000000

=

255.255.255.0

=

/24

Identificação de Endereço IP

- Depende da sua máscara de rede.
- Um endereço IP pode ser:
  - Rede
  - Host
  - Broadcast
- Endereço de rede é o primeiro endereço do range de IPs.
- Endereço de broadcast é o último endereço do range de IPs.
- Endereço de host são todos os endereços IPs restantes.

Identificação de Endereço IP

Exemplos:

- Identifique e classifique cada endereço abaixo:
  - 146.164.10.2 255.255.255.0
  - 200.201.34.176 255.255.0.0
  - 176.20.82.3 /30

- Diga se os endereços dados estão na mesma rede:
  - ip: 192.168.12.62 masc: 255.255.255.192 e ip: 192.168.12.68 masc: 255.255.255.192
  - Ip: 212.84.175.93/17 e 212.84.223.93/17

VLSM – Variable Length Subnet Masking

- Técnica que permite dividir uma rede em outras sub-redes de tamanhos diferentes.
- É um processo recursivo.

  Exemplo:

- Uma filial de um escritório será aberta em uma nova cidade. São necessários:
  - 10 computadores para o setor financeiro
  - 10 computadores para a gerência
  - 63 computadores para os funcionários
  - 28 computadores para o SAC
  - 5 computadores para o setor de RH

Throughput

- De maneira simples, é a quantidade de dados transferidos de um lugar a outro
- Pela sua ampla aplicabilidade, vamos considerar apenas no âmbito de redes
- Dessa forma, definimos como a taxa média de transferência de dados através de um link
- Para transferências baseadas no protocolo TCP calculamos o throughput como:

$$\frac{\text{TCP Window size em bits}}{\text{Latência em segundos}} = \text{Throughput em bits por segundo}$$

Throughput

- Como visto, os sistemas usam o TCP Window Scaling para definir automaticamente o TCP Window Size
- Nos sistemas Windows o padrão é 64KB e podem ir até 16MB
- Nos sistemas Linux isso é ativado no arquivo /proc/sys/net/ipv4/tcp_window_scaling e difinido nos arquivos /proc/sys/net/ipv4/tcp_rmem e /proc/sys/net/ipv4/tcp_wmem

Throughput

- Alguns exemplos:

1. Calcular o throughput de um host windows com latência para o gateway de 2ms

   TCP Window Size = 64KB * 8 = 524.288 bits

   Latência = 2 ms = 0.002 segundos

   524.288 / 0.002 = 262.114.000 bits/segundo

   Convertendo para megabits temos aproximadamente 262Mb/s de transferência entre o host e o gateway

Throughput

2. Calcular o throughput de uma rede com 10 hosts windows tendo como base uma latência de 25ms para determinado site

TCP Window Size = 64KB * 8 = 524.288 bits

Latência = 25 ms = 0.025 segundos

524.288 / 0.025 = 20.971.520 bits/segundo ~ 21Mb/s

Como a rede tem 10 hosts windows então seu throughput total é de 210Mb/s ou 26,25 MB/s

OBS: O host windows foi usado por questão de simplicidade. Caso seja uma rede mista devemos calcular seu total considerando cada tamanho específico. Ex: 2 Win + 3 Linux + ...

Throughput

3. Considere que temos 2 datacenters distintos, um em cada cidade, e temos um link de 10Gb/s entre eles com uma latência de 30ms. Qual o throughput esperado entre eles? Por comodidade, assuma TCP Window de 64KB.

TCP Window Size = 64KB * 8 = 524.288 bits

Latência = 30ms = 0.030 segundos

524.288 / 0.030 = 17.476.266 bits/segundo ~ 17.4Mb/s

Note que o throughput, apesar do link de 10Gb/s, atingirá apenas 17.4Mb/s

Throughput

- No exemplo 3 o link estava subutilizado. Para melhorar esse problema temos duas opções: Alterar o TCP Window Size ou diminuir a latência
- Muitas vezes a latência é difícil, ou até mesmo impossível, de ser melhorada. Então vamos trabalhar no TCP Window Size que é o lado mais fácil
- Como o link é de 10Gb/s e queremos nos aproximar ao máximo disso, temos o seguinte cálculo:

  10.000.000.000b/s * 0.030s = 300.000.000 bits ou 37.5KB

Throughput

- Vale notar que embora com essa redução a taxa de transferência melhore sensivelmente, o uso de memória usada para buffer aumenta.
- Existem também outros fatores que devem ser considerados como taxa de perda de pacotes, jitter (variação da latência), processamento, barramento e etc

Protocolos de Roteamento

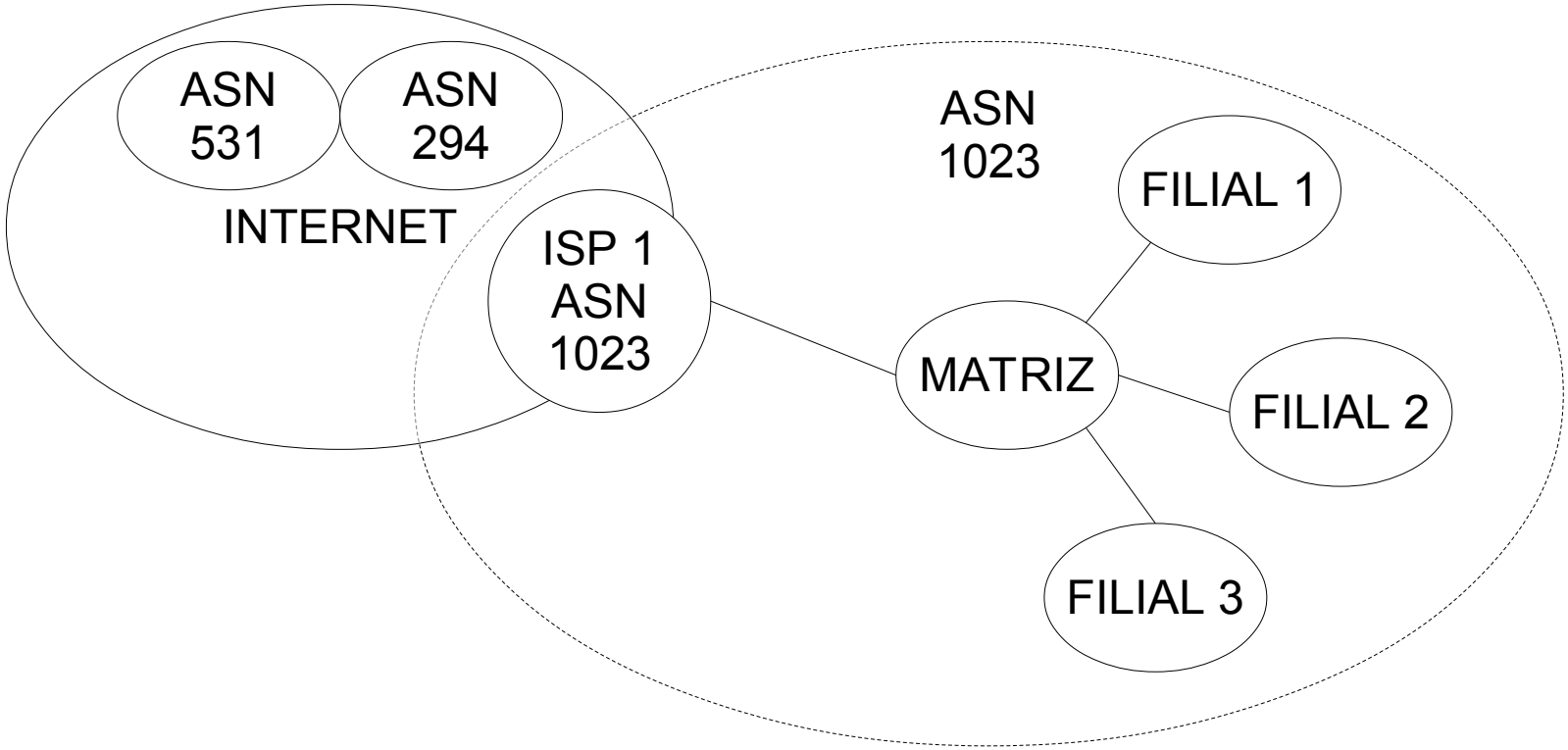
- Roteamento é o nome dado ao processo em que se escolhe qual roteador deve ser usado para que um pacote seja enviado ao seu destino
- Os protocolos de roteamento determinam e/ou atualizam o conteúdo das tabelas de roteamento
- De acordo com o conteúdo das tabelas de roteamento, a escolha do roteador é feita pela análise do prefixo que corresponde ao endereço de destino
- Esses protocolos se dividem em dois tipos:
  - Interior Gateway Protocol (IGP), que distribuem as informações dentro de sistemas autônomos (AS)
  - Exterior Gateway Protocol (EGP), que distribuem as informações entre sistemas autônomos (AS) distintos

Protocolos de Roteamento

- Os protocolos do tipo interno são baseados em dois tipos:
  - Vetor de distância
  - Estado do enlace
- Um sistema autônomo (AS) é um conjunto de redes, ou uma única rede, que além de estar sob uma gestão comum tem características e políticas de roteamento comuns
- Cada AS distinto recebe um número de identificação, que é chamado de ASN

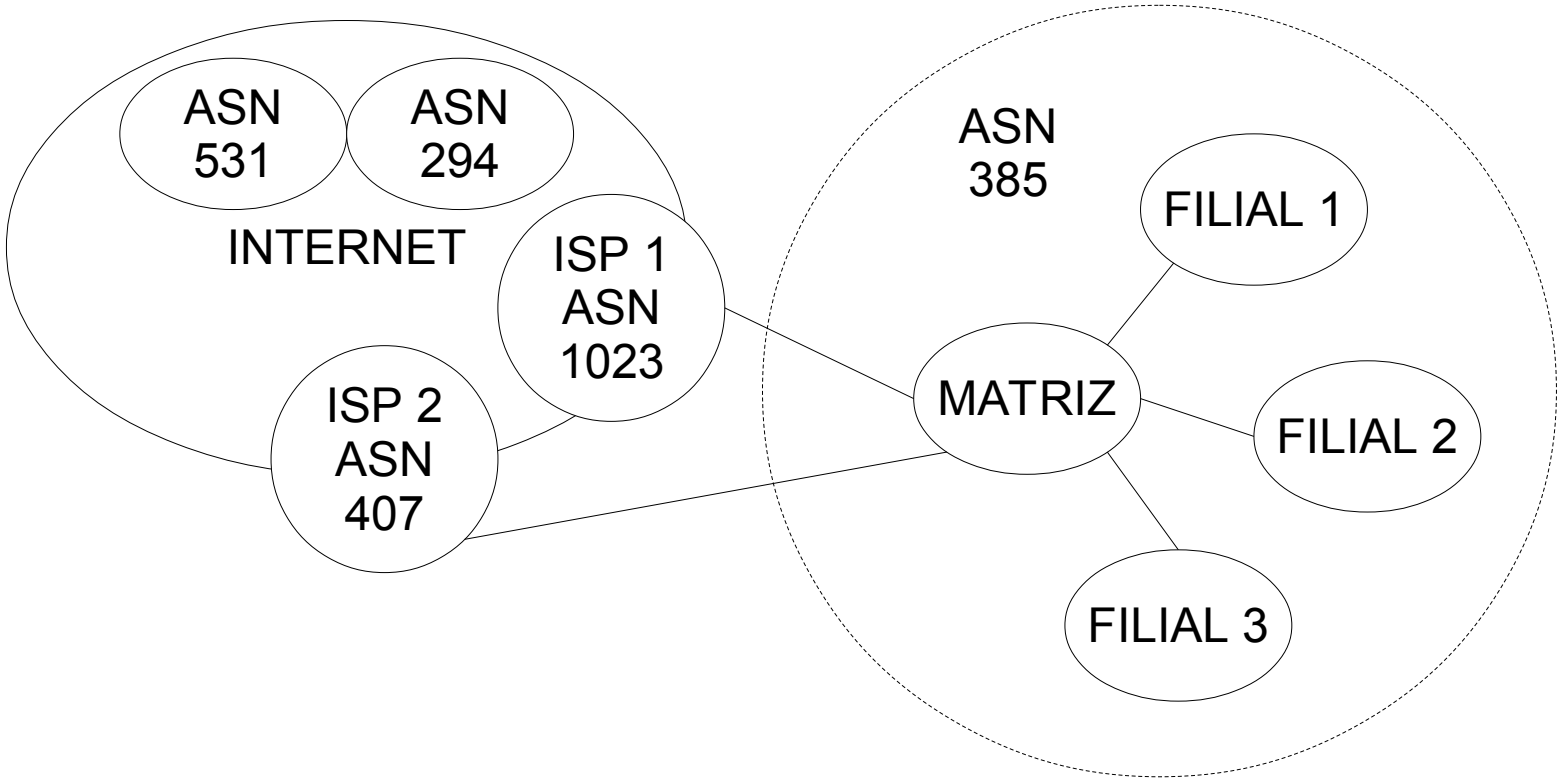
Protocolos de Roteamento

- Vamos imaginar que exista uma empresa com algumas filiais conectada na internet e que disponibilize serviços como e-mail e web. Se os Ips públicos usados nesses serviços são fornecidos por um provedor então a rede dessa empresa seria vista como uma extensão do AS do provedor que ela utiliza.



Protocolos de Roteamento

- Vamos agora imaginar que essa mesma empresa use um segundo ISP para balancear o trafego de entrada e saída e contar com uma redundância. A matriz então pede um range próprio de IPs para que essa rede não continue submissa as politicas do ISP 1 e ISP 2 e consiga, por exemplo, controlar totalmente o balanceamento.



Protocolos de Roteamento

- RIP (Routing Information Protocol)
  - Algoritmo Bellman-Ford
  - Facil configuração
  - Baixo poder de computação
  - Bom para pequenos ambientes
  - Convergência lenta
  - Grande consumo de banda (broadcast da tabela a cada 30 segundos)

Protocolos de Roteamento

- IGRP (Interior Gateway Protocol)
  - Determina o melhor caminho entre dois pontos
  - Considera a largura de banda e a latência
  - Converge mais rápido que o RIP
  - Sem limitação de saltos
  - Evita loops
  - Proprietário da CISCO
- EIGRP (Enhanced Interior Gateway Protocol)
  - Combina protocolos baseados em vetor de distancia e estado de enlace
  - Divulga apenas as redes que sofreram alterações
  - Também é proprietário da CISCO

Protocolos de Roteamento

- OSPF (Open Shortest Path First)
  - Projetado para grandes redes
  - Permite criar áreas de roteamento
  - Área de roteamento é uma coleção de sub-redes relacionadas
  - Redes pequenas podem usar uma única área
  - Envia mensagens Link State Advertisement (LSA) para informar aos vizinhos o estado dos enlaces conhecidos
- BGP (Border Gateway Protocol)
  - Protocolo de roteamento interdomínios
  - Criado pra ser usado nos roteadores principais da internet
  - Evita loops

Algumas Referências

- GOMES SOARES, Luiz Fernando; LEMOS DE SOUZA, Guido; Colcher, Sérgio – Redes de Computadores das LANs MANs e WANs às Redes ATM, Campus.
- TANENBAUM, Andrew S. – Computer Networks, Third Edition, PTR Prentice Hall.
- TITTEL, Ed – Teoria e problemas de redes de computadores, Bookman.
- SCHRODER, Carla – Redes Linux Livro de Receitas – O'Reillly media.
- Cisco Network Academy, disponível em http://cisco.netacad.net, acessado em 06/08/2015, às 16:08.

HORA DO TAG!