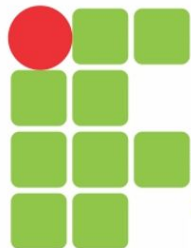


# REDES DE COMPUTADORES

## MÓDULO 2

### ENDEREÇAMENTO IP, PROTOCOLOS E CONFIGURAÇÕES BÁSICAS



INSTITUTO FEDERAL DE  
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA  
RIO GRANDE DO NORTE

✉ [rafael.moraes@ifrn.edu.br](mailto:rafael.moraes@ifrn.edu.br)

# Índice deste Módulo

- [1] Noções Básicas sobre o IPv4
- [2] Estrutura e Classes do IPv4
- [3] Cálculos de Endereçamento IPv4 (com classe)
- [4] Cálculos de Endereçamento IPv4 (sem classe)
- [5] Endereços IPv4 Especiais
- [6] Camada de Transporte, Portas & Sockets
- [7] Protocolo TCP
- [8] Protocolo UDP
- [9] Endereçamentos Públicos e Privados
- [10] Fundamentos IPv6

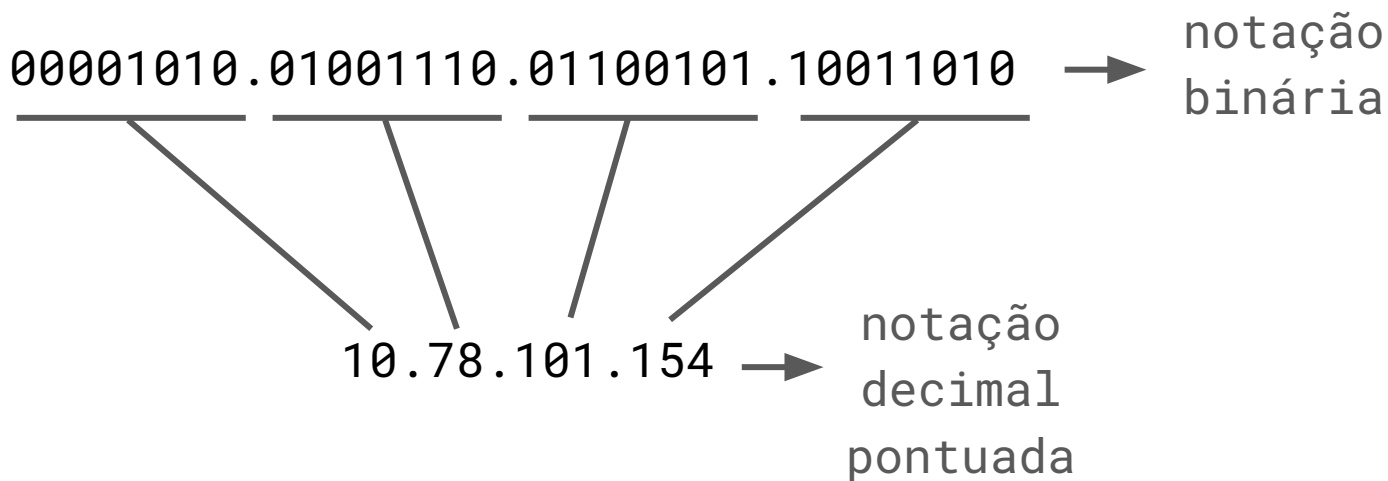
# [1] Noções Básicas sobre o IPv4

# Tipos de Endereços

<b>L4</b>	Transporte	segmentos	Porta (16-bits)	-
<b>L3</b>	Redes	pacotes	IP (32-bits)	Lógico
<b>L2</b>	Enlace	frames	MAC (48-bits)	Físico
<b>L1</b>	Física	bits	-	-

# Endereço IPv4

O endereço IPv4 (Internet Protocol version 4) é um identificador numérico (**obrigatório**) usado para localizar dispositivos conectados a uma rede baseada no protocolo IP, como a internet. Ele funciona como um "endereço" (**32-bits**) que permite a comunicação entre dispositivos na rede.





Rafael Moraes

Find a setting



Home



System



Bluetooth &amp; devices



Network &amp; internet



Personalization



Apps



Accounts



Time &amp; language



Gaming



Accessibility



Privacy &amp; security



Windows Update

## Network &amp; internet &gt; Wi-Fi &gt; wIFRN-Corp

IP assignment:	Automatic (DHCP)	Edit
----------------	------------------	------

DNS server assignment:	Automatic (DHCP)	Edit
------------------------	------------------	------

SSID:	wIFRN-Corp	Copy
-------	------------	------

Protocol:	Wi-Fi 5 (802.11ac)
-----------	--------------------

Security type:	WPA2-Enterprise
----------------	-----------------

Manufacturer:	Realtek Semiconductor Corp.
---------------	-----------------------------

Description:	TP-Link Wireless Nano USB Adapter
--------------	-----------------------------------

Driver version:	1030.44.1014.2024
-----------------	-------------------

Type of sign-in info:	Microsoft: Protected EAP (PEAP)
-----------------------	---------------------------------

Network band (channel):	5 GHz (108)
-------------------------	-------------

Aggregated link speed (Receive/ Transmit):	195/195 (Mbps)
---	----------------

Link-local IPv6 address:	fe80::4473:a3d3:13a0:1ee8%13
--------------------------	------------------------------

IPv4 address:	10.195.1.27
---------------	-------------

IPv4 default gateway:	10.195.0.1
-----------------------	------------

IPv4 DNS servers:	10.198.0.100 (Unencrypted) 10.22.0.12 (Unencrypted)
-------------------	--

Primary DNS suffix:	ifrn.local
---------------------	------------

Physical address (MAC):	24-2F-D0-FA-51-9B
-------------------------	-------------------

Advanced Wi-Fi network properties

Edit

# Limitações do IPv4

O IPv4 permite cerca de 4,3 bilhões de endereços únicos, o que se mostrou insuficiente devido ao crescimento exponencial de dispositivos conectados.

Para resolver esse problema, o protocolo IPv6 foi criado, permitindo um número muito maior de endereços (128 bits).

# Convertendo números em binário

- Os bits mais significativos ficam à esquerda, assim como nos decimais.
- Começar subtraindo a maior potência possível do número desejado.
- Se houve subtração, registre o bit 1, do contrário, registre o bit 0.

QUAL O NÚMERO DECIMAL A SER CONVERTIDO?

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1



# Conversão decimal-binário

Endereço IPv4 45.198.172.4

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

00101101 . 11000110 . 10101100 . 00000100

## Conversão decimal-binário

Endereço IPv4 200.19.132.57

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

11001000.00010011.10000100.00111001

# Conversão binário-decimal

Endereço IPv4 01011001.00000000.10111001.11100001

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

89 . 0 . 185 . 225

# Conversão binário-decimal

Endereço IPv4 01101011.01000101.11101011.01000001

2 <sup>7</sup>	2 <sup>6</sup>	2 <sup>5</sup>	2 <sup>4</sup>	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2 <sup>0</sup>
128	64	32	16	8	4	2	1

107.69.235.65

# Exercícios de Fixação 01

I. Convertam para o formato binário os endereços abaixo:

1. 18.200.17.3 =

2. 202.198.223.4 =

3. 10.11.29.13 =

II. Convertam para o formato decimal pontuado os endereços abaixo:

1. 01000010.11011100.00000001.11100011 =

2. 00000010.00011100.01100001.11100011 =

3. 01001010.11111100.00100001.11101101 =

# Exercícios de Fixação 02

III. Convertam para o formato barramento as máscaras abaixo:

1. 11111111.11110000.00000000.00000000 =
2. 11111111.11000000.00000000.00000000 =
3. 11111111.11111111.11110000.00000000 =
4. 11111111.11111111.11111100.00000000 =
5. 11111111.11111111.11111111.11100000 =

IV. Convertam para o formato de barramento as máscaras:

1. 255.128.0.0 =
2. 255.255.128.0 =
3. 255.255.255.192 =
4. 255.224.0.0 =
5. 255.255.240.0 =
6. 255.255.255.252 =

# Exercícios de Fixação 01 ~ solução

I. Convertam para o formato binário os endereços abaixo:

1. 18.200.17.3 = 00010010.11001000.00010001.00000011 (A)
2. 202.198.223.4 = 11001010.11000110.11011111.00000100 (C)
3. 10.11.29.13 = 00001010.00001011.00011101.00001101 (A)

II. Convertam para o formato decimal pontuado os endereços abaixo:

1. 01000010.11011100.00000001.11100011 = 66.220.1.227 (A)
2. 00000010.00011100.01100001.11100011 = 2.28.97.227 (A)
3. 01001010.11111100.00100001.11101101 = 74.252.33.237 (A)

# Exercícios de Fixação 02 ~ solução

III. Convertam para o formato barramento as máscaras abaixo:

1. 11111111.11110000.00000000.00000000 = /12
2. 11111111.11000000.00000000.00000000 = /10
3. 11111111.11111111.11110000.00000000 = /20
4. 11111111.11111111.11111100.00000000 = /22
5. 11111111.11111111.11111111.11100000 = /27

IV. Convertam para o formato de barramento as máscaras:

1. 255.128.0.0 = /9
2. 255.255.128.0 = /17
3. 255.255.255.192 = /26
4. 255.224.0.0 = /11
5. 255.255.240.0 = /20
6. 255.255.255.252 = /30



## [2] Estrutura e Classes do IPv4

# Estrutura do IPv4

O endereço é dividido em duas partes principais:

- **Parte de rede:** Identifica a rede específica.
- **Parte de host:** Identifica dispositivos individuais (hosts) dentro da rede.

A divisão entre essas partes é definida por uma máscara de sub-rede, que determina o número de bits usados para cada uma.



**Quantas possibilidades existem no lançamento de uma moeda no cara ou coroa?**

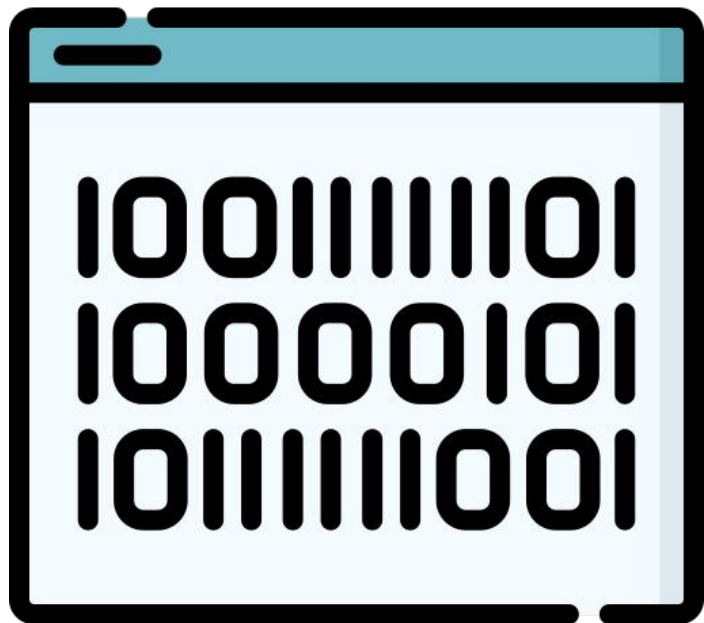
2 possibilidades (C, cara ou K, coroa)

**Quantas possibilidades existem em dois lançamentos da moeda em sequência?**

4 possibilidades (CC, CK, KC, KK)

**Quantas possibilidades existem em três lançamentos da moeda em sequência?**

$2^3 = 8$  possibilidades



**Quantos números podemos escrever com um único bit?**

2 possibilidades (0, zero ou 1, um)

**Quantos números podemos escrever com dois bits?**

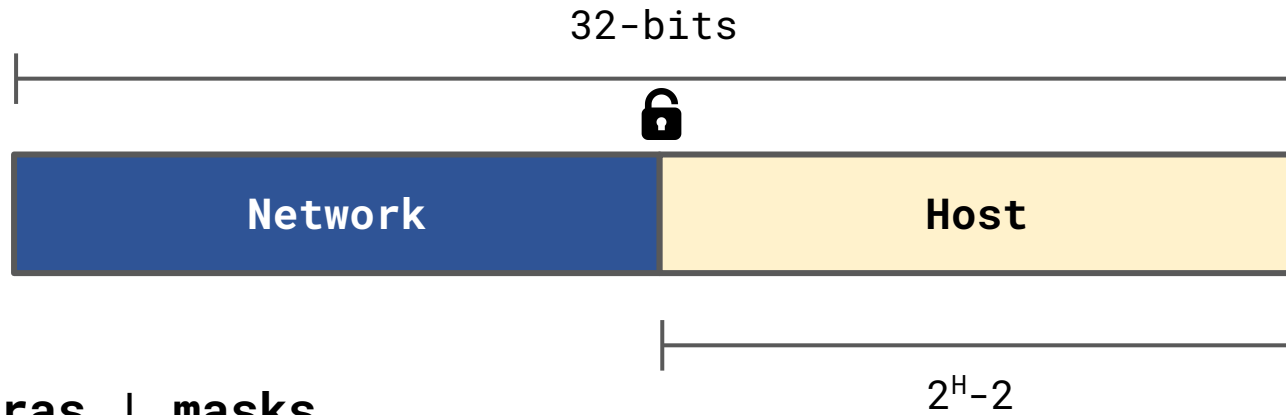
4 possibilidades (00, 01, 10, 11)

**Quantos números podemos escrever com três bits?**

$2^3 = 8$  possibilidades

# Estrutura do IPv4

$$N + H = 32$$



máscaras | masks

255.0.0.0 ou /8

255.255.0.0 ou /16

255.255.255.0 ou /24

0 que são a parte de rede e a parte de host?

**endereço 17.8.17.133 /8**

<b>endereço</b>	<b>17</b>	<b>8</b>	<b>17</b>	<b>133</b>
<b>máscara</b>	<b>255</b>	<b>0</b>	<b>0</b>	<b>0</b>

0 que são a parte de rede e a parte de host?

**endereço 17.8.17.133 /8**

<b>endereço</b>	<b>17</b>	<b>8</b>	<b>17</b>	<b>133</b>
<b>máscara</b>	<b>255</b>	<b>0</b>	<b>0</b>	<b>0</b>
<b>REDE</b>	<b>17</b>	<b>0</b>	<b>0</b>	<b>0</b>

**0 que são a parte de rede e a parte de host?**

**endereço 177.89.1.152 /16**

<b>endereço</b>	<b>177</b>	<b>89</b>	<b>1</b>	<b>152</b>
<b>máscara</b>	<b>255</b>	<b>255</b>	<b>0</b>	<b>0</b>



0 que são a parte de rede e a parte de host?

**endereço 177.89.1.152 /16**

<b>endereço</b>	<b>177</b>	<b>89</b>	<b>1</b>	<b>152</b>
<b>máscara</b>	<b>255</b>	<b>255</b>	<b>0</b>	<b>0</b>
<b>REDE</b>	<b>177</b>	<b>89</b>	<b>0</b>	<b>0</b>

0 que são a parte de rede e a parte de host?

**endereço 198.200.14.17 /24**

<b>endereço</b>	<b>198</b>	<b>200</b>	<b>14</b>	<b>17</b>
<b>máscara</b>	<b>255</b>	<b>255</b>	<b>255</b>	<b>0</b>

0 que são a parte de rede e a parte de host?

**endereço 198.200.14.17 /24**

<b>endereço</b>	<b>198</b>	<b>200</b>	<b>14</b>	<b>17</b>
<b>máscara</b>	<b>255</b>	<b>255</b>	<b>255</b>	<b>0</b>
<b>REDE</b>	<b>198</b>	<b>200</b>	<b>14</b>	<b>0</b>

# Classes de Endereço IPv4

	1º byte	2º byte	3º byte	4º byte
Classe A	1-126			
Classe B	128-191			
Classe C	192-223			
Classe D	224-239			
Classe E	240-255			

Notação Decimal Pontuada

# Classes de Endereço IPv4

	1º byte	2º byte	3º byte	4º byte		1º byte	2º byte	3º byte	4º byte
Classe A	1-126					255	0	0	0
Classe B	128-191					255	255	0	0
Classe C	192-223					255	255	255	0
Classe D	224-239								
Classe E	240-255								
Notação Decimal Pontuada						Notação Binária			

# Classes de Endereço IPv4

200.54.1.23 = C /24 255.255.255.0

125.5.71.223 = A /8 255.0.0.0

224.0.7.1 = D

132.10.7.18 = B /16 255.255.0.0

242.1.1.15 = E

1º byte

Classe A

1-126

Classe B

128-191

Classe C

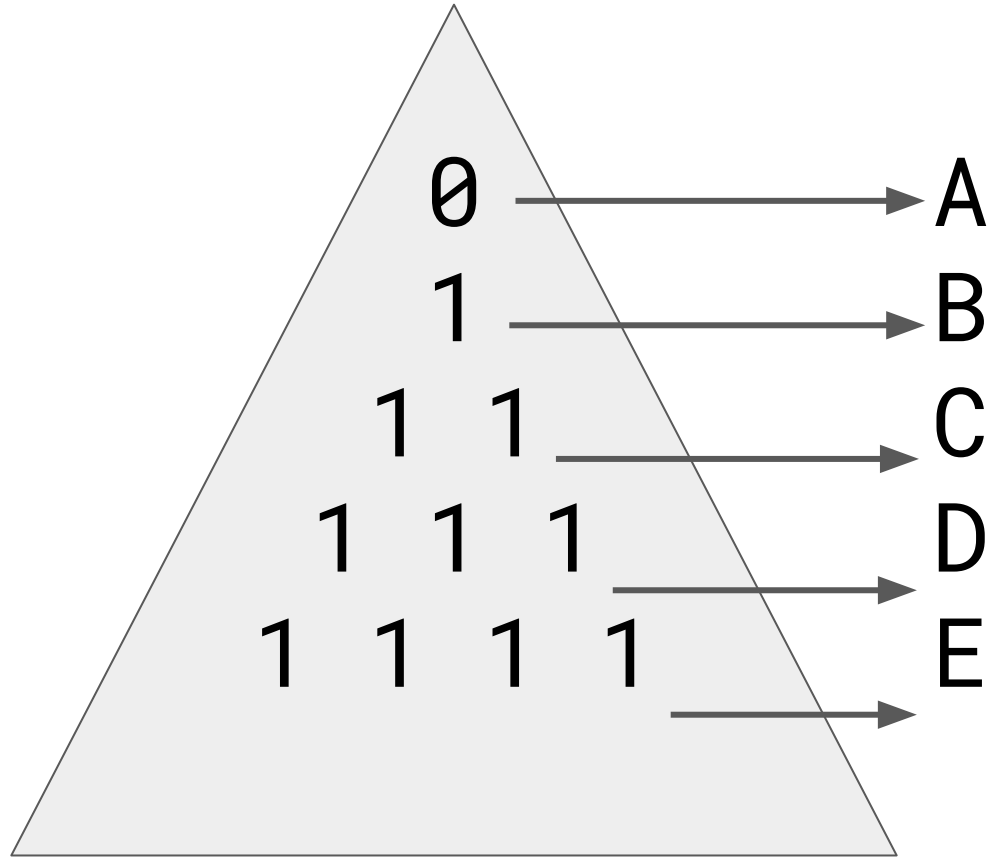
192-223

Classe D

224-239

Classe E

240-255



Classe A <del>0-127</del> 1-126	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
	128	64	32	16	8	4	2	1
	0							

Classe B 128-191	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
	128	64	32	16	8	4	2	1
	1							

$$\begin{array}{r} 0 \\ +128 \\ \hline 128 \end{array}$$

Classe C	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
	128	64	32	16	8	4	2	1
	1	1						

$$\begin{array}{r} 128 \\ +64 \\ \hline 192 \end{array}$$



	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	128
<b>Classe C</b>	128	64	32	16	8	4	2	1	+64
<b>192-223</b>	1	1							<b>192</b>

	<b>2<sup>7</sup></b>	<b>2<sup>6</sup></b>	<b>2<sup>5</sup></b>	<b>2<sup>4</sup></b>	<b>2<sup>3</sup></b>	<b>2<sup>2</sup></b>	<b>2<sup>1</sup></b>	<b>2<sup>0</sup></b>	128
									+64
<b>Classe D</b>	128	64	32	16	8	4	2	1	+32
<b>224-239</b>	1	1	1						<del>224</del>

	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$	128
									+64
	128	64	32	16	8	4	2	1	+32
									+16
<b>Classe E</b> <b>240-255</b>	1	1	1	1					<del>240</del>

# Classes de Endereço IPv4

Classe	Binária	Decimal Pontuada	CIDR
A	11111111.00000000.00000000.00000000	255.0.0.0	/8
B	11111111.11111111.00000000.00000000	255.255.0.0	/16
C	11111111.11111111.11111111.00000000	255.255.255.0	/24

Máscaras-padrão para endereçamento com classes

$128+64+32+16+8+4+2+1 = 255$

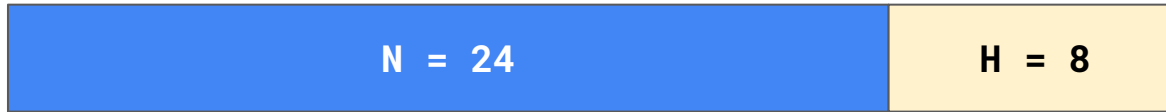
# Classes de Endereço IPv4



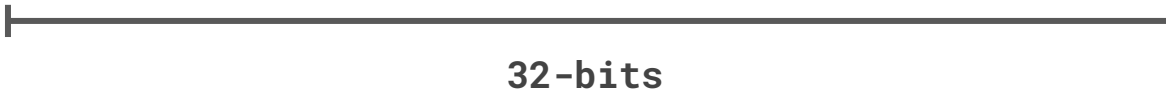
**Classe A:**  
 $2^{24} - 2 = 16.777.214$

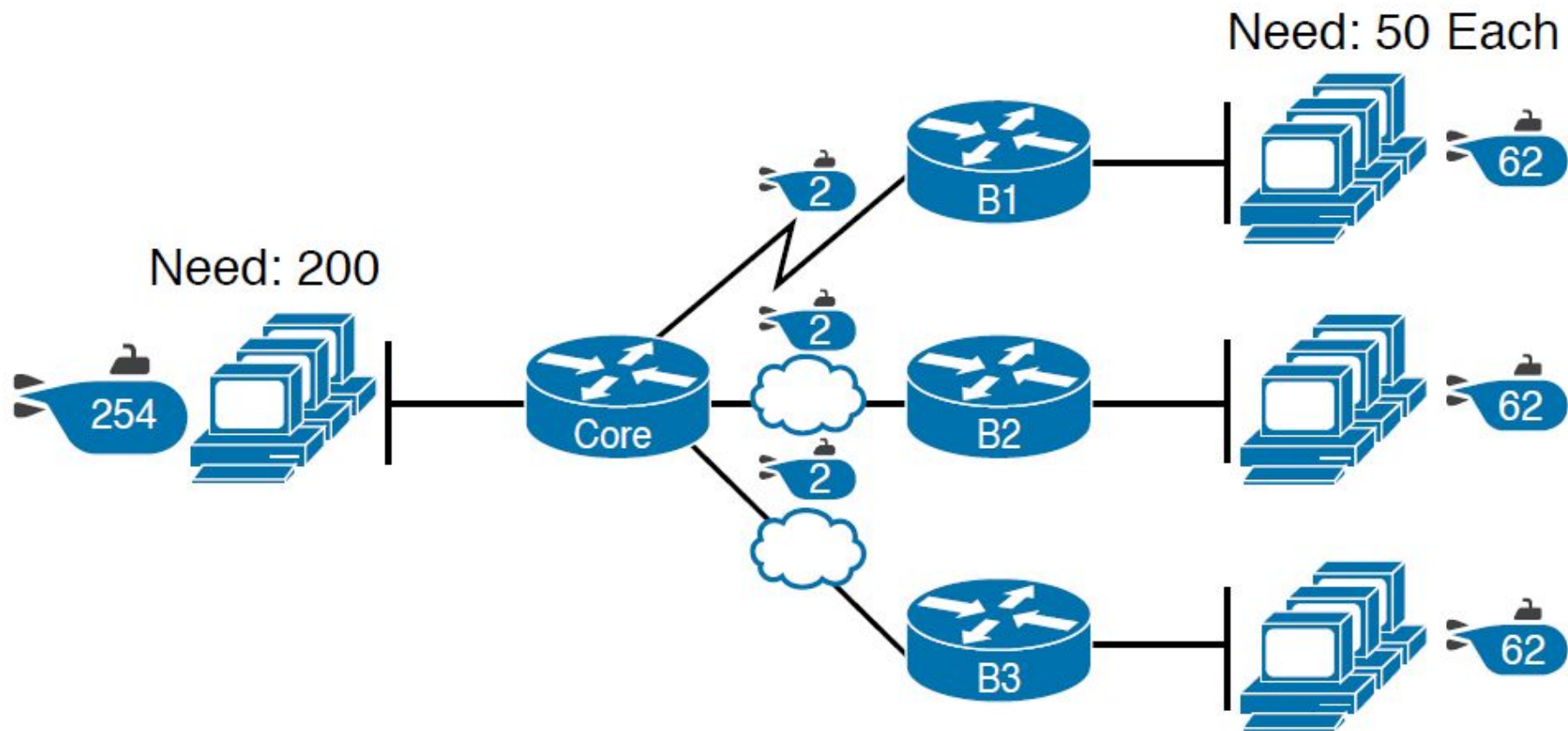


**Classe B:**  
 $2^{16} - 2 = 65.534$



**Classe C:**  
 $2^8 - 2 = 254$





# Exercícios de Fixação 03

ENDEREÇO	CLASSE	MÁSCARA
178.87.19.7		
13.14.15.16		
200.23.56.9		
172.16.0.9		
126.93.17.5		
191.3.2.1		
224.0.0.1		
160.10.20.30		

# Exercícios de Fixação 03 ~ solução

ENDEREÇO	CLASSE	MÁSCARA
178.87.19.7	B	255.255.0.0
13.14.15.16	A	255.0.0.0
200.23.56.9	C	255.255.255.0
172.16.0.9	B	255.255.0.0
126.93.17.5	A	255.0.0.0
191.3.2.1	B	255.255.0.0
224.0.0.1	D	-
160.10.20.30	C	255.255.255.0

# [3] Cálculos de Endereçamento IPv4 - com classe

# Máscaras de Redes

- Nos informam **qual parte do endereço identifica o grupo da rede, como um todo, e qual parte identifica o usuário.**
- Máscaras são usadas para **informar os tamanhos das redes.**
- E exatamente por isso podem **fragmentar as redes (domínios de broadcast).**

Exemplos:

10.10.12.14 255.0.0.0

132.89.144.198 255.255.0.0

192.168.0.14 255.255.255.0



# Definição da Máscara de Rede

$$N + H = 32$$

- Tudo que for 1 representa rede, e tudo que for 0 representa host;
- não pode haver mistura de algarismos 0 e 1;
- não pode haver algarismo 0 antes de algarismo 1.

Exemplos:

11111111.11111111.00000000.00000000

11111111.11111111.11111111.00000000

11111111.00000000.00000000.00000000

# Exercícios de Fixação - Máscaras de Rede

MÁSCARA (notação binária)	É UMA MÁSCARA DE REDE POSSÍVEL?
11110111.00000000.00000000.00000000	
11111111.11000000.00000000.00000000	
01111111.00000000.00000000.00000000	
11111111.00000000.11111111.00000000	
11111111.11111110.00000000.00000000	
11111111.11111111.00001111.00000000	

# Exercícios de Fixação - Máscaras de Rede ~

**solução**

MÁSCARA (notação binária)	É UMA MÁSCARA DE REDE POSSÍVEL?
11110111.00000000.00000000.00000000	NÃO
11111111.11000000.00000000.00000000	SIM
01111111.00000000.00000000.00000000	NÃO
11111111.00000000.11111111.00000000	NÃO
11111111.11111110.00000000.00000000	SIM
11111111.11111111.00001111.00000000	NÃO

# Notações da Máscara de Rede

$$N + H = 32$$

255.0.0.0 (decimal pontuada)

EX1

11111111.00000000.00000000.00000000 (binária)

/8 (CIDR ou barramento)

255.255.0.0 (decimal pontuada)

EX2

11111111.11111111.00000000.00000000 (binária)

/16 (CIDR ou barramento)

255.255.255.0 (decimal pontuada)

EX3

11111111.11111111.11111111.00000000 (binária)

/24 (CIDR ou barramento)

# Exercícios de Fixação - Máscaras de Rede

MÁSCARA	CLASSE	QUANTIDADE DE BITS RESERVADOS PARA A REDE	QUANTIDADE DE BITS RESERVADOS PARA O HOST	TAMANHO DA REDE (em potências de 2)
255.0.0.0				
255.255.0.0				
255.255.255.0				

Exercícios de Fixação - Máscaras de Rede ~

solução

MÁSCARA	CLASSE	QUANTIDADE DE BITS RESERVADOS PARA A REDE	QUANTIDADE DE BITS RESERVADOS PARA O HOST	TAMANHO DA REDE (em potências de 2)
255.0.0.0	A	8	24	$2^{24} - 2 = 16.777.214$
255.255.0.0	B	16	16	$2^{16} - 2 = 65.534$
255.255.255.0	C	24	8	$2^8 - 2 = 254$

# CIDR

## Classless Inter-Domain Routing

\*vulgo “formato de barramento”

É a quantidade de bits 1's existentes em uma máscara de rede.

Exemplos:

$255.0.0.0 = /8$

$255.255.0.0 = /16$

$255.255.255.0 = /24$

# Relação entre o Endereço e a Máscara

A máscara de rede, em relação ao endereço IP, define até onde vai o endereço de rede e onde começa o endereço do host.

## Exemplos

- A. IP 192.168.0.5 255.255.255.0
- B. IP 10.0.10.11 255.0.0.0
- C. IP 172.16.30.14 255.255.0.0

192	168	0	5
255	255	255	0

10	0	10	11
255	0	0	0

172	16	30	14
255	255	0	0



# Relação entre o Endereço e a Máscara

A máscara de rede, em relação ao endereço IP, define até onde vai o endereço de rede e onde começa o endereço do host.

## Exemplos

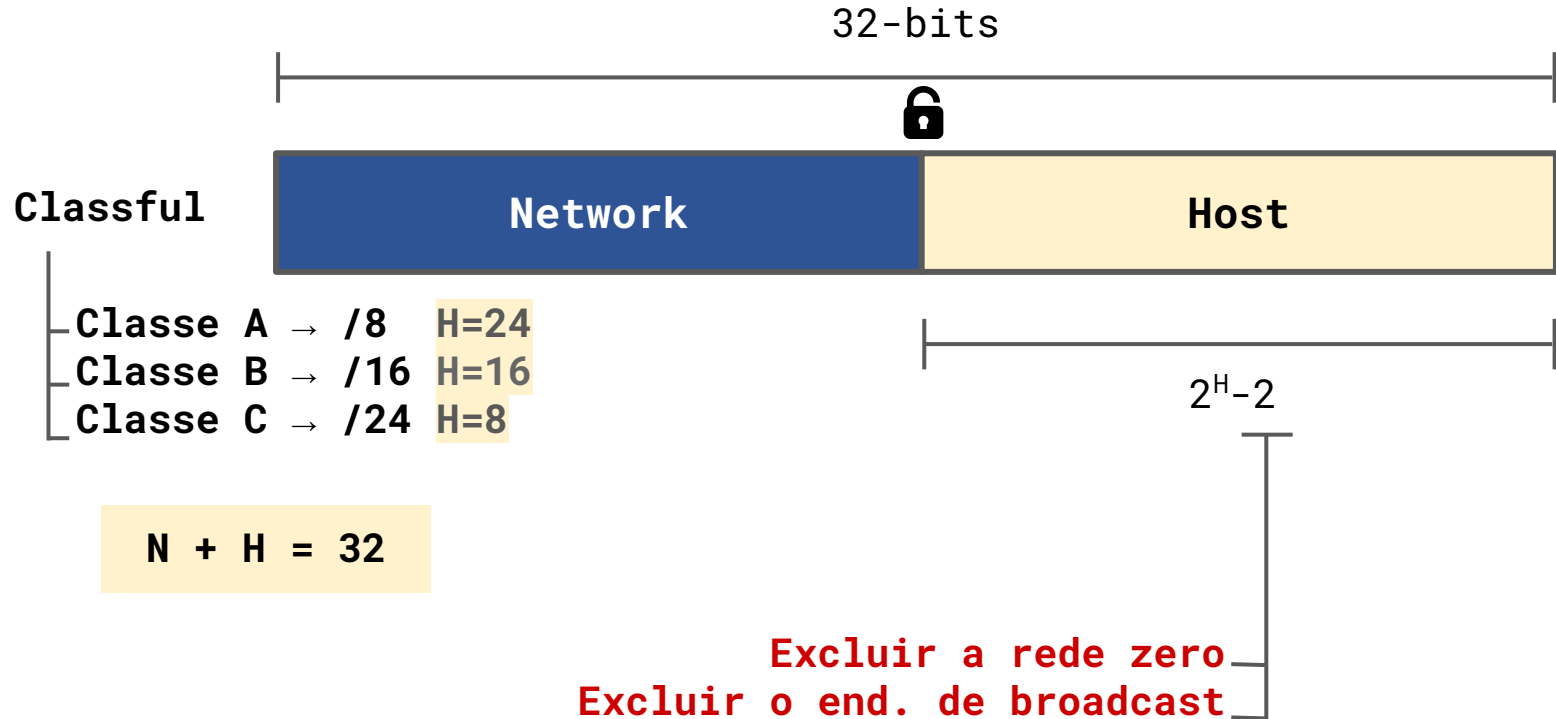
- A. IP 192.168.0.5 255.255.255.0
- B. IP 10.0.10.11 255.0.0.0
- C. IP 172.16.30.14 255.255.0.0

192	168	0	5
255	255	255	0
192	168	0	5
REDE			HOST

10	0	10	11
255	0	0	0
10	0	10	11
REDE	HOST		

172	16	30	14
255	255	0	0
172	16	30	14
REDE		HOST	

# Como se contabiliza o número total de hosts?



EXEMPLO 1	20.1.10.1
Classe	Classe A
Máscara em n.d.p.	255.0.0.0 (/8)
Quantos bits de Network?	8-bits
Quantos bits de Host?	24-bits
Endereço da rede	20.0.0.0
1o end. válido	20.0.0.1
Últ. end. válido	20.255.255.254
End. de broadcast	20.255.255.255
Número máx de hosts/rede	$2^{24} - 2$

EXEMPLO 2	172.21.15.47
Classe	Classe B
Máscara em n.d.p.	255.255.0.0 (/16)
Quantos bits de Network?	16-bits
Quantos bits de Host?	16-bits
Endereço da rede	172.21.0.0
1o end. válido	172.21.0.1
Últ. end. válido	172.21.255.254
End. de broadcast	172.21.255.255
Número máx de hosts/rede	$2^{16} - 2$

EXEMPLO 3	200.1.10.23
Classe	Classe C
Máscara em n.d.p.	255.255.255.0 (/24)
Quantos bits de Network?	24-bits
Quantos bits de Host?	8-bits
Endereço da rede	200.1.10.0
1o end. válido	200.1.10.1
Últ. end. válido	200.1.10.254
End. de broadcast	200.1.10.255
Número máx de hosts/rede	$2^8 - 2$

EXERCÍCIO 1	10.0.10.1
Classe	Classe A
Máscara em n.d.p.	255.0.0.0 (/8)
Quantos bits de Network?	8-bits
Quantos bits de Host?	24-bits
Endereço da rede	10.0.0.0
1o end. válido	10.0.0.1
Últ. end. válido	10.255.255.254
End. de broadcast	10.255.255.255
Número máx de hosts/rede	$2^{24} - 2$

EXERCÍCIO 2	172.16.0.14
Classe	Classe B
Máscara em n.d.p.	255.255.0.0 (/16)
Quantos bits de Network?	16-bits
Quantos bits de Host?	16-bits
Endereço da rede	172.16.0.0
1o end. válido	172.16.0.1
Últ. end. válido	172.16.255.254
End. de broadcast	172.16.255.255
Número máx de hosts/rede	$2^{16} - 2$

EXERCÍCIO 3	192.168.0.5
Classe	Classe C
Máscara em n.d.p.	255.255.255.0 (/24)
Quantos bits de Network?	24-bits
Quantos bits de Host?	8-bits
Endereço da rede	192.168.0.0
1o end. válido	192.168.0.1
Últ. end. válido	192.168.0.254
End. de broadcast	192.168.0.255
Número máx de hosts/rede	$2^8 - 2$



<b>EXERCÍCIO 4</b>	<b>200.10.10.1</b>
Classe	<b>Classe C</b>
Máscara em n.d.p.	<b>255.255.255.0 (/24)</b>
Quantos bits de Network?	<b>24-bits</b>
Quantos bits de Host?	<b>8-bits</b>
Endereço da rede	<b>200.10.10.0</b>
1o end. válido	<b>200.10.10.1</b>
Últ. end. válido	<b>200.10.10.254</b>
End. de broadcast	<b>200.10.10.255</b>
Número máx de hosts/rede	<b><math>2^8 - 2</math></b>

EXERCÍCIO 5	126.0.0.10
Classe	Classe A
Máscara em n.d.p.	255.0.0.0 (/8)
Quantos bits de Network?	8-bits
Quantos bits de Host?	24-bits
Endereço da rede	126.0.0.0
1o end. válido	126.0.0.1
Últ. end. válido	126.255.255.254
End. de broadcast	126.255.255.255
Número máx de hosts/rede	$2^{24} - 2$

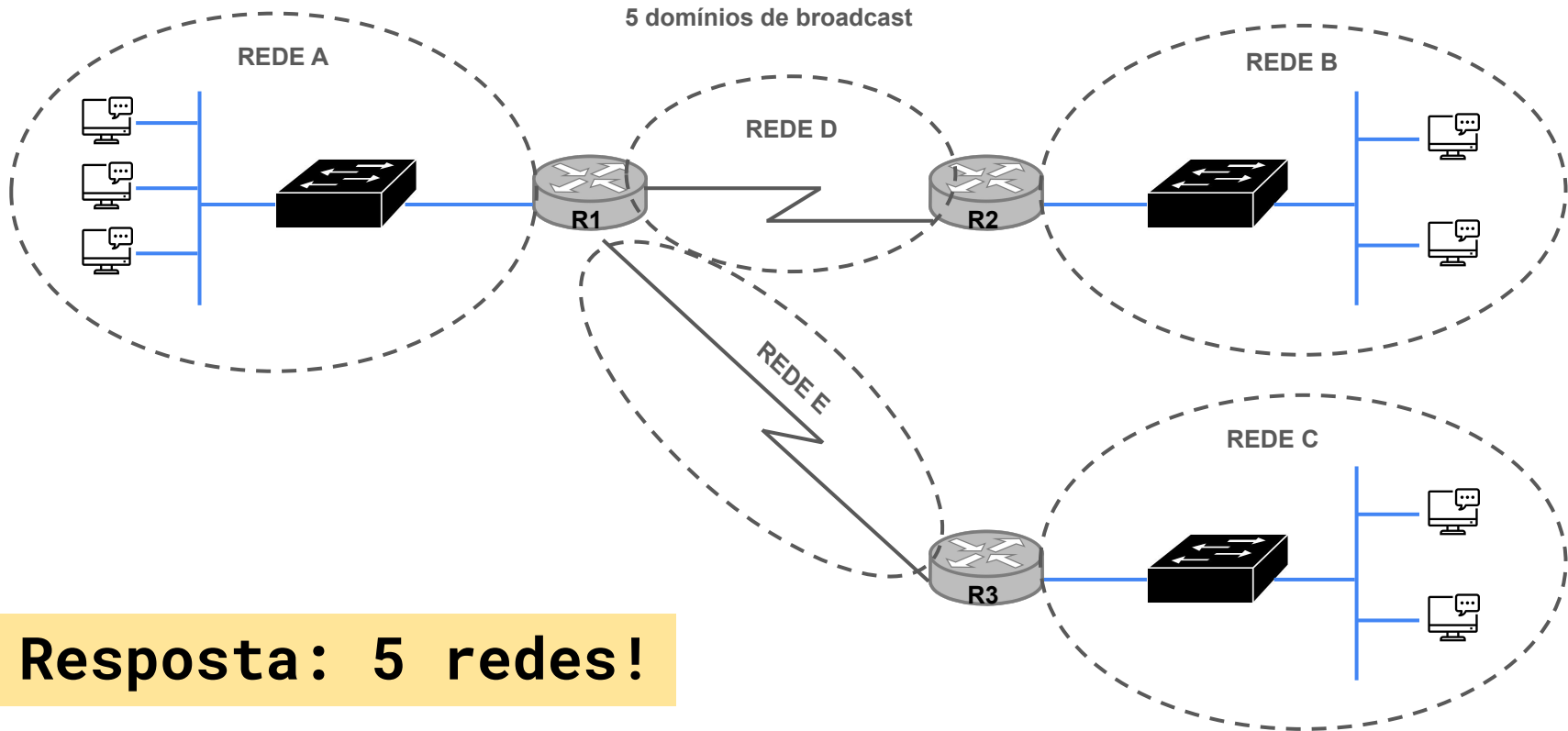
EXERCÍCIO 6	130.131.1.6
Classe	Classe B
Máscara em n.d.p.	255.255.0.0 (/16)
Quantos bits de Network?	16-bits
Quantos bits de Host?	16-bits
Endereço da rede	130.131.0.0
1o end. válido	130.131.0.1
Últ. end. válido	130.131.255.254
End. de broadcast	130.131.255.255
Número máx de hosts/rede	$2^{16} - 2$

EXERCÍCIO 7	191.8.9.19
Classe	Classe B
Máscara em n.d.p.	255.255.0.0 (/16)
Quantos bits de Network?	16-bits
Quantos bits de Host?	16-bits
Endereço da rede	191.8.0.0
1o end. válido	191.8.0.1
Últ. end. válido	191.8.255.254
End. de broadcast	191.8.255.255
Número máx de hosts/rede	$2^{16} - 2$

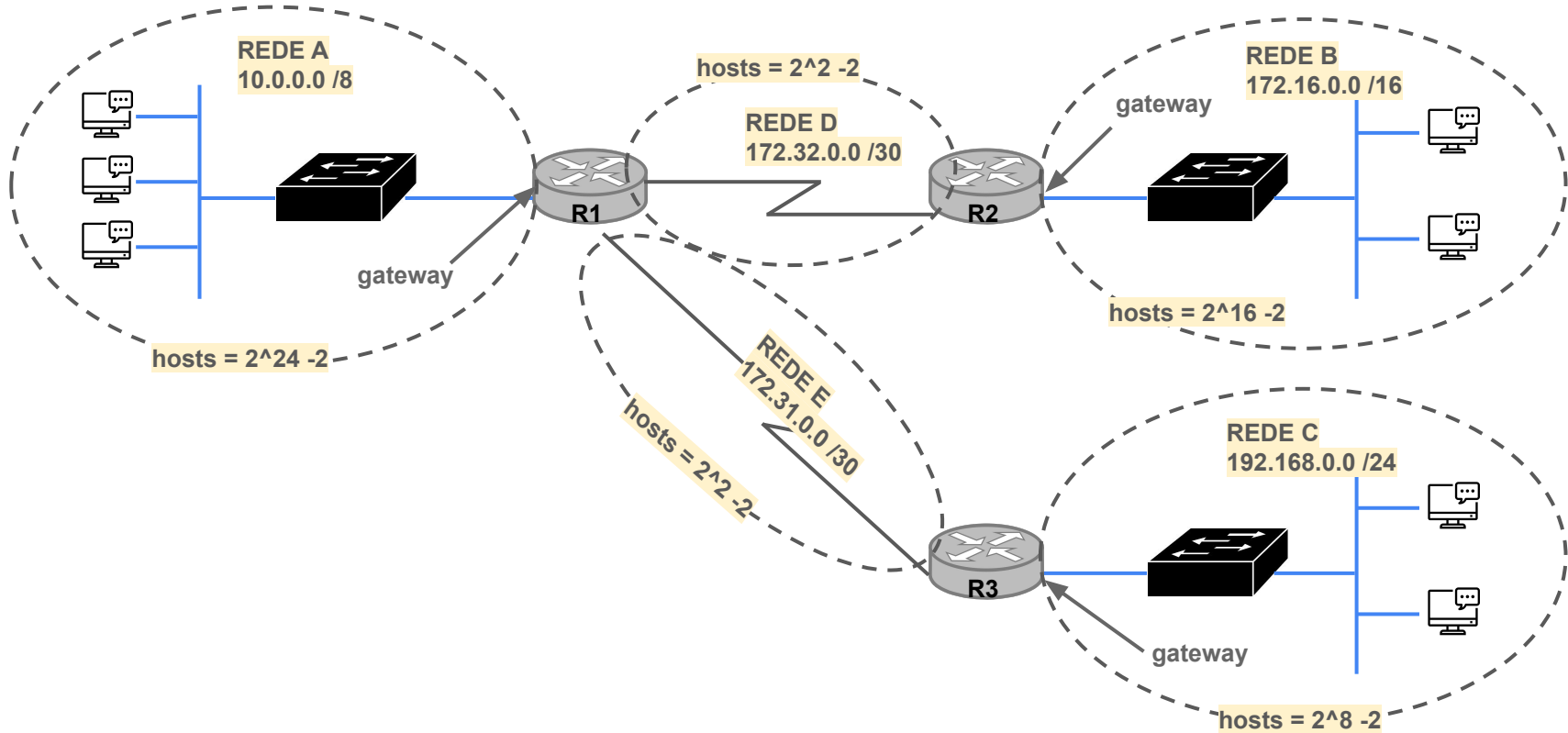
<b>EXERCÍCIO 8</b>	<b>202.10.11.12</b>
Classe	<b>Classe C</b>
Máscara em n.d.p.	<b>255.255.255.0 (/24)</b>
Quantos bits de Network?	<b>24-bits</b>
Quantos bits de Host?	<b>8-bits</b>
Endereço da rede	<b>202.10.11.0</b>
1o end. válido	<b>202.10.11.1</b>
Últ. end. válido	<b>202.10.11.254</b>
End. de broadcast	<b>202.10.11.255</b>
Número máx de hosts/rede	<b><math>2^8 - 2</math></b>

# Comunicação entre Redes Diferentes

Quantas redes possui a topologia abaixo?

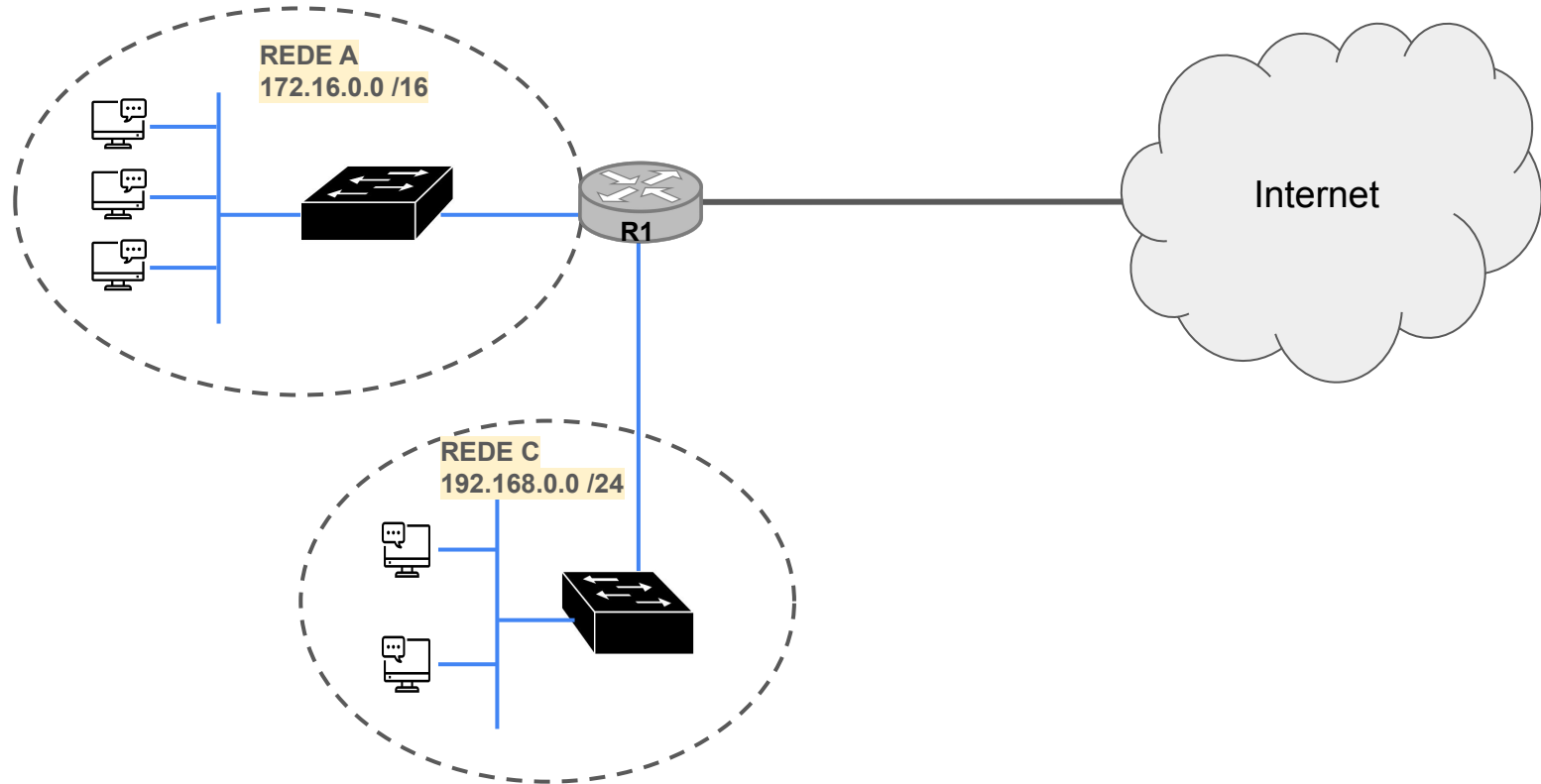


# Comunicação entre Redes Diferentes



# Exercícios de Fixação - Domínios de Broadcast

- A. Quantos domínios de broadcast e quantas redes possuem a topologia abaixo?
- B. Quantos hosts é possível adicionar as redes A e B?

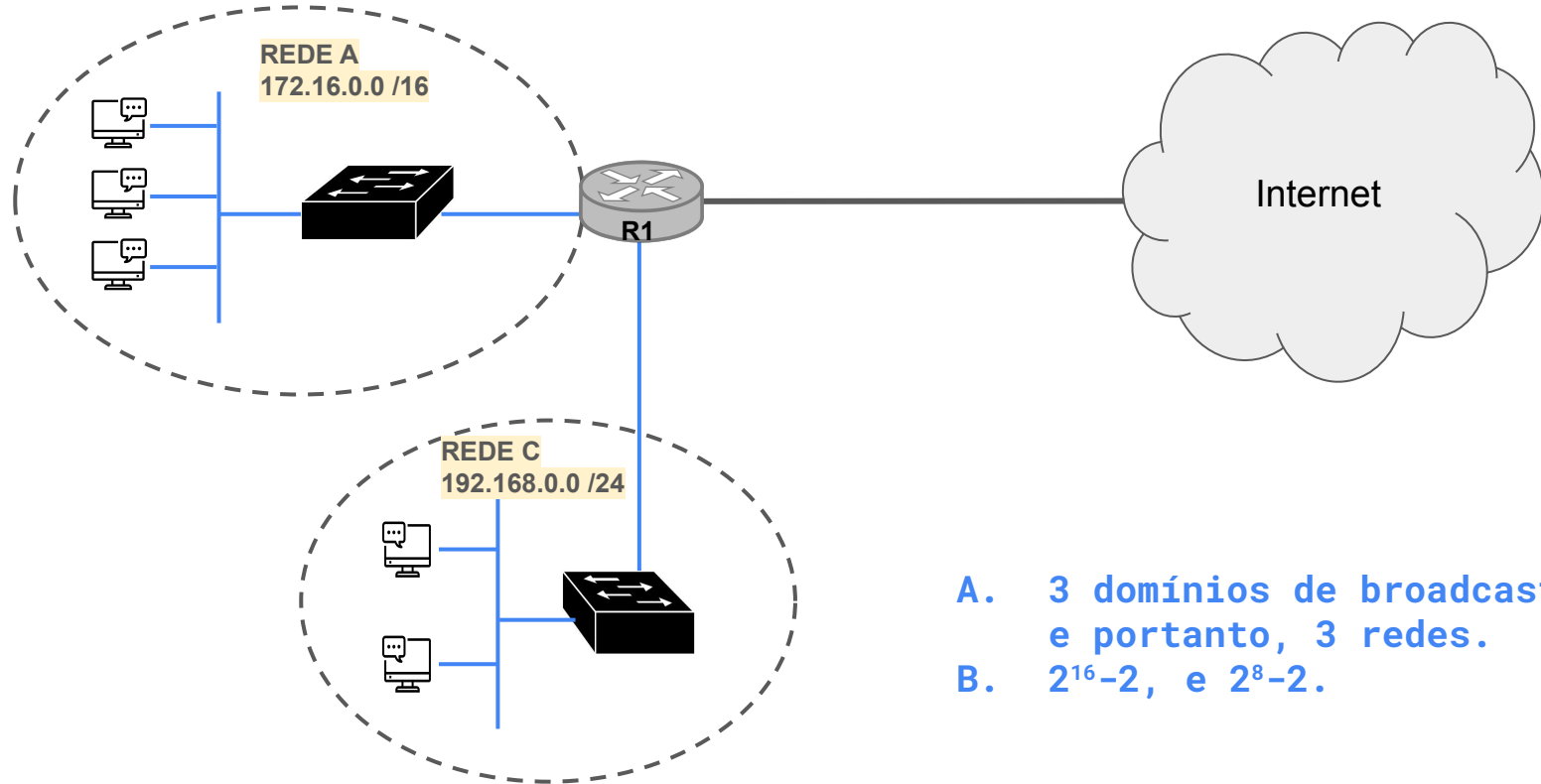




# Exercícios de Fixação - Domínios de Broadcast ~

**solução**

- A. Quantos domínios de broadcast e quantas redes possuem a topologia abaixo?
- B. Quantos hosts é possível adicionar as redes A e B?



- A. 3 domínios de broadcast, e portanto, 3 redes.
- B.  $2^{16}-2$ , e  $2^8-2$ .

# [4] Cálculos de Endereçamento IPv4 - Sem classe

# Endereçamento “classful” e “classless”

- **Endereçamento Classful:** IPv4 = prefixo + host, definidas pela máscara, e regras das Classes A, B e C.
- **Endereçamento Classless:** IPv4 = prefixo + sub-rede + host, definidas pela máscara, com nenhuma consideração pela classe (A, B ou C).

## Máscaras-padrão para endereçamento com classes

CLASSE	BINÁRIA	DECIMAL PONTUADA	CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

\*CIDR (Classless Inter-Domain Routing, em inglês, roteamento interdomínios sem classes)

Refere-se à quantidade de bits 1 existentes em uma máscara de rede.

As máscaras de rede estão caindo em desuso, em lugar está sendo usado o CIDR.

**MÁSCARAS NÃO TRAFEGAM  
NA REDE!**

# Máscaras de Redes Possíveis

BINÁRIA	DECIMAL PONTUADA	CIDR	NÚMERO DE USUÁRIOS
11111111.00000000.00000000.00000000	255.0.0.0	/8	$2^{24} - 2 = 16.777.214$
11111111.11110000.00000000.00000000	255.240.0.0	/12	$2^{20} - 2 = 1.048.574$
11111111.11111111.00000000.00000000	255.255.0.0	/16	$2^{16} - 2 = 65.534$
11111111.11111111.11110000.00000000	255.255.240.0	/20	$2^{12} - 2 = 4.094$
11111111.11111111.11111100.00000000	255.255.252.0	/22	$2^{10} - 2 = 1.022$
11111111.11111111.11111110.00000000	255.255.254.0	/23	$2^9 - 2 = 510$
11111111.11111111.11111111.00000000	255.255.255.0	/24	$2^8 - 2 = 254$
11111111.11111111.11111111.10000000	255.255.255.128	/25	$2^7 - 2 = 126$
11111111.11111111.11111111.11000000	255.255.255.192	/26	$2^6 - 2 = 62$
11111111.11111111.11111111.11111000	255.255.255.248	/29	$2^3 - 2 = 6$
11111111.11111111.11111111.11111100	255.255.255.252	/30	$2^2 - 2 = 2$

# Classes de Endereço IPv4

Faixa	1o. octeto	bits (redes)	máscara	bits (hosts)	Número de blocos	Tamanho do bloco	comunicação
Reservada	0	-	-	-	-	-	-
CLASSE A	1-126	8*	255.0.0.0 (/8)	24	128	16.777.216	Unicast
Reservada	127	-	-	-	-	-	-
CLASSE B	128-191	16*	255.255.0.0 (/16)	16	16.384	65.536	Unicast
CLASSE C	192-223	24*	255.255.255.0 (/24)	8	2.097.152	256	Unicast
CLASSE D	224-239	-	-	-	1	268.435.456	Multicast
CLASSE E	240-255	-	-	-	1	268.435.456	Experimental

Número de blocos e tamanhos no endereçamento IPv4 com classes

# Exercícios de Fixação 08

	Endereço IP	Classe	bits (rede)	bits (hosts)	Network ID (end. rede)	Broadcast Address
1	1.1.1.1					
2	128.1.6.5					
3	200.1.2.3					
4	192.192.1.1					
5	126.5.4.3					
6	200.1.10.7					
7	192.0.0.1					
8	191.255.1.43					
9	223.233.0.1					

# Exercícios de Fixação 08 ~ solução

	Endereço IP	Classe	bits (rede)	bits (hosts)	Network ID (end. rede)	Broadcast Address
1	1.1.1.1	A	8	24	1.0.0.0	1.255.255.255
2	128.1.6.5	B	16	16	128.1.0.0	128.1.255.255
3	200.1.2.3	C	24	8	200.1.2.0	200.1.2.255
4	192.192.1.1	C	24	8	192.192.1.0	192.192.1.255
5	126.5.4.3	A	8	24	126.0.0.0	126.255.255.255
6	200.1.10.7	C	24	8	200.1.10.0	200.1.10.255
7	192.0.0.1	C	24	8	192.0.0.0	192.0.0.255
8	191.255.1.43	B	16	16	191.255.0.0	191.255.255.255
9	223.233.0.1	C	24	8	223.233.0.0	223.233.0.255

# Exercícios de Fixação 09

CLASSE	Valores do 1o. octeto	Propósito
A		
B		
C		
D		
E		



# Exercícios de Fixação 09 ~ solução

CLASSE	Valores do 1o. octeto	Propósito
A	1-126	Endereços Unicast dos hosts
B	128-191	Endereços Unicast dos hosts
C	192-223	Endereços Unicast dos hosts
D	224-239	Multicast
E	240-255	Experimental

# Exercícios de Fixação 10

	CLASSE A	CLASSE B	CLASSE C
Faixa do 1o. octeto			
Total de redes			
Hosts/rede			
Bits (rede)			
Bits (hosts)			
Máscara Padrão			

# Exercícios de Fixação 10 ~ solução

	CLASSE A	CLASSE B	CLASSE C
Faixa do 1o. octeto	1-126	128-191	192-223
Total de redes	$2^7 - 2 = 126$	$2^{14} = 16.384$	$2^{21} = 2.097.152$
Hosts/rede	$2^{24}-2$	$2^{16}-2$	$2^8-2$
Bits (rede)	8	16	24
Bits (hosts)	24	16	8
Máscara Padrão	255.0.0.0	255.255.0.0	255.255.255.0

# Exercícios de Fixação 11

1) Qual a notação decimal pontuada dos seguintes barramentos de máscaras de sub-rede:

- a) /8
- b) /10
- c) /14
- d) /16
- e) /20
- f) /22
- g) /24
- h) /28
- i) /30

2) Descobrir a notação CIDR (barramento) dos seguintes máscaras de sub-rede:

- a) 252.0.0.0
- b) 255.224.0.0
- c) 255.255.255.128
- d) 255.255.254.0

# Exercícios de Fixação 11 ~ solução

1) Qual a notação decimal pontuada dos seguintes barramentos de máscaras de sub-rede:

- a) /8 = 255.0.0.0
- b) /10 = 255.192.0.0
- c) /14 = 255.252.0.0
- d) /16 = 255.255.0.0
- e) /20 = 255.255.240.0
- f) /22 = 255.255.252.0
- g) /24 = 255.255.255.0
- h) /28 = 255.255.255.240
- i) /30 = 255.255.255.252

2) Descobrir a notação CIDR (barramento) dos seguintes máscaras de sub-rede:

- a) 252.0.0.0 = /6
- b) 255.224.0.0 = /11
- c) 255.255.255.128 = /25
- d) 255.255.254.0 = /23

# Exercícios de Fixação 12

1) Descobrir a classe de rede e a máscara de cada um dos endereços abaixo:

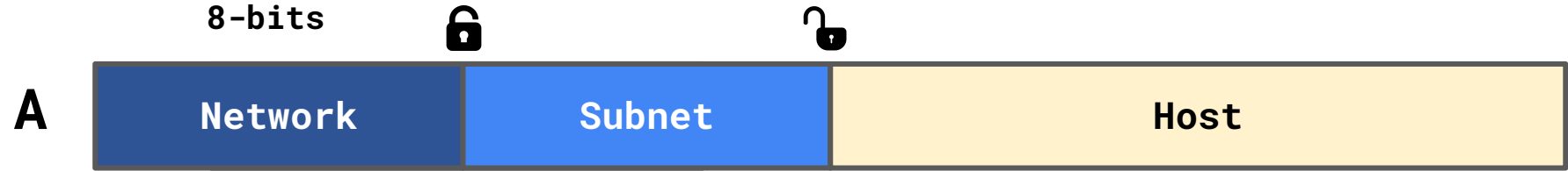
- a) 129.10.11.12
- b) 225.120.12.7
- c) 191.1.12.3
- d) 200.6.12.96
- e) 245.43.21.1
- f) 9.4.2.139
- g) 126.121.2.13
- h) 89.12.1.250
- i) 127.0.0.6
- j) 229.71.56.79
- k) 4.39.29.12
- l) 192.168.0.1
- m) 250.22.23.59

# Exercícios de Fixação 12 ~ solução

1) Descobrir a classe de rede e a máscara de cada um dos endereços abaixo:

- a) 129.10.11.12 = Classe B - /16
- b) 225.120.12.7 = Classe D (Reservado)
- c) 191.1.12.3 = Classe B - /16
- d) 200.6.12.96 = Classe C - /24
- e) 245.43.21.1 = Classe E (Reservado)
- f) 9.4.2.139 = Classe A - /8
- g) 126.121.2.13 = Classe A - /8
- h) 89.12.1.250 = Classe A - /8
- i) 127.0.0.6 = Reservado (Loopback)
- j) 229.71.56.79 = Classe D (Reservado)
- k) 4.39.29.12 = Classe A - /8
- l) 192.168.0.1 = Classe C - /24
- m) 250.22.23.59 = Classe E (Reservado)

# Pegando bits de hosts emprestado para subnets



$$N + S + H = 32$$

$$2^H - 2$$



## EXEMPLO 01

172.16.0.0, 20 subnets, 200 hosts cada.

Qual a classe do endereço? **B**

Quantos bits eu preciso para **Network?** **16-bits**

Quantos bits eu preciso para **Subnets?** **5-bits**

Quantos bits eu preciso para **Hosts?** **8-bits**

Perceba que nesse caso ainda restaram **3-bits**.

Eles podem ser alocados para **S**, para ter **mais subnets**.

Ou alocados para **H**, para ter **mais hosts/subnet**.

**ENDEREÇOS QUE SALTAM NO 4o. OCTETO**  
**(após o /24)**

**200.10.10.50 /28**

**passo-a-passo**

**I. Em qual octeto os endereços estão "pulando"?**

/24 completa o 3o. octeto, portanto: /25-/32 estão no 4o octeto!

**ATENÇÃO:** /31 & /32 não existem, porque não há endereços válidos disponíveis.

**II. Mas está "pulando" de quanto em quanto no 4o. octeto?**

Classe C, N = 24-bits. Lembrando que  **$N + S + H = 32$**

O  $H = 32 - 28$ , portanto  **$H = 4\text{-bits}$** . E logo,  **$S = 4\text{-bits}$** .

Se  $H=4$ , logo a rede "pula" de  **$2^4$  em  $2^4$**  (de 16 em 16).

**200.10.10.50 /28**

**passo-a-passo**

### III. Identificar a rede

Se  $H=4$ , logo a rede "pula" de  $2^4$  em  $2^4$  (de 16 em 16).

200.10.10.0	200.10.10.48
200.10.10.16	200.10.10.49
200.10.10.32	200.10.10.50
200.10.10.48 →	...
200.10.10.64	200.10.10.62
200.10.10.80	200.10.10.63
200.10.10.96	
200.10.10.112	
200.10.10.128	
...	
200.10.10.240	
200.10.10.256	

### IV. Identificar os endereços envolvidos

200.10.10.0	200.10.10.48	→ endereço de rede (rede "zero")
200.10.10.16	200.10.10.49	→ 1o. endereço válido
200.10.10.32	200.10.10.50	
200.10.10.48 →	...	
200.10.10.64	200.10.10.62	→ último endereço válido
200.10.10.80	200.10.10.63	→ endereço de broadcast
200.10.10.96		
200.10.10.112		
200.10.10.128		
...		
200.10.10.240		
200.10.10.256		

**204.0.133.89 /29**

**passo-a-passo**

**I. Em qual octeto os endereços estão "pulando"?**

/24 completa o 3o. octeto, portanto: /25-/32 estão no 4o octeto!

**II. Mas está "pulando" de quanto em quanto no 4o. octeto?**

Classe C, N = 24-bits. Lembrando que  **$N + S + H = 32$**

O  $H = 32 - 29$ , portanto  **$H = 3\text{-bits}$** . E logo,  **$S = 5\text{-bits}$** .

Se  $H=3$ , logo a rede "pula" de  **$2^3$  em  $2^3$**  (de 8 em 8).

**204.0.133.89 /29**

**passo-a-passo**

### III. Identificar a rede

Se  $H=3$ , logo a rede "pula" de  $2^3$  em  $2^3$  (de 8 em 8).

204.0.133.0	
204.0.133.8	
204.0.133.16	
204.0.133.24	
...	
204.0.133.80	
204.0.133.88	→
204.0.133.96	
...	
204.0.133.248	
204.0.133.256	

204.0.133.88
204.0.133.89
204.0.133.90
...
204.0.133.94
204.0.133.95

### IV. Identificar os endereços envolvidos

204.0.133.0	
204.0.133.8	
204.0.133.16	
204.0.133.24	
...	
204.0.133.80	
204.0.133.88 →	204.0.133.88 → endereço de rede (rede "zero")
204.0.133.96	204.0.133.89 → 1o. endereço válido
...	204.0.133.90
204.0.133.248	...
204.0.133.256	204.0.133.94 → último endereço válido
	204.0.133.95 → endereço de broadcast



EXEMPLO 1	200.10.10.5 /26
Com/sem classe?	sem classe (seria C)
Máscara (n.d.p.)	255.255.255.192
End. Público/Privado?	público
N, S & H (bits)?	N = 24   S = 2   H = 6
Número de subredes	$2^2$
Endereço da rede	200.10.10.0
1o end. válido	200.10.10.1
Últ. end. válido	200.10.10.62
End. de broadcast	200.10.10.63
Número máx de hosts/rede	$2^6 - 2$

EXEMPLO 2	192.168.7.100 /27
Com/sem classe?	sem classe (seria C)
Máscara (n.d.p.)	255.255.255.224
End. Público/Privado?	privado
N, S & H (bits)?	N = 24   S = 3   H = 5
Número de subredes	$2^3$
Endereço da rede	192.168.7.96
1o end. válido	192.168.7.97
Últ. end. válido	192.168.7.126
End. de broadcast	192.168.7.127
Número máx de hosts/rede	$2^5 - 2$

EXEMPLO 3	203.168.170.145 /25
Com/sem classe?	sem classe (seria C)
Máscara (n.d.p.)	255.255.255.128
End. Público/Privado?	público
N, S & H (bits)?	N = 24   S = 1   H = 7
Número de subredes	$2^1$
Endereço da rede	203.168.170.128
1o end. válido	203.168.170.129
Últ. end. válido	203.168.170.254
End. de broadcast	203.168.170.255
Número máx de hosts/rede	$2^7 - 2$

EXEMPLO 4	192.168.200.29 /30
Com/sem classe?	sem classe (seria C)
Máscara (n.d.p.)	255.255.255.252
End. Público/Privado?	privado
N, S & H (bits)?	N = 24   S = 6   H = 2
Número de subredes	$2^6$
Endereço da rede	192.168.200.28
1o end. válido	192.168.200.29
Últ. end. válido	192.168.200.30
End. de broadcast	192.168.200.31
Número máx de hosts/rede	$2^2 - 2$

**ENDEREÇOS QUE SALTAM NO 3o. OCTETO**

**(após o /16 até antes de completar o octeto)**

**190.10.35.89 /21**

**passo-a-passo**

**I. Em qual octeto os endereços estão "pulando"?**

/21 não completou o 3o. octeto, portanto: /17-/24 estão no 3o octeto!

**II. Mas está "pulando" de quanto em quanto no 3o. octeto?**

Classe B, N = 16-bits. Lembrando que **N + S + H = 32**

O H = 32 - 21, portanto **H = 11-bits**. E logo, **S = 5-bits**.

Quantos bits faltam para o /21 completar o 3o. octeto, com /24

bits-faltantes = 24 - 21 = 3-bits

Portanto, está pulando no 3o. octeto de  $2^3$  em  $2^3$  (8 em 8)

**190.10.35.89 /21**

**passo-a-passo**

### III. Identificar a rede

Se 3-bits, logo a rede "pula" de  $2^3$  em  $2^3$  (de 8 em 8).

190.10.0.0		190.10.32.0
190.10.8.0		190.10.32.1
190.10.16.0		190.10.32.2
190.10.24.0		...
190.10.32.0	→	190.10.39.254
190.10.40.0		190.10.39.255
190.10.48.0		
190.10.56.0		
...		
190.10.248.0		
190.10.256.0		

**192.10.35.89 /21**

**passo-a-passo**

#### IV. Identificar os endereços envolvidos

190.10.0.0		190.10.32.0	→ endereço de rede (rede "zero")
190.10.8.0		190.10.32.1	→ 1o. endereço válido
190.10.16.0		190.10.32.2	
190.10.24.0		...	
190.10.32.0	→	190.10.39.254	→ último endereço válido
190.10.40.0		190.10.39.255	→ endereço de broadcast
190.10.48.0			
190.10.56.0			
...			
190.10.248.0			
190.10.256.0			



EXEMPLO 1	172.17.10.1 /22
Com/sem classe?	sem classe (seria B)
Máscara (n.d.p.)	255.255.240.0
End. Público/Privado?	privado
N, S & H (bits)?	N = 16   S = 6   H = 10
Número de subredes	$2^6$
Endereço da rede	172.17.8.0
1o end. válido	172.17.8.1
Últ. end. válido	172.17.11.254
End. de broadcast	172.17.11.255
Número máx de hosts/rede	$2^{10} - 2$

EXEMPLO 2	191.100.99.146 /21
Com/sem classe?	sem classe (seria B)
Máscara (n.d.p.)	255.255.248.0
End. Público/Privado?	público
N, S & H (bits)?	N = 16   S = 5   H = 11
Número de subredes	$2^5$
Endereço da rede	191.100.96.0
1o end. válido	191.100.96.1
Últ. end. válido	191.100.103.254
End. de broadcast	191.100.103.255
Número máx de hosts/rede	$2^{11} - 2$

**ENDEREÇOS QUE SALTAM NO 2o. OCTETO**

**(após o /8 até antes de completar o octeto)**

I. Em qual octeto os endereços estão "pulando"?

/13 não completou o 2o. octeto, portanto: /9-/16 estão no 2o octeto!

II. Mas está "pulando" de quanto em quanto no 2o. octeto?

Classe A, N = 8-bits. Lembrando que  $N + S + H = 32$

O  $H = 32 - 13$ , portanto  $H = 19\text{-bits}$ . E logo,  $S = 5\text{-bits}$ .

Quantos bits faltam para o /13 completar o 2o. octeto, com /16

$\text{bits-faltantes} = 16 - 13 = 3\text{-bits}$

Portanto, está pulando no 2o. octeto de  $2^3$  em  $2^3$  (8 em 8)

### III. Identificar a rede

Se 3-bits, logo a rede "pula" de  $2^3$  em  $2^3$  (de 8 em 8).

19.0.0.0		19.8.0.0
19.8.0.0	→	19.8.0.1
19.16.0.0		19.8.0.2
19.24.0.0		...
19.32.0.0		19.15.255.254
19.40.0.0		19.15.255.255
19.48.0.0		
19.56.0.0		
...		
19.248.0.0		
19.256.0.0		

### IV. Identificar os endereços envolvidos

19.0.0.0

19.8.0.0 →

19.16.0.0

19.24.0.0

19.32.0.0

19.40.0.0

19.48.0.0

19.56.0.0

...

19.248.0.0

19.256.0.0

19.8.0.0 → endereço de rede (rede "zero")

19.8.0.1 → 1o. endereço válido

19.8.0.2

...

19.15.255.254 → último endereço válido

19.15.255.255 → endereço de broadcast

EXEMPLO 1	17.23.0.1 /14
Com/sem classe?	sem classe (seria A)
Máscara (n.d.p.)	255.252.0.0
End. Público/Privado?	público
N, S & H (bits)?	N = 8   S = 6   H = 18
Número de subredes	$2^6$
Endereço da rede	17.20.0.0
1o end. válido	17.20.0.1
Últ. end. válido	17.23.255.254
End. de broadcast	17.23.255.255
Número máx de hosts/rede	$2^{18} - 2$

EXEMPLO 2	10.100.99.146 /10
Com/sem classe?	sem classe (seria A)
Máscara (n.d.p.)	255.192.0.0
End. Público/Privado?	privado
N, S & H (bits)?	N = 8   S = 2   H = 22
Número de subredes	$2^2$
Endereço da rede	10.64.0.0
1o end. válido	10.64.0.1
Últ. end. válido	10.127.255.254
End. de broadcast	10.127.255.255
Número máx de hosts/rede	$2^{22} - 2$



# [5] Endereços IPv4 Especiais

# Rede loopback

A rede loopback (127.0.0.0 /8) é uma rede especial que possui as seguintes características:

- Só responde à própria máquina, ou seja, uma máquina não consegue comunicar-se com o endereço IP 127.x.x.x de outra máquina.
- Em princípio, sempre existirá em qualquer máquina que possua rede, pois é um processo interno do kernel do sistema operacional. Em outras palavras, toda máquina que tenha um sistema operacional com a pilha de rede habilitada possuirá o IP 127.0.0.1.
- Todos os endereços da rede loopback podem ser acessados pela máquina local.

Um dos grandes objetivos da rede loopback é permitir que aplicações clientes e servidoras possam estabelecer comunicação privada quando estiverem sendo executadas na mesma máquina.

# Rede link-local

A rede `169.254.0.0/16`, conhecida como bloco de link local (`link-local block`).

Essa rede é utilizada para numerar máquinas automaticamente, de forma que estas possam comunicar-se entre si se estiverem no mesmo segmento de rede.

O processo é o seguinte:

- Uma máquina é ligada.
- A máquina possui IP fixo (configurado localmente em arq. específico).
- A máquina procura um servidor DHCP na rede para obter dados sobre a rede, e não encontra nenhum servidor DHCP na rede.
- O sistema operacional atribui, à placa de rede, um endereço IP da rede `169.254.0.0 /16`. São feitos testes preliminares para saber se o endereço está livre.

# Exercícios de Fixação 13

Quais os blocos de endereçamento reservados para rede loopback e rede link-local, respectivamente?

# Exercícios de Fixação 14

Explique as diferenças entre o que é a rede loopback e a rede link-local.

**[6] Camada de Transporte,  
Portas & Sockets**

## PROTÓCOLOS DA CAMADA DE TRANSPORTE (L4)

TCP (TRANSMISSION CONTROL PROTOCOL)

UDP (USER DATAGRAM PROTOCOL)

TCP = CONTROLE DE FLUXO E RECUPERAÇÃO DE ERROS

USADO PELA MAIORIA DAS APLICAÇÕES (NAVEGAÇÃO WEB)

CONSUME MUITA BANDA DA REDE E MUITO PROCESSAMENTO DA CPU

UDP = NÃO FAZ QUALQUER CONTROLE

USADO PELAS APLICAÇÕES DE TEMPO REAL (VoIP, Video sobre IP)

CONSUME POUCA BANDA DA REDE E POUCO PROCESSAMENTO DA CPU

UNIDADE DA CAMADA DE TRANSPORTE (L4) = SEGMENTOS OU L4PDU

**Protocolo orientado à conexão:** Um protocolo que exige uma troca de mensagens antes de começar a transferir dados, ou que requer o pré-estabelecimento de conexão entre dois pontos finais.

**Protocolo não-orientado à conexão:** Um protocolo que **NÃO** exige uma troca de mensagens antes de começar a transferir dados, ou que **NÃO** requer o pré-estabelecimento de conexão entre dois pontos finais.

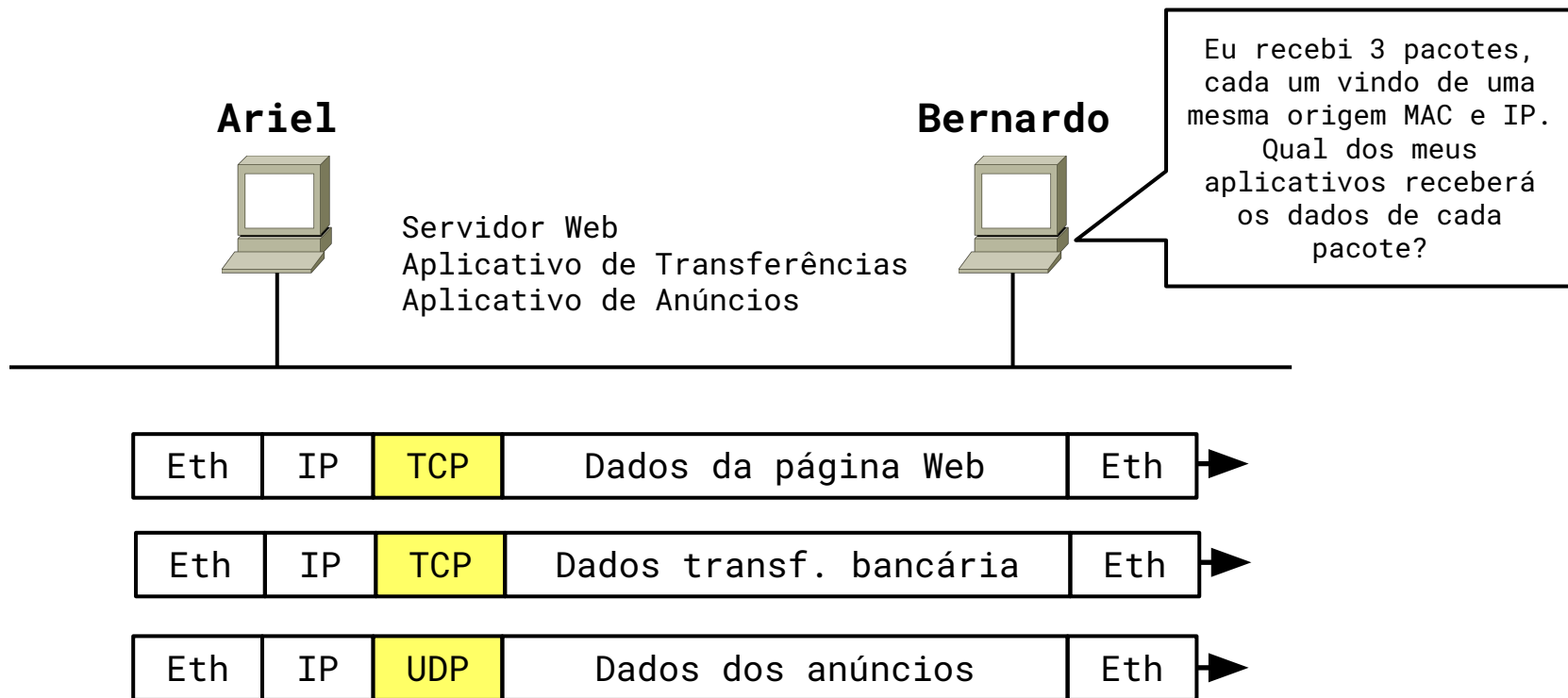
**TCP (TRANSMISSION CONTROL PROTOCOL) = ORIENTADO À CONEXÃO**

**UDP (USER DATAGRAM PROTOCOL) = NÃO ORIENTADO À CONEXÃO**

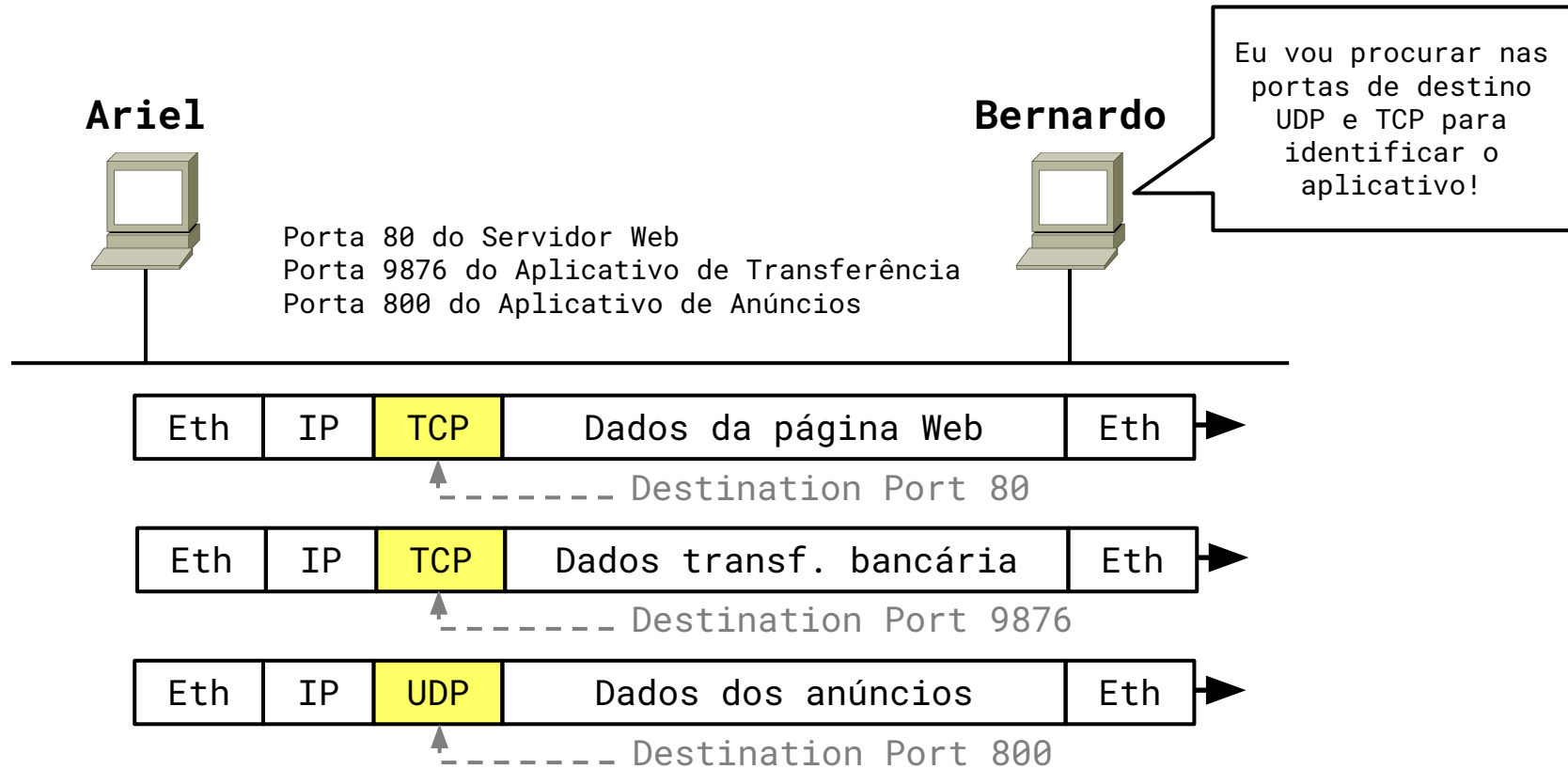


# Multiplexação com os números de porta TCP

A multiplexação é um conceito usado tanto pelo protocolo TCP como UDP. É um processo que faz o computador entender como lidar com o recebimento dos dados.



A multiplexação trabalha em cima de um conceito chamado **socket**. Um socket consiste de três coisas: Um **endereço IP**, um **protocolo de transporte** e um **número de porta**.



# Sockets (RFC 793)

É o nome que se dá ao conjunto IP e porta.

Geralmente sua representação padrão é IP: porta.

## Socket IPv4

### Exemplos:

192.168.0.1:110

192.168.0.1.110

http://rafael.prof.br:80

## Socket IPv6

### Exemplos:

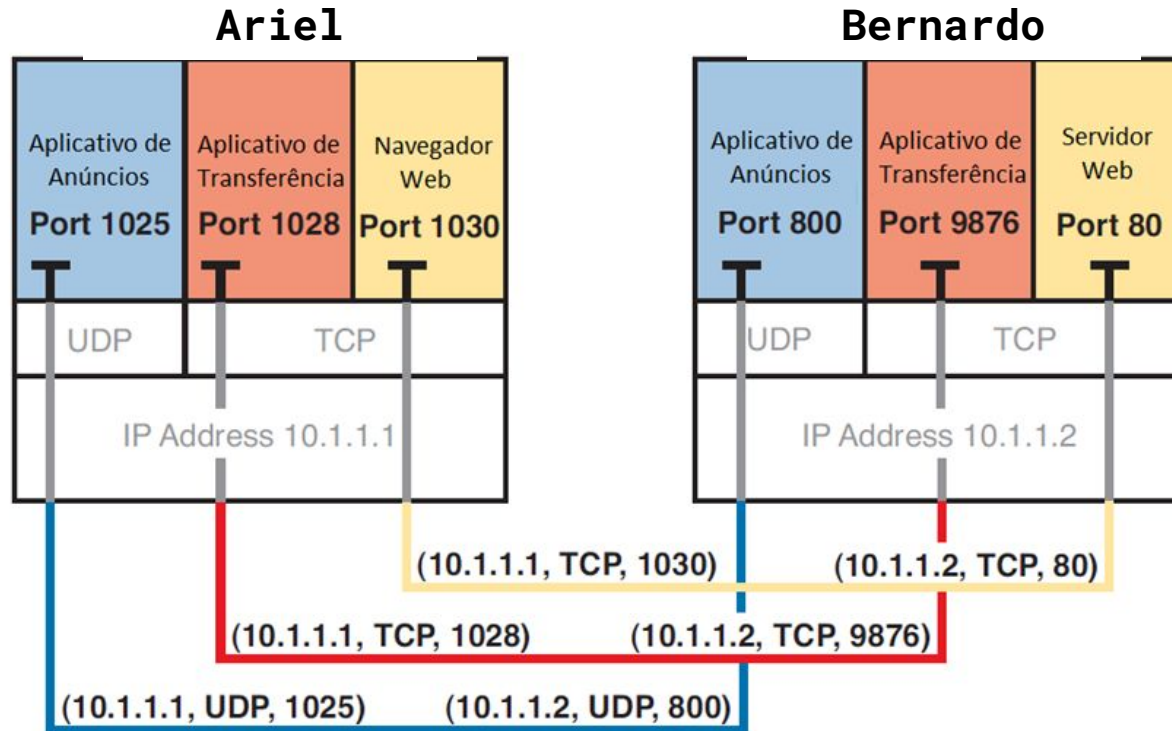
2001:db8::cccc:80

2001:db8::cccc.80

2001:db8::cccc#80

**Toda conexão é iniciada por um cliente e nunca por um servidor.**

Uma conexão entre **dois sockets** precise identificar uma **ligação ÚNICA** na rede.



Geralmente, os clientes utilizam portas aleatórias, enquanto os servidores empregam portas fixas.

PORTAS TCP E UDP		
PORTAS	UTILIZAÇÃO	EXEMPLO
0 a 1023	Geralmente utilizadas por serviços	80 TCP – Navegação web
	Raramente utilizadas por clientes	68 UDP – Cliente DHCP
1024 a 65535	Geralmente utilizadas por clientes	3128 TCP – Proxy HTTP Squid (servidor)
	Também utilizada por muitos serviços	4672 UDP – eMule (porta servidora)

Os três elementos básicos que um cliente deve saber de um servidor a ser acessado:

1. O protocolo a ser empregado.
2. O endereço IP do servidor.
3. A porta do servidor.

A IANA define as portas em três categorias:

<http://www.iana.org/assignments/port-numbers>

**Portas de sistema (well known ports): de 0 a 1023**

Essas portas não devem ser utilizadas em serviços de rede sem um prévio registro na IANA.

Serão utilizadas apenas por serviços inicializados pelo sistema, pelo administrador do sistema ou por usuários privilegiados.

**Portas de usuário (registered ports): de 1024 a 49151**

Essas portas não devem ser utilizadas em serviços de rede sem um prévio registro na IANA.

A diferença é que essas portas podem ser utilizadas por serviços inicializados e gerenciados por usuários comuns do sistema, em vez de administradores.

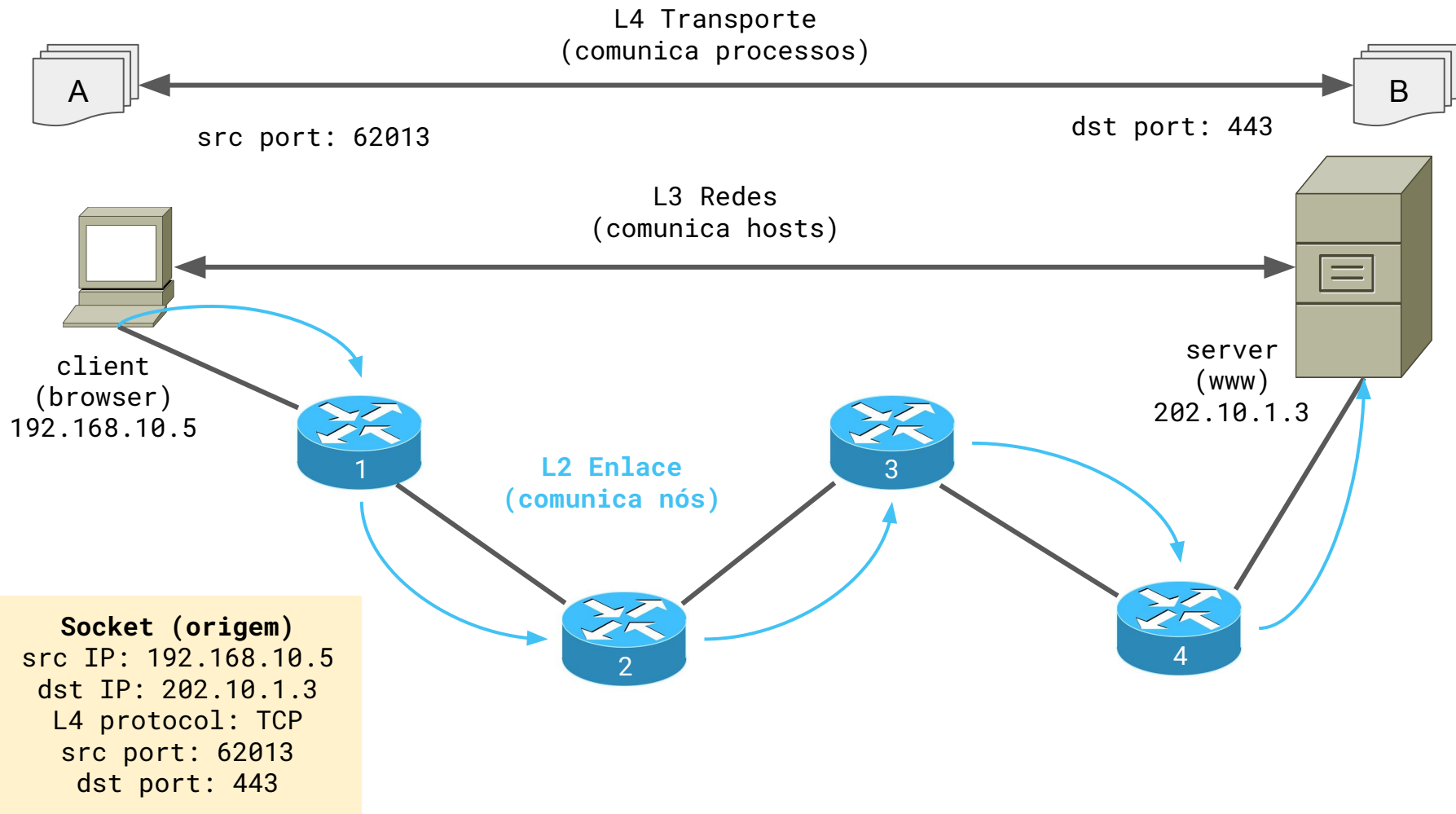
**Portas dinâmicas (private ports): de 49152 a 65535**

Essas portas podem ser utilizadas por qualquer serviço não registrado, uma vez que a IANA não pode registrar tais portas.

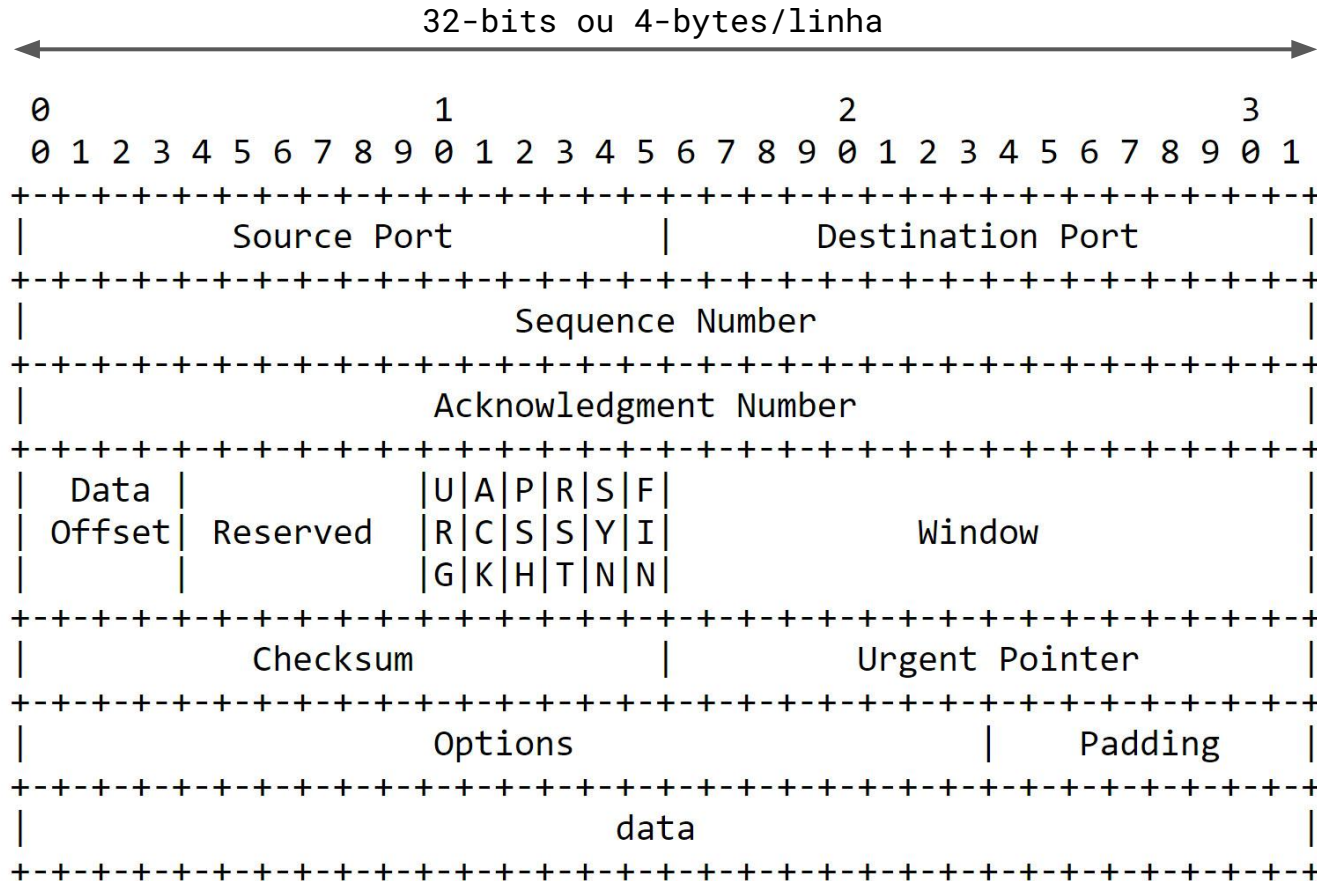
Uma porta é registrada quando a IANA atribui um emprego específico para ela.

# [7] Protocollo TCP

# Diferenças entre a Camada de Redes (L3) e a de Transportes (L4)





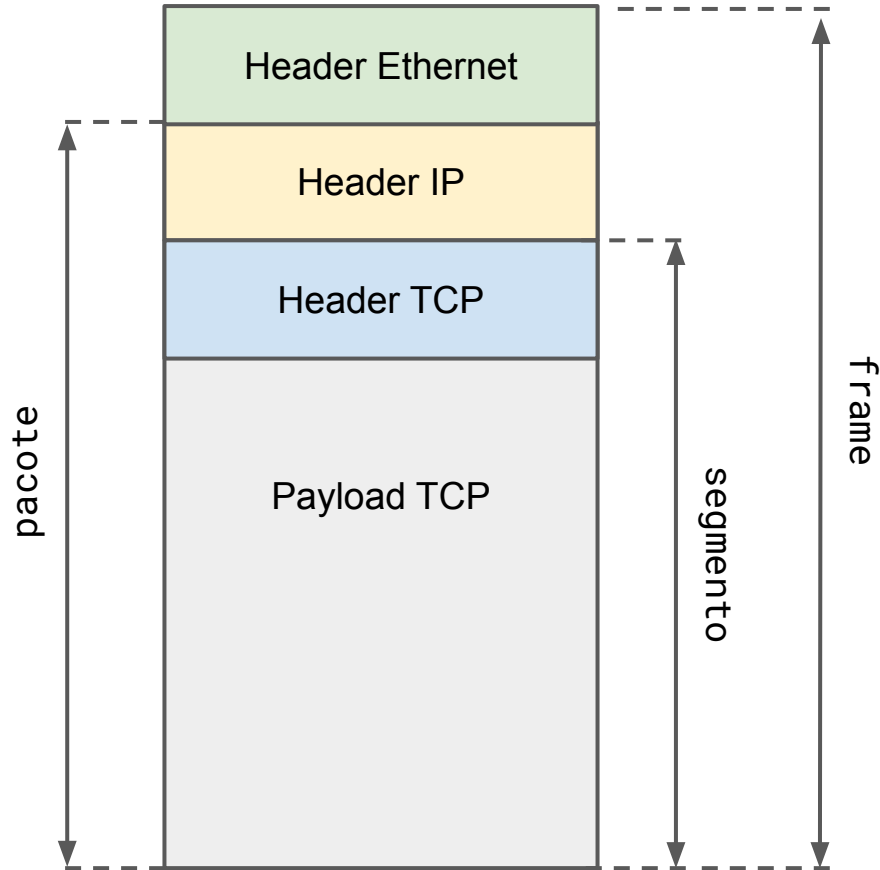


## Cabeçalho do Protocolo TCP, RFC 793

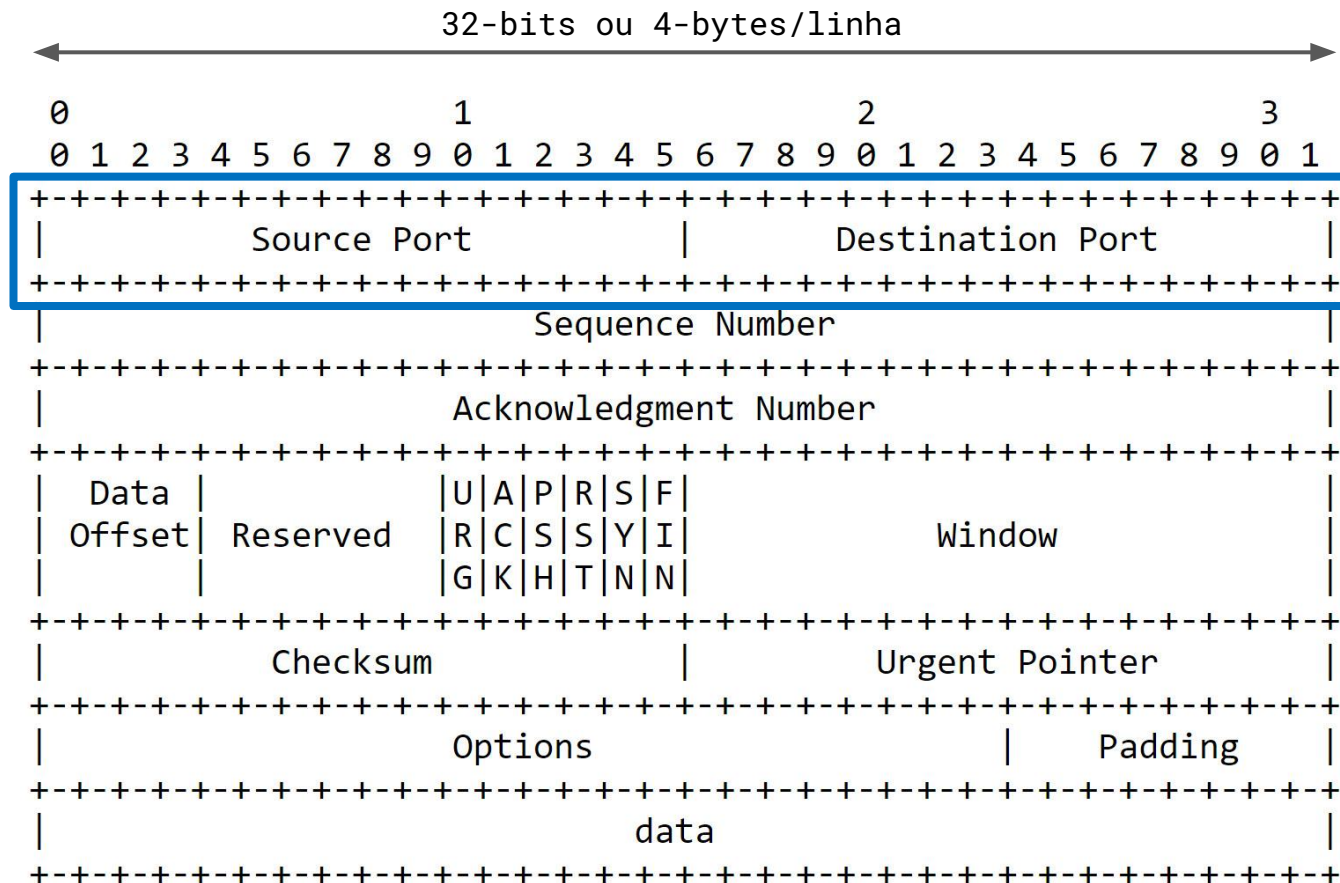
**MTU, Maximum Transmission Unit**

Ethernet Payload = 1500-bytes

Header + Payload = 1518-bytes



Ethernet (frames), se comunica por endereços MAC  
IP (pacotes/datagramas), comunica por endereços IP  
TCP (segmentos), comunicam por número de porta



## Cabeçalho do Protocolo TCP, RFC 793

# Campo Source/Destination Port

**Tamanho:** 16-bits

Porta de origem (16-bits) =  $2^{16}$  portas possíveis = 65.536

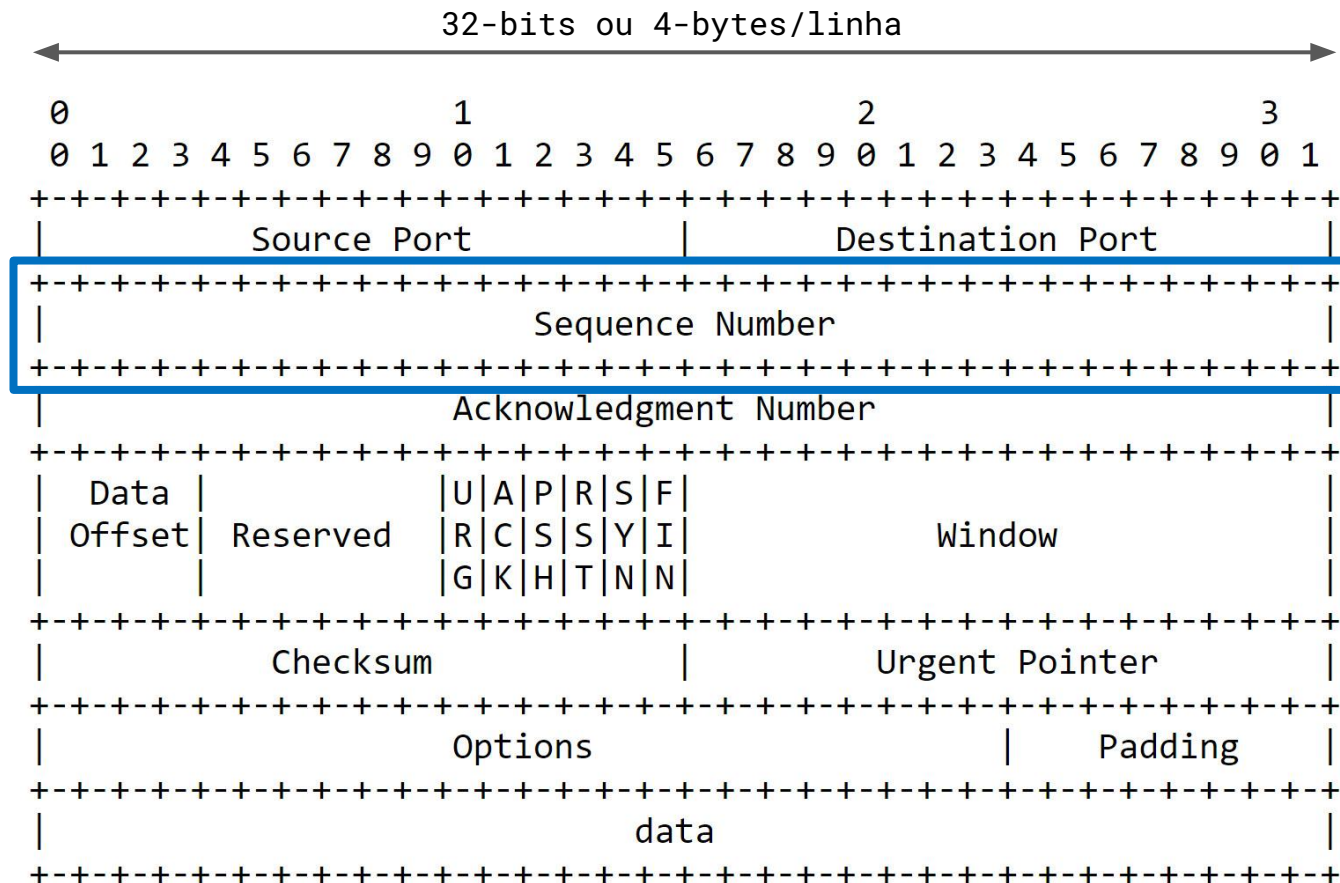
Porta de destino (16-bits) =  $2^{16}$  portas possíveis = 65.536

**Faixa de portas:** 1-65.535, a IANA reserva a porta 0.

**Função:** Identificar com qual porta o host está se comunicando no outro lado.

# Principais Portas TCP

NÚMERO DA PORTA	PROTOCOLO	APLICAÇÃO
20	TCP	FTP dados
21	TCP	FTP controle
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
80	TCP	HTTP (WWW)
110	TCP	POP3
443	TCP	SSL



**Cabeçalho do Protocolo TCP, RFC 793**

# Campo Sequence Number

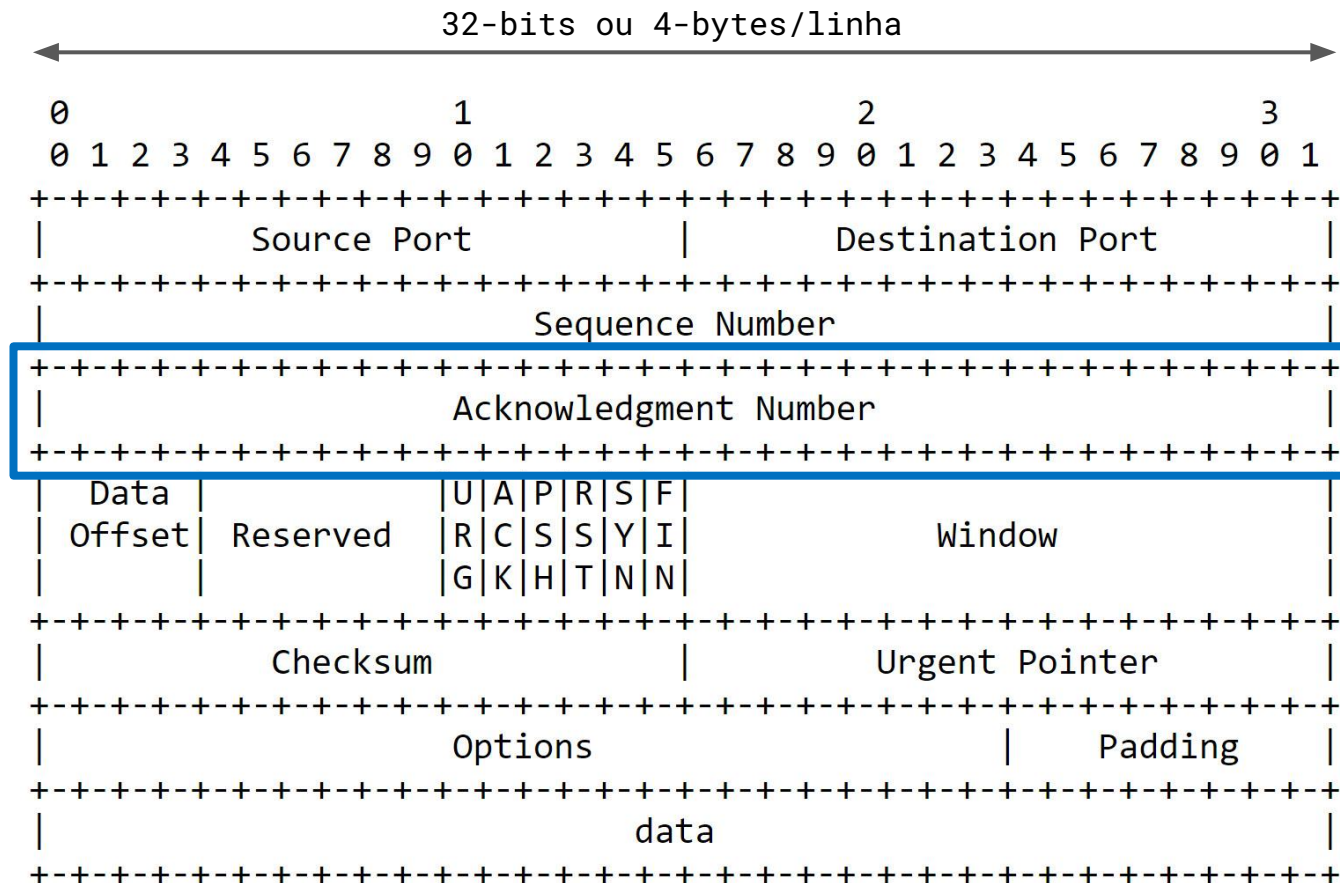
**Tamanho:** 32-bits

$2^{32}$  números possíveis (4.294.967.296 ~ bilhões)

**Faixa:** 0-4.294.967.295.

**Função:** Identificar qual o número de sequência do segmento. O TCP é confiável, garante a entrega do payload, por isso enumera os segmentos.

O primeiro número será aleatório, e o restante, sequencial.



**Cabeçalho do Protocolo TCP, RFC 793**



## Campo Acknowledgment ~ (ACK = confirmação/reconhecimento)

**Tamanho:** 32-bits

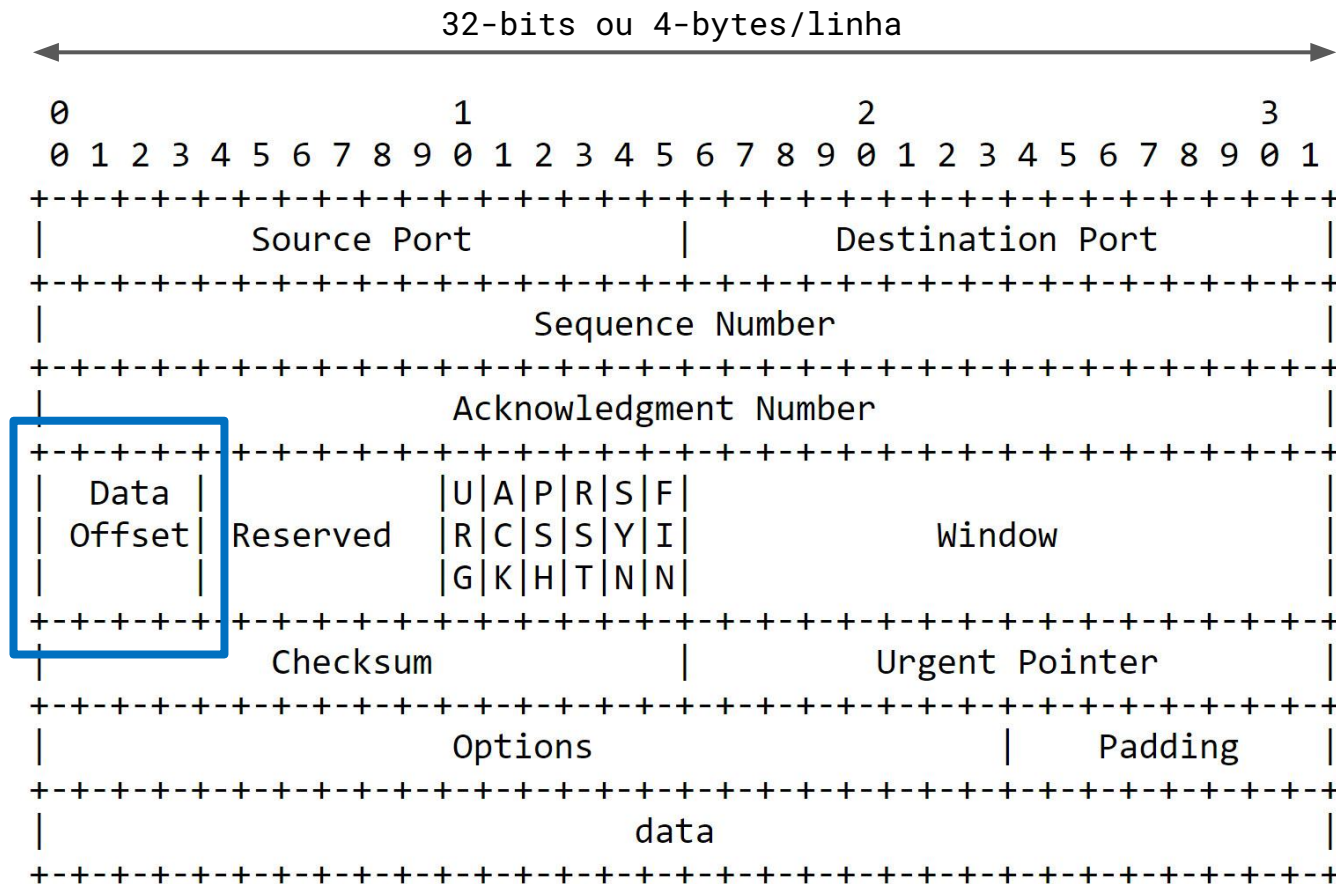
$2^{32}$  números possíveis (4.294.967.296 ~ bilhões)

Igual ao sequence number.

**Faixa:** 0-4.294.967.295.

**Função:** É usado para que o destinatário possa declarar que sabe qual será o próximo número da sequência a ser enviado pelo remetente. E, como consequência, está informando que recebeu o último segmento enviado pelo remetente.

Para calcular o ACK o destinatário precisa ter verificado o número da sequência e o tamanho do payload de tal segmento.



**Cabeçalho do Protocolo TCP, RFC 793**

# Campo Data Offset

**Tamanho:** 4-bits

$2^4$  números possíveis (16)

Igual ao IHL, no header IP.

**Faixa:** 0-15.

**Função:** Informar qts linhas de 32-bits o cabeçalho TCP possui.

Assim como no cabeçalho IP  
**mínimo 5 linhas** (20-bytes), **máximo 15 linhas** (60-bytes)  
IP + TCP ~ 40-bytes (mínimo)-120-bytes (máximo)

# Campo Window

**Tamanho:** 16-bits

$2^{16}$  números possíveis (65.536)

**Função:** Determina a quantidade máxima de bytes que o host poderá receber no próximo segmento TCP. Em outras palavras, determina qual espaço será alocado no buffer de recepção para o próximo segmento enviado pelo lado oposto.

```
21:23:42.975112 IP 192.168.1.180.43296 > 203.0.113.10.80:  
Flags [S], seq 3192956305, win 14600, options [mss  
1460,sackOK, TS val 7632203 ecr 0, nop, wscale 7], length 0
```

# Window Scale

RFC 1323, um novo campo opcional é definido no primeiro segmento SYN enviado pelo host.

O Window Scale é um valor que pode variar de 0 a 14.

Antes as máquinas ficavam limitadas a 64 KB por segmento.  
Após isso o limite passou a ser  $65535 \times 2^{14} = 1 \text{ GB}$  (aprox).

Em uma transmissão TCP, os Window Scales das duas máquinas envolvidas não precisam ser iguais.

# Campo Checksum

**Função:** Similar ao Checksum do IP, mas com a diferença que no TCP também realiza a conferência do conteúdo Payload. O TCP também adiciona a conferência um pseudocabeçalho IP.

Source Address		
Destination Address		
00	Protocol	TCP Length

Pseudocabeçalho IP

**Header TCP + Payload + Pseudocabeçalho IP**

# Campo Urgent Pointer

**Função:** É utilizado em conjunto com a flag URG, ou seja, só será lido se a flag URG estiver ativa. O objetivo é enviar informações que sejam urgentes para o tráfego na rede.

# Campo Options

**Tamanho:** até 40-bytes

**Função:** O campo options no TCP é bastante utilizado. Sempre que for necessário adicionar alguma funcionalidade ao TCP, bastará criar tal funcionalidade no Options, e documentar isso em uma RFC.

```
15:24:41.201429 IP 130.239.18.176.80 > 192.168.1.180.54925:  
Flags [P.], seq 3948095188:3948096636, ack 2705436037, win  
122, options [nop,nop, TS val 480142605 ecr 5503596], length  
1448
```



## Campo Padding

O campo Padding do TCP é idêntico ao Padding do IP.

Ele serve para preencher o fim do campo Options com zeros, caso isso seja necessário, a fim de tornar o tamanho de todo o cabeçalho TCP múltiplo de 4-bytes (32-bits).

# Características do TCP

FUNÇÃO	DESCRIÇÃO
Multiplexing usando-se portas	Função que permite que os hosts que estão recebendo dados escolham o aplicativo correto para o qual os dados se destinam, com base no número da porta.
Recuperação de erros (confiabilidade)	Processo de se numerar e reconhecer dados com os campos sequência e reconhecimento do cabeçalho.
Controle de fluxo e o uso do janelamento (windowing)	Processo que usa tamanhos de janela para proteger o espaço de buffer e os dispositivos de roteamento.
Estabelecimento e término de conexão	Processo usado para se inicializar números de portas e campos de sequência e reconhecimento.
Transferência ordenada de dados e segmentação	Fluxo conjunto de bytes vindo de um processo da camada superior que é “segmentado” para transmissão e entregue aos processos da camada superior no dispositivo receptor, com os bytes na mesma ordem.

# 3-way handshake do Protocolo TCP

# Principais Portas TCP

NÚMERO DA PORTA	PROTOCOLO	APLICAÇÃO
20	TCP	FTP dados
21	TCP	FTP controle
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
67, 68	UDP	DHCP (Server, Client)
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL

fonte: Wikipedia

A IANA define as portas em três categorias:

<http://www.iana.org/assignments/port-numbers>

**Portas de sistema (well known ports): de 0 a 1023**

Essas portas não devem ser utilizadas em serviços de rede sem um prévio registro na IANA.

Serão utilizadas apenas por serviços inicializados pelo sistema, pelo administrador do sistema ou por usuários privilegiados.

**Portas de usuário (registered ports): de 1024 a 49151**

Essas portas não devem ser utilizadas em serviços de rede sem um prévio registro na IANA.

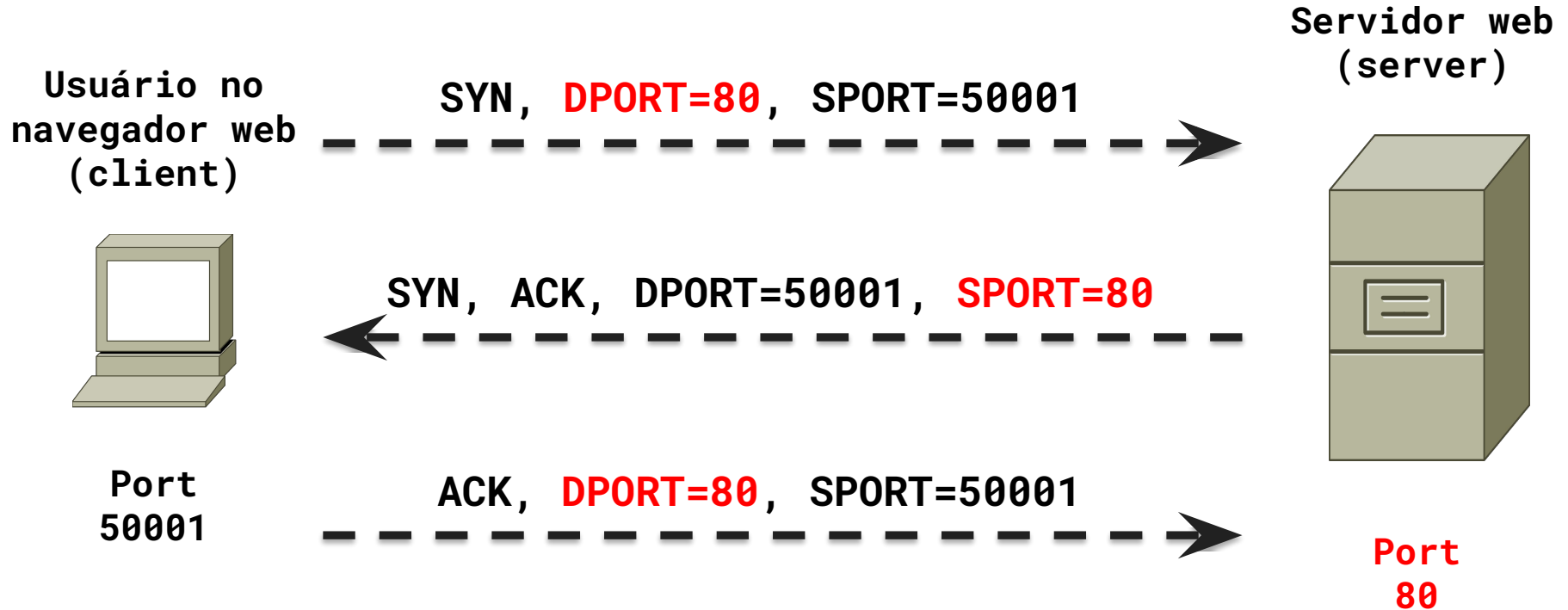
A diferença é que essas portas podem ser utilizadas por serviços inicializados e gerenciados por usuários comuns do sistema, em vez de administradores.

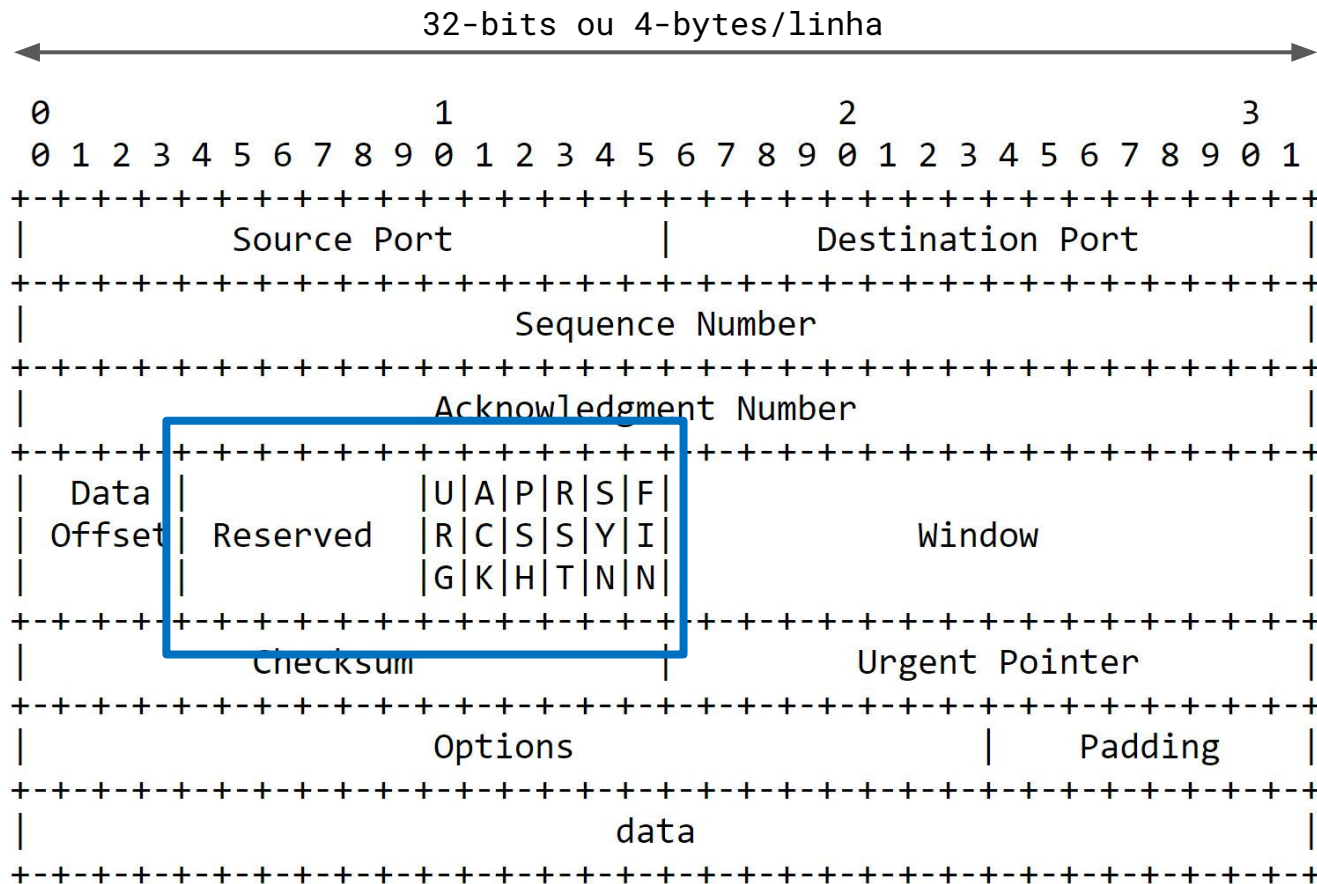
**Portas dinâmicas (private ports): de 49152 a 65535**

Essas portas podem ser utilizadas por qualquer serviço não registrado, uma vez que a IANA não pode registrar tais portas.

Uma porta é registrada quando a IANA atribui um emprego específico para ela.

## three-way handshake connection





## Cabeçalho do Protocolo TCP, RFC 793

# Flags TCP

Através das flags o TCP exerce controle no fluxo de informação.

**Tamanho:** 12-bits

4 bits reservados + <sup>(5)</sup>CWR + <sup>(6)</sup>ECE + <sup>(7)</sup>URG + 8-12 bits

└──────────┘  
Explicit Congestion  
Notification (ECN),  
ligados ao QoS.  
Mas nem todos os equip.  
entendem.

└──────────┘  
├── (8) ACK, acknowledgment  
├── (9) PSH, push  
├── (10) RST, reset  
├── (11) SYN, synchronize  
└── (12) FIN, finish



## **ACK, ou acknowledgment (confirmando/reconheço)**

A flag mais empregada.

Serve para que o lado que recebeu o segmento confirme, para quem o enviou, que sabe qual será o número da sequência do próximo segmento.

## **PSH, ou push (empurrar)**

Serve para sinalizar que há dados no payload do segmento TCP.

## **RST, ou reset (reiniciar)**

Serve para sinalizar que “não entendi”.

## **SYN, ou synchronize (sincronize)**

Usada para iniciar uma conexão. O protocolo TCP precisa abrir conexão nos dois sentidos (cliente/servidor, primeiro, e depois servidor/cliente) antes de iniciar o fluxo de mensagens.

## **FIN, ou finish (finalizar)**

Usada para finalizar uma conexão - “não tenho mais o que enviar”.

A conexão será fechada nos dois sentidos. Tanto cliente quanto servidor podem finalizar primeiro.

1. 19:07:36.214300 IP 192.168.1.180.33115 > 192.168.1.100.80:  
Flags [S], seq 4094690724, win 14600, options [mss 1460,sackOK,TS val 1606263 ecr 0,nop,wscale 7], length 0
2. 19:07:36.214480 IP 192.168.1.100.80 > 192.168.1.180.33115:  
Flags [S.], seq 394810791, ack 4094690725, win 14480, options [mss 1460, sackOK,TS val 428943567 ecr 1606263,nop,wscale 5], length 0
3. 19:07:36.214514 IP 192.168.1.180.33115 > 192.168.1.100.80:  
Flags [.), ack 394810792, win 115, options [nop,nop,TS val 1606263 ecr 428943567], length 0
4. 19:07:36.267058 IP 192.168.1.180.33115 > 192.168.1.100.80:  
Flags [P.), seq 4094690725:4094691097 ack 394810792, win 115, options [nop,nop,TS val 1606276 ecr 428943567], length 372
5. 19:07:36.267279 IP 192.168.1.100.80 > 192.168.1.180.33115:  
Flags [.), ack 4094691097, win 486, options [nop,nop,TS val 428943580 ecr 1606276], length 0

# Janelamento & Controle de Fluxo do Protocolo TCP

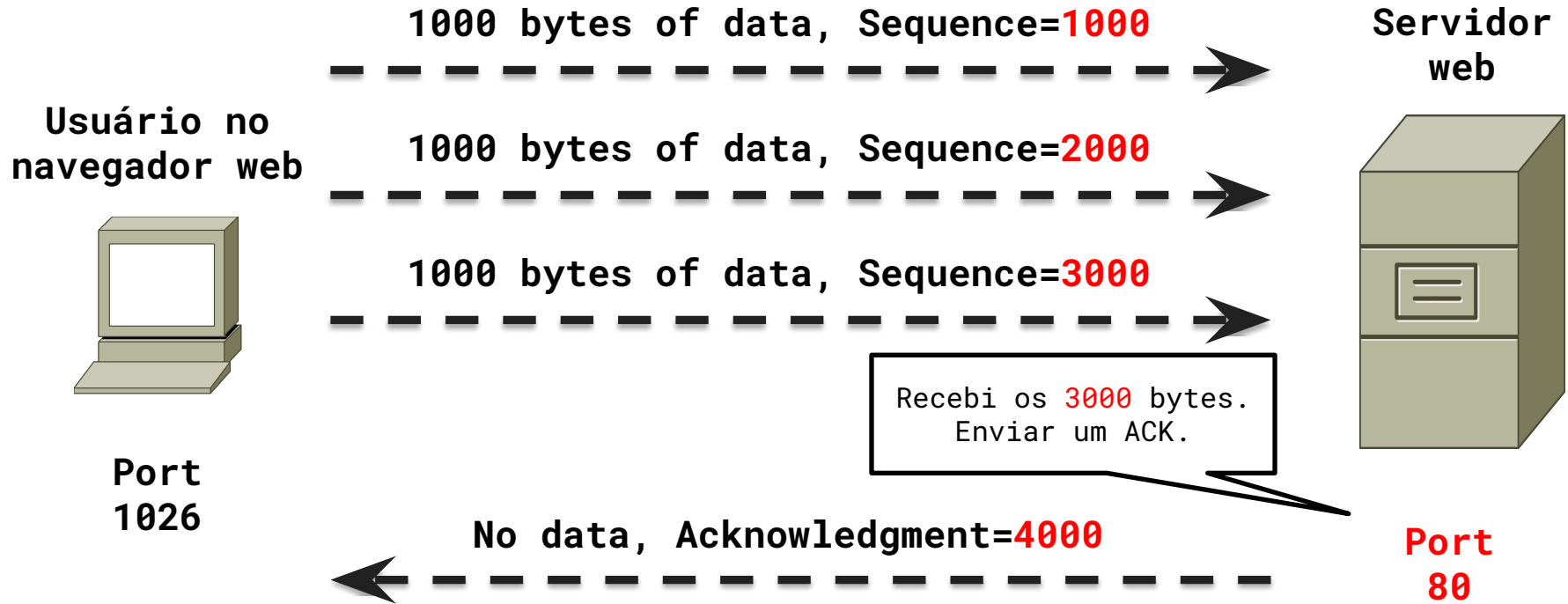
# Sliding Window

**Função:** É um protocolo de transmissão de dados que permite o envio de vários segmentos em série, sem a necessidade de confirmação individual.

A ideia central é ter uma janela (Window) predefinida com um determinado tamanho. Com base nesse tamanho, poderão ser enviados vários segmentos PSH em série, sendo que haverá a confirmação apenas do último deles. Isso indicará que os anteriores também foram recebidos. Assim, a conexão ganhará extrema agilidade e a velocidade final de transferência de dados será bem maior.

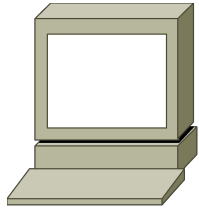
1. 15:24:41.201429 IP 130.239.18.176.80 >  
192.168.1.180.54925: Flags [P.], seq  
3948095188:3948096636, ack 2705436037, win 122, options  
[nop,nop, TS val 480142605 ecr 5503596], length 1448
2. 15:24:41.202736 IP 130.239.18.176.80 >  
192.168.1.180.54925: Flags [P.], seq  
3948096636:3948098084, ack 2705436037, win 122, options  
[nop,nop, TS val 480142605 ecr 5503596], length 1448
3. 15:24:41.202760 IP 192.168.1.180.54925 >  
130.239.18.176.80: Flags [.], ack 3948098084, win 8937,  
options [nop,nop, TS val 5503710 ecr 480142605], length 0

# RECUPERAÇÃO DE ERROS E CONFIABILIDADE

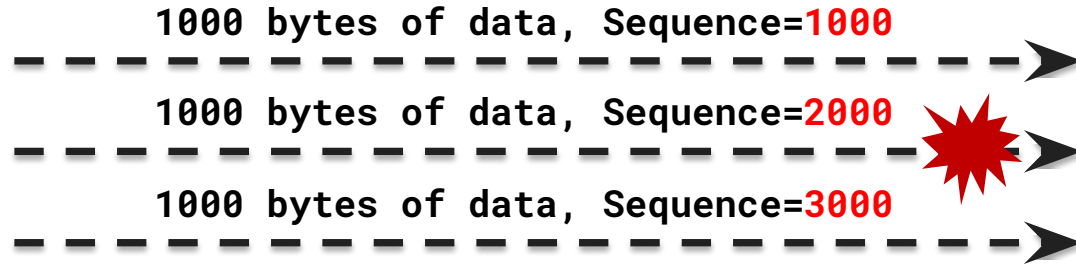


# RECUPERAÇÃO DE ERROS E CONFIABILIDADE

Usuário no navegador web



Port  
1026



Recebi 1000-1999 & Recebi 3000-3999.  
Solicitar o 2000 a seguir!

No data, Acknowledgment=2000

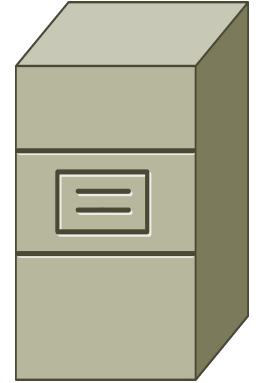
Ele perdeu o segmento SEQ=2000.  
Reenviar!

1000 bytes of data, Sequence=2000

Recebi 2000-2999 & tenho 3000-3999.  
Solicitar o 4000 a seguir!

No data, Acknowledgment=4000

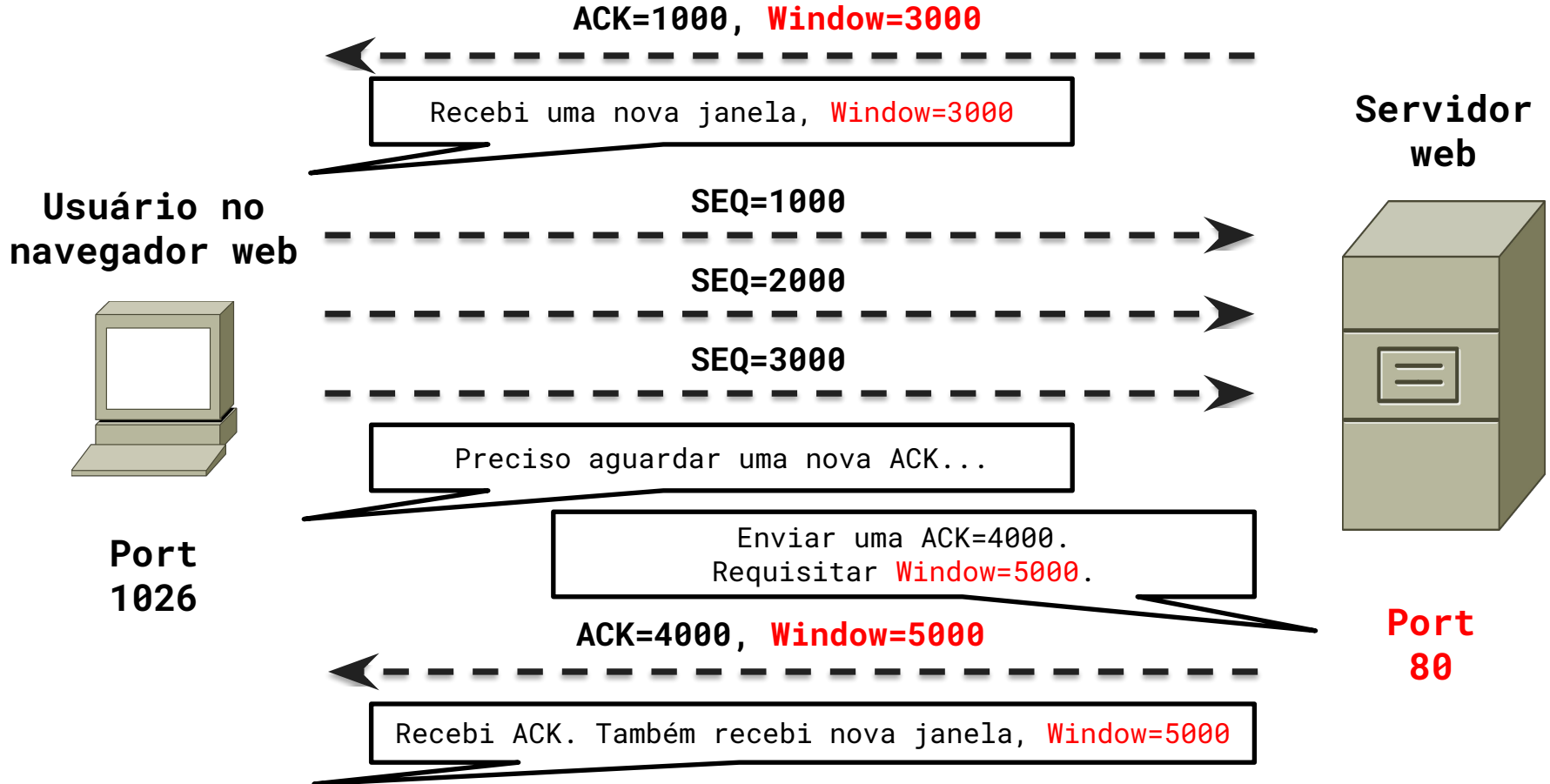
Servidor web



Port  
80



# CONTROLE DE FLUXO USANDO JANELAMENTO



# [8] Protocollo UDP

# UDP (User Datagram Protocol)

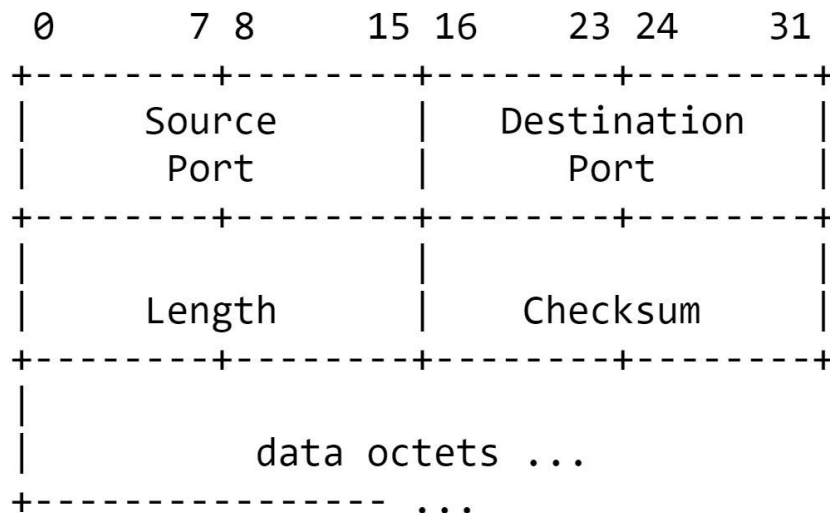
O UDP é um **protocolo de transporte sem conexão** (não há numeração de sequência, nem mecanismos de estabelecimento/término de conexão) **e não-confiável** (sem controle de fluxo e erros).

Ele não adiciona nenhum controle adicional aos serviços de entrega do IP, exceto pelo fato de implementar a **comunicação entre processos**, ao invés da comunicação entre hosts.

# Portas Conhecidas UDP

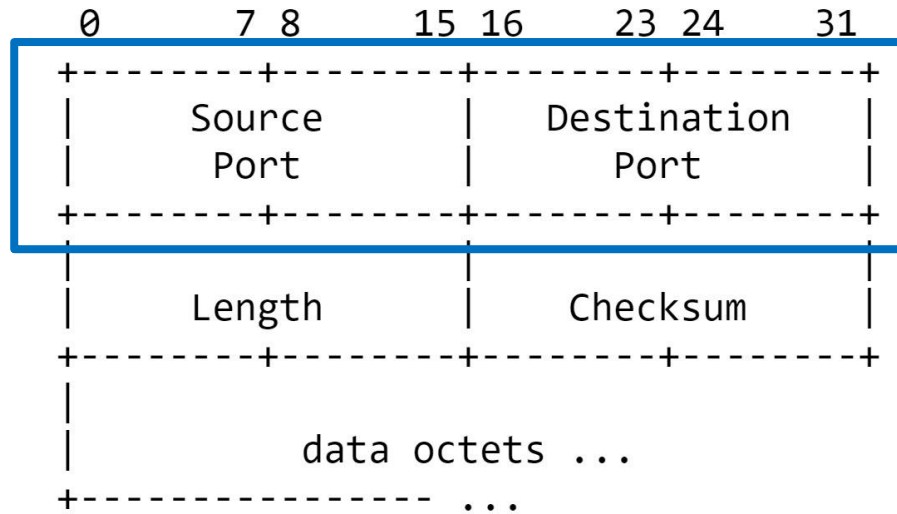
NÚMERO DA PORTA	PROTOCOLO	APLICAÇÃO
53	TCP/UDP	DNS
67, 68	UDP	DHCP (Server, Client)
69	UDP	TFTP, Trivial File Transfer Protocol
123	UDP	NTP, Network Time Protocol
161	UDP	SNMP, Simple Network Management Protocol
162	UDP	SNMP, Simple Network Management Protocol (trap)

# UDP, User Datagram Protocol [RFC 768]



- Linhas de 32-bits ou 4-bytes
- Cabeçalho em tamanho fixo de 8-bytes
- Trafega dentro de um pacote IP

# Campo Source & Destination Port

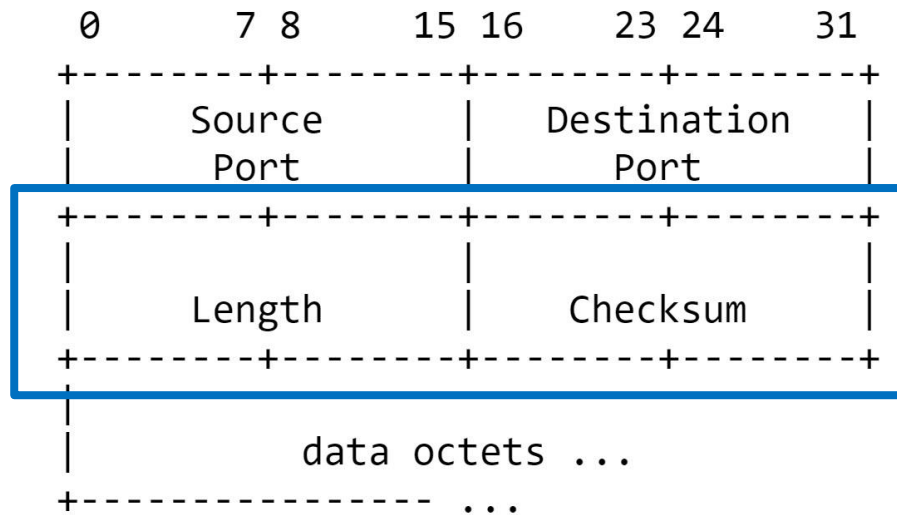


## Campos obrigatórios

Porta de origem (16-bits) =  $2^{16}$  portas possíveis = 65.536 portas

Porta de destino (16-bits) =  $2^{16}$  portas possíveis = 65.536 portas

# Campo Source & Destination Port



- **Length.** O tamanho total do segmento UDP, em bytes (16-bits).
- **Checksum.** É calculado de forma idêntica ao TCP. É opcional.

# Tráfego UDP

1. 09:52:30.388231 IP 198.51.100.249.49355 > 192.168.1.180.21463: UDP, length 115
2. 09:52:30.405975 IP 192.168.1.180.21463 > 198.51.100.249.49355: UDP, length 92
3. 09:52:30.409270 IP 198.51.100.249.49355 > 192.168.1.180.21463: UDP, length 102
4. 09:52:30.430316 IP 198.51.100.249.49355 > 192.168.1.180.21463: UDP, length 98
5. 09:52:30.446434 IP 192.168.1.180.21463 > 198.51.100.249.49355: UDP, length 90
6. 09:52:30.450862 IP 198.51.100.249.49355 > 192.168.1.180.21463: UDP, length 111
7. 09:52:30.466729 IP 198.51.100.249.49355 > 192.168.1.180.21463: UDP, length 105
8. 09:52:30.486880 IP 192.168.1.180.21463 > 198.51.100.249.49355: UDP, length 93

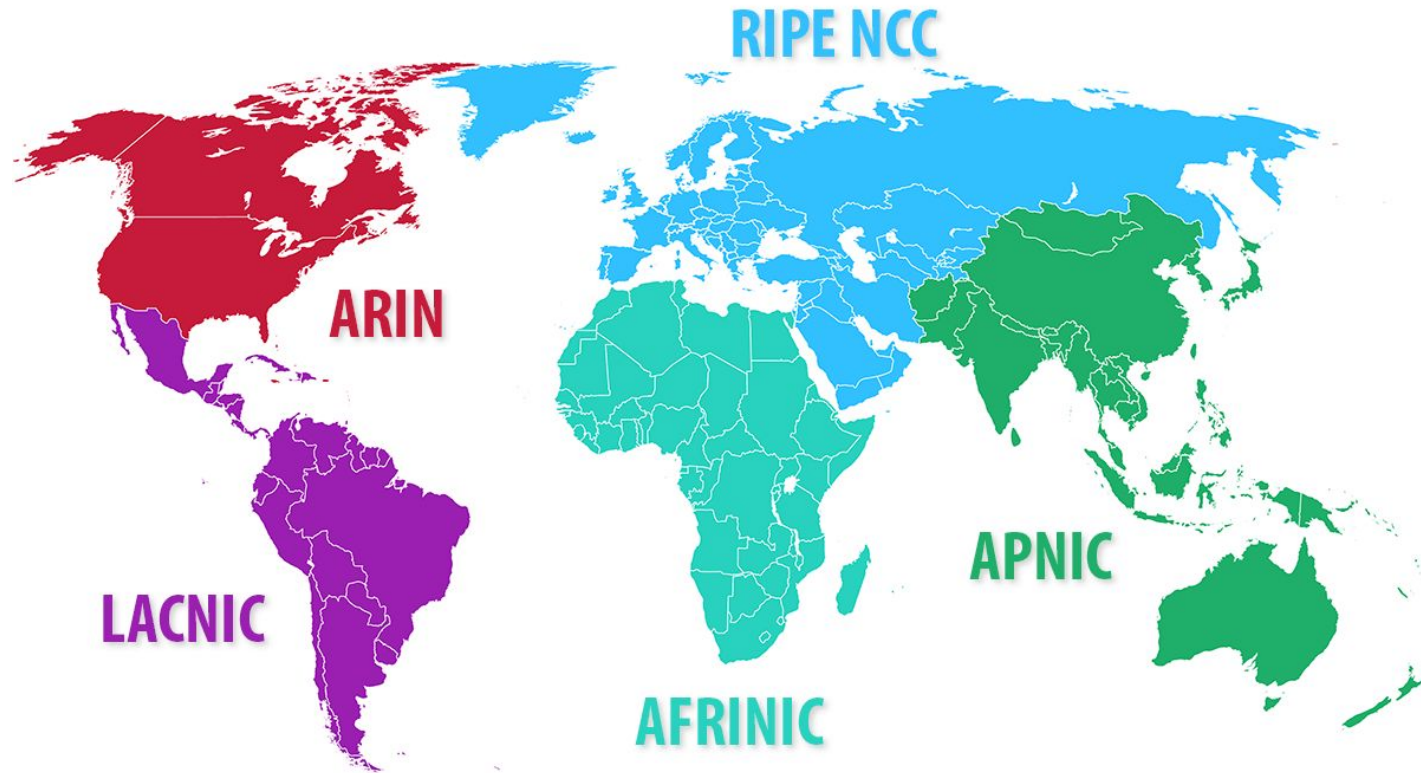


# Considerações gerais sobre o UDP

- Grande velocidade de tráfego em razão de possuir poucos controles.
- Necessita de controle adicional por parte de aplicação que o emprega.
- Não é confiável, pois não garante a conexão nem a entrega de dados.
- Não é orientado à conexão, pois não realiza o three-way handshake.
- Não faz controle de fluxo (janelamento), ou erros (confirmações).
- O UDP é utilizado por aplicações que precisam de mais velocidade e menos controle. Nisso se enquadram bem os tráfegos de voz, áudio e vídeo.
- É usado em alguns protocolos como o DNS (53), DHCP (67-68), TFTP (69) e SNMP (161-162).

# [9] Endereços Públicos e Privados

# Espaços de Endereçamento



Latin American and Caribbean Network Information Centre  
<http://www.lacnic.net>, RIR da América Latina

# Distribuição de Endereços IP válidos

## RIR, Regional Internet Registry

As faixas de IP distribuídas mundialmente estão disponíveis no site da IANA nas seguintes URLs:

IPv4: <http://www.iana.org/assignments/ipv4-address-space>

IPv6: <http://www.iana.org/assignments/ipv6-address-space>

# Endereços Privados

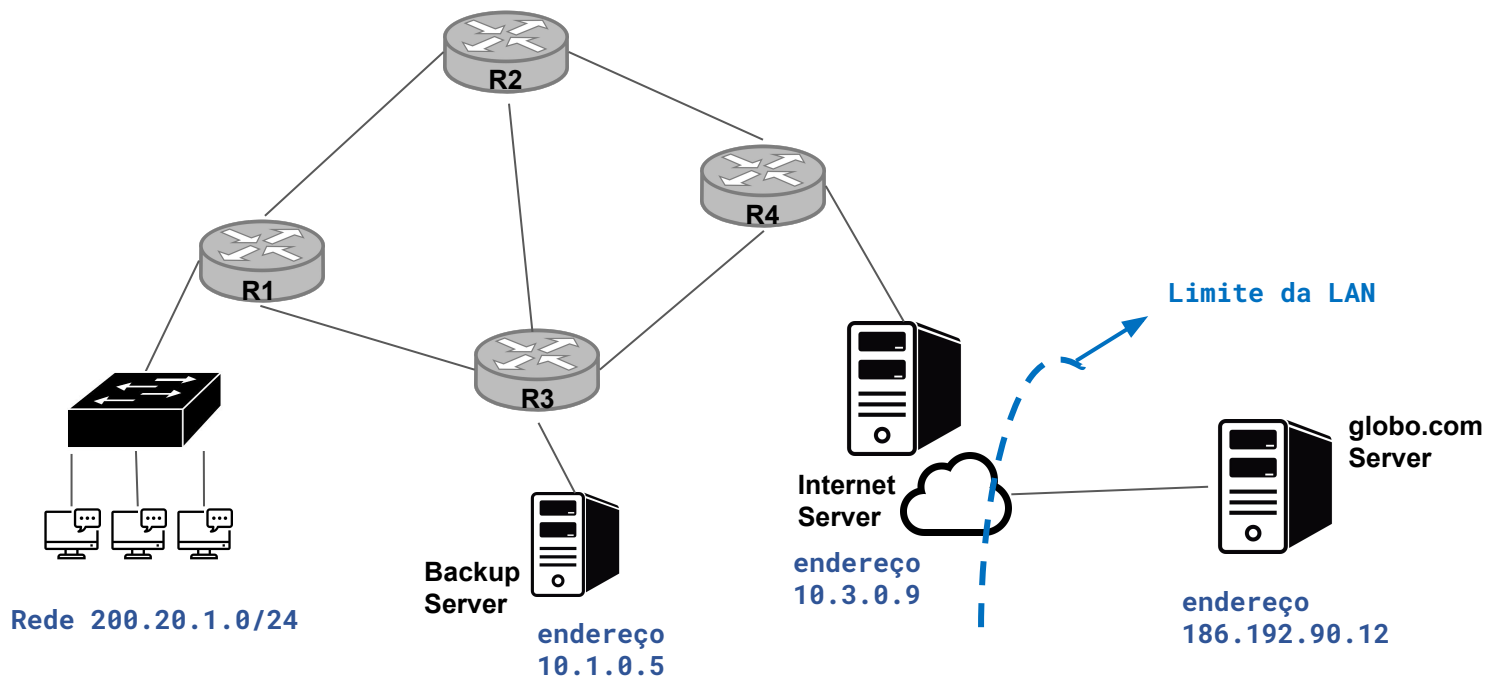
Classe	Faixa de Endereçamento Privado	Número de redes
A	10.0.0.0 - 10.255.255.255 (ou 10.0.0.0/8)	1
B	172.16.0.0 - 172.31.255.255 (ou 172.16.0.0/12)	16
C	192.168.0.0 - 192.168.255.255 (ou 192.168.0.0/16)	256

Faixas de Endereçamento Privado, RFC 1918

- Isola uma parte da rede para que não tenha acesso à Internet;
- Evita o esgotamento dos endereços IPv4;
- Reduz o tamanho da tabela de roteamento dos roteadores na Internet.

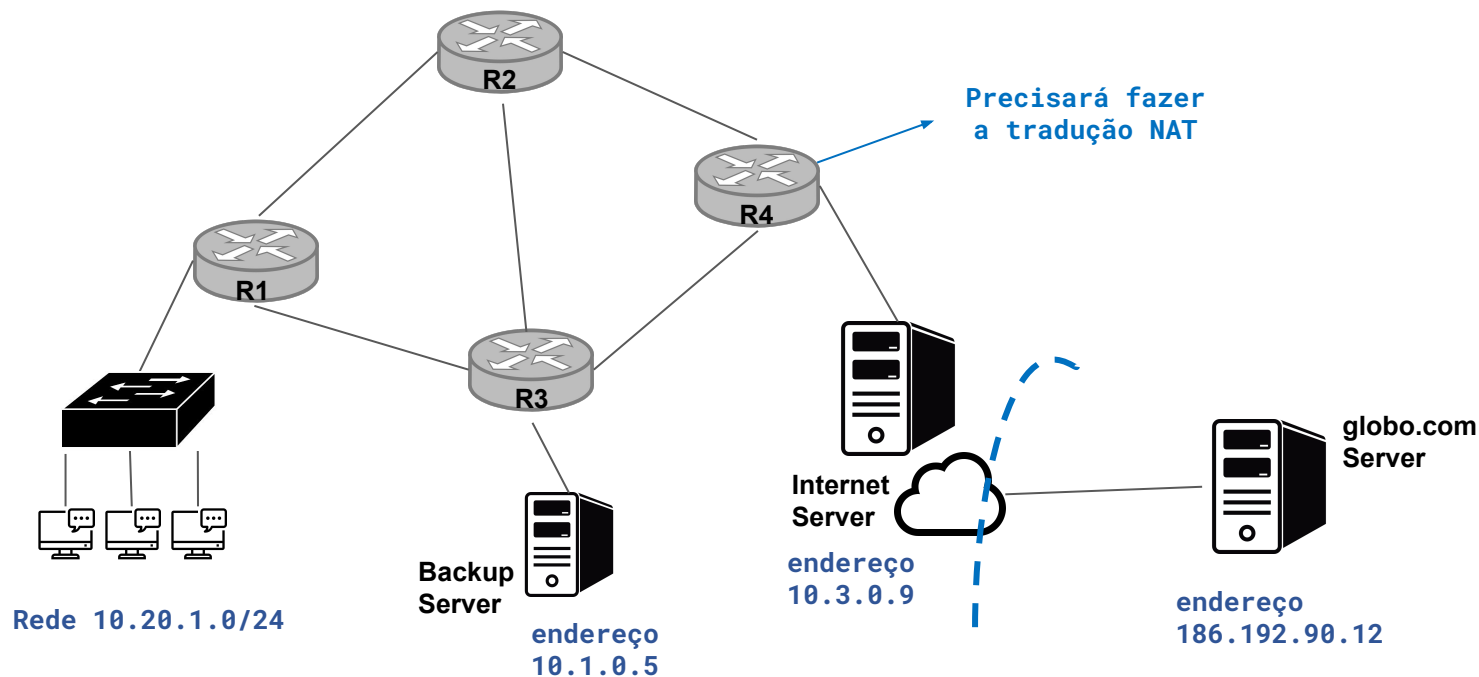
# Endereços Públicos

- Devem ser registrados pela empresa/entidade junto a IANA/RIR e autoridade local, NIC.br (no caso do Brasil).
- São '**roteáveis**' na Internet.
- São **escassos**, estão esgotados na maior parte do mundo.



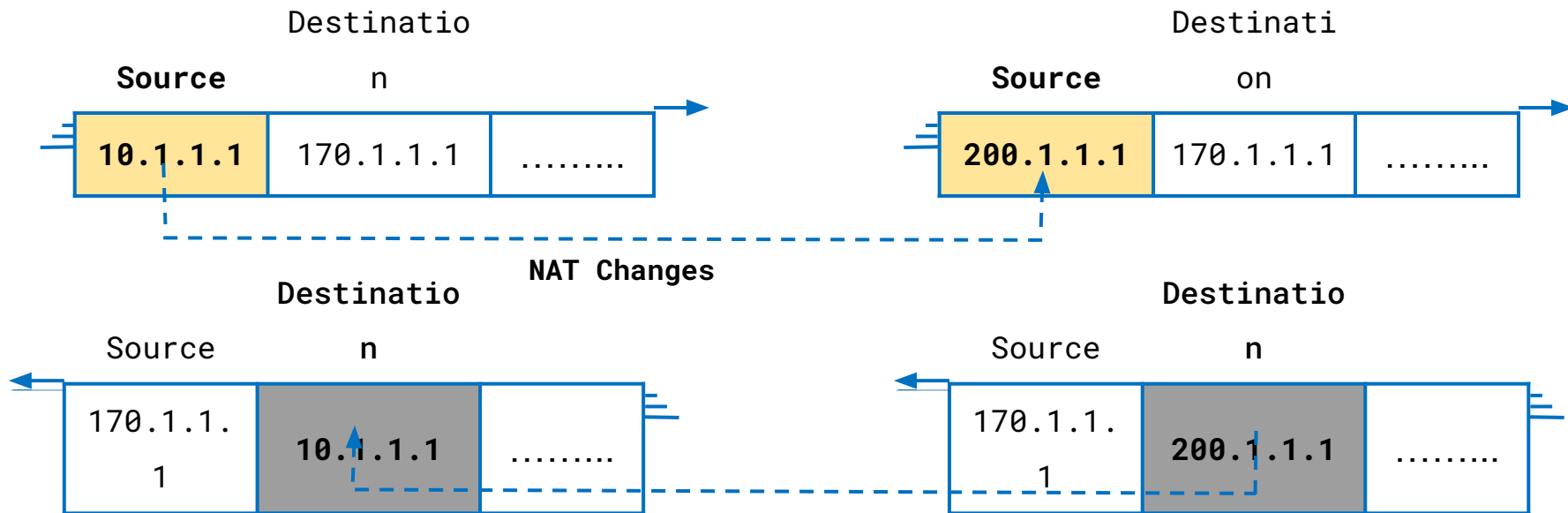
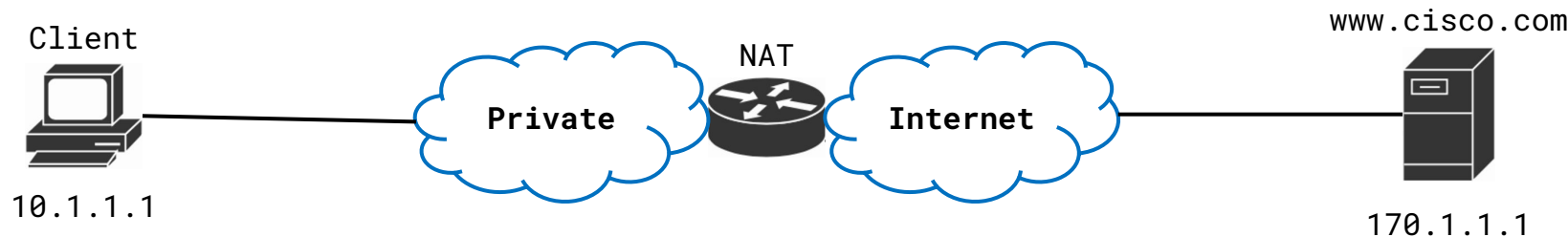
# Endereços Privados

- Podem ser usados **sem registro** em qualquer LAN.
- **Não são roteáveis** na Internet.
- Podem existir milhões de **redes iguais em cada LAN**.
- Necessitam do **recurso NAT** para serem utilizados na Internet.

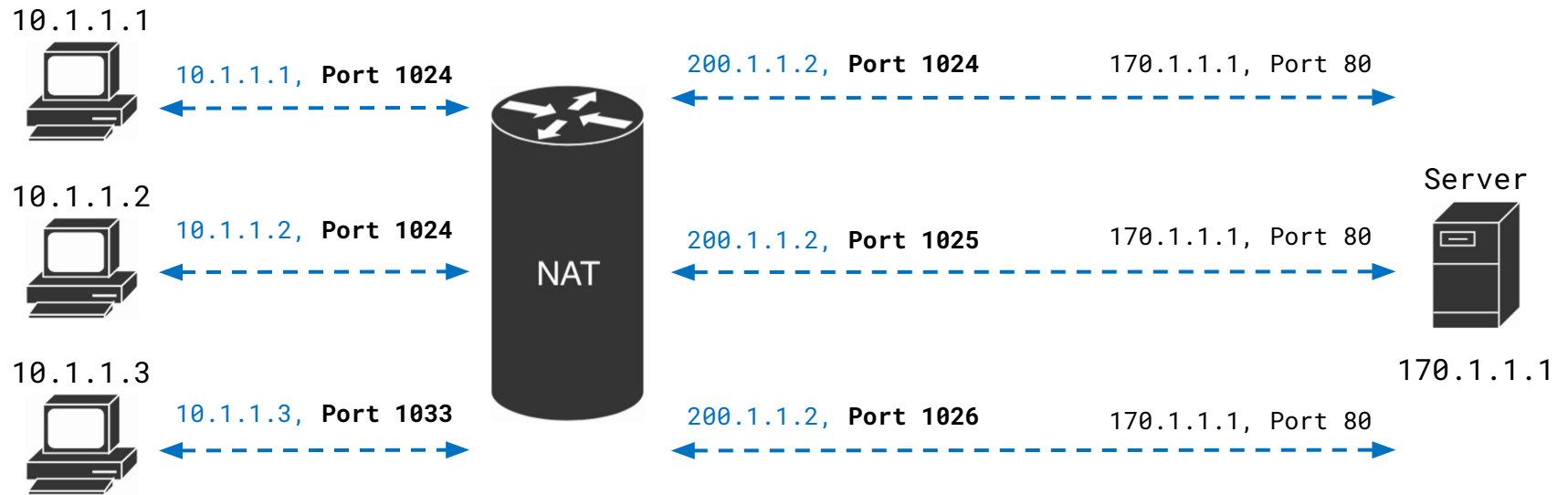


# Network Address Translation (NAT)

## Tradução de Endereços de Rede







Inside Local	Inside Global
10.1.1.1: 1024	200.1.1.2: 1024
10.1.1.2: 1024	200.1.1.2: 1025
10.1.1.3: 1033	200.1.1.2: 1026

Dynamic NAT Table, With Overloading

# REDES DE COMPUTADORES

## CURSO TÉCNICO DE INFORMÁTICA

### Tradução de endereços de rede (NAT) - Teoria



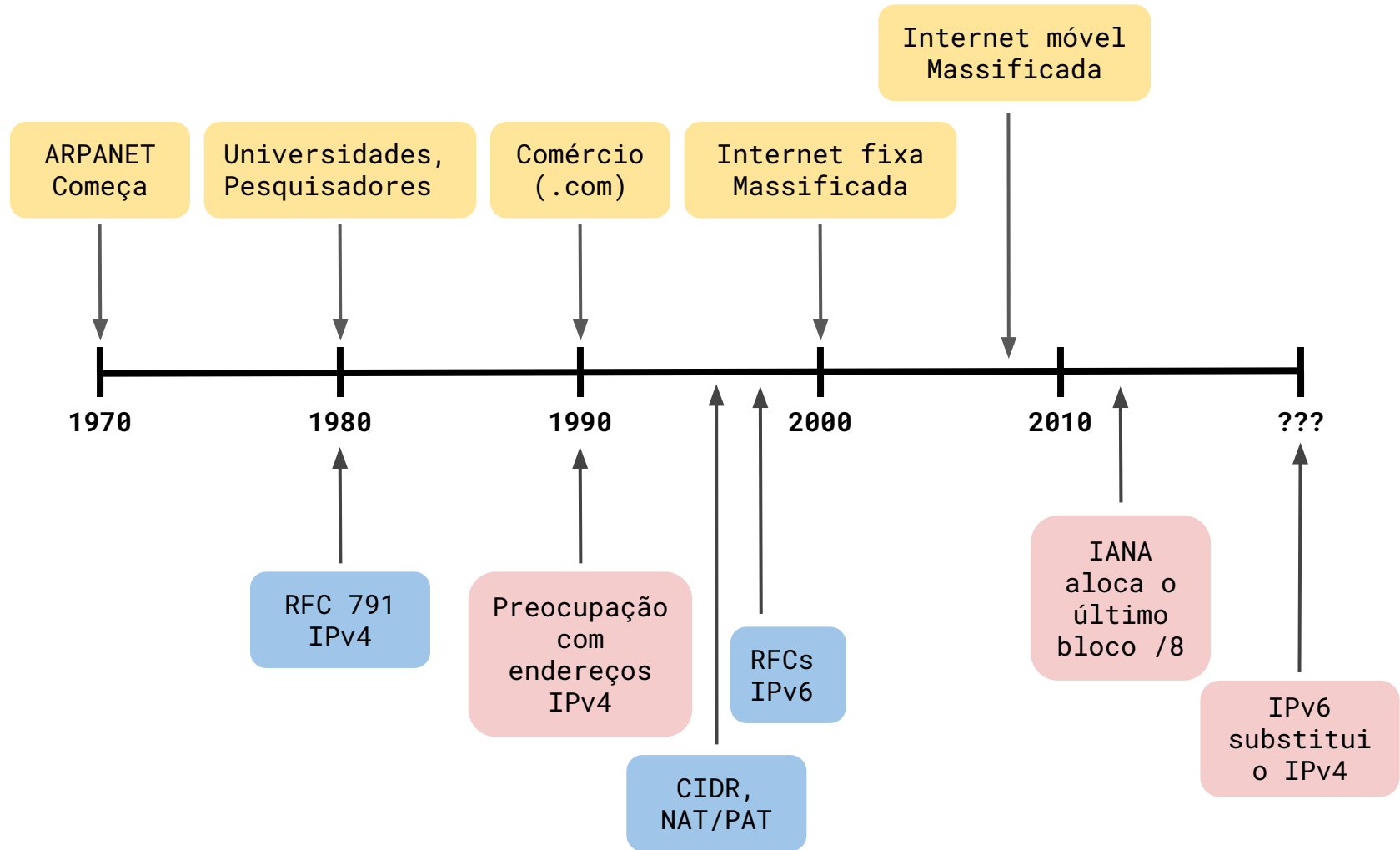
**INSTITUTO FEDERAL**  
Rio Grande do Norte  
Campus EaD

# Exercícios de Fixação 15

Explique para que são usados e defina as faixas de endereçamentos privados de classe A, B e C.

# Fundamentos do IPv6

# Linha do tempo do esgotamento de endereços IP



## Esgotamento de Endereços IPv4

RIR (Regional Internet Registries)	Região de Atuação	Projeção de Esgotamento
APNIC	Ásia e Pacífico	19/04/2011
RIPENCC	Europa	29/02/2012
LACNIC	América Latina	19/03/2014
ARIN	América do Norte	26/05/2014
AFRINIC	África	31/07/2020

# Comparativo IPv4 & IPv6

IPv4, 32-bits ~ 4B endereços

Endereços normalmente escritos em decimal.

Máscaras escritas em notação decimal ou barramento.

Podem ter classe cheia ou não ter classe.

IPv6, 128-bits ~ 340 undecilhões de endereços

Endereços normalmente escritos em hexadecimal.

~~Máscaras~~ (prefixo) escritas em notação de barramento apenas.

Não possuem classe nunca.

## Por que a transição para IPv6 demora tanto a se consolidar?

- Equipamentos
- Impacta outros protocolos
  - RIPv2 = RIPv6 (Routing Information Protocol next generation)
  - OSPFv2 = OSPFv3 (Open Shortest Path First)
  - BGP = BGP-4 (Border Gateway Protocol)
  - ICMP = ICMPv6 (Internet Control Message Protocol)
  - ARP = NDP (Neighbor Discovery Protocol)
- Conhecimento técnico dos profissionais



# Exercícios de Fixação 11

Com que finalidade foi criado o IPv6?

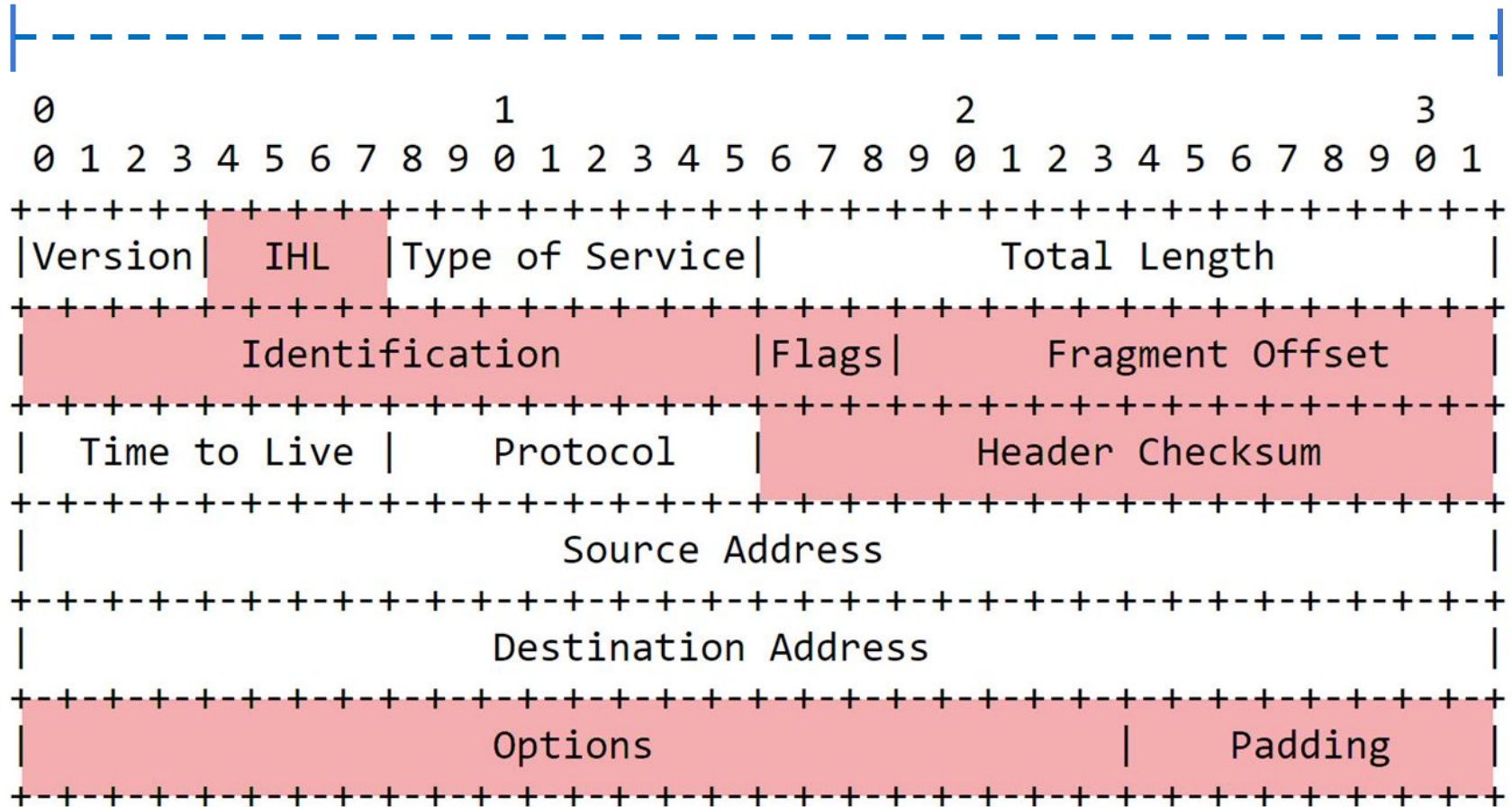
# Exercícios de Fixação 12

Explique o porquê da rede IPv4 não ter transacionado completamente para IPv6.

# Protocolos de Roteamento do IPv6

Protocolo de Roteamento	Definido por	Nota
RIPng (next generation)	RFC	A próxima geração do RIP para IPv6.
OSPFv3	RFC	A nova versão do OSPFv2 para operar com IPv6.
EIGRPv6	Cisco	O protocolo proprietário da Cisco para IPv6.
MP BGP-4	RFC	Multiprotocol BGP version 4, para IPv6.

4-bytes



RFC 791. IPv4

# Header IPv6

4-bytes

Version (4-bits)	Traffic Class (8-bits)	Flow Label (20-bits)	
Payload Length (16-bits)		Next Header (8-bits)	Hop Limit (8-bits)
Source Address (128-bits) 16-bytes			
Destination Address (128-bits) 16-bytes			

40-bytes

## IPv4 (12 campos fixos)

- IHL (header entre 20-bytes e 60-bytes)
- Identification + Flags + Fragment Offset
- Header Checksum
- Options + Padding

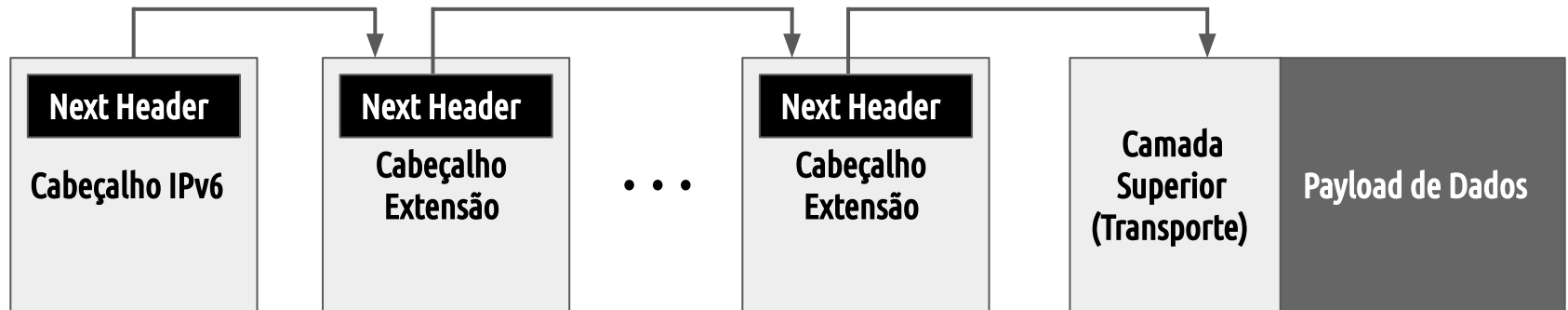
## IPv6 (8 campos fixos)

- header (fixo) 40-bytes
- Payload Length = Total Length
- Traffic Class + Flow Label = Type of Service
- Hop Limit = TTL
- Next header = apontador para próximo cabeçalho.

Cumpre diversas funções

## Next header

- Hop-by-hop
- Destination Options
- Routing
  - IPv4 = Options + Padding
- Fragmentation
  - IPv4 = Identification + Flag + Fragment Offset
- AH + ESP
  - AH (Authentication Header), RFC 2402
  - ESP (Encapsulating Security Header), RFC 2406



# Notação do endereço IPv6 em binário e hexadecimal

001000000000000010000011011011100011000001000111100000000000000000100011100111000000000000000001111011101110111000100001010101100

2001 : 0DB8 : C11E : 0000 : 8E70 : 0000 : FEEE : 10AC

8 quartetos hexadecimais

128-bits = 32-hex

Os endereços podem ser escritos em letras maiúsculas ou minúsculas.

2001:0DB8:C11E:0000:8E70:0000:FEEE:10AC

=

2001:0db8:c11e:0000:8e70:0000:feee:10ac



Hex	Binário	Hex	Binário
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

# Abreviação do IPv6

Duas regras básicas permitem reduzir ou abreviar um endereço IPv6:

1. Dentro de cada quarteto de quatro dígitos hex, **remova os 0s à esquerda do quarteto**. Um quarteto **0000** será escrito apenas como **0**.
2. Encontre **uma linha de dois ou mais quartetos exclusivamente de hex 0s** e substitua esse grupo de quartetos por **dois dois-pontos (::)**. O **::** significa “dois ou mais quartetos de apenas 0s”. Entretanto, **você só pode usar :: uma única vez em um endereço**, pois de outra forma o IPv6 pode não ser claro.

# Exercícios de Fixação 13

Completa	Abreviação
2340:0000:0010:0100:1000:ABCD:0101:1010	
	30A0:ABCD:EF12:3456:ABC:B0B0:9999:9009
2222:3333:4444:5555:0000:0000:6060:0707	
	3210::
210F:0000:0000:0000:CCCC:0000:0000:000D	
	34BA:B:B::20
FE80:0000:0000:0000:DEAD:BEFF:FEEF:CAFE	
	FE80::FACE:BAFF:FEBE:CAFE

# Exercícios de Fixação 13 ~ solução

Completa	Abreviação
2340:0000:0010:0100:1000:ABCD:0101:1010	2340:0:10:100:1000:ABCD:0101:1010
30A0:ABCD:EF12:3456:0ABC:B0B0:9999:9009	30A0:ABCD:EF12:3456:ABC:B0B0:9999:9009
2222:3333:4444:5555:0000:0000:6060:0707	2222:3333:4444:5555::6060:0707
3210:0000:0000:0000:0000:0000:0000:0000	3210::
210F:0000:0000:0000:CCCC:0000:0000:000D	210F::CCCC:0:0:D
34BA:000B:000B:0000:0000:0000:0000:0020	34BA:B:B::20
FE80:0000:0000:0000:DEAD:BEFF:FEEF:CAFE	FE80::DEAD:BEFF:FEEF:CAFE
FE80:0000:0000:0000:FACE:BAFF:FEBE:CAFE	FE80::FACE:BAFF:FEBE:CAFE

# Calculando o Prefixo IPv6

PPPP:PPPP:PPPP:PPPP

HHHH:HHHH:HHHH:HHHH /64

2340:0EF9:AAAA:BBBB

**Prefixo: Copiar**

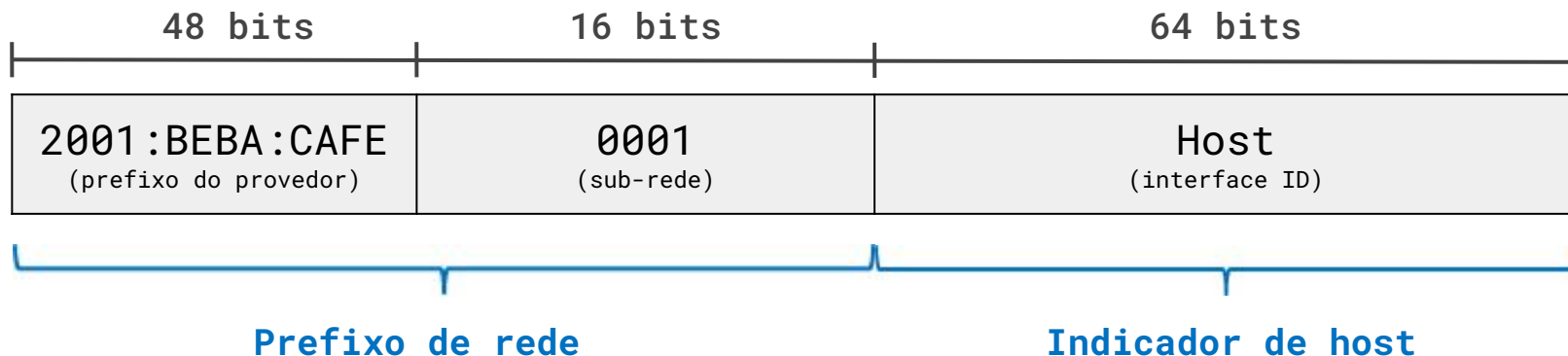
2340:0EF9:AAAA:BBBB

1234:5678:8CDE:ABCD

**Host: Ajustar para 0**

0000:0000:0000:0000

## Estrutura do endereço IPv6



No IPv6, a **máscara** de rede, **obrigatoriamente** deve ser escrita **na notação CIDR** & todas as **redes locais** devem ser **necessariamente /64** (RFC 4291).

Nos navegadores os endereços IPv6 devem estar entre colchetes:

`http://[2001:beba:cafe::1]:8080/index.html`

RFC 2732

# Exercícios de Fixação 14

Endereço/Comprimento	Prefixo
2340:0:10:100:1000:ABCD:101:1010/64	
30A0:ABCD:EF12:3456:ABC:B0B0:9999:9009/64	
2222:3333:4444:5555::6060:707/64	
3210::ABCD:101:1010/64	
210F::CCCC:B0B0:9999:9009/64	
34BA:B:B:0:5555:0:6060:707/64	
3124::DEAD:CAFE:FF:FE00:1/64	
2BCD::FACE:BEFF:FEBE:CAFE/64	

# Exercícios de Fixação 14 ~ solução

Endereço/Comprimento	Prefixo
2340:0:10:100:1000:ABCD:101:1010/64	2340:0:10:100::/64
30A0:ABCD:EF12:3456:ABC:B0B0:9999:9009/64	30A0:ABCD:EF12:3456::/64
2222:3333:4444:5555::6060:707/64	2222:3333:4444:5555::/64
3210::ABCD:101:1010/64	3210::/64
210F::CCCC:B0B0:9999:9009/64	210F:0:0:CCCC::/64
34BA:B:B:0:5555:0:6060:707/64	34BA:B:B:0::/64
3124::DEAD:CAFE:FF:FE00:1/64	3124:0:0:DEAD::/64
2BCD::FACE:BEFF:FEBE:CAFE/64	2BCD::/64



# Exercícios de Fixação 15

Endereço/Comprimento	Prefixo
34BA:B:B:0:5555:0:6060:707/80	
3124::DEAD:CAFE:FF:FE00:1/80	
2BCD::FACE:BEFF:FEBE:CAFE/48	
3FED:F:E0:D00:FACE:BAFF:FE00:0/48	
210F:A:B:C:CCCC:B0B0:9999:9009/40	
34BA:B:B:0:5555:0:6060:707/36	
3124::DEAD:CAFE:FF:FE00:1/60	
2BCD::FACE:1:BEFF:FEBE:CAFE/56	

# Exercícios de Fixação 15 ~ solução

Endereço/Comprimento	Prefixo
34BA:B:B:0:5555:0:6060:707/80	34BA:B:B:0:5555::/80
3124::DEAD:CAFE:FF:FE00:1/80	3124:0:0:DEAD:CAFE::/80
2BCD::FACE:BEFF:FEBE:CAFE/48	2BCD::/48
3FED:F:E0:D00:FACE:BAFF:FE00:0/48	3FED:F:E0::/48
210F:A:B:C:CCCC:B0B0:9999:9009/40	210F:A::/40
34BA:B:B:0:5555:0:6060:707/36	34BA:B::/36
3124::DEAD:CAFE:FF:FE00:1/60	3124:0:0:DEA0::/60
2BCD::FACE:1:BEFF:FEBE:CAFE/56	2BCD:0:0:FA00::/56

## Vantagens decorrentes da adoção do IPv6:

- Espaço quase ilimitado de endereços;
- Header simplificado e de tamanho fixo;
- Dispensa adoção de NAT, preservando modelos fim-a-fim;
- Processamento simplificado nos roteadores;
- Segurança embutida com o IPSec;
- Suporte à mobilidade com o MIPv6.

# Exercícios de Fixação 16

Destaque três vantagens da adoção do IPv6.

# Referências Bibliográficas

## 1. IPv6: o Novo Protocolo da Internet (Samuel Henrique Bucke Brito, 2013)

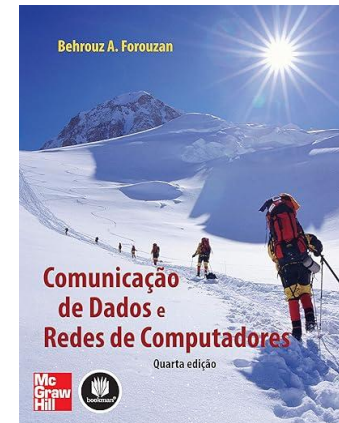
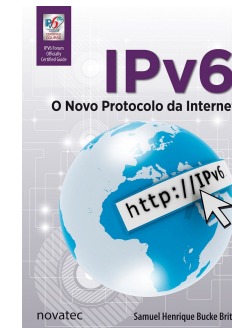
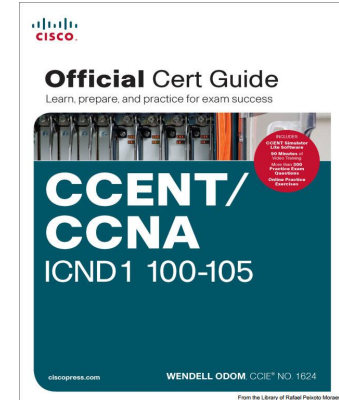
- Capítulo 1 - Evolução da Internet
- Capítulo 2 - Cabeçalho do protocolo IPv6
- Capítulo 3 - Estrutura do endereço IPv6

## 2. Comunicação de Dados e Redes de Computadores (Forouzan, 2013)

- Parte 4: A Camada de Rede (Capítulos 19-22)

## 3. CCNA ICND1 200-301 Official Cert Guide Premium Edition (Odom, 2020)

- Chapter 11 - Perspectives on IPv4 Subnetting
- Chapter 12 - Analyzing Classful IPv4 Networks
- Chapter 13 - Analyzing Subnet Masks
- Chapter 14 - Analyzing Existing Subnet



## CONTATOS

google classroom: **utgsoel**

email: **rafael.moraes@ifrn.edu.br**

site: **<https://moraesrafael.net/redes/>**

blog: **<https://moraesrafael.medium.com/>**

YouTube: **Mundo Tecnauta**