Protocolos de Rede - I

Laboratório de Redes de Computadores

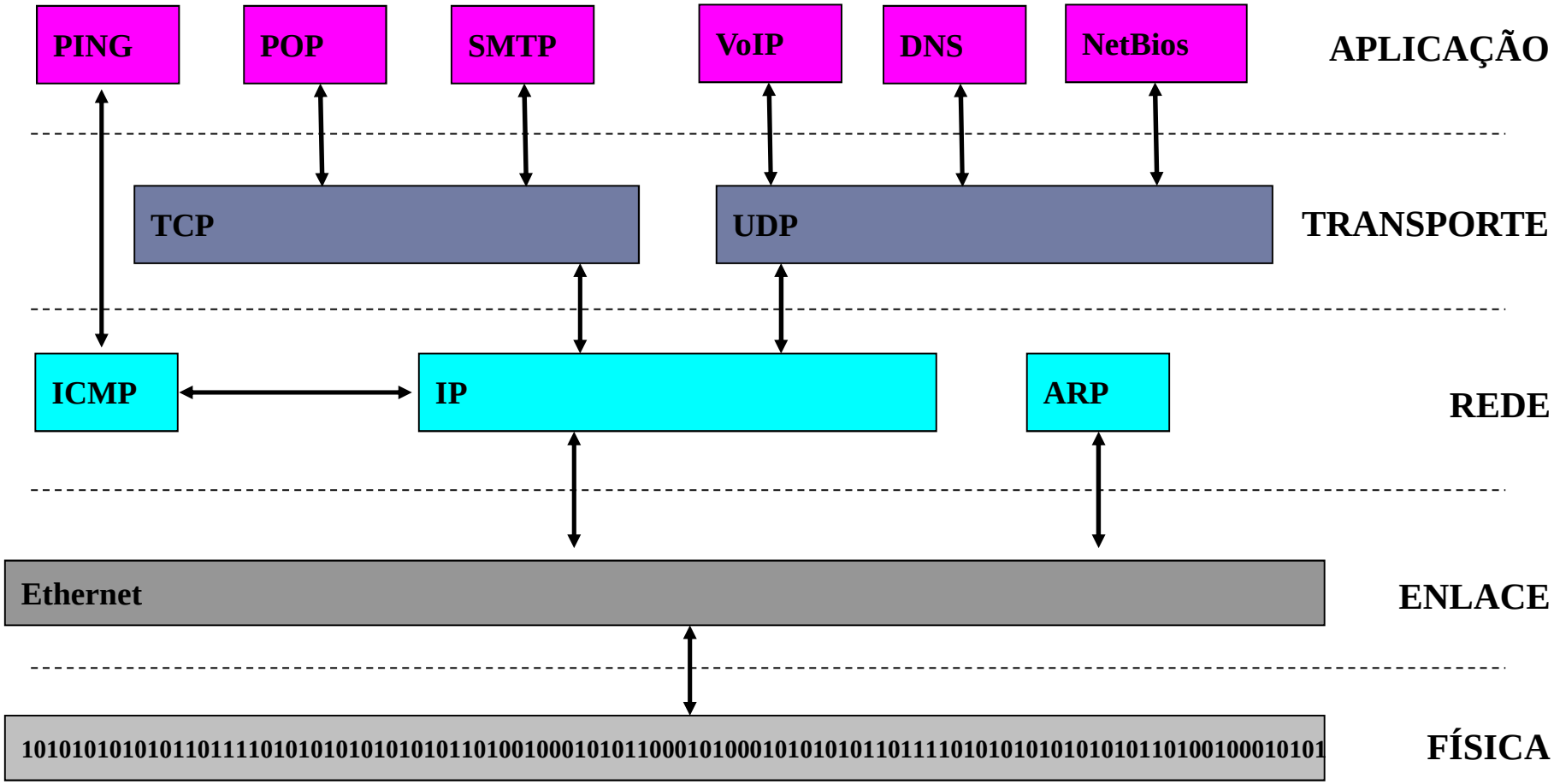
LUIS CLAUDIO DOS SANTOS

Versão 2.0 – 01/02/2012

Roteiro

- * Ethernet (não faz parte da pilha TCP/IP)
- ARP/RARP
- IP
- ICMP
- TCP/UDP

A Pilha TCP/IP



Ethernet

Ethernet

Padrão pela **Xerox** (*R. Metcalfe*) no início da década de 70.

A primeira versão padronizada do *Ethernet* pertencia ao consórcio ***Digital***, ***Intel*** e ***Xerox*** (*DIX Ethernet)*.

Em 1985 *Institute of Electrical and Electronics Engineers* entregou à comunidade um padrão aberto: ***IEEE 802.3***.

No início, o *Ethernet* sofreu concorrência de padrões para rede local: o **IEEE 802.4** (da GM) e o **IEEE 802.5** (da IBM).

Ethernet

DIX Ethernet

PRE (8)	END DEST (6)	END ORIG (6)	TYPE (2)	DATA (de 46 a 1500)	CRC (4)

IEEE 802.3

PRE (7)		END DEST (6)	END ORIG (6)	COMP (2)	DATA (de 46 a 1500)	CRC (4)

sof

Um quadro Ethernet tem entre **46** e **1500** bytes de dados.

Ethernet

DIX Ethernet

PRE (8)	END DEST (6)	END ORIG (6)	TYPE (2)	DATA (de 46 a 1500)	CRC (4)

IEEE 802.3

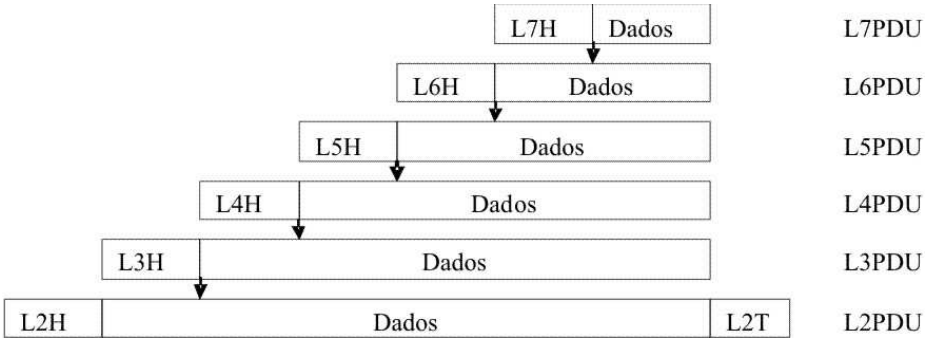
PRE (7)		END DEST (6)	END ORIG (6)	COMP (2)	DATA (de 46 a 1500)	CRC (4)

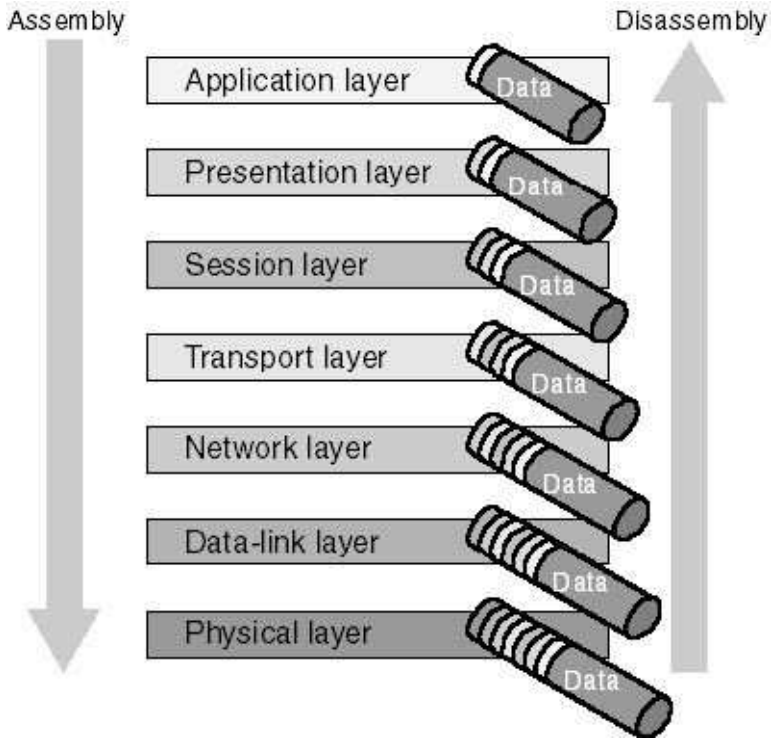
sof

No 802.3, **Comp** indica o tamanho do campo de dados (< 1500).

No Ethernet, **Type** indica que protocolo superior (0x0800 para IP; 0x0806 para ARP; 0x86dd para IPv6; etc.).

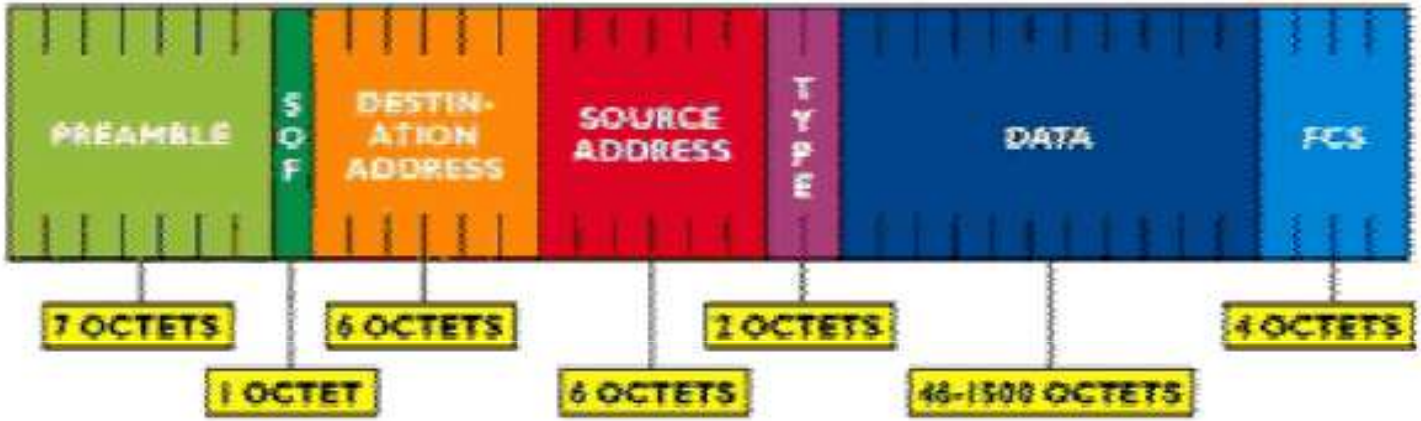
Ethernet


L7H
Dados
L7PDU
L6H
Dados
L6PDU
L5H
Dados
L5PDU
L4H
Dados
L4PDU
L3H
Dados
L3PDU
L2H
Dados
L2T
L2PDU


Assembly
Disassembly
Application layer
Data
Presentation layer
Data
Session layer
Data
Transport layer
Data
Network layer
Data
Data-link layer
Data
Physical layer
Data

Ethernet

IEEE 802.3



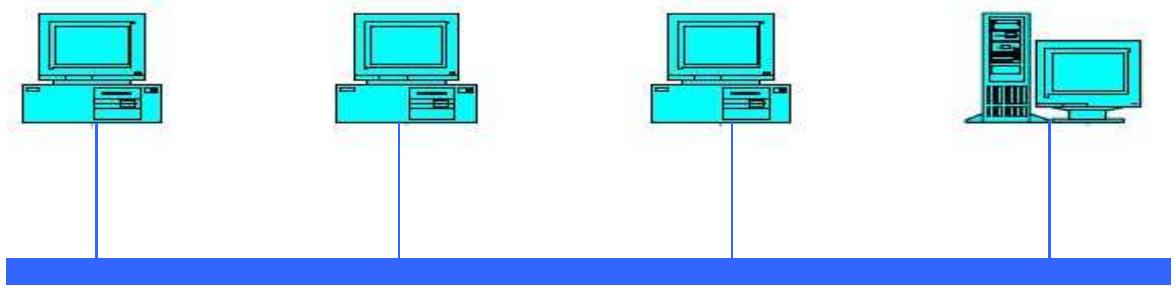
END DEST e END ORIG são os **endereços físicos** (*Media Access Control*) normalmente representados na forma HEXADECIMAL.

00 E0 7D 99 65 3D

Organizationally Unique Identifiers (OUIs)

Ethernet

As primeiras redes *Ethernet* ofereciam ambientes onde havia apenas **um domínio de colisão no meio**.



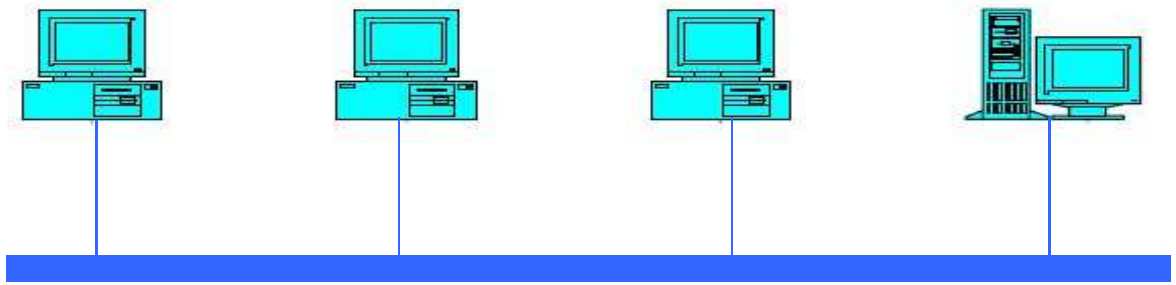
Em ambientes de **difusão**, o método de arbitragem utilizado pelo *Ethernet* era o CSMA/CD (*Carrier Sense Multiple Access/Colision Detection*).

Nestes ambientes, a distância máxima de cada segmento é dada por:

Tx = Tiv=> 46 bytes / 10Mbps = 2d / (300.000 Km/s)

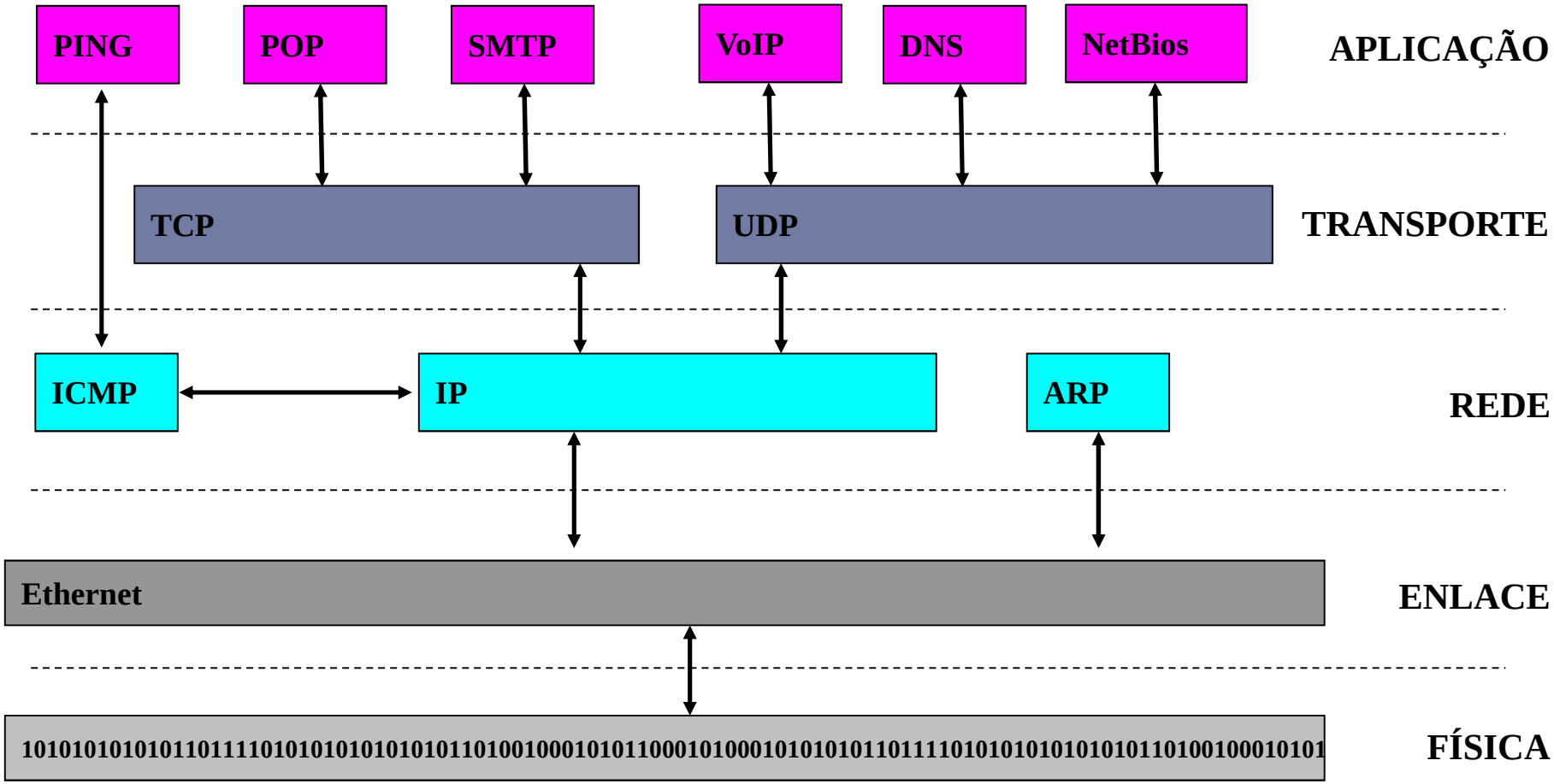
Ethernet

CSMA/CD



Hoje em dia o CSMA/CD **não é** muito utilizado nas redes cabeadas, pois os equipamentos de interconexão geralmente oferecem um domínio de colisão por porta.

A Pilha TCP/IP



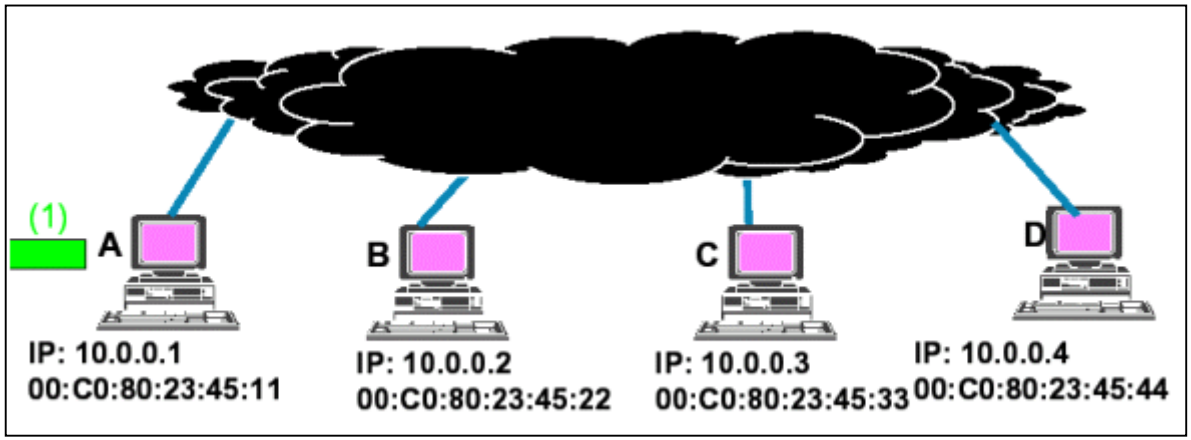
ARP (Address Resolution Protocol)

Arp

- O protocolo ARP é usado para descobrir o endereço MAC de um sistema cujo endereço IP já conhecemos.
- RCF 826.

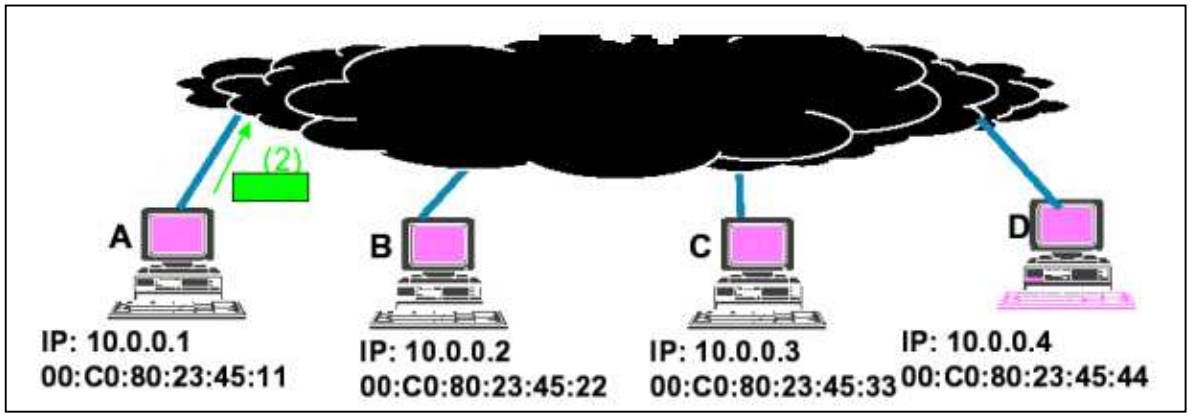
Arp Funcionamento

- 1. A máquina “A” precisa transmitir para o endereço IP 10.0.0.4. Porém, “A” não conhece o endereço MAC do endereço da máquina destino 10.0.0.4.



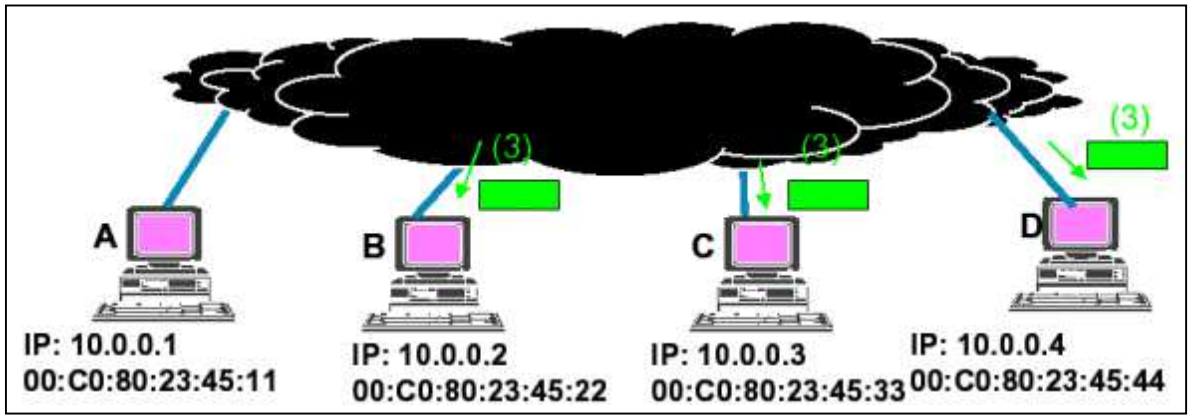
Arp Funcionamento

- 2. O computador "A" precisa descobrir o endereço MAC da interface que está configurada com o endereço IP 10.0.0.4. Para isto, envia um pacote MAC para "broadcast" contendo a seguinte mensagem ARP request: "Quem possuir o endereço MAC associado ao endereço IP 10.0.0.4 enviar a resposta para "00:C0:80:23: 45:11" .



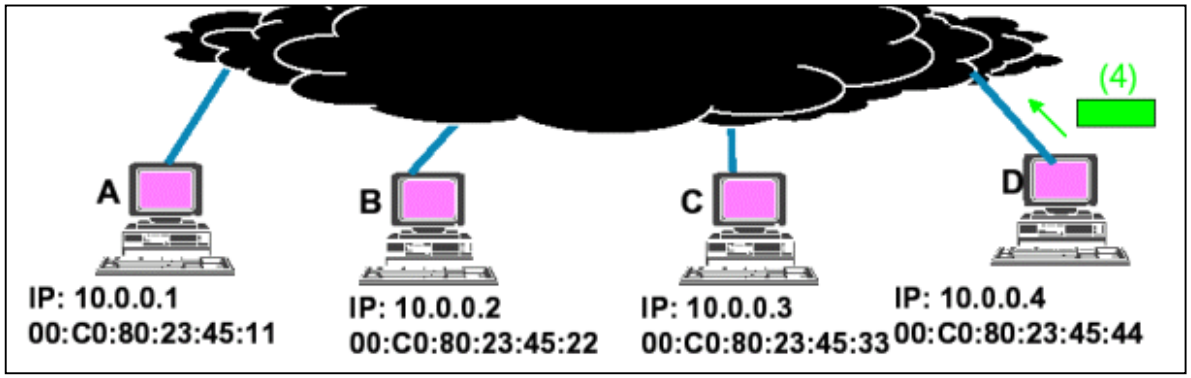
Arp Funcionamento

- 3. O pacote MAC envidado por A irá para todas as máquinas da rede local.



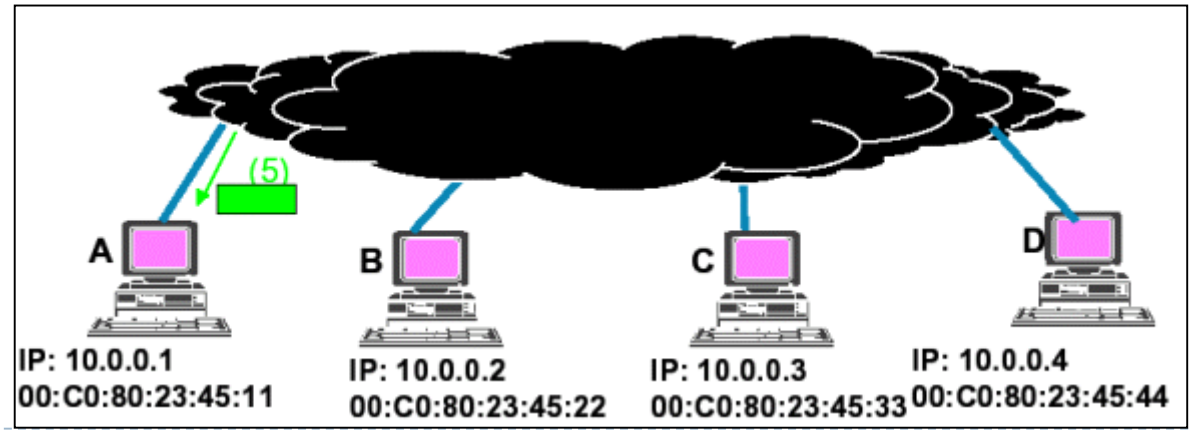
Arp Funcionamento

- 4. O computador "D" ao receber este pacote percebe que alguém está requisitando o endereço MAC associado à interface que está configurada com o endereço IP "10.0.0.4". O computador "D" envia um pacote MAC para 00:C0:80:23:45:11 contendo o seguinte pacote "ARP reply": "O endereço Ethernet associado ao endereço IP 10.0.0.4 é 00:C0:80:23:45:44".



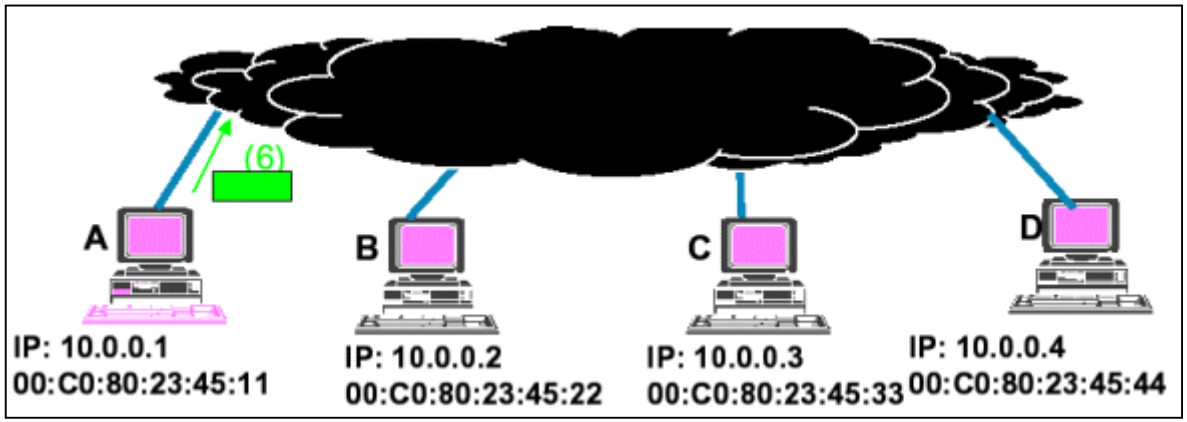
Arp Funcionamento

- 5. O computador “A” recebe o pacote “ARP reply” e descobre que o endereço Ethernet associado ao endereço IP 10.0.0.4 é “00:C0:80:23:45:44”.



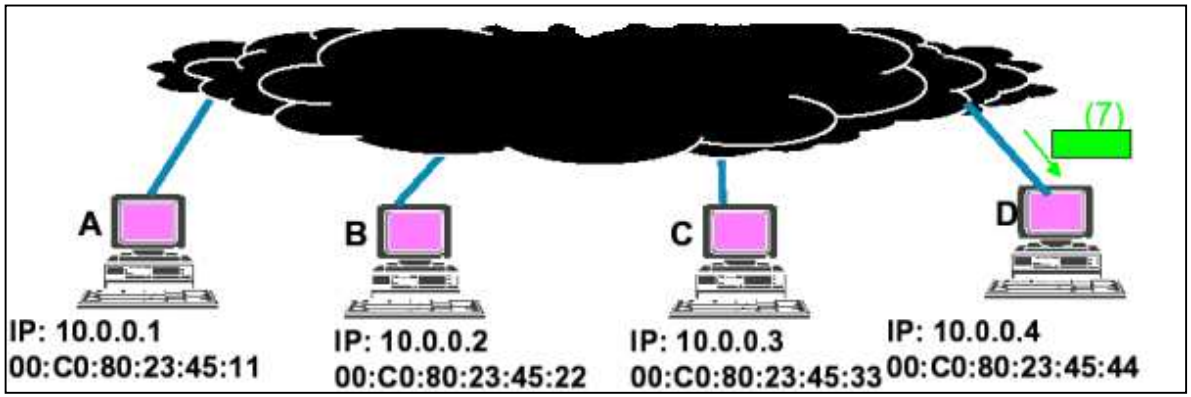
Arp Funcionamento

- 6. O computador "A" envia um pacote Ethernet com endereço Ethernet destino "00:C0:80:23:45:44" contendo o pacote IP.



Arp Funcionamento

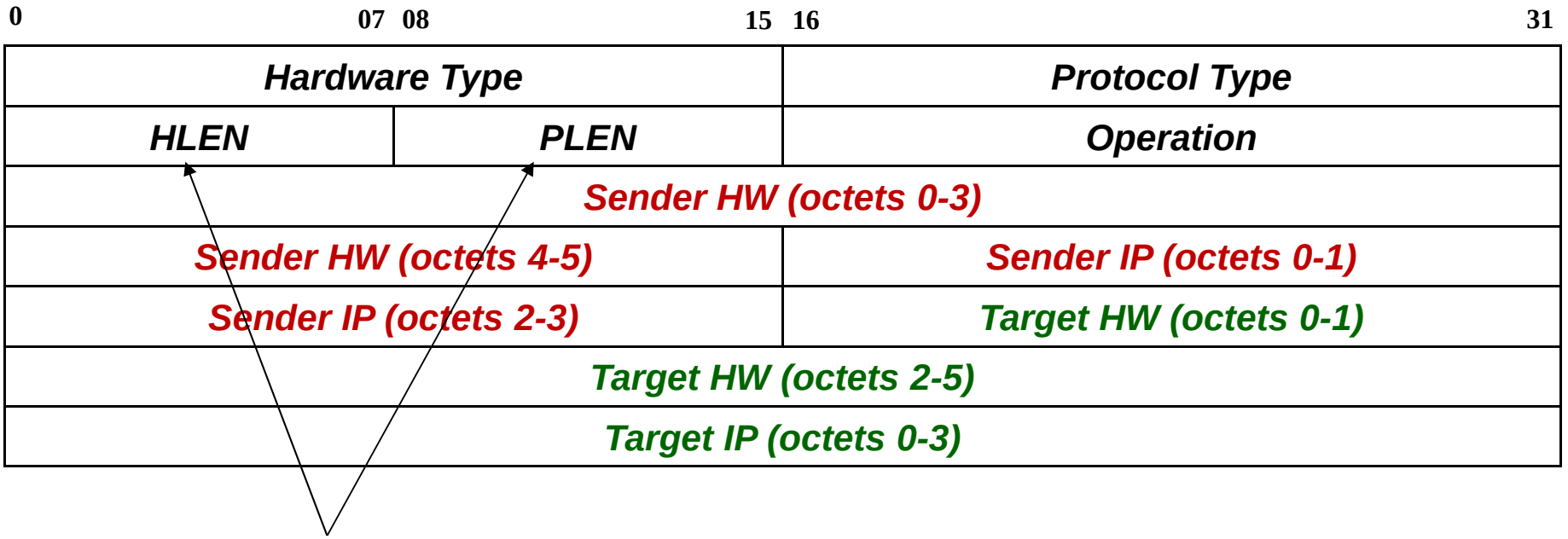
- 7. O computador "D" recebe o pacote MAC enviado por A. Após o recebimento do pacote, é retirado o conteúdo transportado: um pacote IP.



Formato do cabeçalho ARP

Tamanho	Função
2 bytes	Espaço de endereçamento físico.
2 bytes	Espaço de endereçamento do lógico.
1 byte	Comprimento do endereço físico (n).
1 byte	Comprimento do endereço lógico (m).
2 bytes	Código da operação
N bytes	Endereço físico de origem.
M bytes	Endereço físico de destino.
N bytes	Endereço lógico de origem.
M bytes	Endereço lógico de destino.

Formato do cabeçalho ARP



O ARP não possui um cabeçalho de tamanho fixo.
O ARP pode ser otimizado utilizando *caches*, *timers,* etc.
No ARP request, qual campo segue não preenchido?

Utilitário arp

Utilitário arp:

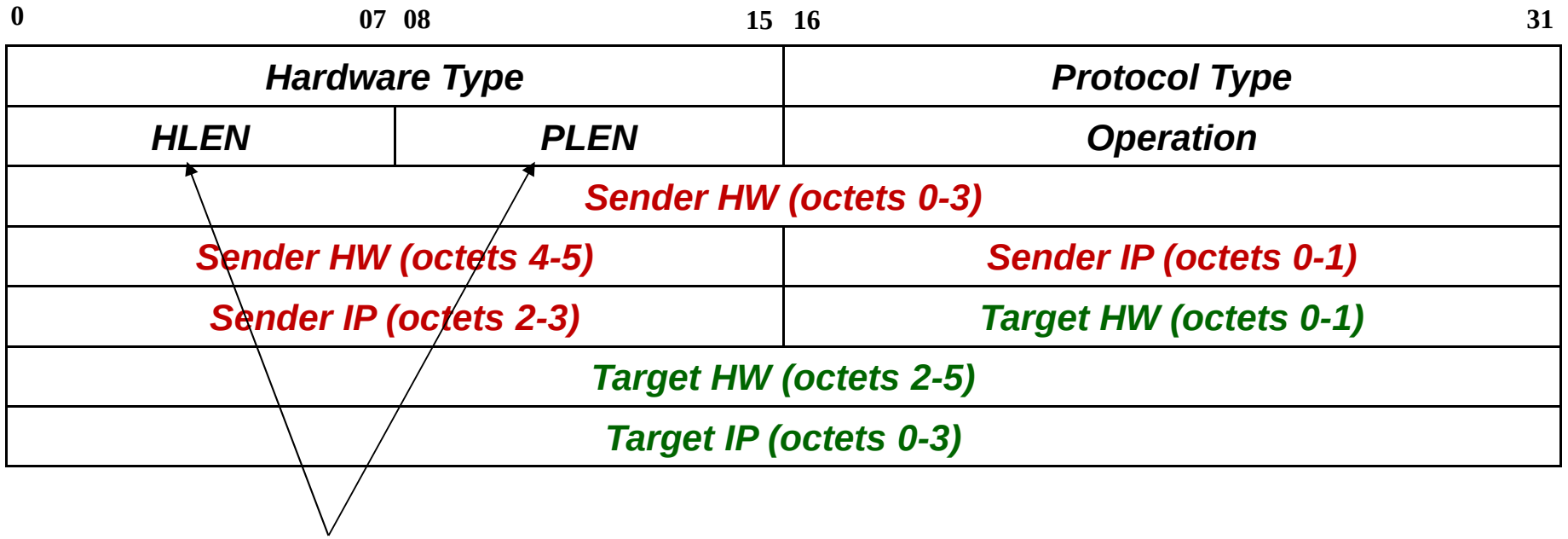
- -a: mostra a tabela ARP corrente.
- -a host: mostra somente a tradução de "host".
- -n: não resolve endereços DNS.
- -i: interface seleciona interface.
- -s host MAC: adiciona uma entrada permanente à tabela.
- -d host delete: remove entrada.
- -f: zera a tabela ARP.

Protocolo RARP (Reverse ARP)

Protocolo RARP

- Quando a máquina não possui um disco para inicialização do sistema (estação diskless) para carregar o seu endereço IP, a imagem de memória daquela estação fica armazenada no servidor.
- Cada máquina com uma placa de rede possui uma identificação única e que não se repete. Esta identificação é uma seqüência de bits, gravado no chip da placa, que é utilizada como endereço físico na rede (MAC address). A estação diskless utiliza um protocolo que permite a obtenção do endereço IP fazendo uso do endereço físico da placa. Este protocolo é o RARP.

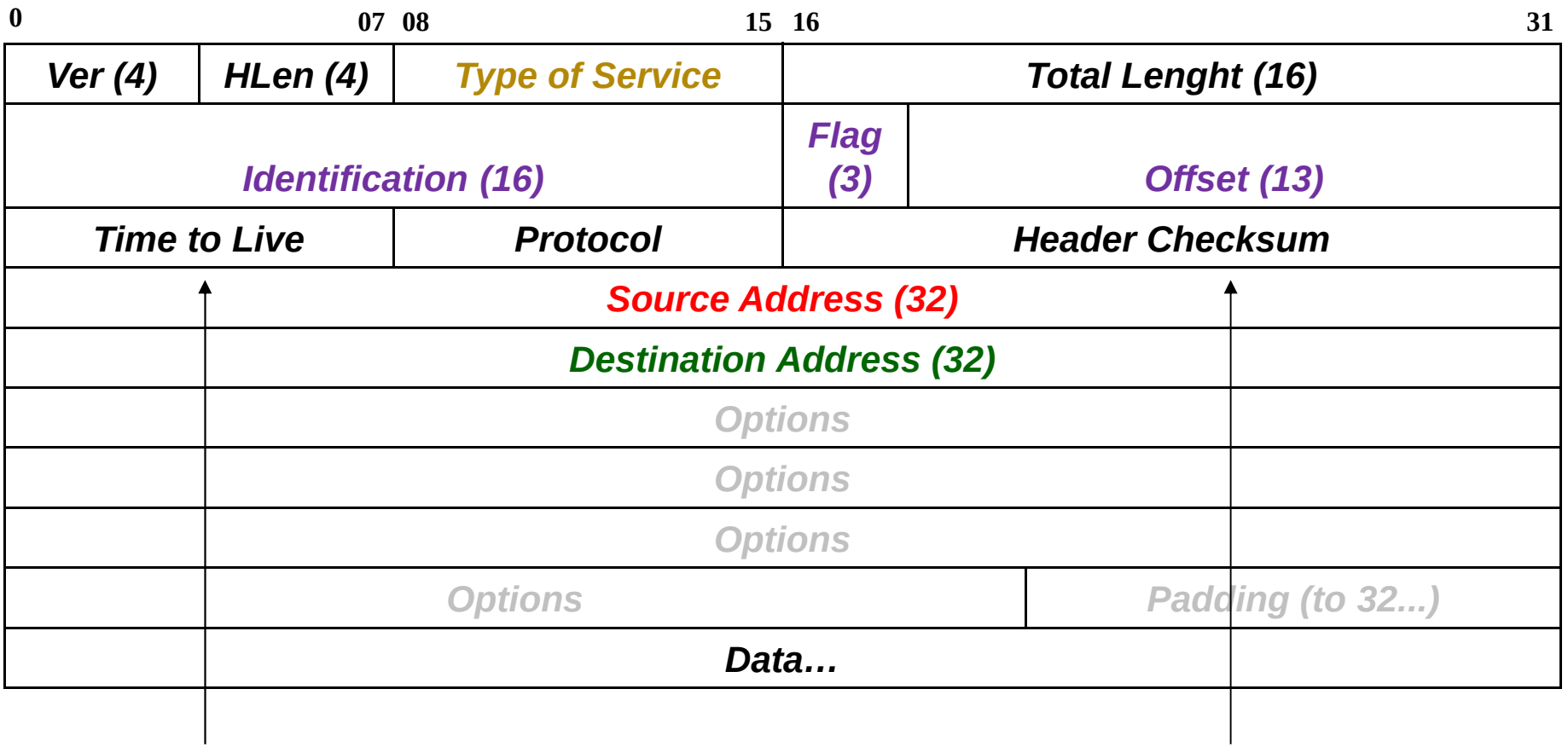
Formato do cabeçalho ARP



O ARP não possui um cabeçalho de tamanho fixo.
O ARP pode ser otimizado utilizando *caches*, *timers,* etc.
No ARP request, qual campo segue não preenchido?

Protocolo IP (Internet Protocol)

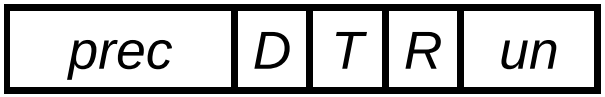
IP (RFC 791) - Cabeçalho



IP (RFC 791) - Cabeçalho

Campo *Type of Service*.

BIT	Significado
Precedence (3)	Precedência do serviço entre 0 (normal) e 7 (controle).
D (1)	Retardo (***D****elay*).
T (1)	Vazão (***T****hrougput*).
R (1)	Confiabilidade (***R****eliability*).
unused (2)	Bits não usados.



Campos prec, D, T e R viraram o Differentiated Services CodePoint.

IP (RFC 791) - Cabeçalho

Identification (16)	***Flag (3)***	***Offset (13)***

Os campos ***Identification***, ***Flags*** e ***Offset***, do cabeçalho IP são utilizados para fragmentação de datagramas.

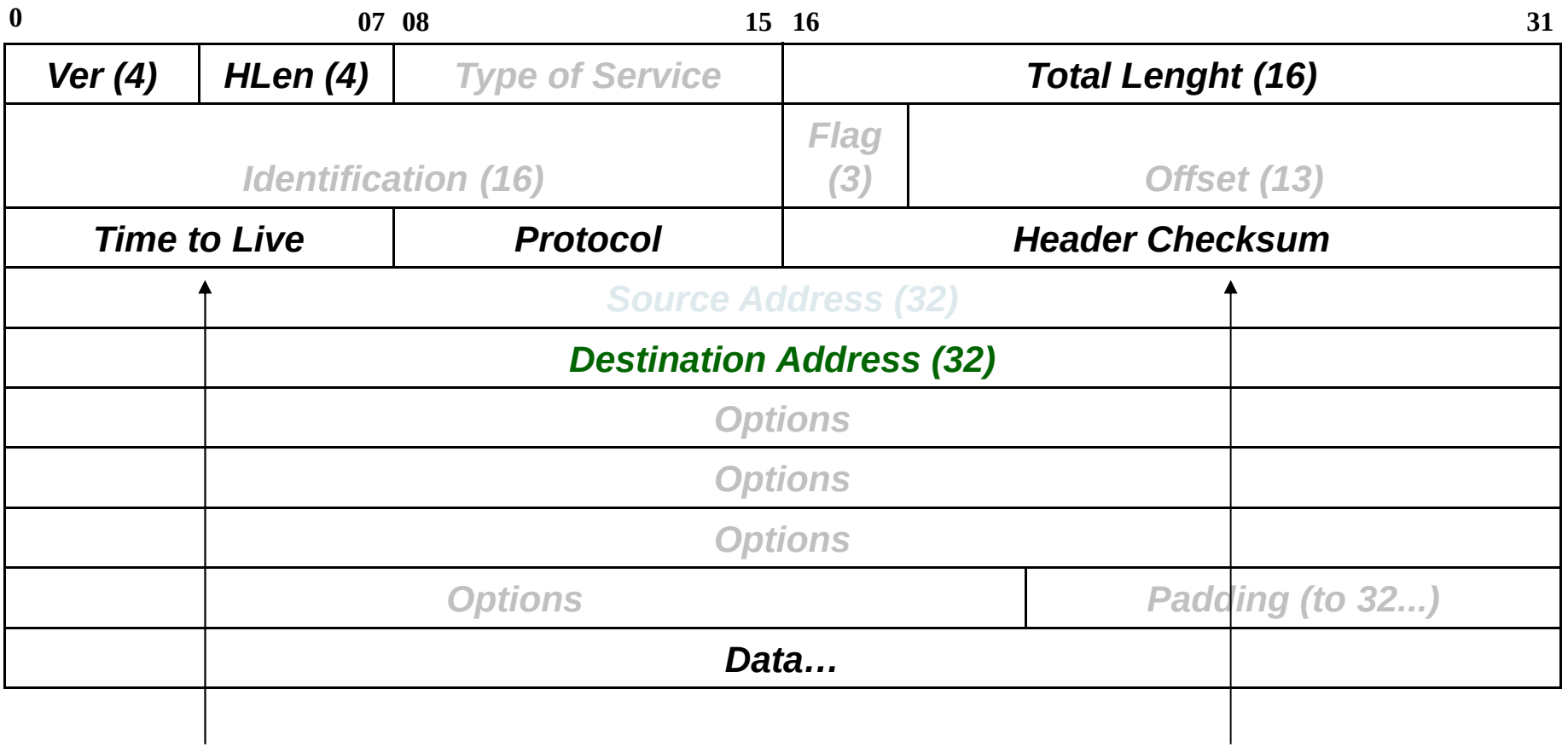
Uma vez fragmentado, a junção dos diversos pacotes ocorrerá apenas no *host* de destino.

IP (RFC 791) - Cabeçalho

Campo *Options*

Opção	Significado
Strict Source Routing	Mostra o caminho completo a ser seguido (roteador a roteador).
Loose Source Routing	Mostra alguns roteadores por onde o datagrama deve passar. Pode haver intermediários, mas sem alterar a sequência.
Record Route	Cada roteador que trata o datagrama acrescenta o seu endereço IP ao cabeçalho (*options*).
Timestamp	Cada roteador que trata o datagrama acrescenta, além do seu endereço IP, o seu timbre de hora.

IP (RFC 791) - Cabeçalho



Time to Live!

Só do cabeçalho!

IP (RFC 791) - Endereços

Cada endereço IP é composto por 4 octetos.

10011011	10110101	10110001	00111011

Geralmente o endereço IP é escrito como um conjunto de 04 números decimais separados por um "ponto".

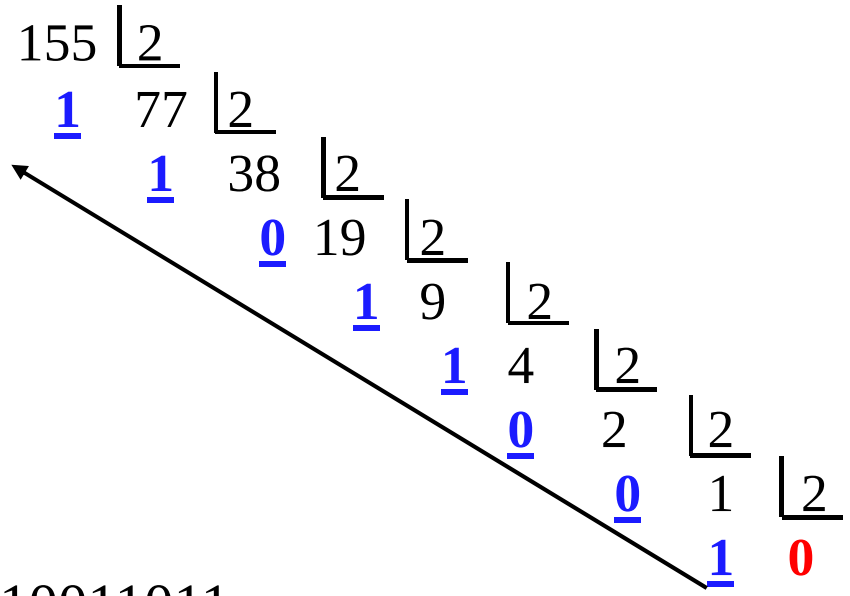
10011011	10110101	10110001	00111011
155	**181**	**177**	**59**

IP = 155.181.177.59

O endereço lógico, acompanhado da máscara, fornece duas informações: o endereço da rede e o endereço do host.

IP (RFC 791) - Endereços

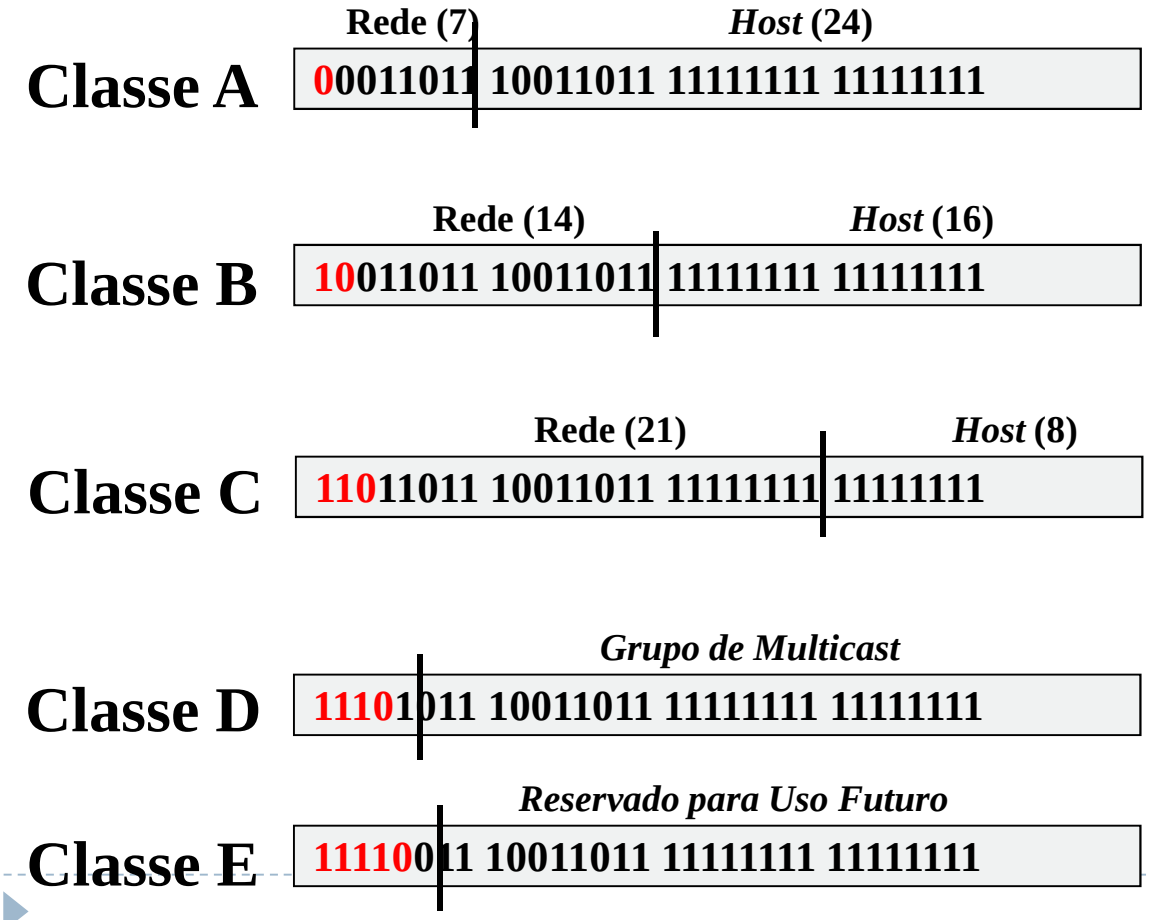
Conversão decimal-binário: Dividir por ***dois*** o número decimal sucessivas vezes até que o resto seja ***zero***. O número, em formato binário, será a seqüência - de baixo para cima - de todos os restos (***zeros*** ou ***uns***) obtidos.



Ou seja, $155 = 10011011_2$

IP (RFC 791) - Endereços

Os endereços IPv4 são divididos em 05 classes:



IP – Redes e Endereços Válidos

Intervalo de Redes

CLASSE	INTERVALO
A	1.0.0.0 a 127.0.0.0
B	128.0.0.0 a 191.255.0.0
C	192.0.0.0 a 223.255.255.0

Intervalo de Endereços

CLASSE	INTERVALO
A	1.0.0.0 a 127.255.255.255
B	128.0.0.0 a 191.255.255.255
C	192.0.0.0 a 223.255.255.255

IP – Redes e Endereços Válidos

Intervalo de Endereços

CLASSE	INTERVALO
A	1.0.0.0 a 127.255.255.255
B	128.0.0.0 a 191.255.255.255
C	192.0.0.0 a 223.255.255.255

Algumas das excesões:

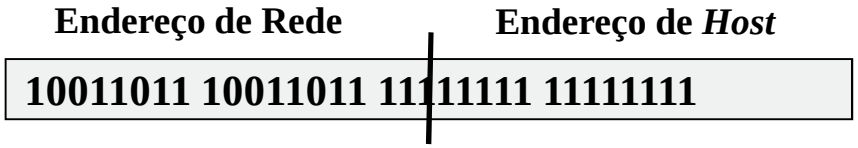
127.*.*.*	Usados para *loopback*;
10.*.*.*	Inválido (usado em redes privadas);
172.16.*.* a 172.31.*.*	Idem;
192.168.*.*	Idem;

IP – Redes e Endereços Válidos

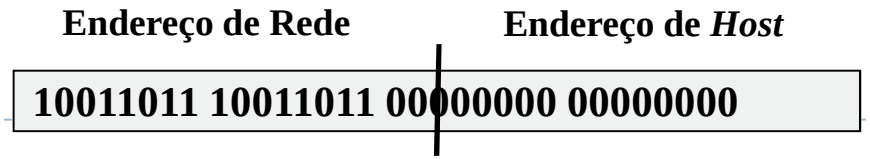
Intervalo de Endereços

CLASSE	INTERVALO
A	1.0.0.0 a 127.255.255.255
B	128.0.0.0 a 191.255.255.255
C	192.0.0.0 a 223.255.255.255

HostID "1...1" identifica *broadcast*.



HostID "0...0" identifica a rede.



Protocolo ICMP (Internet Control Message Protocol)

Protocolo ICMP

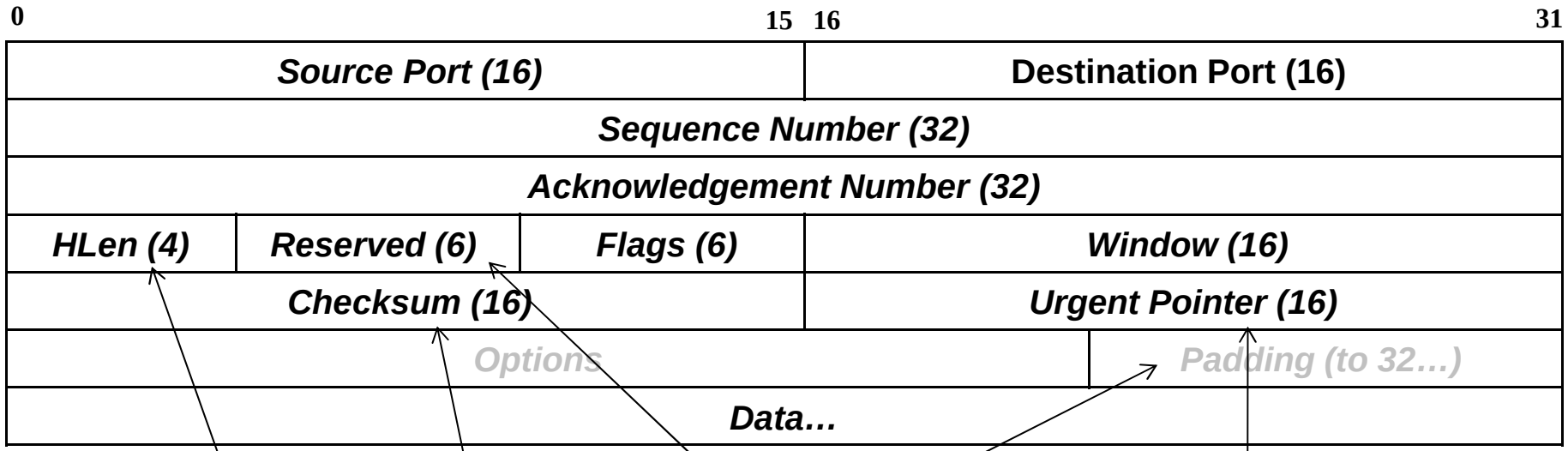
- Avisa aos participantes da rede quando determinada atitude foi ou vai ser tomada.
- Definido na RCF 1885 e RFC 1970.
- Utilizado em várias aplicações, como o **ping**, o **tracert** (ou traceroute).

Camada 4
TCP

TCP

- O TCP é um protocolo que possui diversas características implementadas a partir da interpretação, pelas máquinas, dos campos de seu cabeçalho. O TCP:
  - É orientado a conexão;
  - É confiável;
  - Garante a entrega em sequência;
  - Possui controle de fluxo;
  - Implementa multiplexação (portas);
  - É interpretado fim-a-fim.

TCP - Cabeçalho



Em palavras de 32 bits.

Tanto dos cabeçalho quanto dos daos.

Sempre igual a 0.

So é válido se URG = 1.
Indica o *offset*, em bytes, contando do campo *Seq. Number* atual, onde os dados urgentes terminam.

TCP - Cabeçalho

- Porta de origem: indica a aplicação que está enviando o segmento;
- Porta de destino: indica a aplicação que irá receber o segmento;
- Número de seqüência: identifica a ordem de cada segmento dentro de uma conexão e garante a entrega na seqüência correta para a aplicação.
- Número de confirmação: próximo octeto TCP esperado.
- HLEN: número de palavras de 32 bits no cabeçalho.
- Reservado: definido como zero.
- Flags: várias funções de controle (sincronização, etc).
- Window: número de octetos que podem ser enviados pela origem antes de receber a primeira confirmação do destino (ACK);
- Checksum: calculado do cabeçalho e dos campos de dados.
- Indicador de urgência: indica o final dos dados urgentes.
- Opções: tamanho máximo do segmento TCP.
- Dados: dados do protocolo da camada superior.

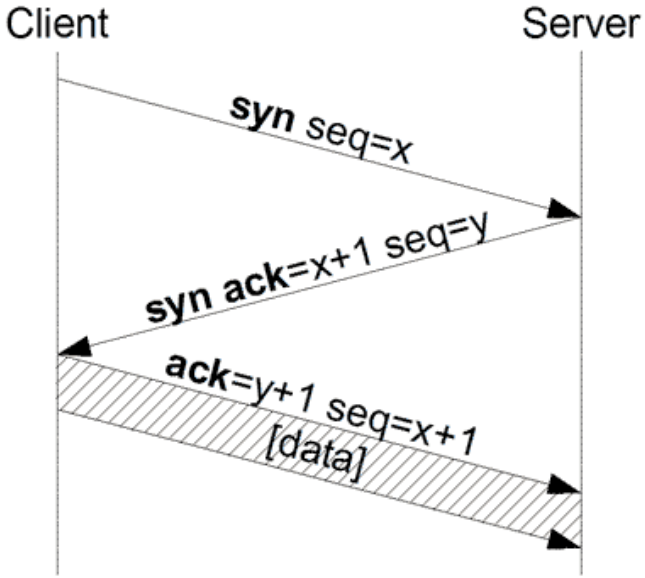
TCP – Cabeçalho (flags)

Campo *flags* do cabeçalho TCP:

BIT (esq p/ dir)	Significado
URG	Existência de dados urgentes (até *Urgent Pointer*).
ACK	*Acknowledgement* é válido.
PSH	Envia os dados o quanto antes à camada IP (*push)*.
RST	Finaliza (ou rejeita...) a conexão **abruptamente** (*reset*).
SYN	Sincroniza os *sequence numbers*.
FIN	Fecha a conexão **normalmente** (nível de aplicação).

TCP – Handshake (flags, ack, syn)

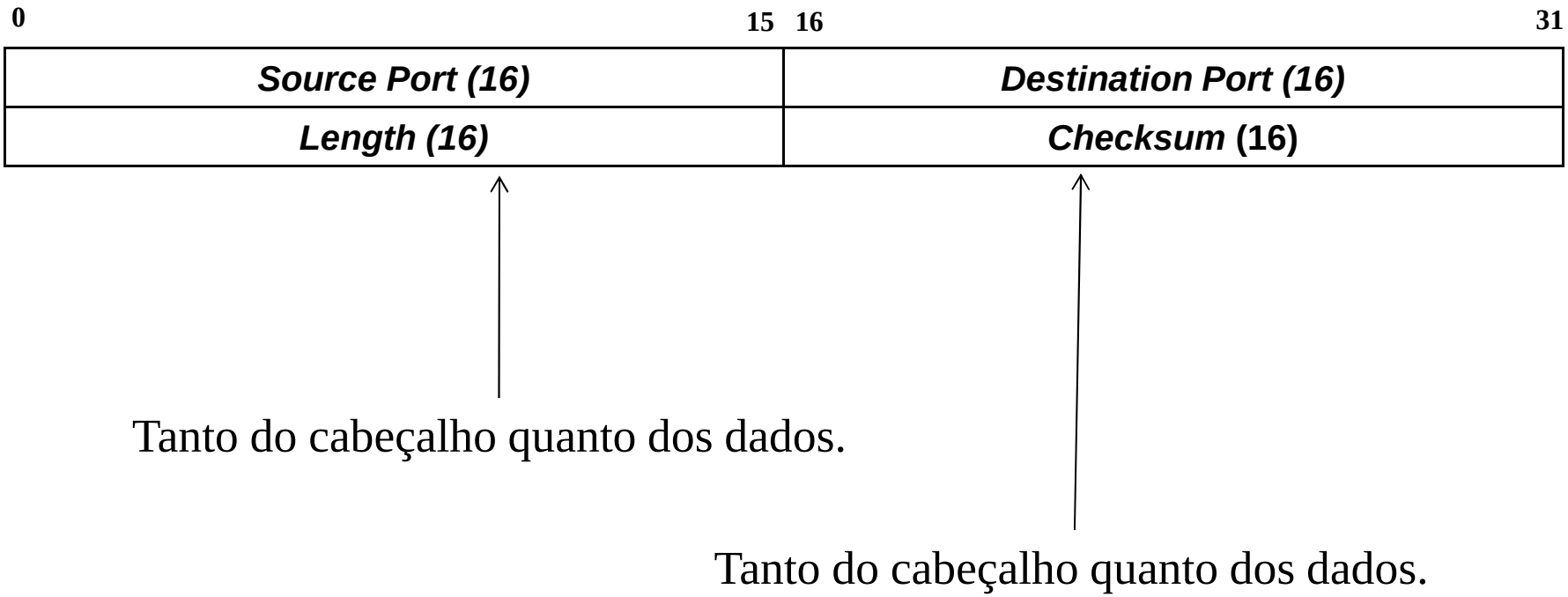
- Para que uma conexão seja estabelecida, as duas estações terminais devem sincronizar os números de seqüência TCP iniciais uma à outra. A seqüência de conexão é usada para recuperar dados perdidos. A *sincronização* é feita através da troca de segmentos que transportam os ISNs e um bit de controle chamada *SYN*. A sincronização exige que cada lado envie seu ISN e receba uma confirmação(ACK) e o ISN do outro lado da conexão.
- Um handshake triplo é necessário porque os TCPs podem usar diferentes mecanismos para o ISN.



TCP – Janelamento (window, ack)

- Para **controlar o fluxo de dados** entre os dispositivos, a camada TCP do host de recebimento relata um tamanho de janela ao host de envio.
- O tamanho da janela refere-se ao número de bytes que podem ser transmitidos em sequência antes que seja recebida uma confirmação.
- O tamanho da janela determina quantos dados a estação receptora pode aceitar de uma só vez.
- A finalidade do janelamento é aperfeiçoar o controle de fluxo e a confiabilidade.

UDP – Cabeçalho



UDP não faz nenhum contato com o destino antes de enviar informações.
Length é o tamanho do segmento (cabeçalho + dados).
Checksum é o cálculo para todo o segmento (cabeçalho + dados).

UDP

- O UDP é um protocolo que não implementa a maior parte das funcionalidades possíveis da camada de transporte.
  - Não é orientado a conexão;
  - Não é confiável;
  - Não garante a entrega em sequência;
  - Não possui controle de fluxo;
  - Implementa multiplexação (portas);
  - É interpretado fim-a-fim.

Portas (TCP e UDP)

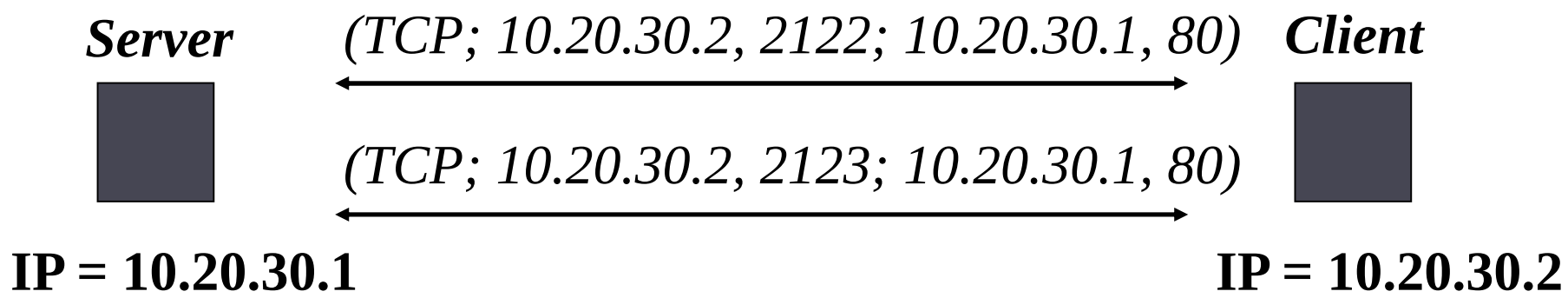
- Tanto o TCP quanto o UDP usam números de *porta* para identificar a aplicação que deverá receber os dados na camada superior.
- Os números de porta estão definidos no RFC1700.
- Esses números de portas são usados como endereços de origem e destino no segmento TCP.
- Os números de portas têm os seguintes conjuntos atribuídos:
  - Números abaixo de 255 - para aplicações públicas .
  - Números de 255 a 1023 - atribuídos às empresas para aplicações comerciais.
  - Números acima de 1023 - não são regulamentados.

Portas (TCP e UDP)

- Os sistemas terminais usam números de portas para selecionar os aplicativos corretos. Os números de porta de origem, normalmente alguns números maiores que 1023, são dinamicamente atribuídos pelo host de origem.

A conexão TCP

Conexão: A porta e o IP de um lado da conexão determina um socket; as mesmas informações do outro lado (porta e IP), determinam outro socket. A conexão é definida por ambos.



Sessão: A sessão é formada pelo fluxo de todos os segmentos numerados de uma conexão. Note que, no caso do TCP, cada segmento carrega um número de sequência.