ARQUITETURA DE REDES DE COMPUTADORES CAMPUS ANCHIETA

Prof. Dr. João Carlos Lopes Fernandes
Joao.fernandes1@docente.unip.br
2022 – 1

Material de apoio didático

ELEMENTOS DAS REDES

- Camada física: elementos fundamentais para o funcionamento das redes
  - SERVIDORES: oferecem os recursos e serviços para as ESTAÇÕES DE TRABALHO (conjunto de computadores que compartilham recursos de hardware e acessam computadores remotos ou outras redes);
  - CLIENTES (ou Estações de Trabalho): solicitam serviços aos servidores;

ELEMENTOS DAS REDES

- PERIFÉRICOS: recursos compartilhados pelos clientes;
- PLACAS DE REDE: presente em servidores e clientes. Permite a comunicação entre máquinas;
- MEIOS DE TRANSMISSÃO: possibilita às placas de rede fazerem a comunicação entre servidores e clientes.

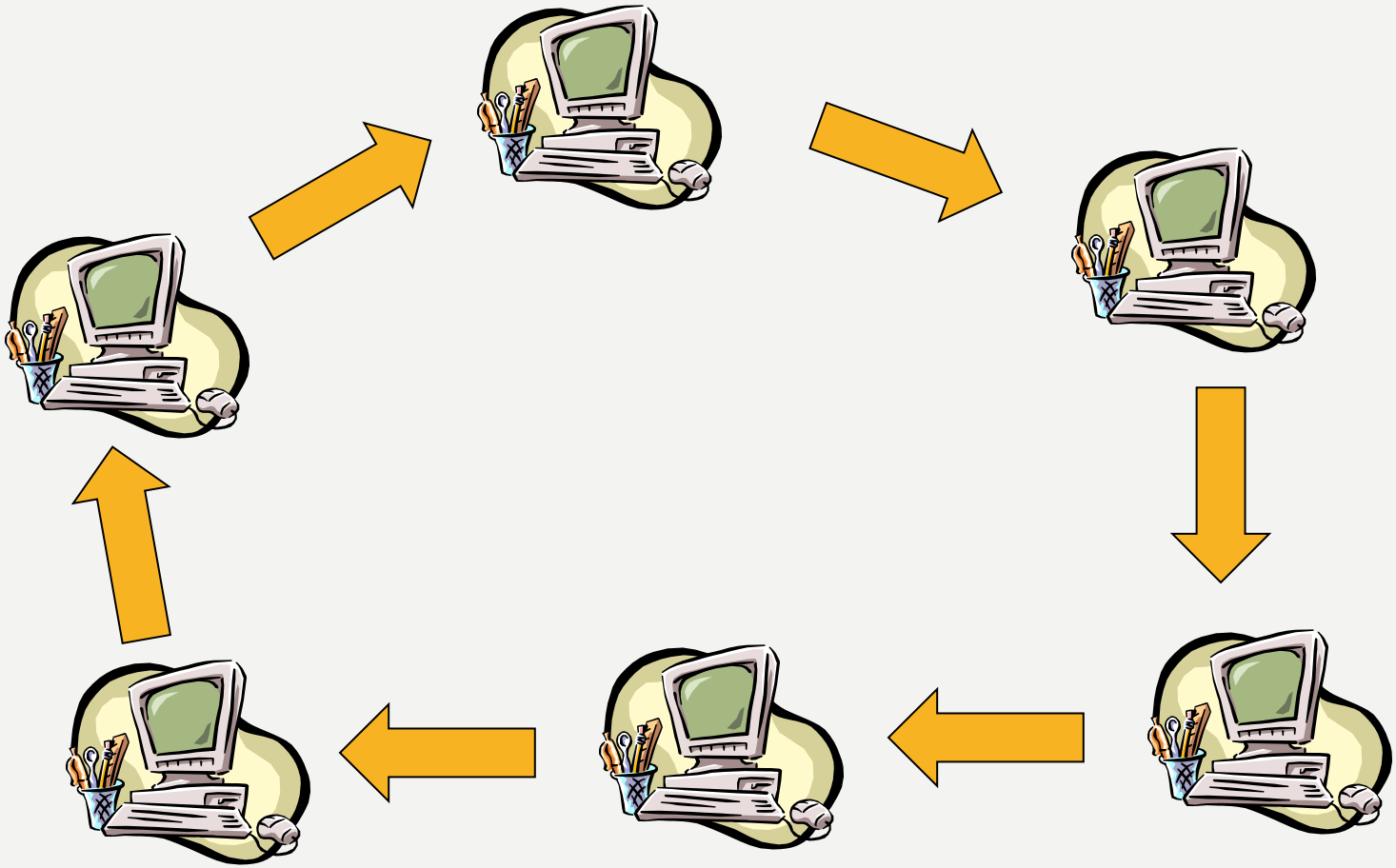
TOPOLOGIA DAS REDES

- É a forma como os computadores estão conectados;

TOPOLOGIA EM ANEL

- É um laço físico e fechado, consistindo de links ponto a ponto. Cada ponto age como um repetidor, amplificando a informação de um computador anterior para um posterior.
- Vantagem: pouca degradação do sinal;
- Desvantagens:
  - Uma quebra no anel desativa a rede;
  - É mais cara.

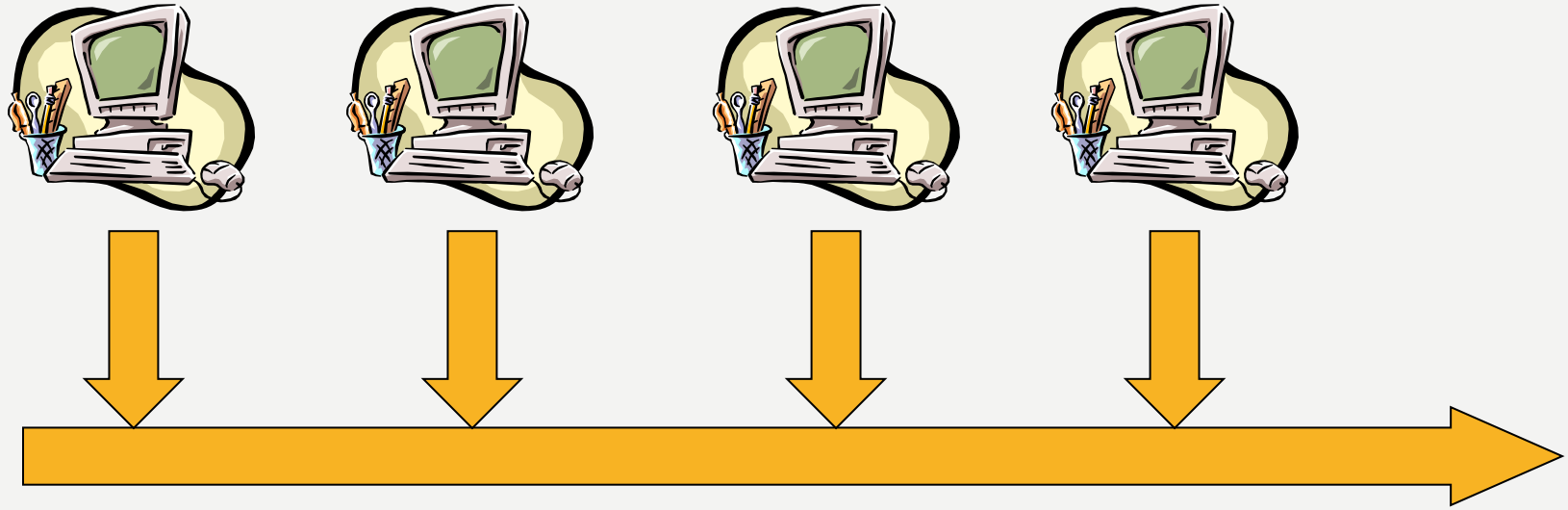
TOPOLOGIA EM ANEL



TOPOLOGIA EM BARRAMENTO

- Todos os dispositivos se ligam ao mesmo meio de transmissão.
- Vantagem: mais barata que a topologia em anel;
- Desvantagens:
  - Problemas no barramento desativam a rede;
  - Dificuldades de corrigir problemas.

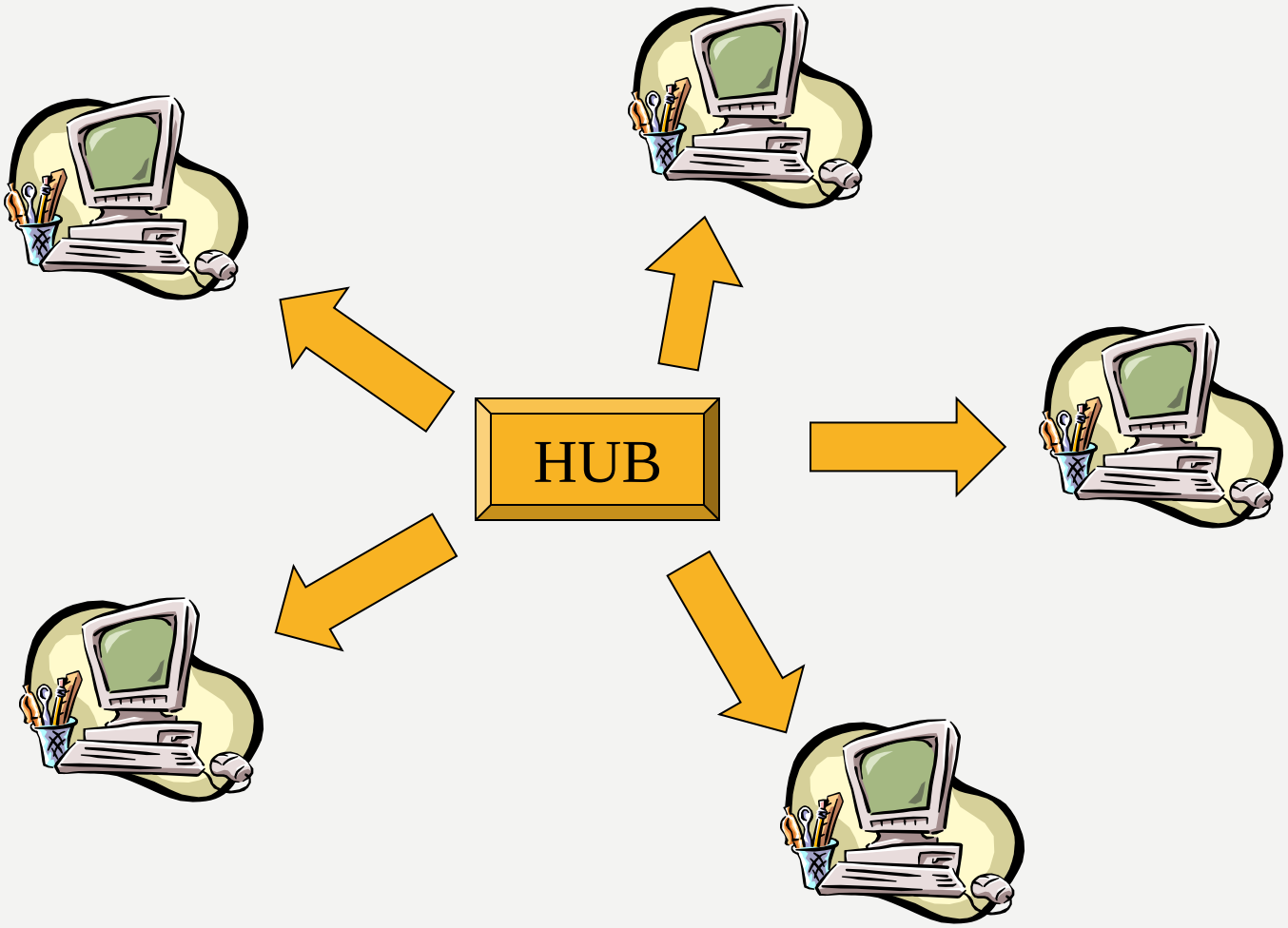
TOPOLOGIA EM BARRAMENTO



TOPOLOGIA EM ESTRELA

- Cada dispositivo é ligado a um ponto central (HUB - descontinuado);
- Vantagem: conexão mais estável e rápida (problema em um cabo afeta somente o computador ao qual está conectado);
- Desvantagem: a desativação de um HUB desativa toda a rede.

TOPOLOGIA EM ESTRELA



MEIOS DE CONEXÃO

- Determina a estabilidade de uma rede. Pesquisas revelam que cerca de 80% dos problemas físicos têm origem no cabeamento.

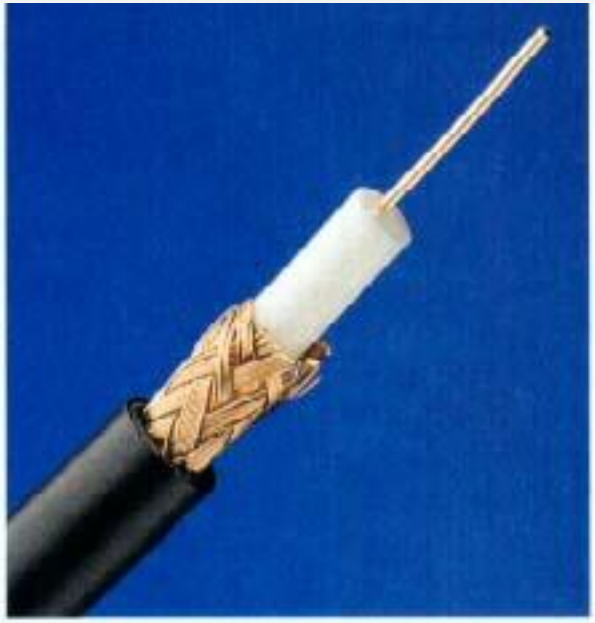
CABO COAXIAL

- Primeiro tipo disponível no mercado;
- Semelhante aos cabos utilizados nas antenas de TV;
- Consiste em um fio de cobre rígido que forma o núcleo. Ele é envolto por um material isolante, que por sua vez é envolto por uma malha metálica. Tudo é coberto por uma capa protetora.

CABO COAXIAL

- O principal problema das redes com cabo coaxial é a fragilidade das conexões (mal contato).

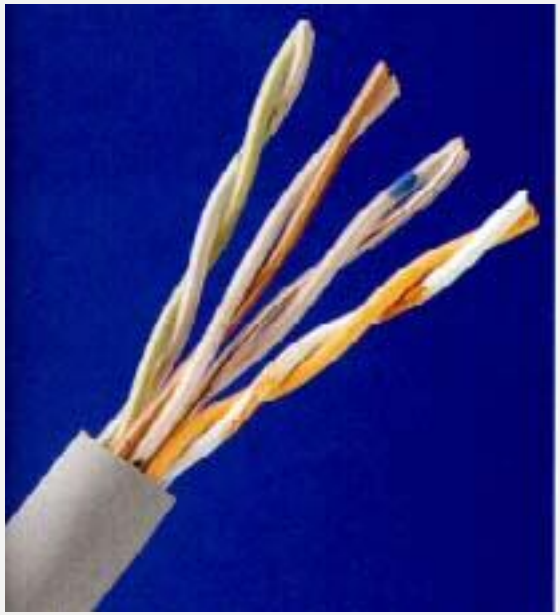
CABO COAXIAL



CABO DE PAR TRANÇADO

- Alternativa aos problemas do cabo coaxial;
- Conexões mais rápidas e estáveis;
- A rede depende do HUB, o que força a topologia ser em estrela;
- Muito utilizado em telefonia;
- Pode ser com blindagem (STP) ou sem blindagem (UTP) para interferências eletromagnéticas.

CABO DE PAR TRANÇADO



Categoria	Taxa máxima de transmissão	Aplicação usual
CAT 1	Até 1 Mbps (1 MHz)	Voz Analógico (POTS) ISDN (Integrated Services Digital Network) Basic Rate Interface Fiação tipo fio de telefone
CAT 2	4 Mbps	Utilizado em sistemas de cabeamento IBM Token Ring
CAT 3	10 / 16 Mbps	Voz e dados em rede 10BASE-T Ethernet
CAT 4	16 / 20 Mbps	Usado em redes Token Ring de 16 Mbps
CAT 5	100 Mbps 1 Gbps (4 pares)	100 Mbps TPDDI 155 Mbps ATM Não é mais utilizado, substituído pelo CAT 5E
CAT 5E	1 Gbps (10 Gbps – protótipo)	100 Mbps TPDDI 155 Mbps ATM Gigabit Ethernet
CAT 6	Até 400 MHz	Aplicações de banda larga "super-rápidas"
CAT 6A	Até 625 MHz (testado em campo até 500 MHz)	Suporta completamente 10 Gigabit Ethernet (10GBASE-T)
CAT 7	600-700 MHz 1.2 GHz em pares com conector Siemon	Vídeo em Full-motion Telerradiologia Redes especializadas de governo Redes especializadas de manufatura Redes especializadas de ensino Sistema blindado

FIBRA ÓTICA

- Necessário devido o aumento da distância de conexão e o desejo de aumentar a velocidade de conexão;
- Utiliza o cabo ótico;
- Sinais digitais dos computadores são transformados em pulsos de luz, que são transmitidos pela fibra até o ponto receptor.

FIBRA ÓTICA

Padrão	Taxa	Comprimento de onda	OS1	OS2
10GBASE-SR/SW	10Gb/s	850nm		
10GBASE-LR/LW	10Gb/s	1310nm	4,2Km	10Km
10GBASE-LRM	10Gb/s	1310nm		
10GBASE-LX4	10Gb/s	1310nm	4,2Km	10Km
10GBASE-ER/EW	10Gb/s	1550nm	8,9Km	22,25Km
10GBASE-ZR/ZW	10Gb/s	1550nm		80Km
40GBASE-SR4	40Gb/s	850nm		
40GBASE-LR4	40Gb/s	1310nm	4.7Km	10Km
100GBASE-SR10	100Gb/s	850nm		
100GBASE-LR4	100Gb/s	1295/1310nm	8.3Km	10Km
100GBASE-LR10	100Gb/s	1310nm	8.3Km	10Km
100GBASE-ER4	100Gb/s	1295/1310nm	16Km	40Km

WIRELESS (SEM FIO)

- Permite conexão entre computadores e redes através da transmissão e recepção de sinais de rádio;
- É necessário uma placa para acesso sem fio e um concentrador;
- Bom para redes locais;
- Devido ao alcance do sinal, os dados podem ser capturados.

CRESCIMENTO DAS REDES

- Redes Locais (LANs): características próprias de topologia, tipo de conexão, etc;
- Para estabelecer a conexão entre várias LANs, é preciso estabelecer um conjunto de regras (protocolo) para comunicação;
- Protocolo mais conhecido: TCP/IP
  - TCP (Protocolo de Controle e Transmissão);
  - IP (Protocolo de Internet).

TCP

- Responsável pelo formato de envio das informações;
- Especifica o formato dos pacotes de dados e de reconhecimentos que dois computadores trocam para realizar uma transferência confiável, assim como os procedimentos que os computadores usam para assegurar que os dados chegam corretamente, ou seja:

TCP

- Distinguir uma máquina determinada entre múltiplos destinos;
- Fazer recuperação de erros.

IP

- É responsável pelo endereçamento das informações.

CRESCIMENTO DAS REDES

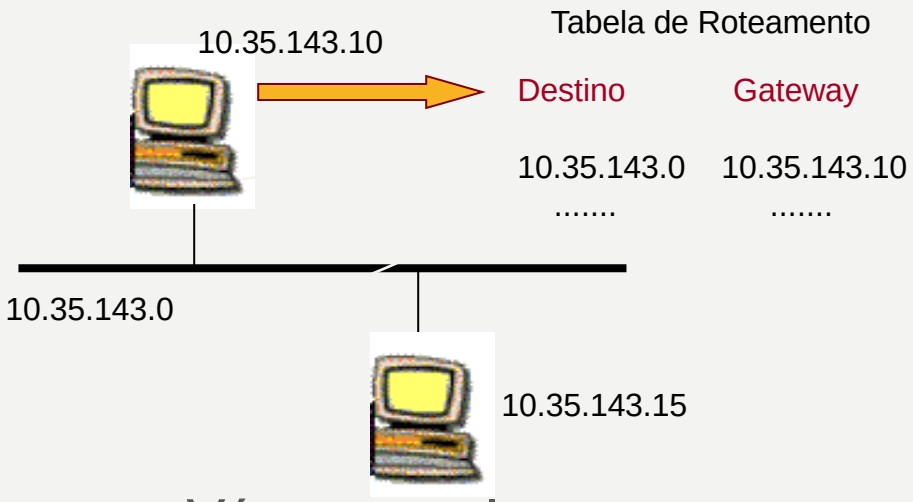
- Com a interligação das LANs, surge as WANs (redes de longa distância);

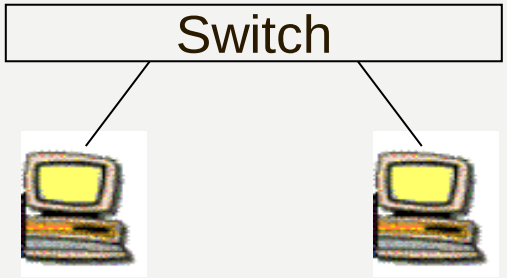
IP X PROTOCOLO DE ROTEAMENTO

- O protocolo IP é responsável pelo roteamento das informações na rede
  - A variável *ipforwarding* indica se o protocolo está executando roteamento ou não
    - *Ipforwarding = 0 (não executa roteamento)*
    - *Ipforwarding = 1 (executa roteamento)*
- Os protocolos de roteamento são responsáveis pela divulgação de rotas e atualização das tabelas de roteamento

ROTEAMENTO DIRETO

- Origem e Destino na mesma rede

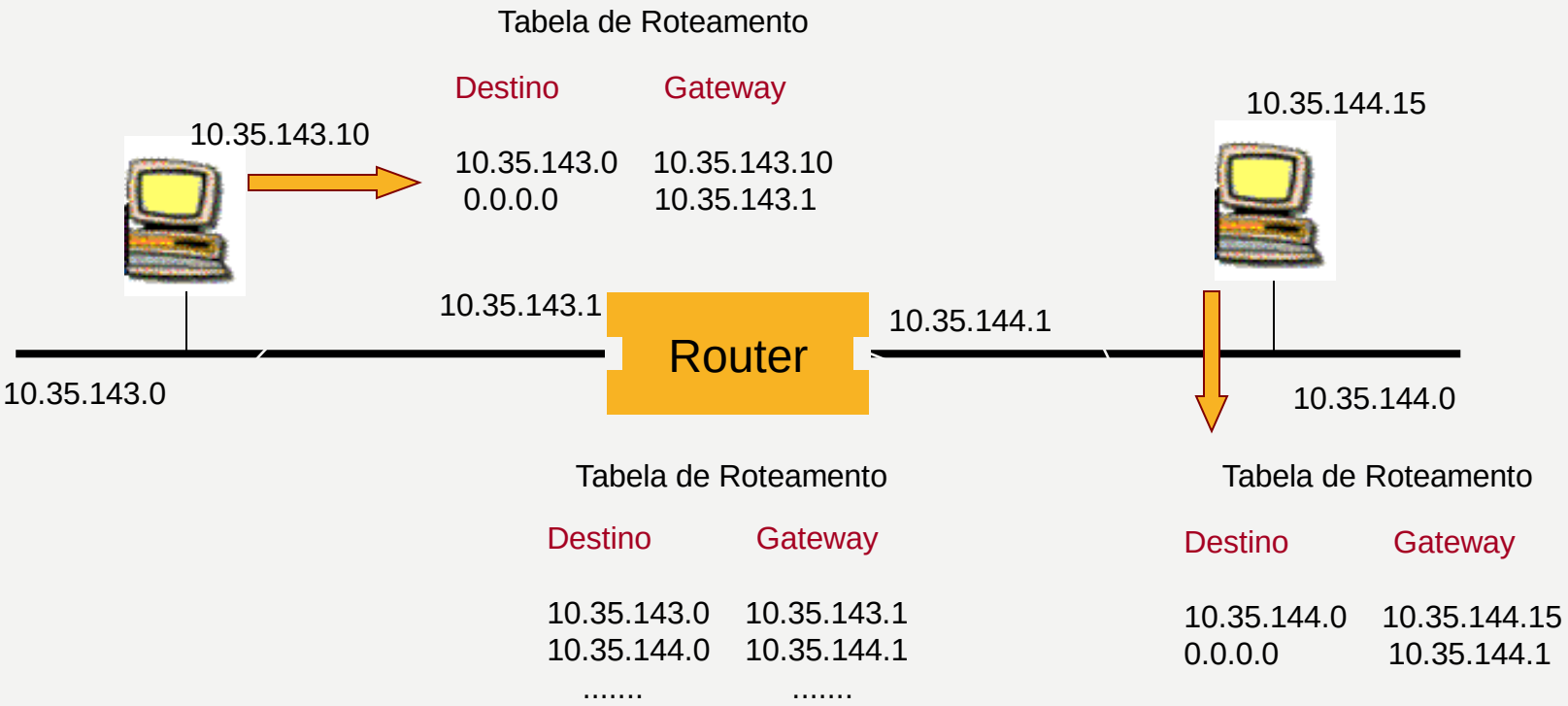




- Várias topologias
  - Lembre-se equipamentos de nível 2 não tratam endereço IP

ROTEAMENTO INDIRETO

- Origem e Destino estão em redes diferentes



ROTEAMENTO ESTÁTICO E DINÂMICO

- Roteamento Estático
  - Normalmente configurado manualmente
  - A tabela de roteamento é estática
    - As rotas não se alteram dinamicamente de acordo com as alterações da topologia da rede
  - Custo manutenção cresce de acordo com a complexidade e tamanho da rede
  - Sujeito a falhas de configuração

ROTEAMENTO ESTÁTICO E DINÂMICO

- Roteamento Dinâmico
  - Divulgação e alteração das tabelas de roteamento de forma dinâmica
    - Sem intervenção constante do administrador
  - Alteração das tabelas dinamicamente de acordo com a alteração da topologia da rede
    - Adaptativo
  - Melhora o tempo de manutenção das tabelas em grandes redes
  - Mas também está sujeito a falhas

SISTEMAS AUTÔNOMOS

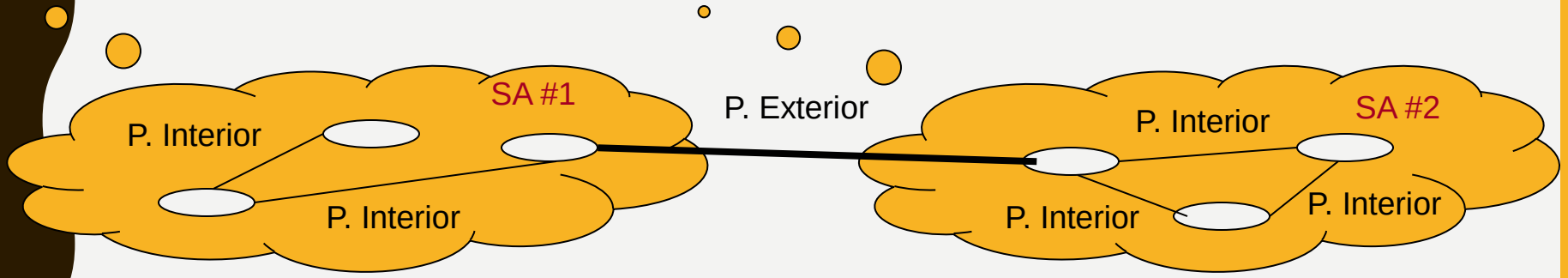
- Um SA (Sistema Autônomo) pode ser definido como

  "Um grupo de redes e roteadores controlados por uma única autoridade administrativa."

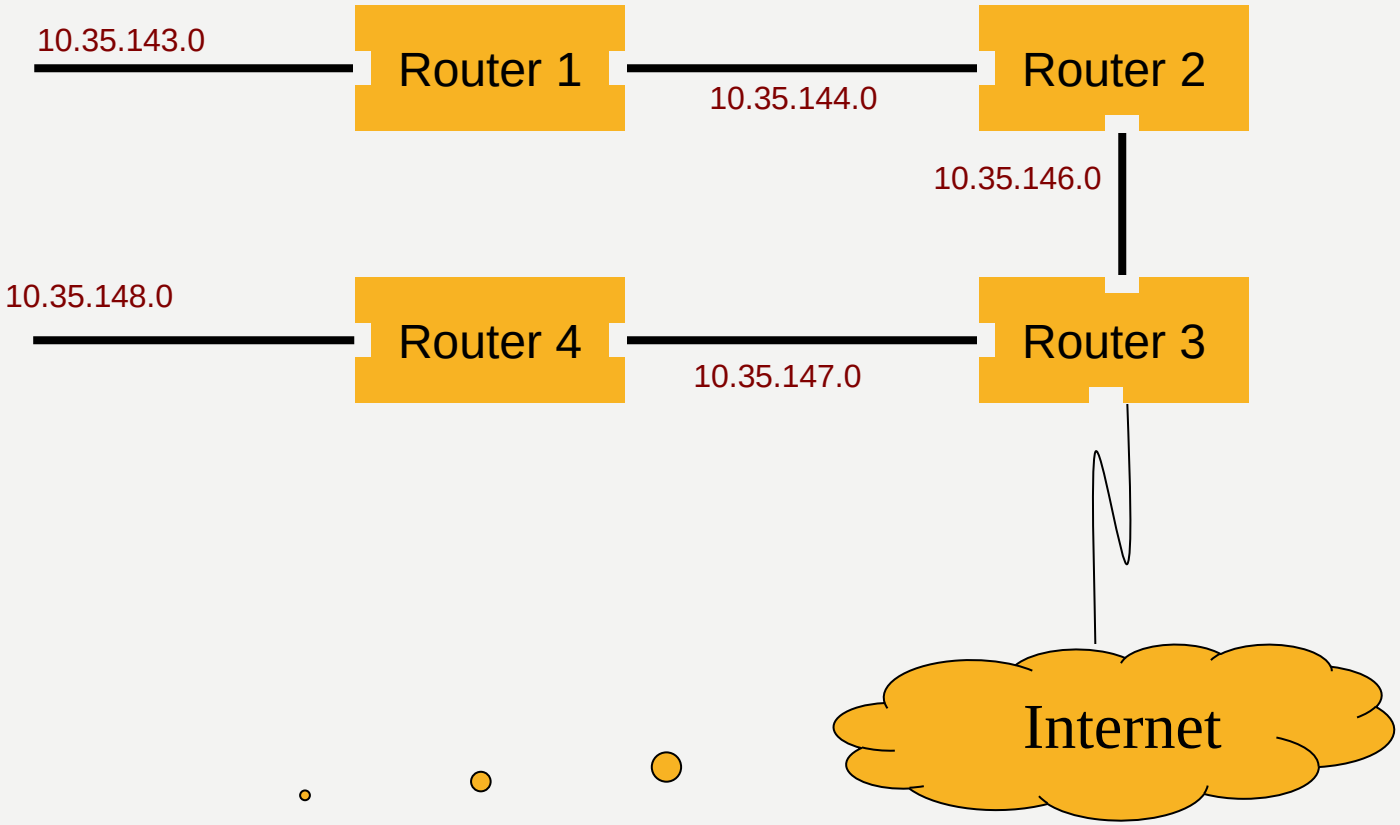
- Roteadores em um sistema autônomo seguem as mesma "regras" de roteamento
- Protocolos de roteamento são classificados de acordo com sua atuação

PROTOCOLO INTERIORES E EXTERIORES

- Protocolos Interiores
  - São aqueles utilizados para comunicação entre roteadores de um mesmo sistema autônomo
- Protocolos Exteriores
  - São aqueles utilizados para comunicação entre roteadores de sistemas autônomos diferentes



ROTEAMENTO ESTÁTICO - EXEMPLO



ALGORITMOS DE ROTEAMENTO

- Os protocolos de roteamento implementam um ou mais algoritmos de roteamento
- Exemplos de Algoritmos
  - Vetor Distância, Flooding, SPF (Shortest Path First), ...
- Exemplos de protocolos
  - RIP, OSPF, IGRP, BGP, ...

VETOR-DISTÂNCIA

- Bellman-Ford
- É um algoritmo simples
  - Um roteador mantém uma lista de todos as rotas conhecidas em uma tabela
  - Cada roteador divulga para os seus vizinhos as rotas que conhece
  - Cada roteador selecionas dentre as rotas conhecidas e as divulgadas os melhores caminhos

VETOR-DISTÂNCIA - MÉTRICA

- A escolha do melhor caminho é baseada na comparação da métrica do enlace
  - Normalmente: Melhor = menor caminho
- A métrica é o custo de envio em um enlace
- Pode ser diferentes informações
  - Taxa de transmissão em bps
  - Vazão
  - Atraso
  - Número de saltos (no. de *hops*) (+ usado)

VETOR-DISTÂNCIA

- Processo
  1. Quando o roteador executa o "boot" ele armazena na tabela informações sobre cada uma das redes que estão diretamente conectada a ele. Cada entrada na tabela indica uma rede destino, o gateway para a rede e a sua métrica.
  2. Periodicamente cada roteador envia uma cópia da sua tabela para qualquer outro roteador que seja diretamente alcançável.
  3. Cada roteador que recebe uma cópia da tabela, verifica as rotas divulgadas e suas métricas. O roteador soma à métrica divulgada o custo do enlace entre ele e o roteador que fez a divulgação. Após, compara cada uma das entradas da tabela divulgada com as da sua tabela de roteamento. Rotas novas são adicionadas, rotas existentes são selecionadas pela sua métrica.

VETOR-DISTÂNCIA ...

3.1 Se a rota já existe na tabela e a métrica calculada é menor do que a da rota conhecida, então remove a entrada anterior e adiciona a nova rota divulgada.

3.2 Se a rota já existe na tabela e a métrica calculada é igual a da rota conhecida, então não altera a entrada.

3.3. Se a rota já existe na tabela e a métrica divulgada é maior do que a da rota conhecida, então verifica se o gateway para desta rota é o mesmo que está fazendo nova divulgação

3.3.1 Se o gateway é o mesmo então altera a métrica para esta rota

3.3.2 Se o gateway não é o mesmo não altera a rota conhecida

ROUTING INFORMATION PROTOCOL (RIP)

- Protocolo interior
- Implementa o algoritmo Vetor Distância
- A métrica utilizada é o número de máquinas intermediárias (no. de *hops*)
- Não permite o balanceamento de tráfego
- Cada roteador divulga sua tabela periodicamente a cada 30 segundos
- As mensagens divulgadas levam *n tuplas* contendo

<redes destino, métrica>

RIP ...

- A divulgação para os vizinhos é realizada por *broadcast*
  - O *router* um *broadcast* em todas as redes diretamente conectadas a ele
- No procedimento normal, se a rota não for atualizada em 180 segundos é considerada inatingível
- A informação de rota inatingível é repassada aos roteadores "vizinhos" (diretamente alcançáveis)

RIP - PROBLEMAS

- Não tem mecanismos de segurança
  - É suscetível a *spoofing*
- Não tem controle de "idade" das mensagens
  - Mensagens "velhas" podem ser processadas após mensagens "novas"
    - Inconsistência nas tabelas de roteamento
- Problemas de laços na divulgação das rotas
- Limitação de número de roteadores intermediários
  - Métrica = 16, indica rota inalcançável
- Não suporta máscara de subrede

RIP - EXEMPLO

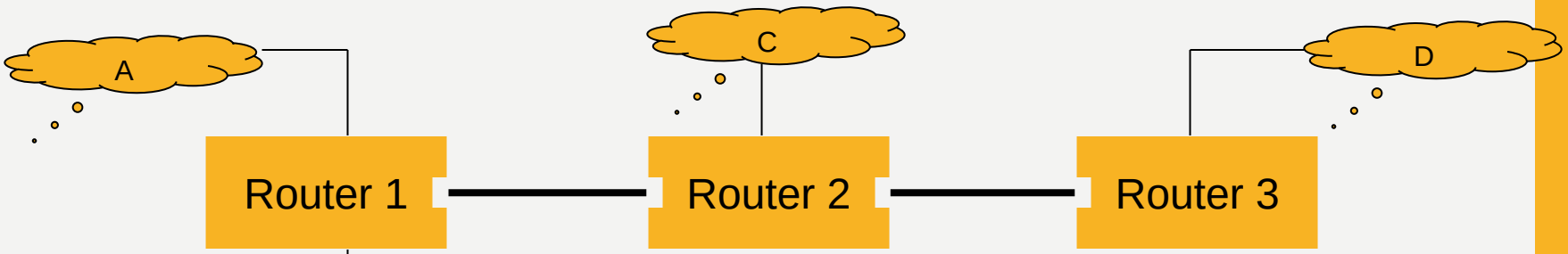


Tabela de Roteamento

Destino	Gateway	Métrica
A	Router1	0
B	Router1	0
.....	.....	

Tabela de Roteamento

Destino	Gateway	Métrica
C	Router2	0
.....	.....	

Tabela de Roteamento

Destino	Gateway	Métrica
D	Router3	0
.....	.....	

<A, 0>
<B, 0>

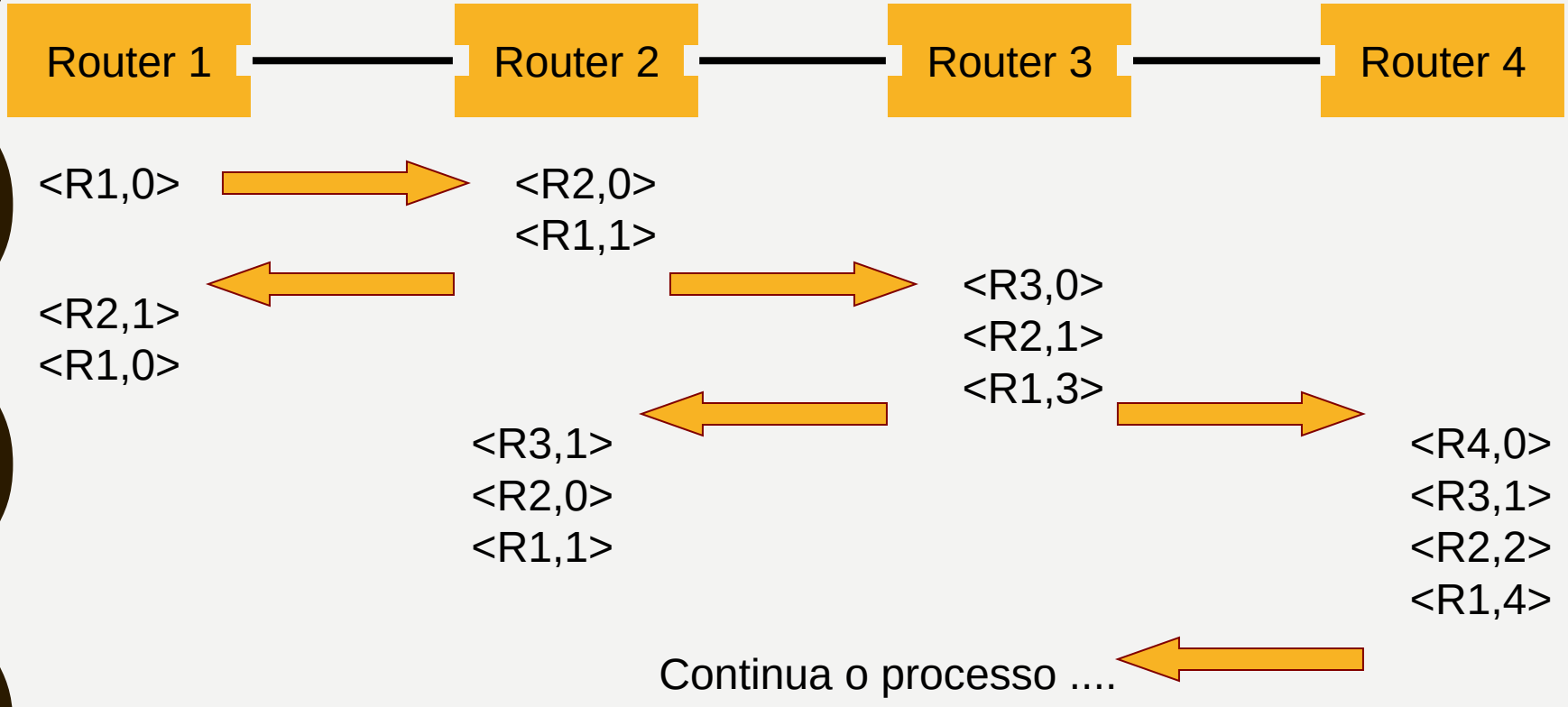
Tabela de Roteamento

Destino	Gateway	Métrica
C	Router2	0
A	Router1	1
B	Router1	1

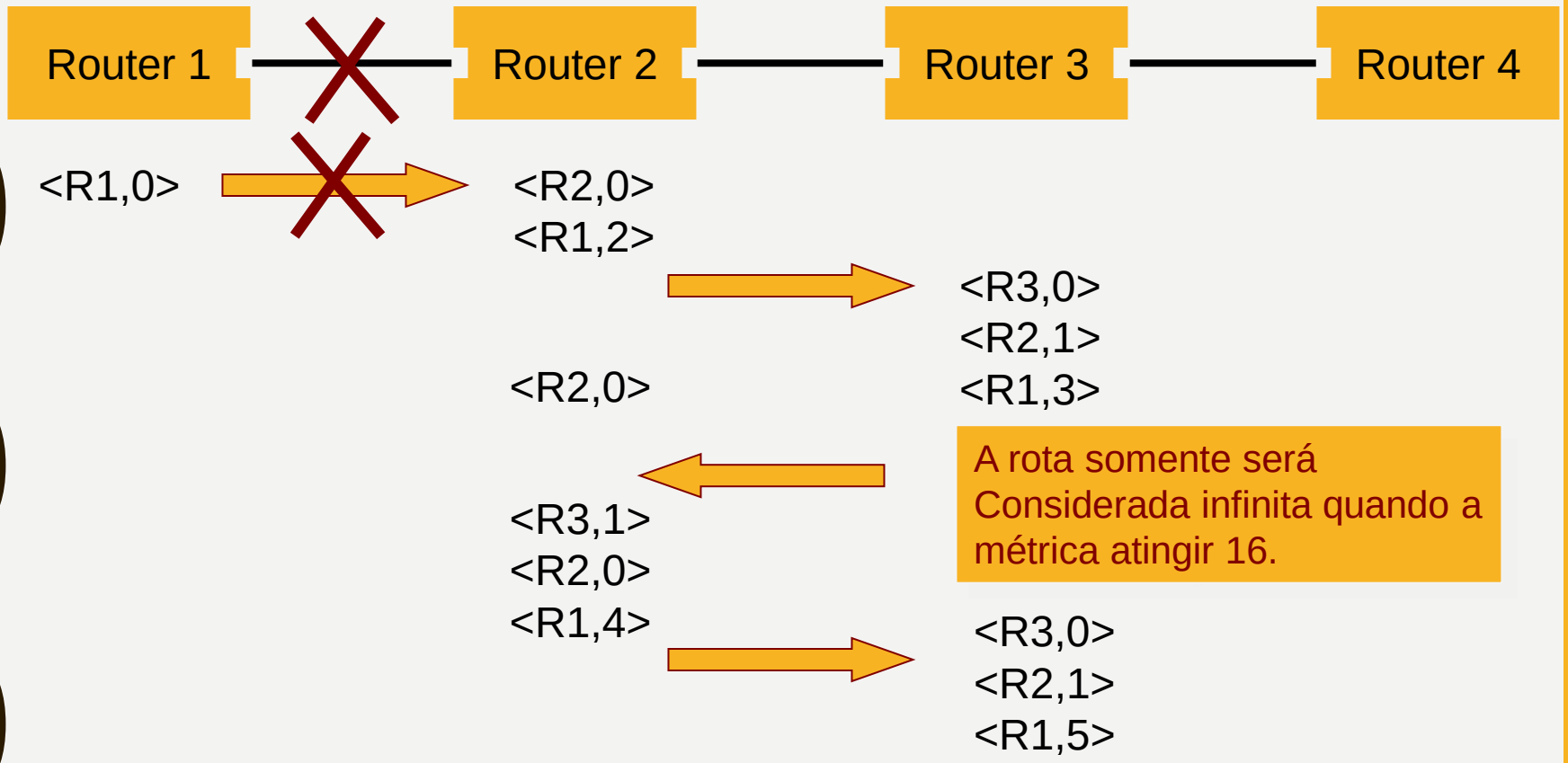
Tabela de Roteamento

Destino	Gateway	Métrica
D	Router3	0
C	Router2	1
A	Router2	2
B	Router2	2

CONVERGÊNCIA LENTA



CONVERGÊNCIA LENTA



SOLUÇÕES

- Split Horizon
  - A informação de roteamento não deve ser divulgada para a máquina que a originou
- Poison Reverse
  - Aumenta a métrica e coloca em *hold-down*
- Hold-Down
  - Previne que mensagens de atualização restabeleçam precipitadamente uma rota que caiu.

FRAME DO RIP

command	version	zero
family of net 1		zero
IP Address of Net 1		
zero		
zero		
distance to net 1		
zero		
family of net 2		zero
IP Address of Net 2		
zero		
zero		
distance to net 2		
.....		

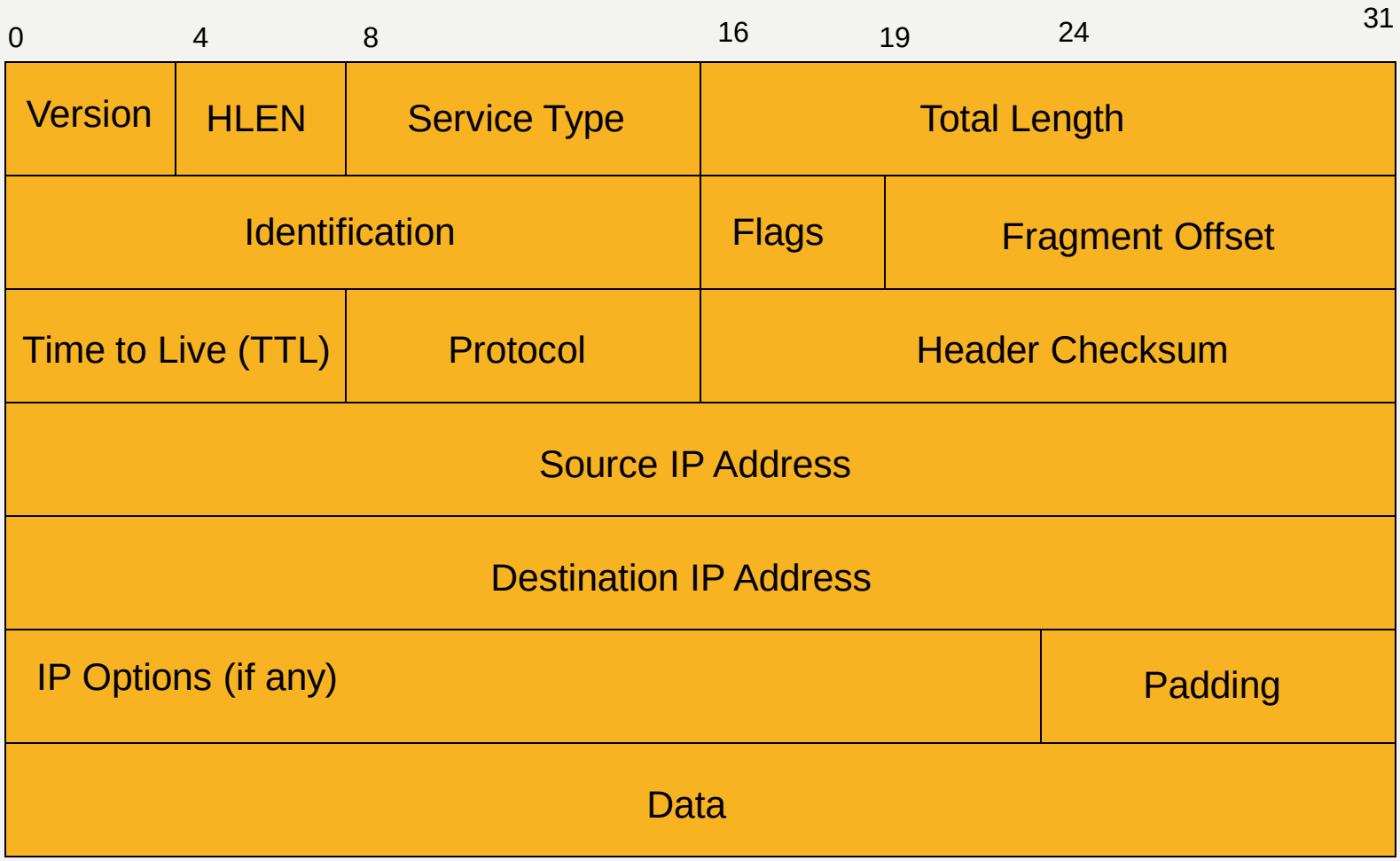
CARACTERÍSTICAS DO IP

- Sistema de entrega fim-a-fim
- É um protocolo
  - Não orientados à conexão
  - Sem controle de erros e sem reconhecimento
  - Isso significa que o protocolo IP não executa:
    - Controle de erros sobre os dados da aplicação
    - Controle de fluxo
    - Sequenciamento de dados
    - Entrega ordenada

CARACTERÍSTICAS DO IP

- Serviço de entrega: Best-effort
  - Os pacotes não são descartados sumariamente, o protocolo torna-se não confiável somente quando há exaustão de recursos
- Datagrama de tamanho variável
  - IPv4: tamanho máximo 64 Kbytes
- Provê envio e recebimento
  - Erros: ICMP

FRAME IP


0
4
8
16
19
24
31
Version
HLEN
Service Type
Total Length
Identification
Flags
Fragment Offset
Time to Live (TTL)
Protocol
Header Checksum
Source IP Address
Destination IP Address
IP Options (if any)
Padding
Data

CAMPOS IP

- Version (4 bits)
- HLEN (4 bits)
  - Tamanho em no. de palavras de 32 bits
  - *Header* sem opções: 5 (20 bytes)
  - *Header* com opções: tamanho máximo 15 (60 bytes)
- Service Type
  - Confiabilidade, precedência, atraso e *throughput*

CAMPOS DO IP

- Total Length (16 bits)
  - tamanho do *header* + área de dados
- Identification (16 bits)
  - Identifica de forma única um pacotes IP
- Flags (3 bits)
  - More Fragments (MF)
  - Don´t Fragment (DF)
  - Reserved

CAMPOS DO IP

- Fragment Offset (13 bits)
  - Múltiplo de byte
- Time to Live (8 bits)
- Protocol (8 bits)
  - Próximo nível a receber dados (protocolo que está encapsulado no frame IP)
  - ICMP (1), TCP (6), UDP (17)
- Header Checksum (16 bits)
  - Soma dos complementos de 1 de blocos de 16 bits, contendo informações do *header* do IP

CAMPOS IP

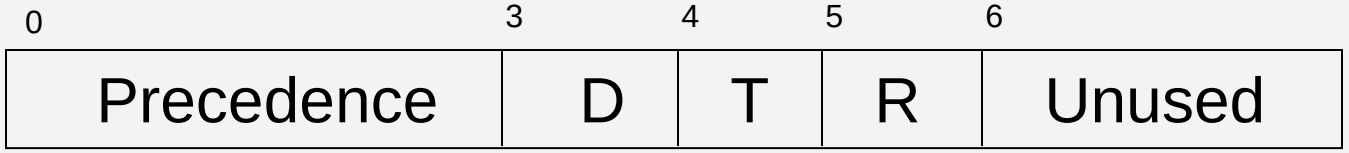
- Endereço Origem (32 bits)
  - Origem dos dados
  - Não é alterado ao longo da transmissão
- Endereço Destino (32 bits)
  - Destino dos dados
  - Não é alterado ao longo da transmissão
- Opções (variável)
  - Security, source route, record route, stream id (used for voice) for reserved resources, timestamp recording

CAMPOS DO IP

- Padding (variável)
  - Faz com que o header seja múltiplo de 4
- Data (variável)
  - Data + header < 65,535 bytes

SERVICE TYPE

- TOS (*Type of Service*)
- Especifica como o Datagrama deve ser tratado
- Divisão Original



  - Precedence: importância do datagrama
  - D: baixo atraso
  - T: alto throughput
  - R: alta confiabilidade

SERVICE TYPE

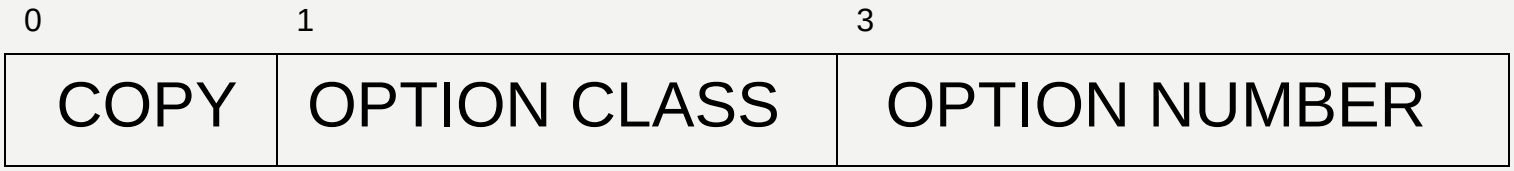
- Problema
  - Difícil para a Internet atender as solicitações de tipo de serviço
  - Então passa a ser usado como uma "dica" para algoritmos de roteamento não como uma demanda
- Em 1990 o IETF redefiniu o "*service type*" para acomodar os "*differentiated services*"

SERVICE TYPE – COMPATIBILIDADE

- Distinção entre os bits do *codepoint*
- Se os últimos 3 bits (*codepoint*) contém 0 (zero)
  - São definidas 8 classes de serviços que seguem a definição original
  - Precedência especial: 6 e 7
    - Roteador deve implementar ao menos 2 esquemas
      - Baixa prioridade
      - Alto prioridade
    - 3 bits em 0 e precedência 6 ou 7: alta prioridade

IP OPTIONS

- O campo de opções do protocolo IP é opcional
  - Inicia após o endereço do destino
  - Pode estender o *header* do IP até o tamanho máximo de 60 bytes
- Formato do campo de opções



IP OPTIONS

- Copy (1 bit)
  - Controla como os roteadores tratam as opções durante o processo de fragmentação
- Option Class (2 bits)
  - Especifica a classe geral de opções

Option Class	Descrição
0	Controle da rede ou datagrama
1	Reservado
2	Depuração
3	Reservado

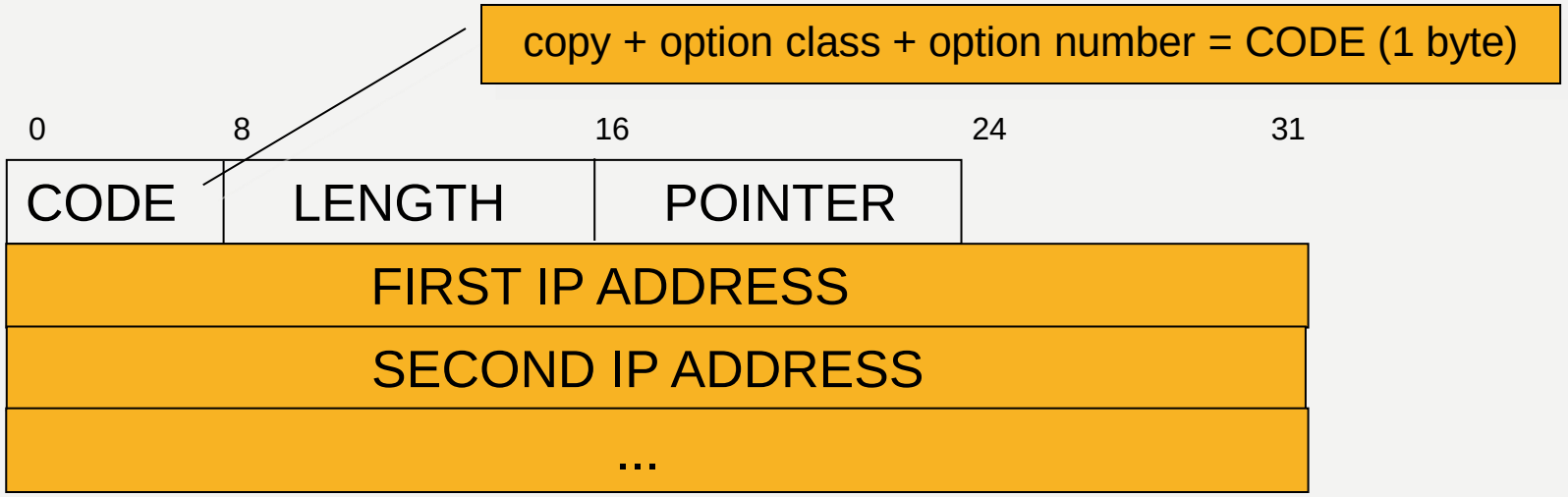
IP OPTIONS

- Option Number (5 bits)
  - Especifica uma classe específica dentre da classe geral

Option Number	Descrição
1	No operation
2	Security
3	Loose Route
7	Recorde Route
8	Stream Identifier
9	Strict Source Route
11	MTU Probe
12	MTU Reply
4	Timestamp
18	Traceroute

RECORD ROUTE OPTION

- Provê uma forma de monitorar como os datagramas são roteados
- Cada roteador que "roteia" o datagrama acrescenta seu endereço IP ao campo de opções



CODE E POINTER

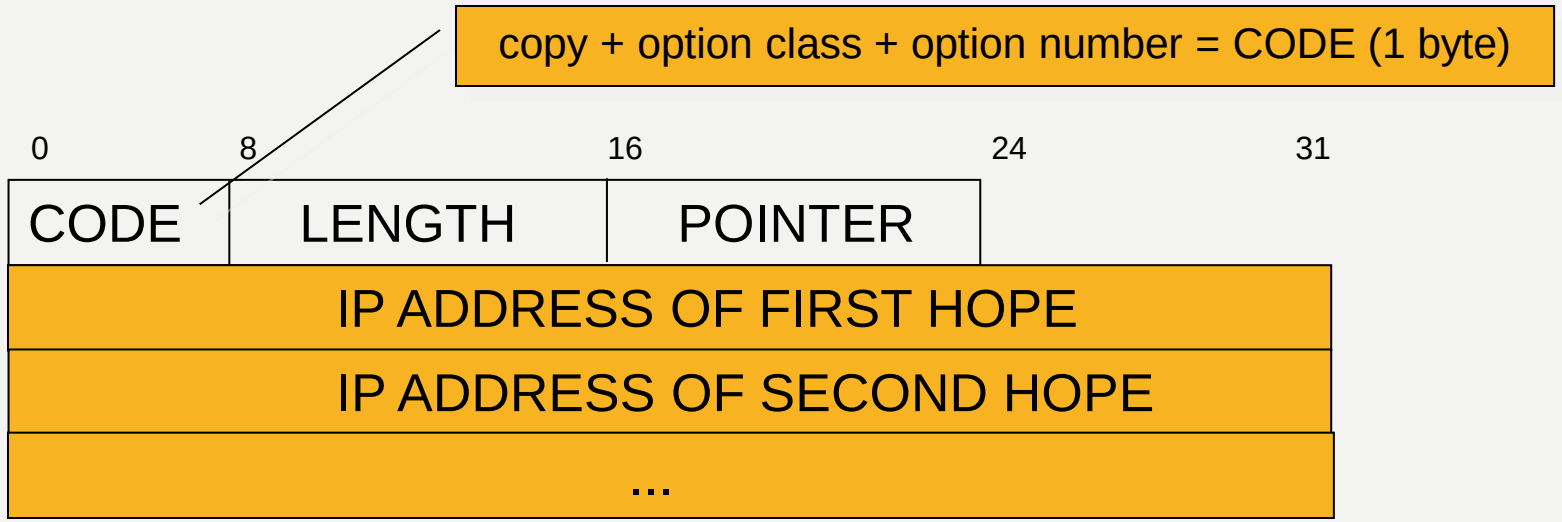
- Code (8 bits)
  - Representa os campos copy, option class e option number
    - Exemplo:

    copy = 0, option class = 0, option number = 7 ➡ code = 7

    copy = 1, option class = 0, option number = 9 ➡ code = 137
- Pointer (8 bits)
  - Aponta para próxima área a ser preenchida ou "consultada"
  - Deve ser alterada pelo host ou roteador que manipula dados do campo de opções

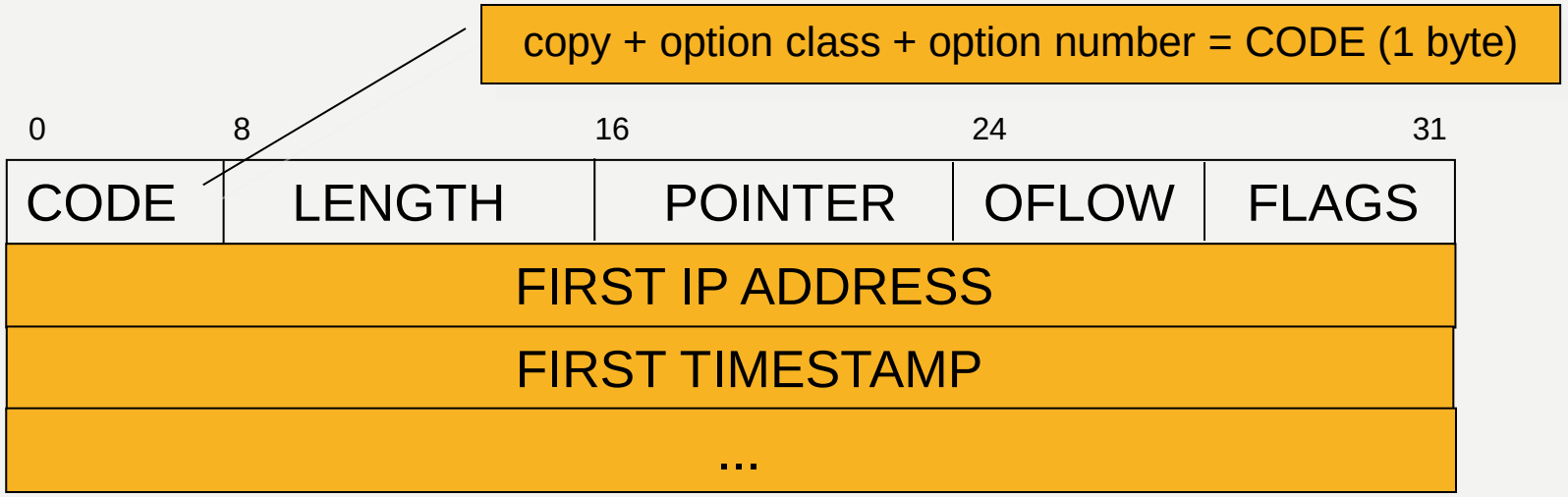
SOURCE ROUTE OPTION

- Source Route
  - Strict Source Route: rota exata a ser seguida
  - Loose Source Route: deve passar pelo menos por um dos roteadores



TIMESTAMP OPTION

- Similar ao Record Route
- Inicialmente contém uma lista vazia de roteadores e tempos
- Cada roteador acrescenta seus dados



TIMESTAMP OPTION

- Cada entrada na lista contém
  - IP address (32 Bits)
  - Timestamp (inteiro de 32 bits)
- OFLOW (4 bits)
  - Contador do número de roteador que não puderam acrescentar informações
- FLAGS
  - Controla o formato exato do campo de timestamp

TIMESTAMP - FLAGS

- Os valores possíveis são

Valor das Flags	Descrição
0	Registre apenas o timestamp, omita o endereço IP
1	Acrescente o endereço IP e após o timestamp
3	Endereços IP são especificados pela origem. O roteador só irá registrar seu timestamp se o próximo IP na lista for o seu.

FRAGMENTAÇÃO

- Cada padrão de rede tem um MTU diferenciado
  - Ethernet: 1500 bytes
  - ATM: 53 bytes
  - FDDI: 4500 bytes
  - ...
- Datagramas maiores do que a MTU da rede devem ser fragmentados

FRAGMENTAÇÃO

- Cada fragmento recebe uma cópia do *header* IP do datagrama original e uma porção de dados

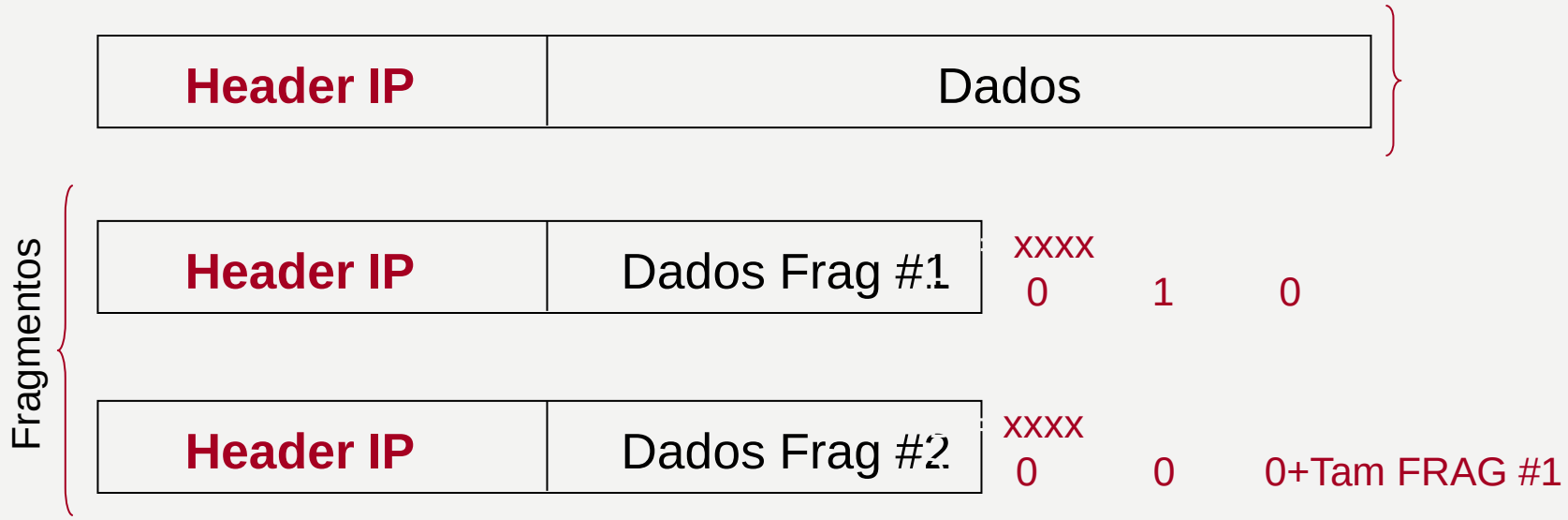
Header IP	Dados

Header IP	Dados Frag #1

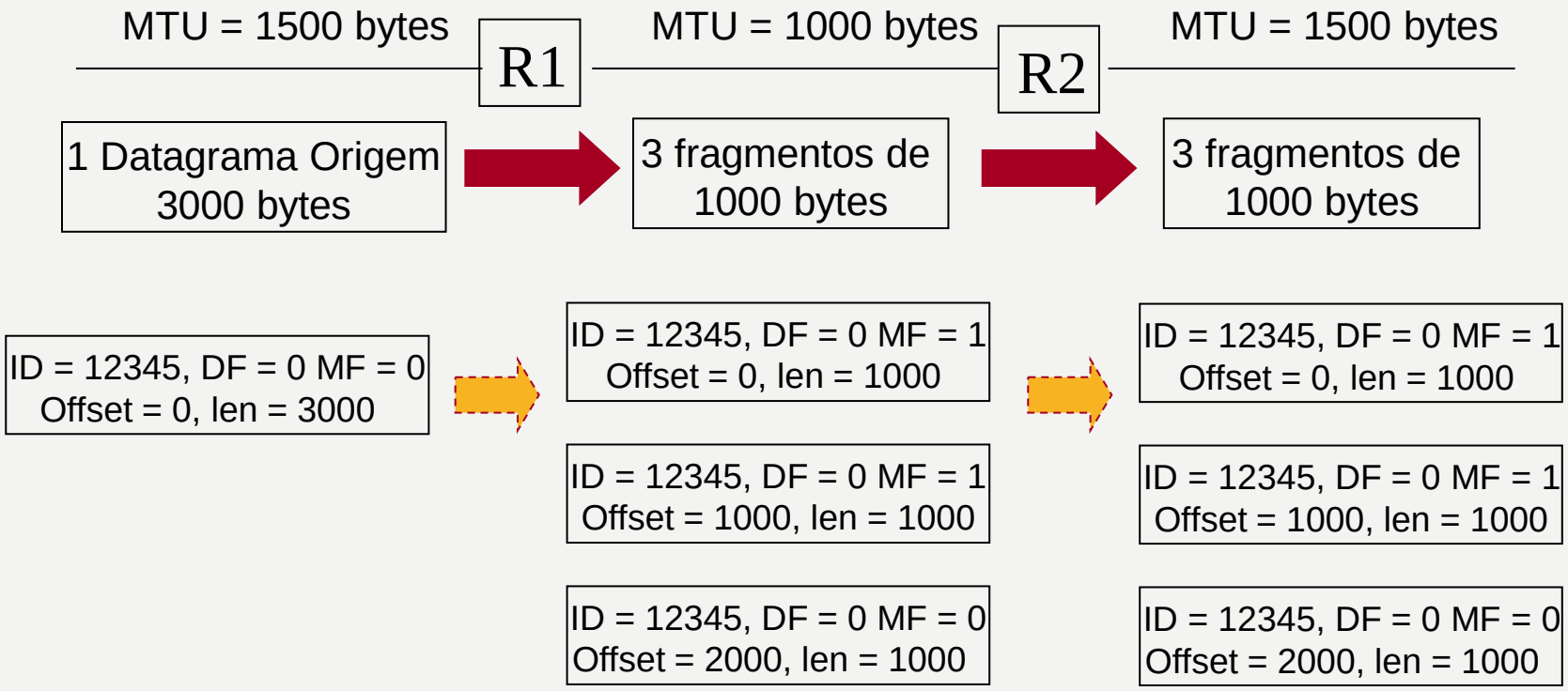
Header IP	Dados Frag #1

FRAGMENTAÇÃO

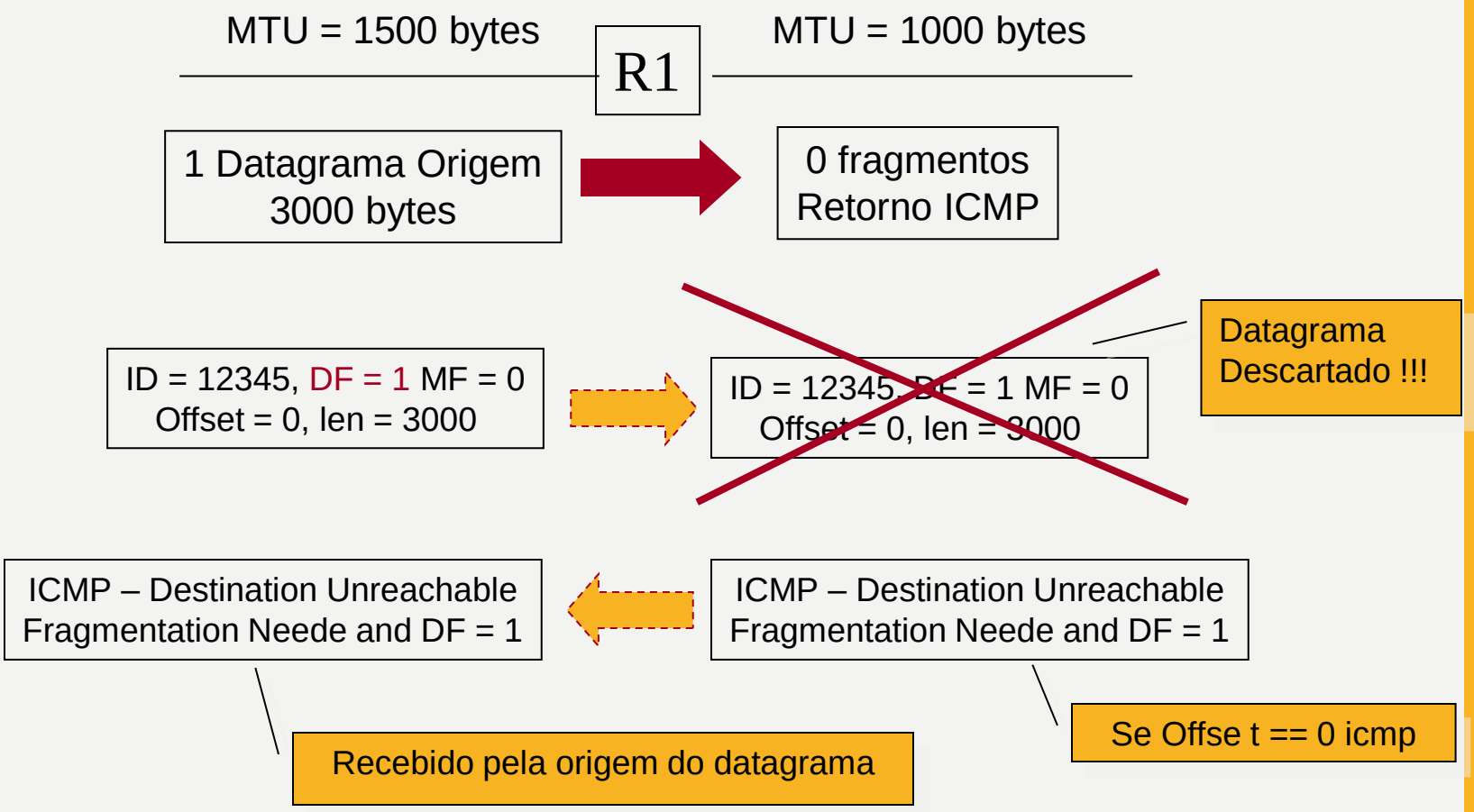
- No *header* IP dos fragmentos alteram-se os campos
  - Flags, Fragment Offset, Total Length



FRAGMENTAÇÃO - EXEMPLO



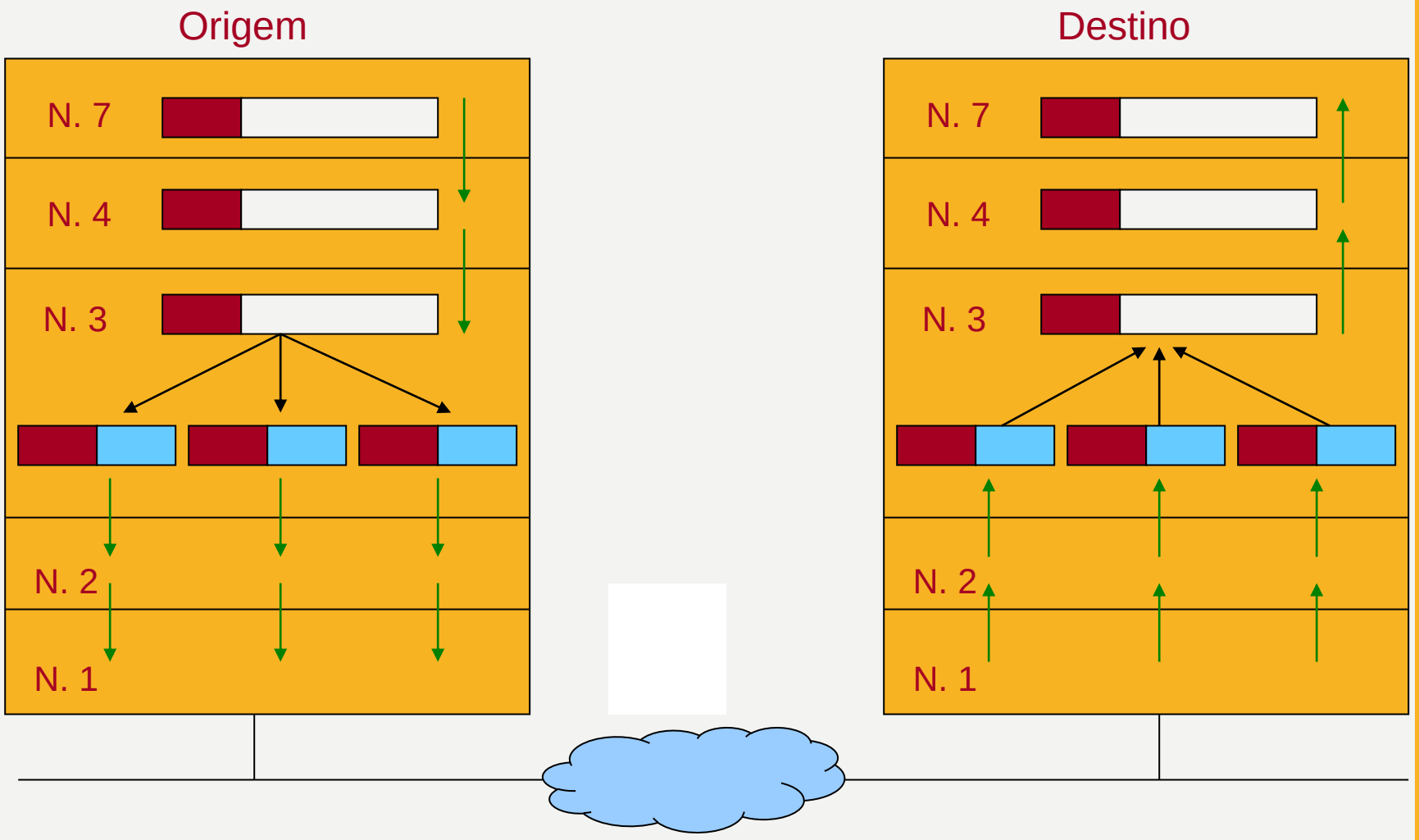
FRAGMENTAÇÃO COM DF = 1



REMONTAGEM

- Fragmentos são remontados somente no destino
  - Roteadores intermediários não devem remontar datagramas
    - Gasto de memória e processamento
    - Comutação de pacotes = fragmentos com rotas diferenciadas
- Tempo máximo para remontagem
  - Se faltam fragmentos e o tempo se esgota, os fragmentos são descartados
  - Destino envia para origem um ICMP de Time Exceeded

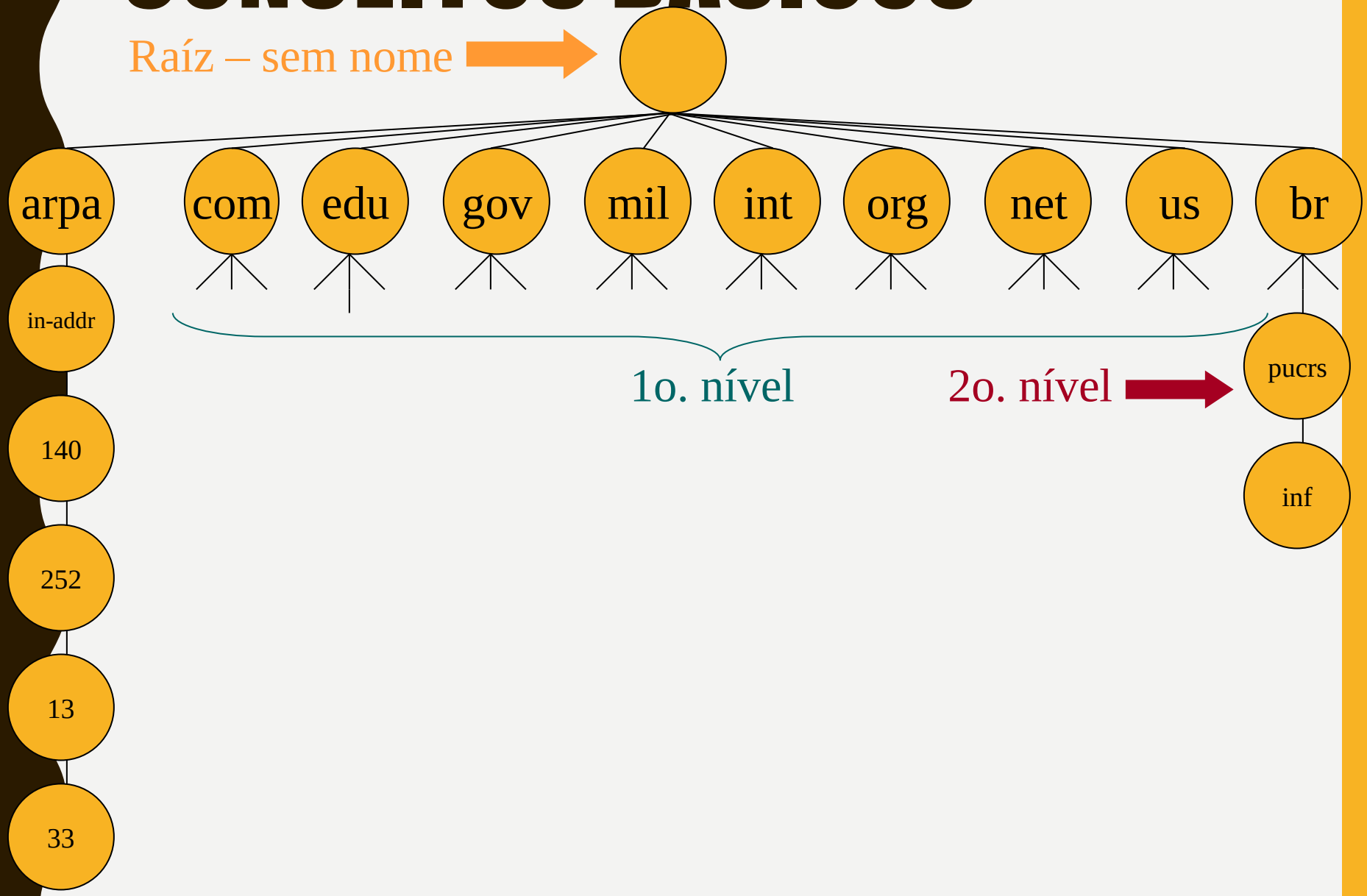
FRAGMENTAÇÃO & REMONTAGEM



DNS (DOMAIN NAME SYSTEM)

- Usado em redes TCP/IP para mapear nomes simbólicos em endereços IP
- Base de dados distribuída
- A aplicação tem acesso ao DNS através de um *resolver*.
  - UNIX
    - gethostbyname
    - gethostbyaddr
- RFC´s: 1034, 1035, 1713

CONCEITOS BÁSICOS



ZONAS

- Uma zona é uma subárvore de um domínio administrada separadamente.
- Autoridade de uma zona
  - Primary Server
  - Secondary Server
- Obtenção de informações
  - Zone Transfer – secundário obtém informações (*load*) do servidor primário
  - Atualizações periódicas

SERVIDORES

- Primary Server
  - Autoritário (Authoritative)
- Secondary Server
  - Não Autoritário (Nonauthoritative)
- Cache Server
  - *Name caching*
    - Mantém nomes recentemente resolvidos
  - Redução de tráfego (custo para rede)
  - Problemas?

Atualização das Informações

DNS CACHE

- Informações em cache são marcadas como *nonauthoritatives*
- Freqüência de alterações de nomes é baixa
- Atualizações periódicas
  - Tempo de permanência de uma informação na cache é determinada pelo TTL atribuído pelo servidor primário
  - Servidor descarta informações velhas
  - Busca no servidor Primário informações novas

Grande Timeout x Pequeno Timeout

CONSULTAS

- Recursivas
  - Consulta distribuída automática
  - Devolve a resolução
  - Problema: mascaramento de servidores
- Interativas
  - Consulta distribuída não é automática
  - Devolve endereço de servidores que podem resolver

FORMATO DA MENSAGEM

- Identification (16 bits)
- Flags (16 bits)
- Number of questions (16 bits)
- Number of answers (16 bits)
- Number of authority RRs (16 bits)
- Nunber of additional RRs (16 bits)
- Questions
- Answers
- Authority
- Additional information

12 bytes

FLAGS

- QR (0 – query, 1 - response)
- Opcode
- AA (authoritative answer)
- TC (truncated)
- RD (recursion desired)
- RA (recursion available)
- Zero (3 bits)
- Rcode (return code) (error, name error)

QUESTIONS

- Query name
  - 1 byte – contador
  - Tamanho máximo de um label: 63
  - Exemplo

6 g e m i n i 3 t u c 4 n o a o 3 e d u 0

- Query type
  - SOA, A, NS, CNAME, PTR, HINFO, MX, AXFR
- Query class (1 – Internet Addr)

RESOURCE RECORDS – RESPONSE MESSAGE

- Domain name
  - Mesmo formato utilizado na "*question*"
- Type
- Class
  - Normalmente 1 (Internet Address)
- TTL
  - Número de dias que pode ficar na cache
- Resource length data
- Resource data

IMPLEMENTAÇÃO E CONFIGURAÇÃO - UNIX

- Bind
  - Named (deamon)
- Arquivos de Configuração
  - Servidor
    - Arq.zone
    - Arq.revzone
    - Arq.ca
    - Arq.boot
  - Cliente
    - /etc/resolv.conf

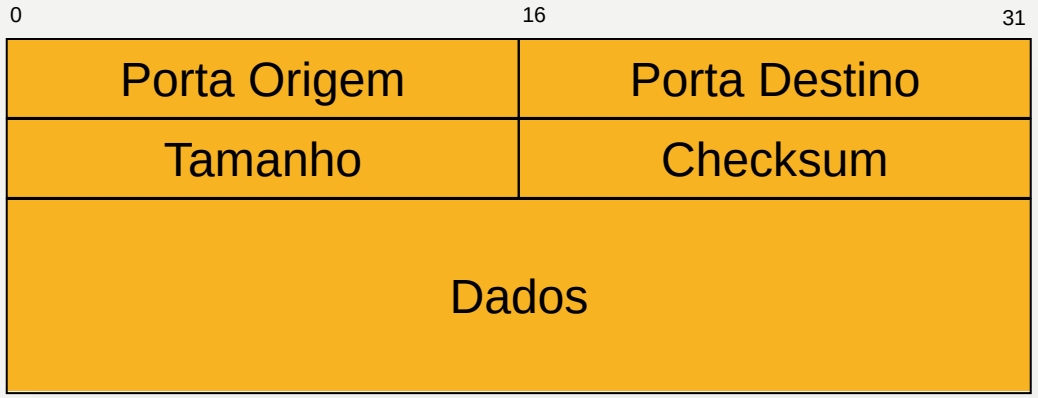
PROBLEMAS DO DNS

- Segurança
  - Bind passa a implementar criptografia e autenticação digital
  - Mascaramento de servidores
- Carga do servidor
  - Mecanismo de Round-Robin para distribuição das consultas localmente
- Erros de Configuração
  - Lamer: "*...name server is listed in the NS records for some domain and in fact it is not a server for that domain.*"

UDP (USER DATAGRAM PROTOCOL)

- O protocolo UDP é bastante simples
  - Orientado a datagrama
  - Não orientado à conexão
  - Não executa controle de fluxo, controle de erro e sequenciamento
  - Não tem reconhecimento dos datagramas (ACK/NACK)
- Devido a sua simplicidade é considerado não confiável

HEADER UDP



Onde,

Porta Origem e Porta Destino identificam o processo de aplicação que está enviando dados e o processo de aplicação que irá receber os dados.

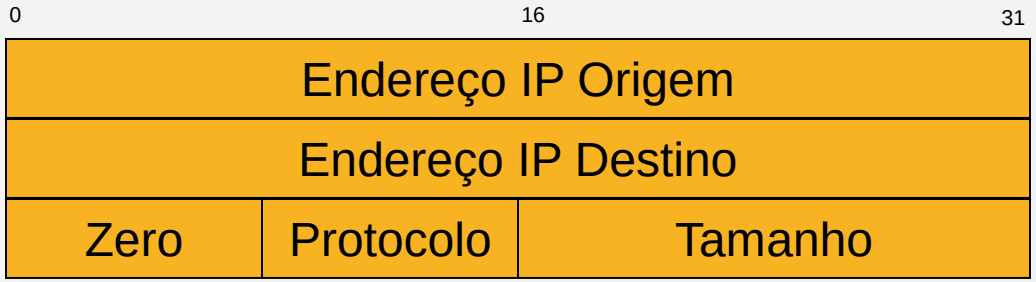
Tamanho é representa o tamanho total do frame UDP

Checksum é calculado usando o header UDP e também a área de dados, e destina-se a verificação de erros de transmissão.

CHECKSUM UDP

- O Checksum no UDP é opcional
  - Campo de checksum = 0, não executa verificação
  - Campo de checksum <> 0, executa verificação
- O cálculo do checksum utiliza o header, os dados e também o Pseudo-Header
  - Este pseudo-header é utilizado para verificação adicional e confirmação de que o datagrama chegou ao destino correto

PSEUDO-HEADER



Onde,

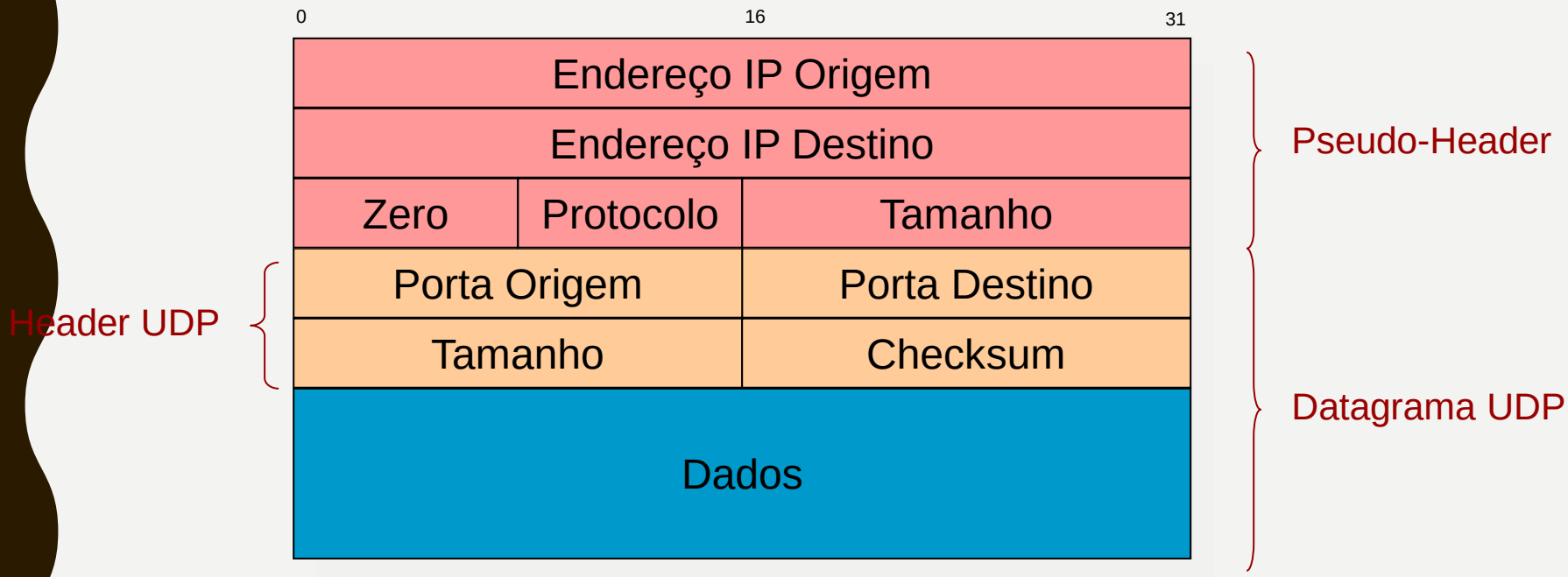
Endereço IP Origem e Endereço IP destino são do nível de rede (protocolo IP) utilizadas para a segunda validação do destino do datagrama.

Zero é um campo com valor zero para complementar a estrutura do pseudo-header.

Protocolo indica qual o protocolo de transporte (TCP ou UDP), pois o pseudo-header é utilizado para os dois protocolos.

Tamanho indica o tamanho do frame de transporte (UDP ou TCP)

ORDEM DE HEADER PARA O CHECKSUM DO UDP



Atenção!

O Pseudo-Header não é transmitido junto com o datagrama UDP, ele é utilizado apenas para cálculo do Checksum.

PROCESSAMENTO DO CHECKSUM

- Na origem, as informações necessárias são organizadas em blocos de 16 bits para o cálculo do checksum
  - Caso o cálculo resulte em zero, os 16 bits do checksum serão configurado todos em 1 (valor = 65535)
- Se optar-se por não utilizar checksum, os 16 bits serão configurados todos em 0

PROCESSAMENTO DO CHECKSUM

- Se o checksum recebido tem todos os bits em zero, não é necessário calculá-lo (pois não está sendo utilizado)
- Caso contrário, o cálculo do checksum é realizado novamente
  - Se o cálculo resultar em Zero, o datagrama não contém erros
  - Se o cálculo resultar diferente de Zero, o datagrama é descartado

TAMANHO MÁXIMO DO DATAGRAMA

- Teoricamente o tamanho máximo é de 64Kb
  - Porque no IP o campo tamanho total é de 16 bits
  - Mas deve-se considerar que no IP estão sendo calculado
    - Tamanho do Header do IP (20 bytes)
    - Datagrama UDP (8 bytes)
  - Assim, o tamanho máximo é de 65507 bytes

TAMANHO MÁXIMO DO DATAGRAMA

- Outros fatores podem influenciar
  - Programas de aplicação podem ser limitados pela interface de programação
  - Implementação do kernel do TCP/IP
- Truncando Datagramas
  - Apesar do tamanho máximo, nem todas as aplicações podem estar preparadas para receber um datagrama maior que esperado
    - Truncar ou não? Depende da implementação de cada interface de programação

UDP E ICMP SOURCE QUENCH

- Mensagens ICMP Source Quench
  - Podem ser geradas pelo sistema quando ele recebe dados a uma taxa maior que ele consegue processar
  - Não é obrigatória a geração, mesmo que o sistema descarte os datagramas
- "O sentimento corrente é que esta mensagem deve ser considerada obsoleta"
  - Porque consome largura de banda e é ineficaz para o controle de congestionamento
    - Almquist 1993 (RFC???)

UDP E ICMP SOURCE QUENCH

- Várias sistemas operacionais não geram estas mensagens
- Vários sistemas operacionais não repassam tais mensagens para o protocolo UDP
- Somente o TCP é notificado quando estas mensagens ocorrem!!!

TCP (TRANSMISSION CONTROL PROTOCOL)

- Protocolo de transporte considerado confiável
  - Orientado à conexão
  - Controle de erros com retransmissão
  - Controle de fluxo
  - Sequenciamento
  - Entrega ordenada
- Orientado a *"byte stream"*

HEADER TCP

Porta origem			Porta destino
Número de Seqüência			
Acknowlegement			
Tam.	Reser.	Flags	Window
Checksum			Urgent Pointer
Opções (se houver)			
Dados			

HEADER TCP

Onde,

Porta Origem e Porta Destino identificam o processo de aplicação que está enviando dados e o processo de aplicação que irá receber os dados.

Número de seqüência identifica os bytes enviados. Na prática ele é a identificação do primeiro byte de dados contido no segmento enviado. Os demais são seqüenciados a partir deste byte.

Acknowledgement identifica os bytes que foram recebidos e tratados sem erro pelo destino, bem como a seqüência do próximo byte esperado

Tamanho é representa o tamanho total do frame TCP

Reservado é um campo ainda não utilizado

FLAGS identifica as flags (syn, fin, psh, rst, ack, urg)

Window identifica o tamanho da janela para o controle de fluxo

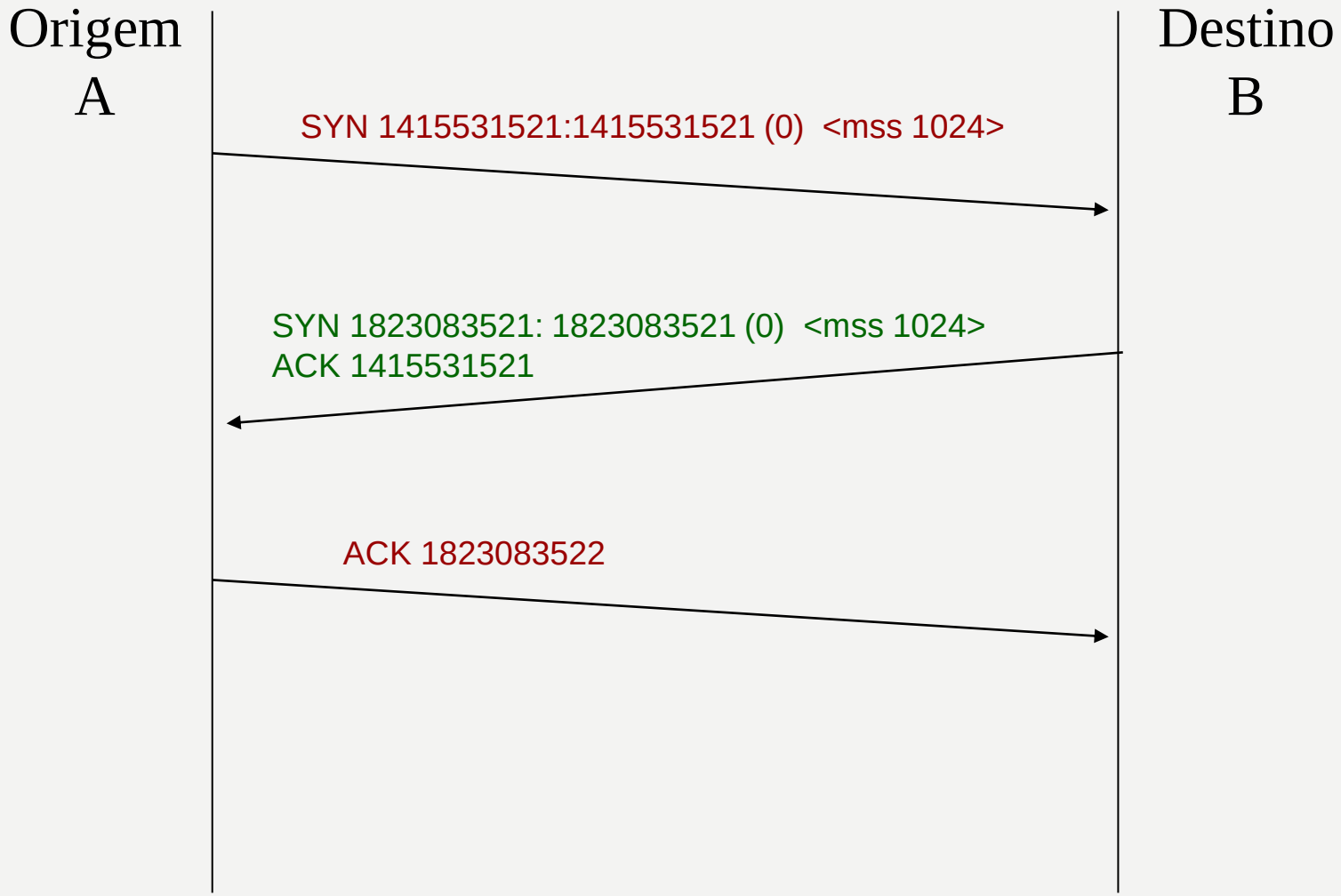
Checksum destina-se a verificação de erros de transmissão. É calculado usando o pseudo header, o header TCP e também a área de dados

Urgent Poninter é um ponteiro para dados urgentes, contidos na área de dados.

CONTROLE DE CONEXÃO TCP

- Três Fases
  - Estabelecimento da Conexão
  - Transmissão de Dados
  - Encerramento da Conexão
- Flags
  - SYN – solicitação de conexão
  - FIN – Finalização da Conexão
  - RST – Reset da Conexão
  - ACK – Reconhecimento de recebimento

ESTABELECIMENTO DA CONEXÃO



ESTABELECI MENTO DA CONEXÃO

- Ativo x passivo
  - A origem da solicitação de conexão executa o "*active open*"
  - O destino que recebe a solicitação de conexão executa o "*passive open*"
- Origem e destino enviam seus número de seqüência iniciais para a conexão em curso
  - Este número deve ser alterado ao longo do tempo e ser diferente de conexão para conexão

INICIALIZAÇÃO DO NÚMERO DE SEQÜÊNCIA

RFC 793

- Número de 32 bits
- É incrementado a cada 4 microsegundos

Como escolher o número inicial?

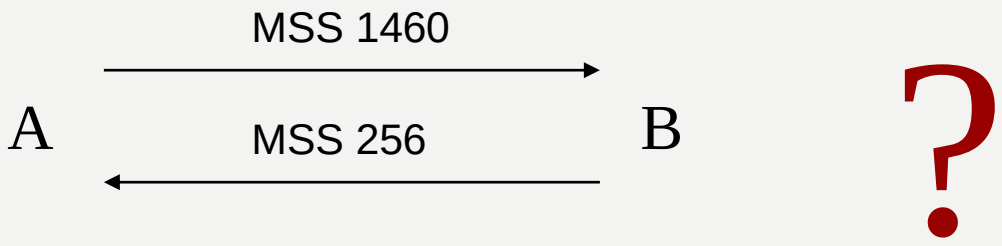
- 4.4BSD
  - Quando sistema é inicializado o número de seqüência é 1 (violação da RFC)
  - A variável é incrementada de 64.000 a cada ½ segundo
  - Isso significa que irá retornar a 0 em períodos de 9 horas e ½

MSS (MAXIMUM SEGMENT SIZE)

- O MSS representa o tamanho do maior bloco de dados que poderá ser enviado para o destino.
- Não é negociável, cada host divulga o seu MSS
  - Default: 536 bytes (20 bytes IP, 20 bytes TCP, para um total de 576 bytes)
  - Ethernet: 1460 bytes (20 bytes IP, 20 bytes TCP, para um total de 1500 bytes)

MSS...

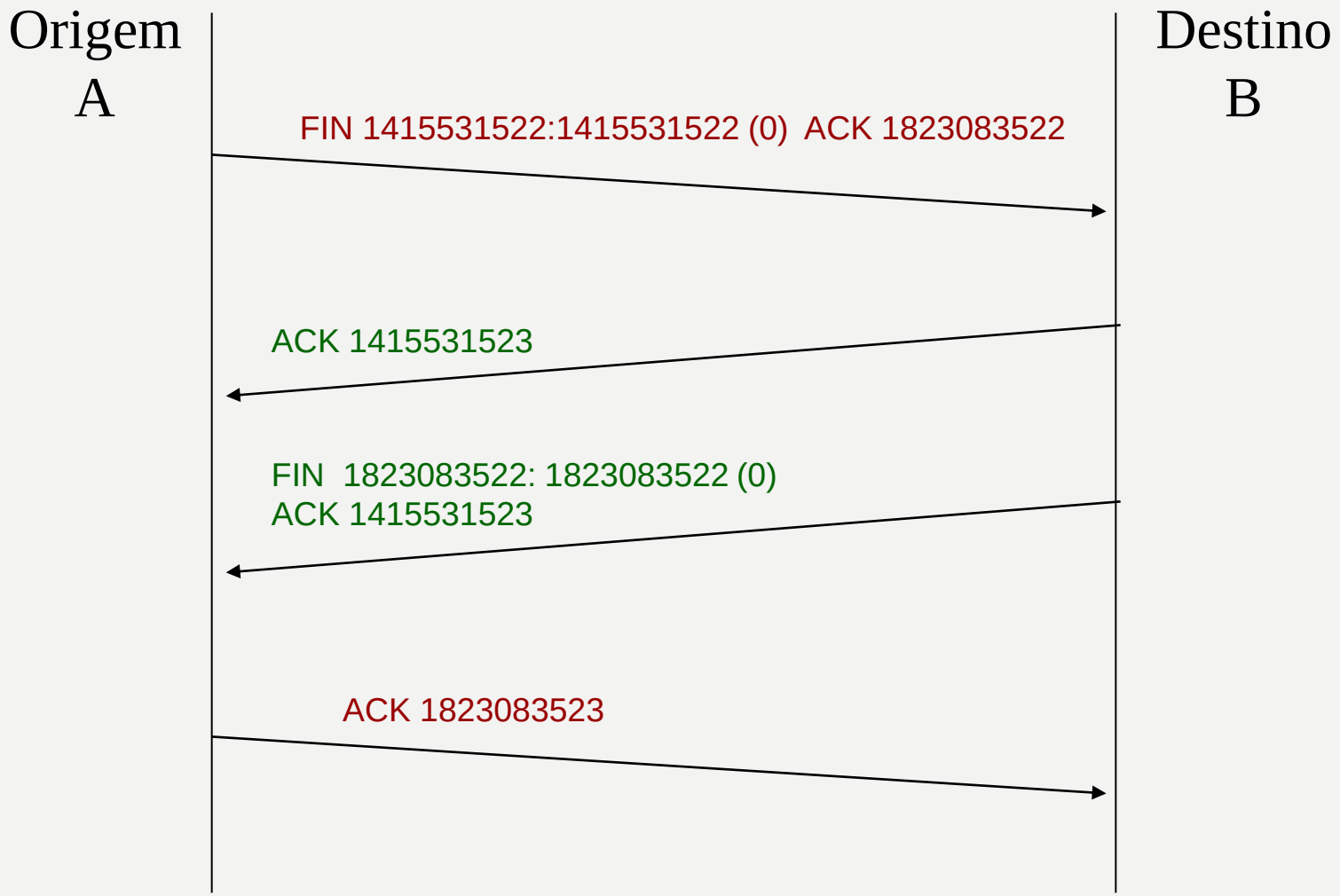
- Em geral, quanto maior o MSS melhor, até que ocorra fragmentação
  - Quanto maior a quantidade de dados enviados em um único bloco, menor o overhead de headers do TCP e do IP
- Exemplo



OUTRAS OPÇÕES TCP

- End of option list (1 byte)
- No operation (NOP) (1 byte)
- Windows scale factor (3 bytes)
- Timestamp (10 bytes)
- MSS (4 bytes)

ENCERRAMENTO DA CONEXÃO



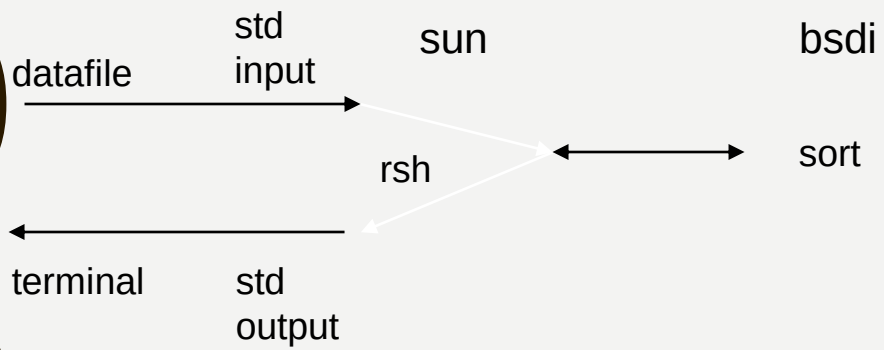
ENCERRAMENTO DA CONEXÃO

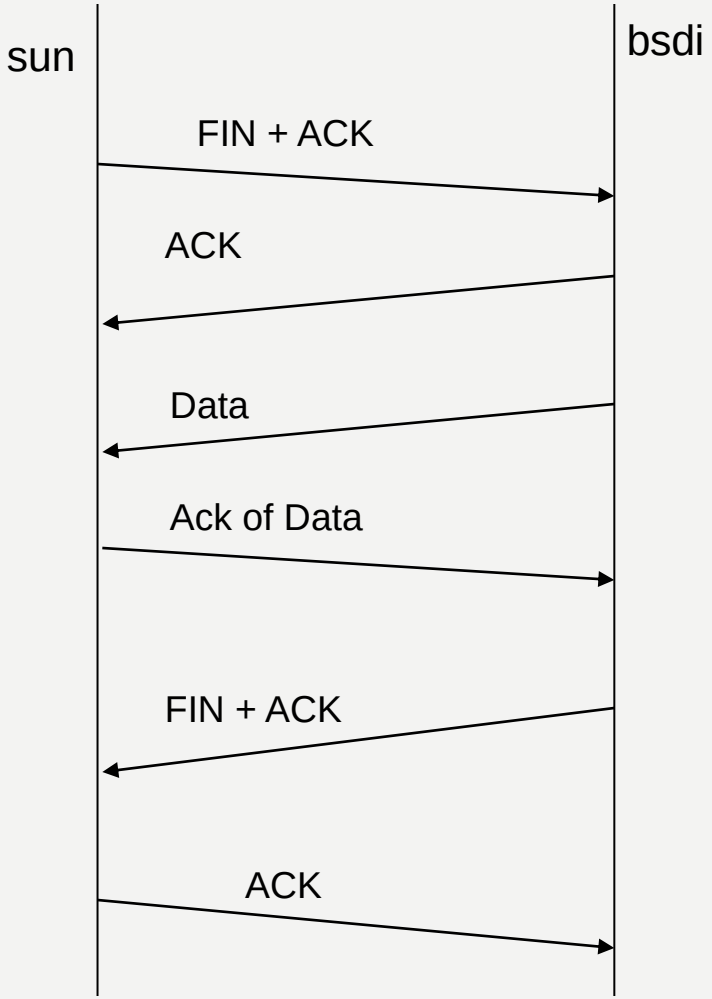
- *Half Close*
  - Conexões TCP são *full-duplex*, logo cada lado da conexão deve finalizar a conexão de forma independente
  - Quando um dos lados envolvidos recebe uma solicitação de finalização deve enviar a notificação para a aplicação
    - Uma aplicação após receber o pedido de finalização ainda pode mandar dados

HALF CLOSE - EXEMPLO

Exemplo:

sun% rsh bsdi < datafile



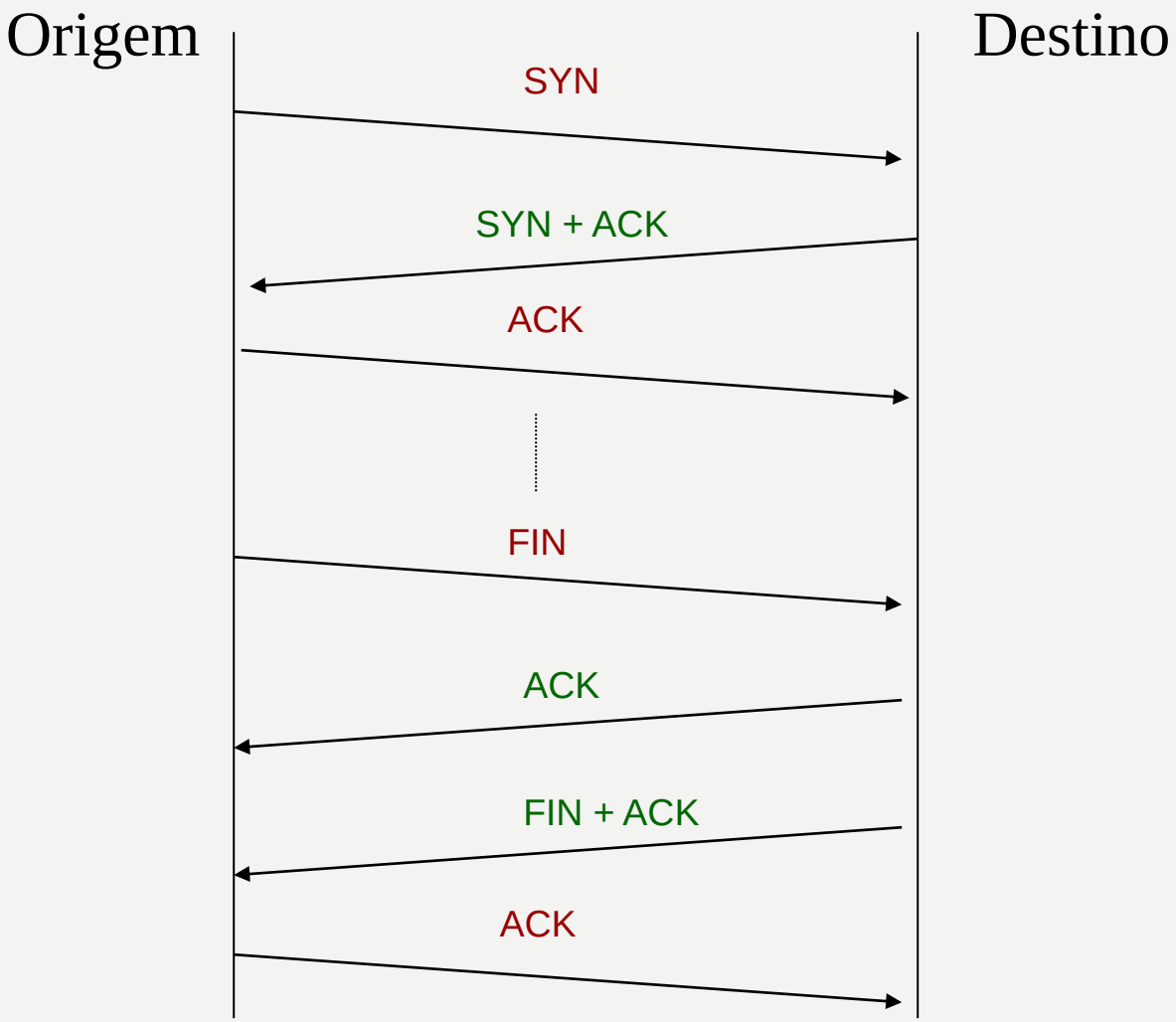


TIMEOUT NO ESTABELECIMENTO DA CONEXÃO

- Trecho de tráfego monitorado (tcpdump)

- Importante: tempo entre cada tentativa vs. tempo máximo exigido na RFC
  - Tempo: 75 segundos
  - 4.4 BSD: leva 76 segundos
  - Problema: Timeout

ESTADOS X MENSAGENS



RESET DE CONEXÕES

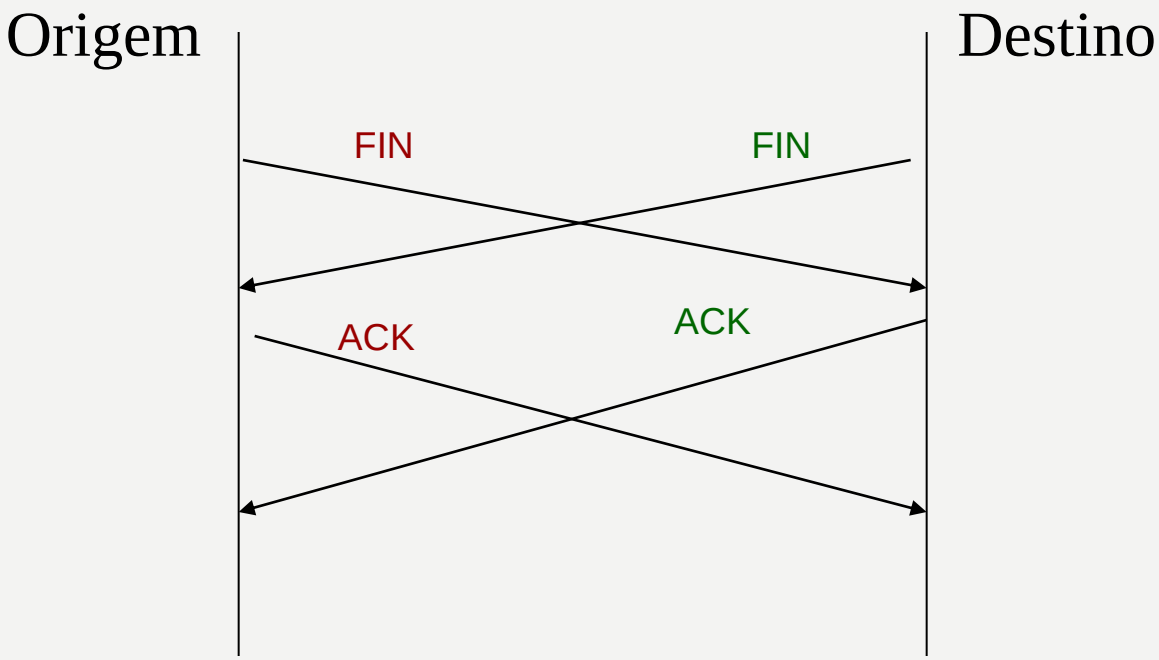
- Em geral, um Reset é gerado sempre que é recebido um segmento que não parece estar correto para a conexão identificada.
- Casos
  - Solicitações de conexões para portas inexistentes
  - Aborto de conexões
  - Solicitações de conexões falsas

ESTABELECIMENTO DE CONEXÕES SIMULTÂNEAS

- É possível que 2 hosts tentem estabelecer conexão entre eles simultaneamente
  - Ambos executam um *active open*
  - Exemplo:
    - Host A solicita conexão ao Host B na porta 777 e usa como porta local 888
    - Host B solicita conexão ao Host A na porta 888 e usa como porta local 777
- TCP foi projetado para suportar estes casos
  - Apenas uma conexão resulta, não duas

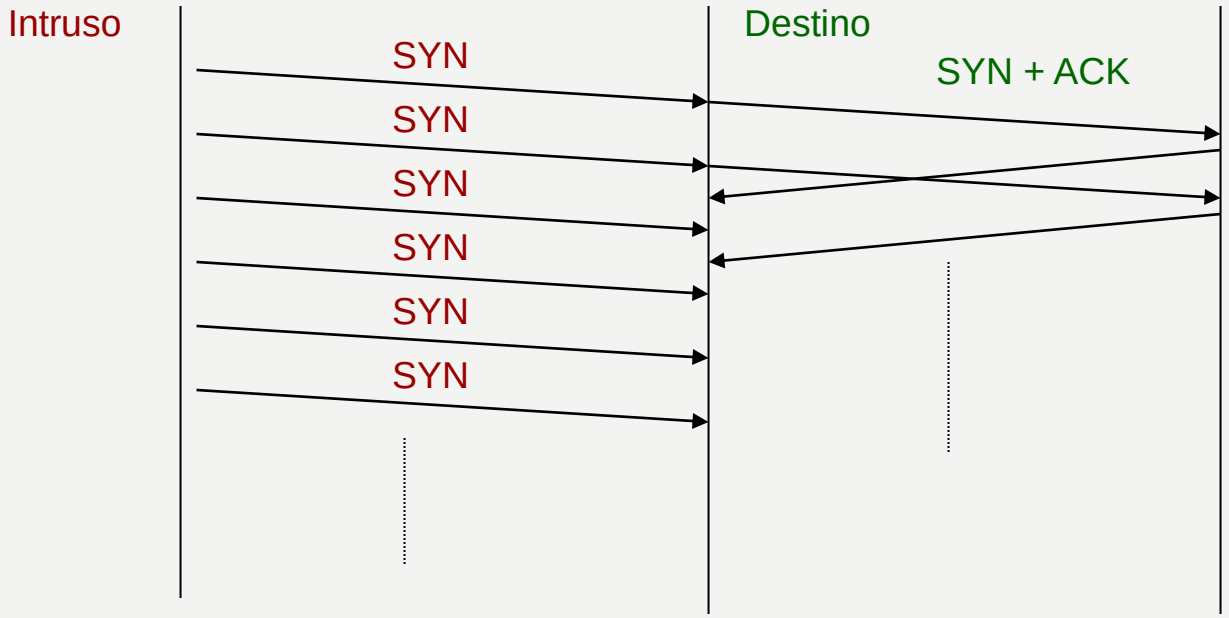
ENCERRAMENTO DE CONEXÕES SIMULTÂNEAS

- Os hosts também podem tomar a iniciativa de encerrar a conexão simultaneamente



SYN FLOOD

- Flooding de solicitações de conexão falsas
  - Normalmente usa IP Spoofing

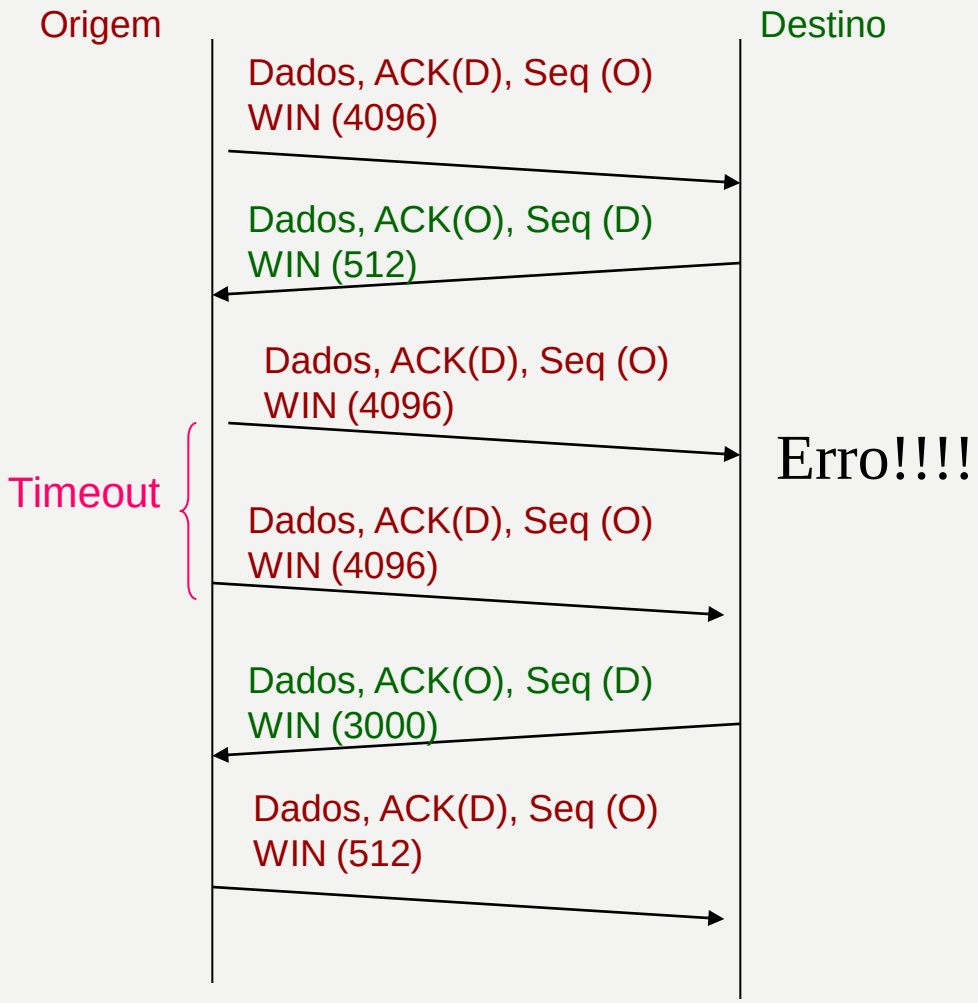


CONTROLE DE ERROS

- O TCP executa controle de erro com retransmissão
  - Neste caso o checksum não é opcional
  - Se um segmento TCP é recebido com checksum igual a zero, ele é descartado
  - O destino envia mensagens de reconhecimento positivo
    - Não envia NACK
    - A necessidade de realizar uma retransmissão é detectada pela ausência do ACK

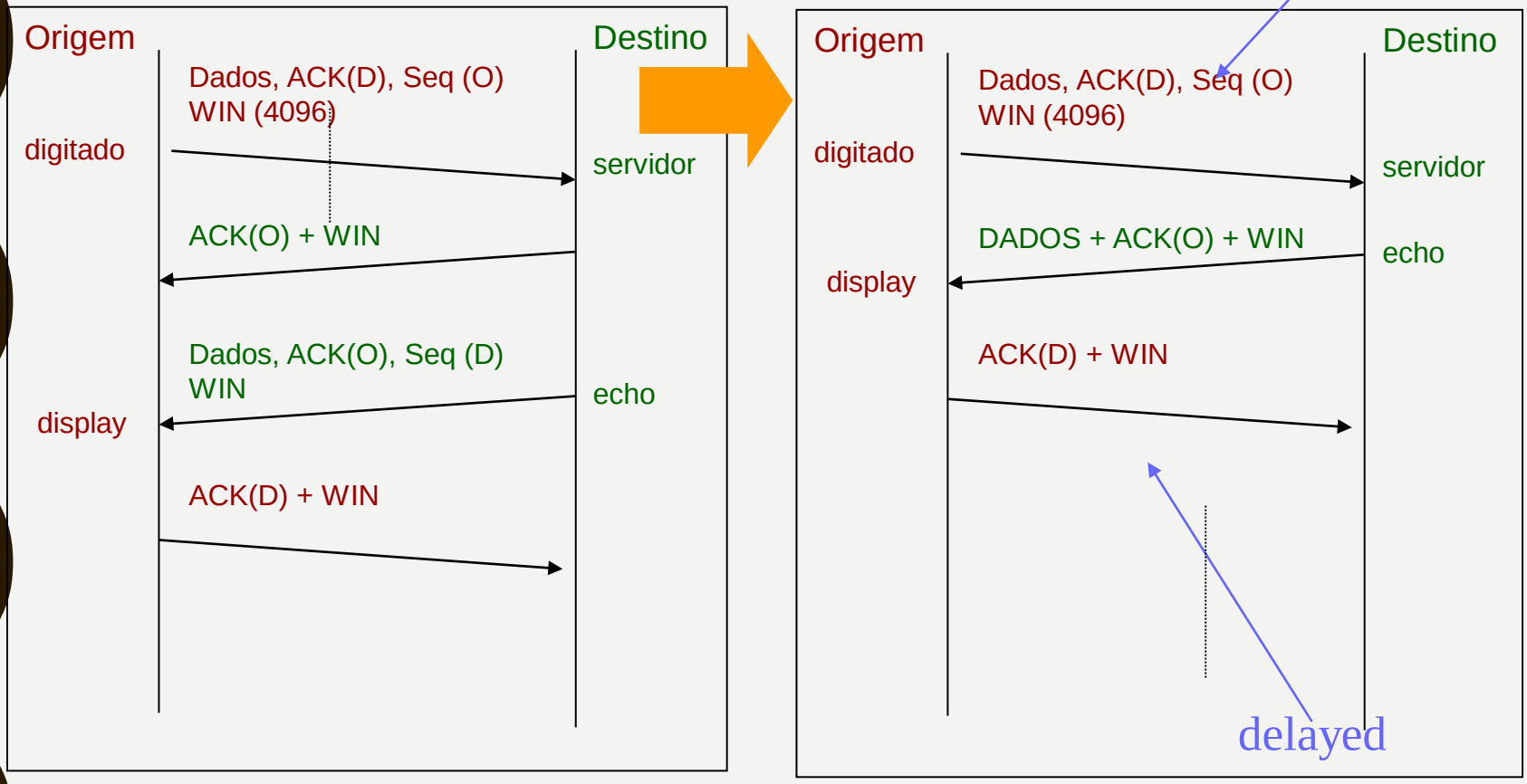
CONTROLE DE FLUXO

- O TCP executa o algoritmo de janela deslizante
  - A cada envio de mensagens o host informa o número de bytes que podem ser recebidos



FLUXO INTERATIVO

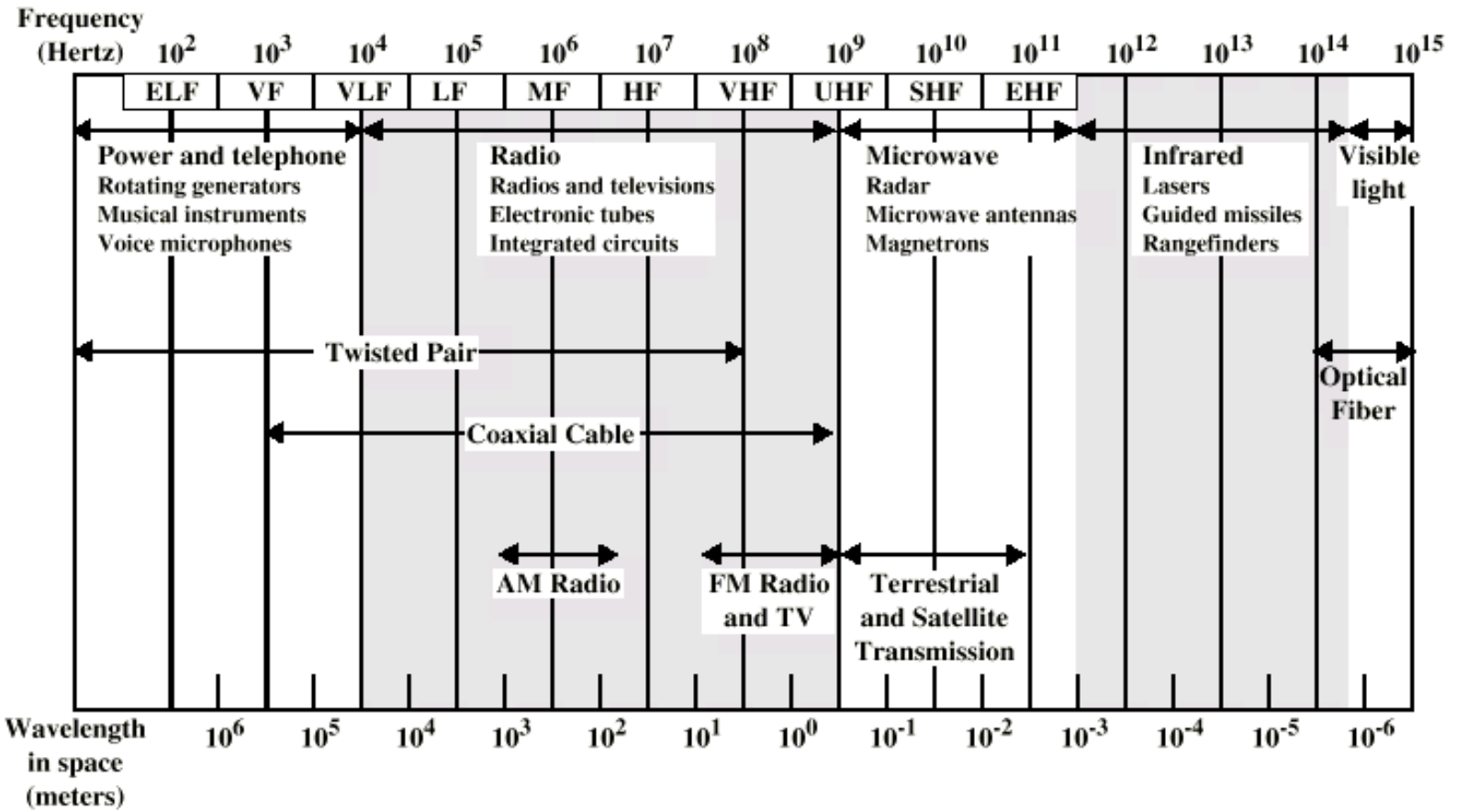
- Exemplo: rlogin



MEIOS FÍSICOS

- Pares Metálicos
  - Cabo coaxial
  - Par Trançado
  - Pares bifiliares
- Condutores Óticos
  - Fibra
- Rádio
- Infravermelho

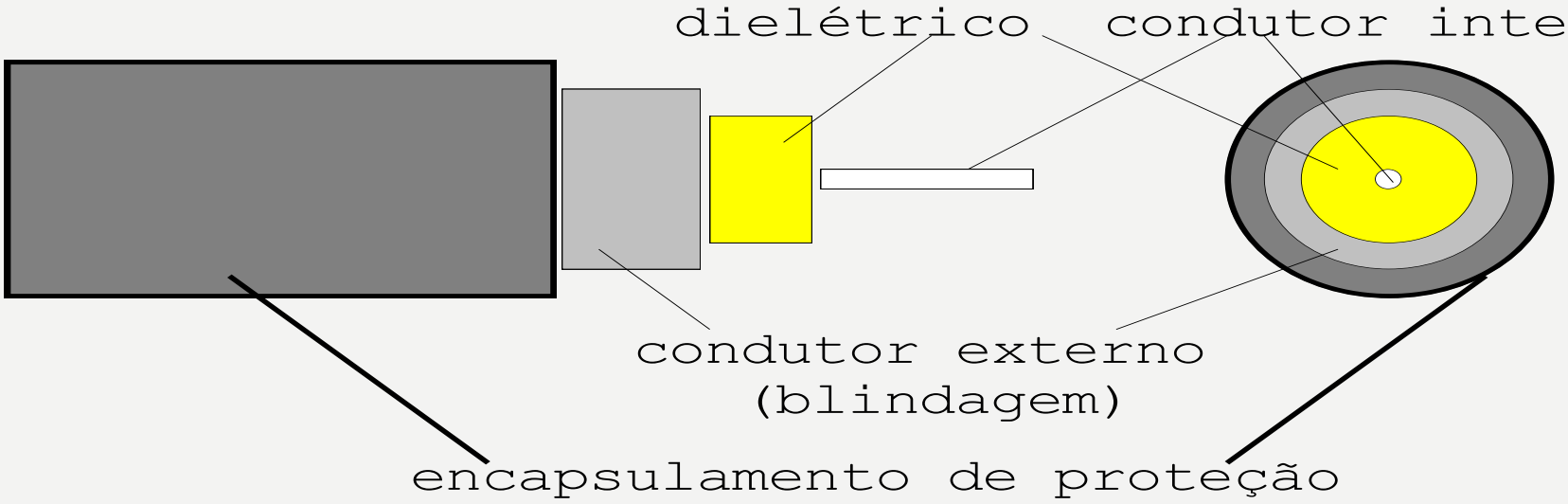
ESPECTRO ELETROMAGNÉTICO



ELF = Extremely low frequency
VF = Voice frequency
VLF = Very low frequency
LF = Low frequency
MF = Medium frequency
HF = High frequency
VHF = Very high frequency
UHF = Ultrahigh frequency
SHF = Superhigh frequency
EHF = Extremely high frequency

CABO COAXIAL

Construção



APLICAÇÕES DO CABO COAXIAL

- Distribuição de Televisão
  - TV a Cabo
- Transmissões telefônicas de longas distâncias
  - Está sendo substituído por fibra
- Enlaces de redes locais de curta distância

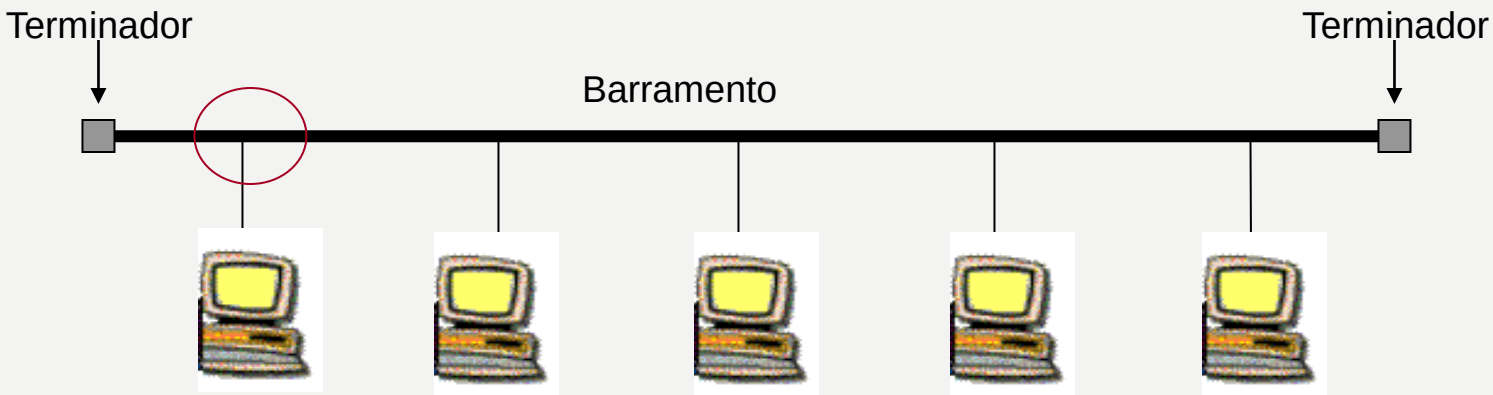
10BASE5

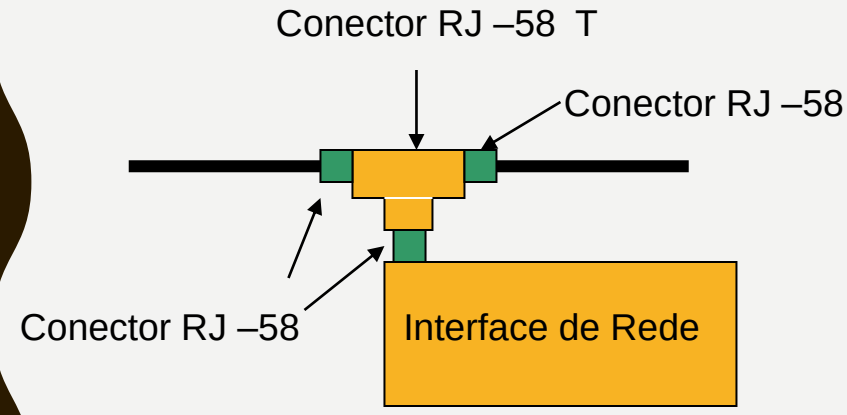
- Ethernet - cabo grosso (50 ohms).
- Taxa de 10Mbps com sinalização em banda-base e codificação manchester.
- Topologia em barramento.
- Máximo de 5 segmentos de 500 m.
- Conexão da placa de rede ao cabo por uma unidade ativa (transceptor): o conector-vampiro. A mordida (conexão) só deve ser feita nas marcas do cabo.
- Distância mínima entre transceptores de 2,5 m.
- Um segmento de cabo é contínuo, sem conexões que possam interromper o barramento

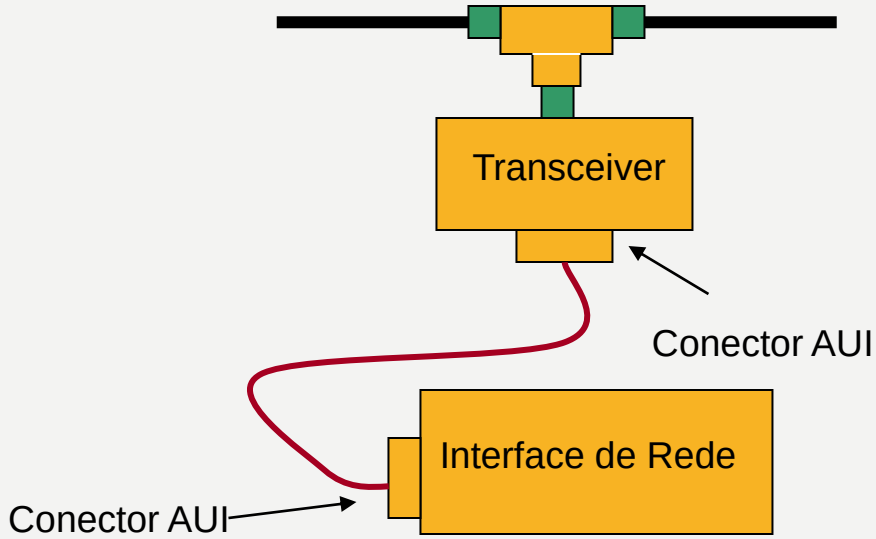
10BASE2

- Cabo fino
- Taxa de 10Mbps com sinalização em banda-base e codificação manchester.
- Topologia em barramento.
- Máximo de 5 segmentos de 185 m. Total de 925m.
- Máximo de 30 nós por segmento (existem placas que permitem até 100 nós, por segmento).
- Cada ligação com a placa de rede utiliza um conector tipo **T**, ligando dois trechos de cabo e a placa. Cada trecho de cabo deve ter o mínimo de 45 cm.
  - Fonte potencial de problemas
  - Existem soluções com tomadas de parede (AMP) que minimizam a possibilidade do usuário causar o rompimento do barramento.

USANDO O CABO COAXIAL



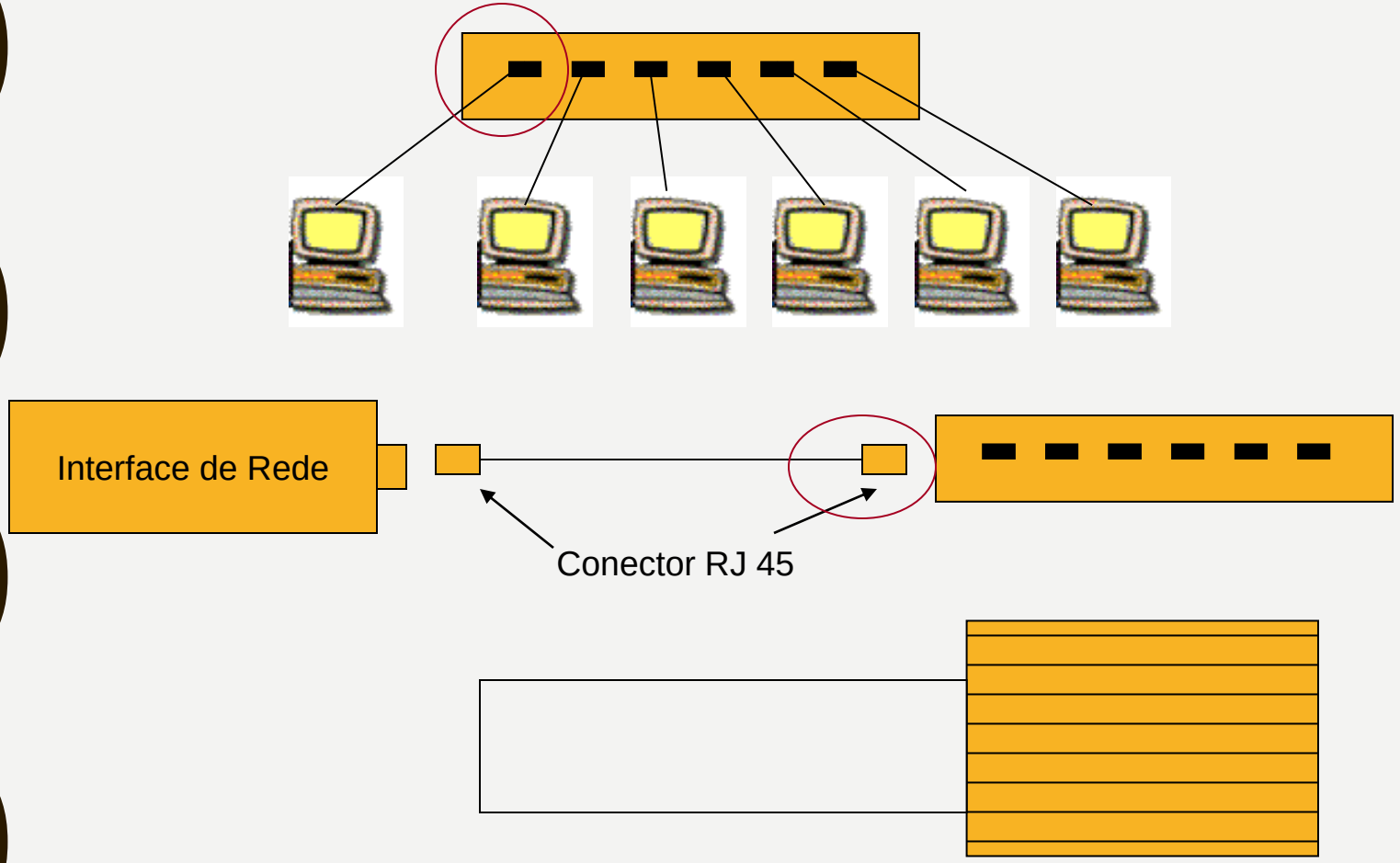




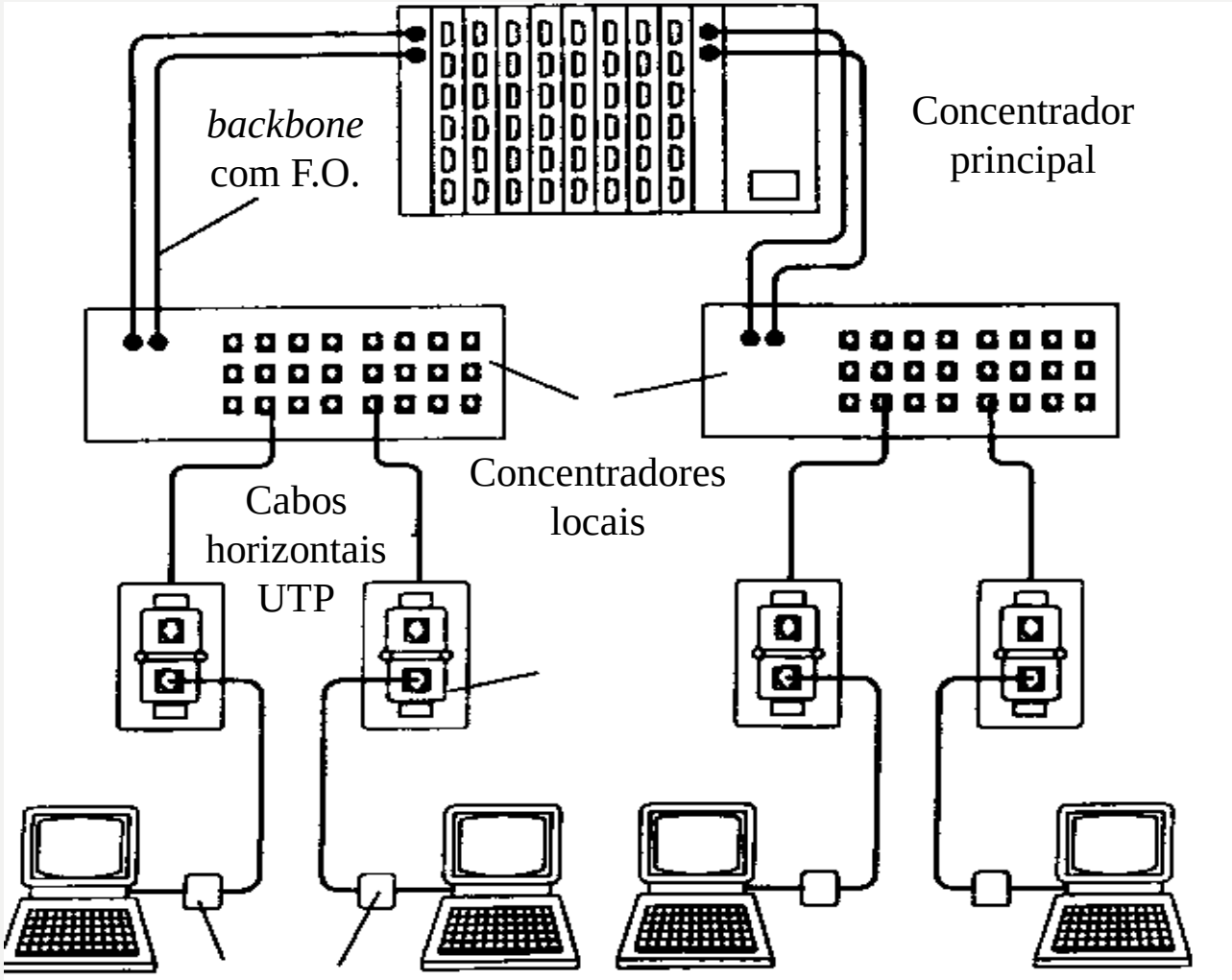
PAR TRANÇADO

- Duas categorias
  - UTP (Unshielded Twisted Pair)
  - STP (Shielded Twisted Pair)
- Esquema de fiação com concentradores de fiação (*HUBs*)
  - Topologia em estrela.
- Distância máxima de 100 m entre *HUB* e estação, no caso de redes Ethernet e Fast Ethernet
- Não existem terminadores
- Aplicações
  - Sistema Telefônico
  - Redes de Computadores

USANDO O PAR TRANÇADO



USANDO UM PATCH PANEL



EIA/TIA - 568

- Especifica somente cabos de pares, trançados ou não, sem blindagem.
- Descreve especificações de desempenho do cabo e sua instalação.
- É um padrão aberto, não contendo marca de nenhum fabricante.

EIA - CATEGORIAS 1 E 2

- Categoria 1
  - Especificações técnicas pouco precisas.
  - Cabos não trançado AWF 22 ou 24.
  - Grande variação de impedância e atenuação.
  - Não recomendado para taxas de sinalização superiores a 1 Mbps.
- Categoria 2
  - Pares trançados AWG 22 ou 24.
  - Largura de banda máxima de 1 MHz.
  - Não é testado com relação à paradiafonia.
  - Derivado da especificação de cabo Tipo 3 da IBM.

EIA - CATEGORIAS 3 E 4

- Categoria 3
  - Pares trançados sólidos AWG 24.
  - Impedância de 100 ohms.
  - Testado a 16 MHz para atenuação e paradiafonia.
  - Utilizável até 16 Mbps.
  - Padrão mínimo para 10Base-T.
  - Bom p/ *token ring* a 4 Mbps.
- Categoria 4
  - Pares trançados sólidos AWG 22 ou 24.
  - impedância de 100 ohms.
  - testado para largura de banda de 20Mhz

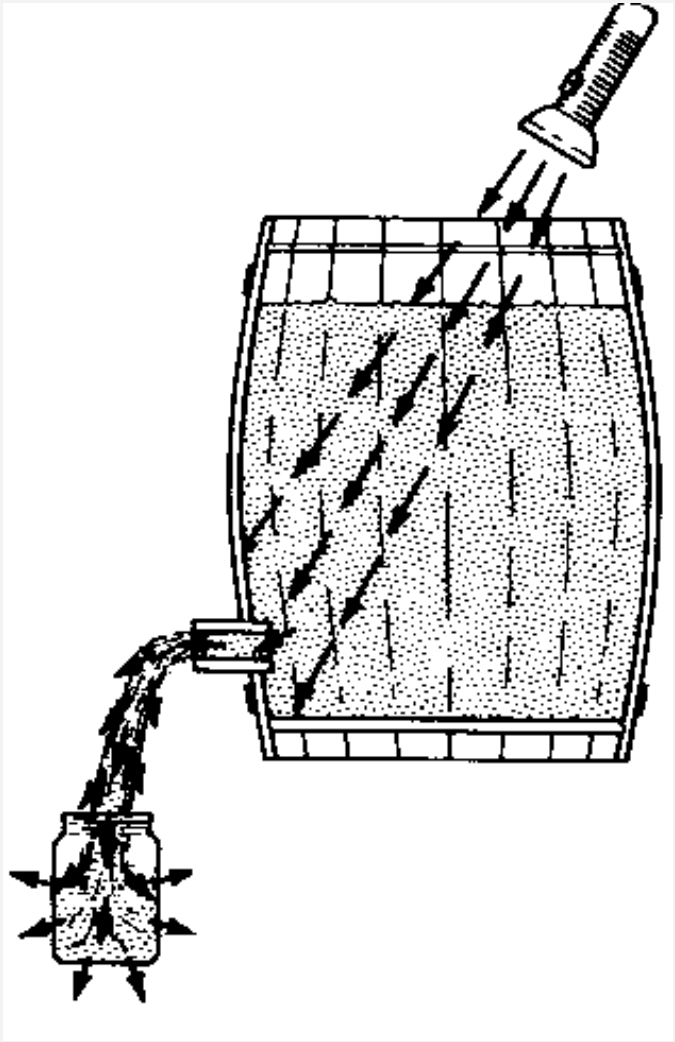
EIA - CATEGORIA 5

- Pares trançados AWG 22 ou 24.
- Impedância de 100 ohms.
- Testado para largura de banda de 100 MHz.
- Pode ser usado para taxas de 100 Mbps.
- É recomendado para as novas instalações, de modo a ser aproveitado em futuros aumentos de taxa de transmissão.

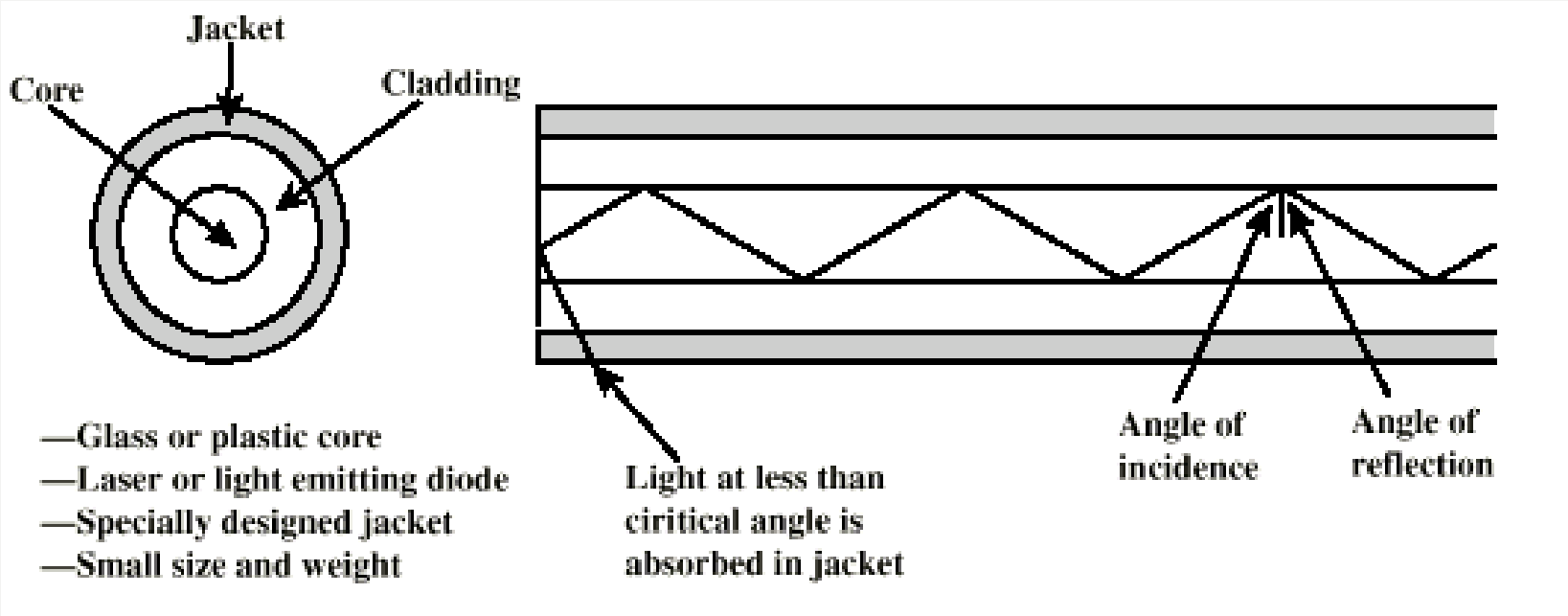
Categoria	Taxa máxima de transmissão	Aplicação usual
CAT 1	Até 1 Mbps (1 MHz)	Voz Analógico (POTS) ISDN (Integrated Services Digital Network) Basic Rate Interface Fiação tipo fio de telefone
CAT 2	4 Mbps	Utilizado em sistemas de cabeamento IBM Token Ring
CAT 3	10 / 16 Mbps	Voz e dados em rede 10BASE-T Ethernet
CAT 4	16 / 20 Mbps	Usado em redes Token Ring de 16 Mbps
CAT 5	100 Mbps 1 Gbps (4 pares)	100 Mbps TPDDI 155 Mbps ATM Não é mais utilizado, substituído pelo CAT 5E
CAT 5E	1 Gbps (10 Gbps – protótipo)	100 Mbps TPDDI 155 Mbps ATM Gigabit Ethernet
CAT 6	Até 400 MHz	Aplicações de banda larga "super-rápidas"
CAT 6A	Até 625 MHz (testado em campo até 500 MHz)	Suporta completamente 10 Gigabit Ethernet (10GBASE-T)
CAT 7	600-700 MHz 1.2 GHz em pares com conector Siemon	Vídeo em Full-motion Telerradiologia Redes especializadas de governo Redes especializadas de manufatura Redes especializadas de ensino Sistema blindado

Meios de Transmissão

- LUZ
  - ⇨Laser
  - ⇨Fibras ópticas

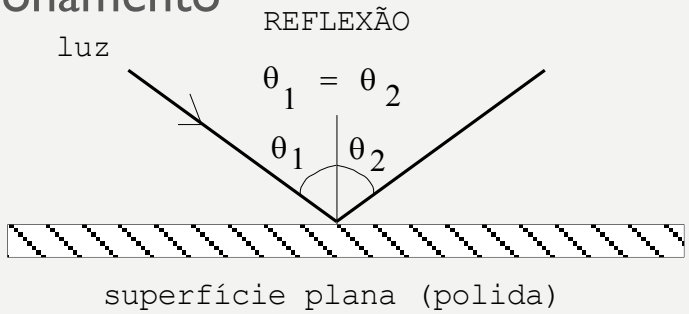


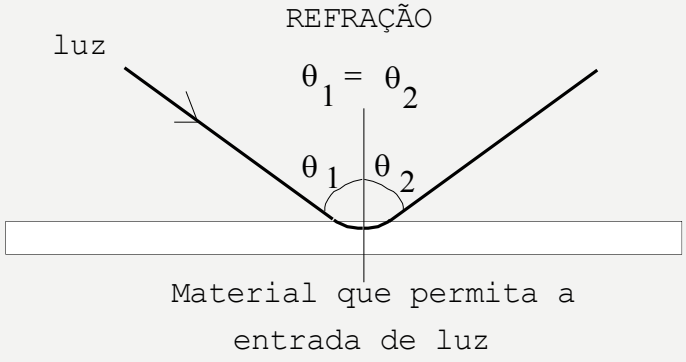
FIBRA ÓTICA


Jacket
Core
Cladding
—Glass or plastic core
—Laser or light emitting diode
—Specially designed jacket
—Small size and weight
Light at less than ciritical angle is absorbed in jacket
Angle of incidence
Angle of reflection

FIBRA ÓPTICA

- Princípio de funcionamento





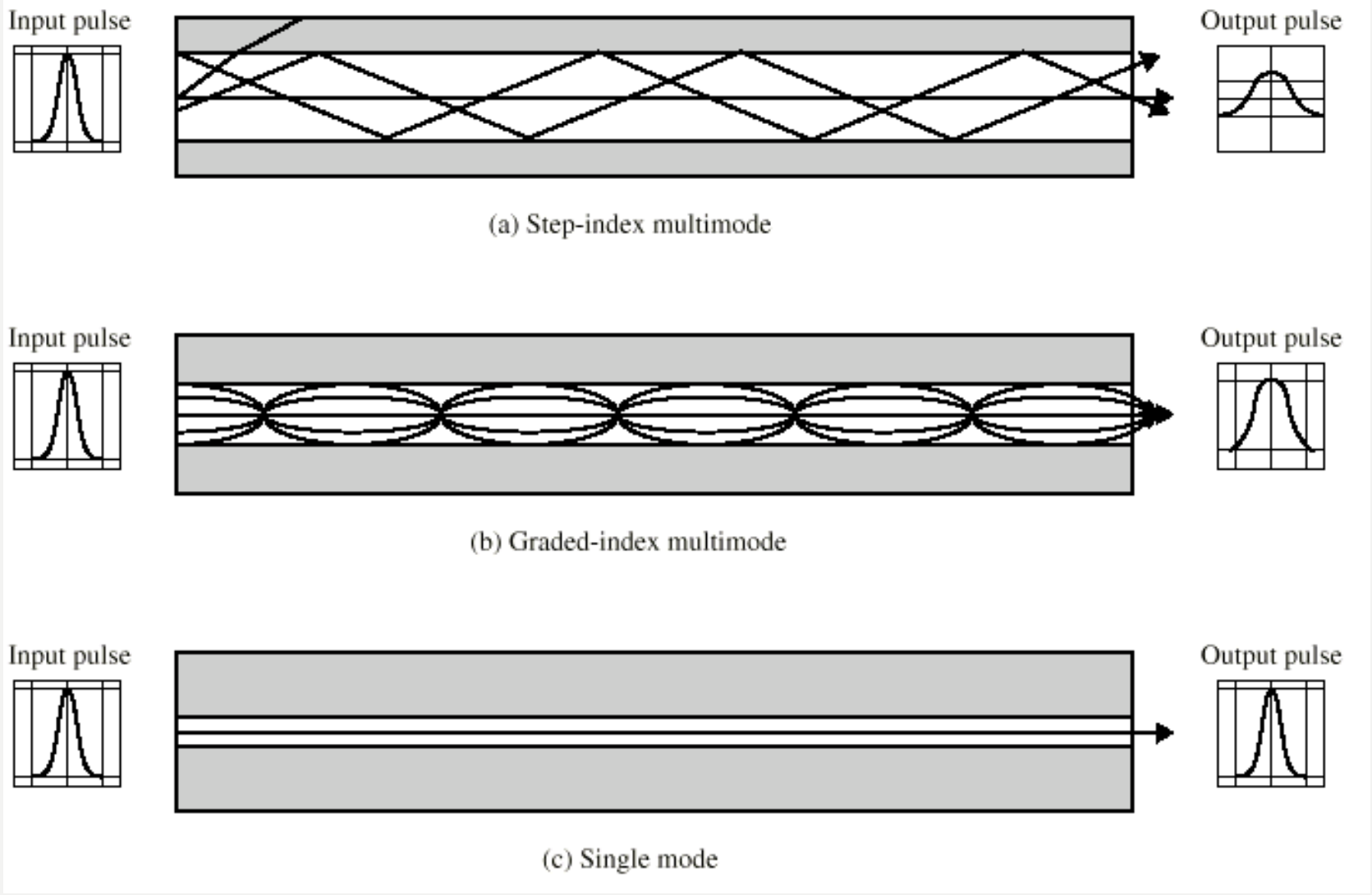
Fibra óptica

- Vantagens
  - ⇨ banda larga
  - ⇨ leve e pequena (fina)
  - ⇨ baixa perda de sinal
  - ⇨ livre de interferências eletromagnéticas
  - ⇨ segura
  - ⇨ confinamento do sinal
  - ⇨ custo

CARACTERÍSTICAS DE TRANSMISSÃO

- Onda guiada para 10^{14} to 10^{15} Hz
  - Porções de infravermelho e espectro visível
- Light Emitting Diode (LED)
  - Mais barato
- Injection Laser Diode (ILD)
  - Mais eficiente
  - Maior taxa de dados

MODOS DE OPERAÇÃO



Padrão	Taxa	Comprimento de onda	OS1	OS2
10GBASE-SR/SW	10Gb/s	850nm		
10GBASE-LR/LW	10Gb/s	1310nm	4,2Km	10Km
10GBASE-LRM	10Gb/s	1310nm		
10GBASE-LX4	10Gb/s	1310nm	4,2Km	10Km
10GBASE-ER/EW	10Gb/s	1550nm	8,9Km	22,25Km
10GBASE-ZR/ZW	10Gb/s	1550nm		80Km
40GBASE-SR4	40Gb/s	850nm		
40GBASE-LR4	40Gb/s	1310nm	4.7Km	10Km
100GBASE-SR10	100Gb/s	850nm		
100GBASE-LR4	100Gb/s	1295/1310nm	8.3Km	10Km
100GBASE-LR10	100Gb/s	1310nm	8.3Km	10Km
100GBASE-ER4	100Gb/s	1295/1310nm	16Km	40Km

AR

- Ar - Rádio-freqüência
  - Faixas de freqüência
    - ELF / VLF / LF / MF / HF
    - VHF / UHF
    - Satélite
    - Microondas (UHF / SHF)
      - Visibilidade

TRANSMISSÃO NO AR

FAIXA DE FREQÜÊNCIA (Hz)	DESIGNAÇÃO TÉCNICA	CARACTERÍSTICA DE PROPAGAÇÃO ÚTIL	PRINCIPAL UTILIZAÇÃO
300 a 3.000	ELF (Extremely Low Frequency)	Penetram na superfície terrestre e na água	Comunicação para submarinos e escavações de minas.
3K a 30K	VLF (Very Low Frequency)	Ótima reflexão na ionosfera e alguma penetração na superfície	Comunicação para submarinos e escavações de minas.
30K a 300K	LF (Low Frequency)	Reflexão na ionosfera até 100K. Acima de 100K, ondas de superfície	Serviços marítimos e auxílio a navegação aérea.
300K a 3.000K	MF (Medium Frequency)	Ondas de superfície com pouca atenuação	Radiodifusão local.
3M a 30M	HF (High Frequency)	Refração na ionosfera	Radiodifusão local e distante. Serviços marítimos
30M a 300M	VHF (Very High Frequency)	Pode ser focalizada por antenas convenientes	TV, sistemas comercias e particulares de comunicação.
300M a 3.000M	UHF (Ultra High Frequency)	Direcionamento por antenas mais eficiente, tropodifusão (1 a 2 GHz)	TV, serviços de segurança pública
3G a 30G	SHF (Super High Frequency)		Comunicação pública à longa distância
30G a 300G	EHF (Extremely High Frequency)		

RÁDIO FREQÜÊNCIA: RECENTES UTILIZAÇÕES

- Telefonia celular
- Redes locais sem fio (*Wireless LAN*)
  - Meio não guiado
    - Transmissão e recepção via antena
  - Direcional
    - Alinhamento
  - Omnidirectional
    - Sinal espalha-se em todas as direções
    - Pode ser recebido por muitas antenas

FREQÜÊNCIAS

- 2GHz to 40GHz
  - Microondas
  - Altamente direcional
  - Ponto a Ponto
  - Satélite
- 30MHz to 1GHz
  - Omnidirectional
  - Rádio em Broadcast
- 3×10^{11} to 2×10^{14}
  - Infravermelho
  - Aplicação local

MICROONDAS TERRESTRE

- Antenas Parabólicas
- Visada direta
- Altas freqüências = alta taxa de dados
- Problemas
  - Períodos de precipitação intensa
  - Desalinhamento das antenas

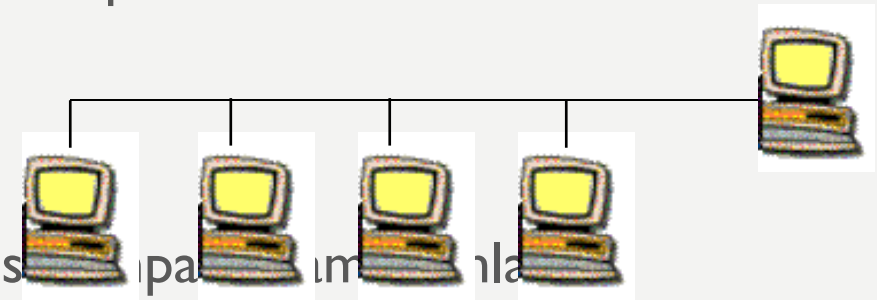
MICROONDAS - SATÉLITE

- O Satélite é uma estação de *"relay"*
- O satélite recebe em uma freqüência amplifica ou repete o sinal e transmite em outra freqüência
- Órbita geo-estacionária
- Usado para
  - Televisão
  - Telefônia de longa distância
- Redes Privadas

LIGAÇÕES - TOPOLOGIA

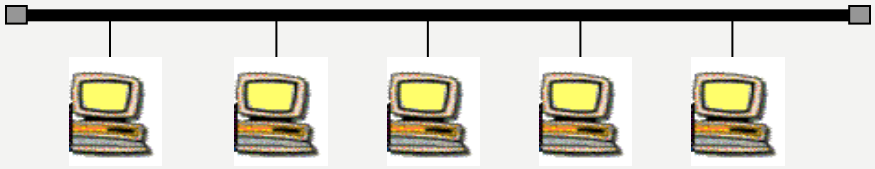
- Enlace Direto
  - Sem dispositivos intermediários
- Enlace Ponto-a-Ponto
  - Enlace direto
  - Somente 2 dispositivos compartilham o enlace

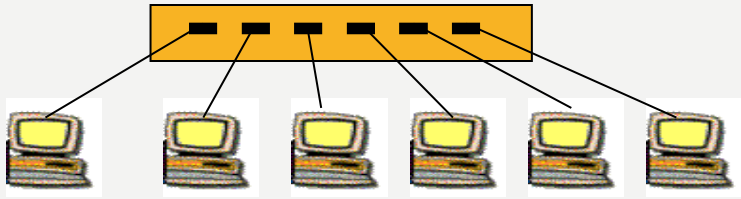
- Enlace Multiponto
  - Mais de dois dispositivos pa[illegible] m[illegible] la

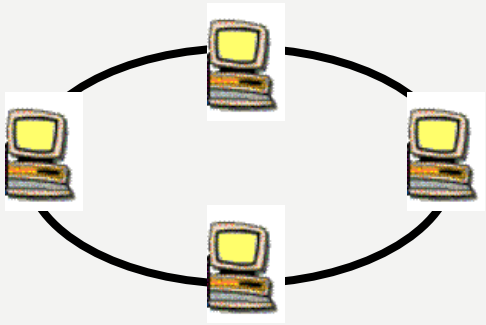


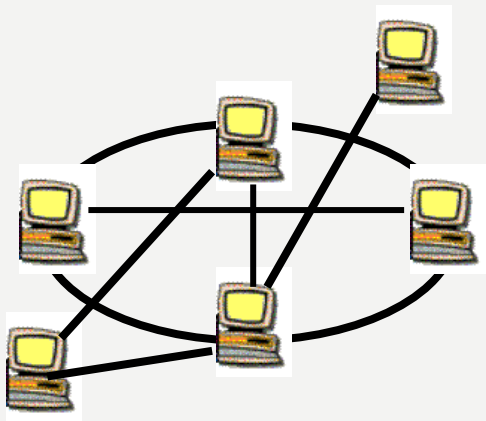
TOPOLOGIAS

- Barramento
- Estrela
- Anel
- Malha









ENDEREÇAMENTO DE REDE IPV4

Classe	Primeiro Octeto	Parte da rede (N) e parte para hosts (H)	Máscara	Nº Redes	Endereços por rede
A	1-127	N.H.H.H	255.0.0.0	**126** (2^7 -2)	**16,777,214** (2^{24} -2)
B	128-191	N.N.H.H	255.255.0.0	**16,382** (2^{14}-2)	**65,534** (2^{16}-2)
C	192-223	N.N.N.H	255.255.255.0	**2,097,150** (2^{21}-2)	**254** (2^8-2)
D	224-239	Multicast	NA	NA	NA
E	240-255	experimental	NA	NA	NA