

CURSO ENGENHARIA DA COMPUTAÇÃO

2022-1



**Redes, Sistemas Distribuídos e Cloud
Prof. Me. Nivaldo T. Marcusso**

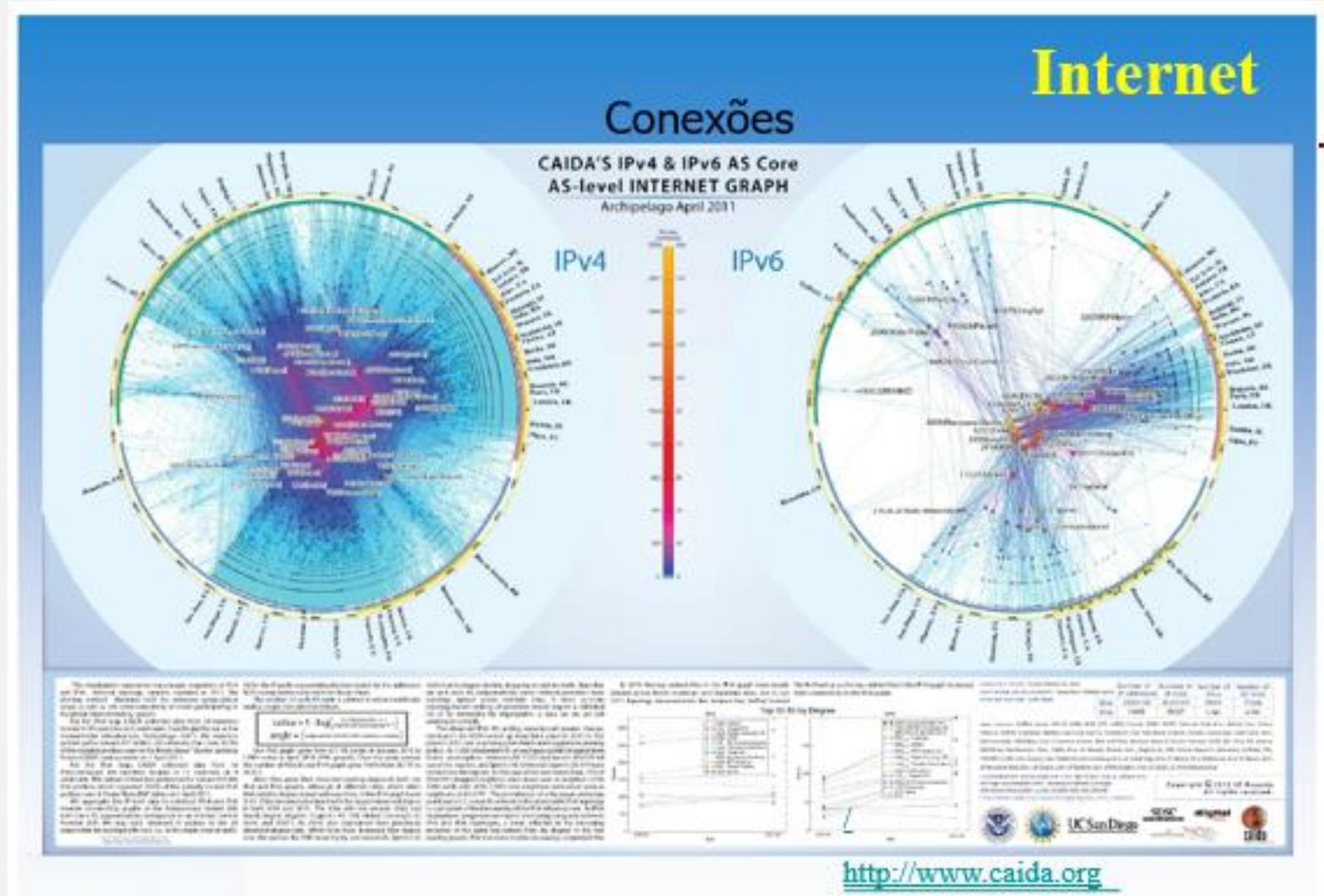


www.unisal.br

A Camada Física



Conexões - Internet



Órgãos da administração de endereços Internet

APNIC

(Asia-Pacific Network Information Center)

Ásia e Pacífico

ARIN

(American Registry for Internet Numbers)

America do Norte e África

LACNIC

(Regional Latin American and Caribbean IP Address Registry)

America Latina e Ilhas do Caribe

RIPE NCC

(Reseau IP Europeens – Network Coordination Center)

Europa, Oriente Médio, Ásia Central e países da África localizados ao norte do equador.

No Brasil, essa administração é confiada ao NIC.br e registro.br, subordinados ao CGI.br – Comitê Gestor da Internet no Brasil

Alocação de Endereço IP - Internet

Área	Endereçamento Reservado
Europa	194.0.0.0 a 195.255.255.255
América do Norte	198.0.0.0 a 199.255.255.255
América Latina	200.0.0.0 a 201.255.255.255
Pacífico	202.0.0.0 a 203.255.255.255

O Internic transferiu ao Brasil a gestão dos blocos 200.17.0.0 a 200.20.0.0 e 200.128.0.0 a 200.255.0.0, que correspondem a 1024 e 32000 classes C, respectivamente, ou a 8 milhões de endereços. Assim ganhou autonomia e não necessita recorrer ao Comitê Internacional a cada nova atribuição.

RFC 1918 - Endereços Privados

10.0.0.0 a 10.255.255.255
172.16.0.0 a 172.31.255.255
192.168.0.0 a 192.168.255.255

Internet - Conceito de Classes de endereços

- Classe A Provedores de Internet e Governos
 - Classe B Empresas de grande porte e multinacionais
 - Classe C Empresas menores
 - Classe D Multicast
 - Classe E Reservado/Experimental/Futuro

CLASSE	Primeiro Octeto	Exemplo 1:	
A	1-126	8.165.17.1	<i>Classe A</i>
B	128-191	127.0.0.1	<i>Loopback</i>
C	192-223	165.12.123.5	<i>Classe B</i>
D	224-239	197.12.223.123	<i>Classe C</i>
E	240-255	233.1.3.5	<i>Multicast-Classe D</i>
		250.1.2.19	<i>Experimental-Classe E</i>
		255.255.255.255	<i>Broadcast</i>

Internet - Obstáculos ao crescimento

- Dados coletados pelos membros do IETF em 1991 sobre o crescimento da Internet apontam para 1994 a exaustão do estoque de endereços
- O espaço de endereçamento organizado por classes provoca enorme desperdício
- As tabelas de roteamento cresce demais e dificulta o gerenciamento
- Faltam recursos para prover mobilidade e auto-configuração de dispositivos móveis
- Os mecanismos de apoio à qualidade de serviço são ineficazes
- O suporte à segurança é precário

Internet

Ações emergenciais

- Classless Internet Domain Routing (CIDR)
 - RFC 1519 (PS)
 - Endereço de Rede = prefixo / prefixo
 - Agregação de rotas
- Plano de endereçamento privado - RFC 1918
- Uso de Network Address Translation (NAT) -
RFC 2663 2993 3022

CIDR – Classless Inter Domain Routing

- O estoque de endereços da INTERNET estava se esgotando, devido principalmente a má utilização das classes de endereço
- Uma solução emergencial foi oferecida pela RFC 1519 - CIDR (“Classless Inter Domain Routing”)
- Os números IP da Internet deixaram de ser organizados em classes, sendo distribuídos com uma máscara binária que define a sub-rede

Arquitetura TCP/IP

Camada de Rede

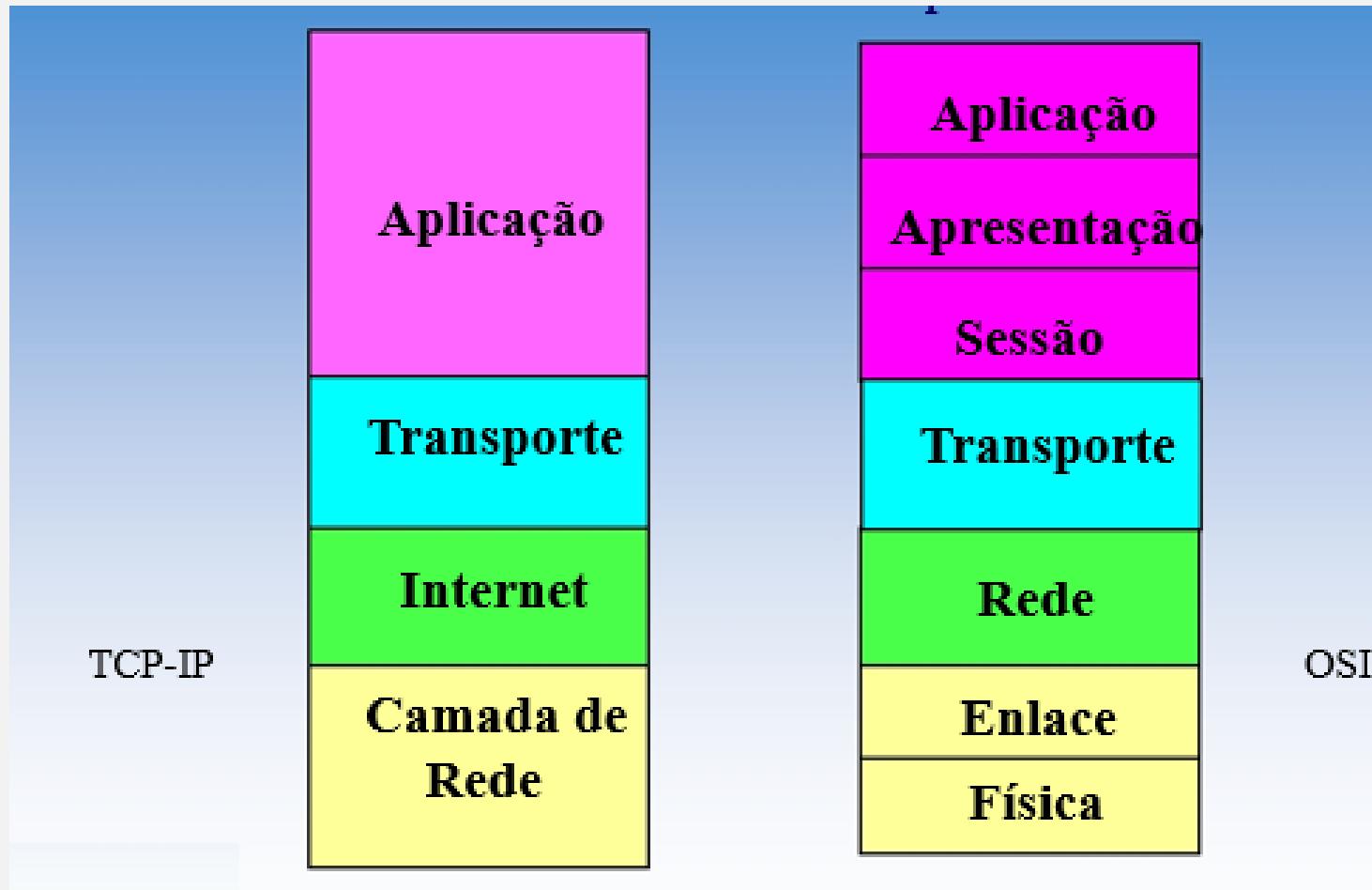
Objetivo

- Explicar as funções da camada de rede
 - Roteamento
(seleção de rotas ou escolha de caminho)
 - Escalabilidade (endereçamento IP)
 - Como funciona um roteador
(protocolos de roteamento da Internet)
 - Tópicos avançados: IPv6, multicast, anycast, unicast
- Instanciação e implementação na Internet

Arquitetura TCP/IP

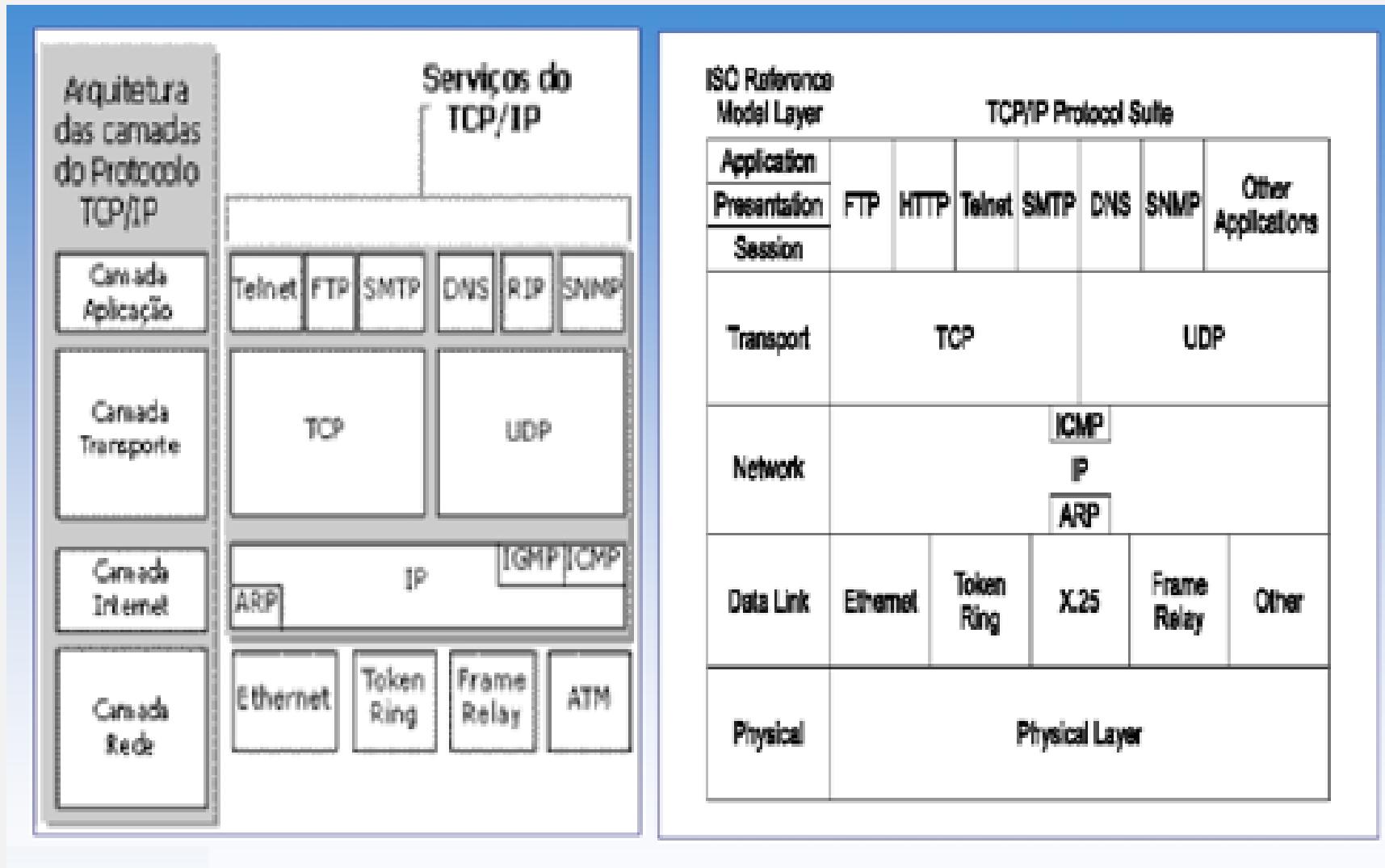


Arquitetura TCP/IP – Equivalência dos modelos



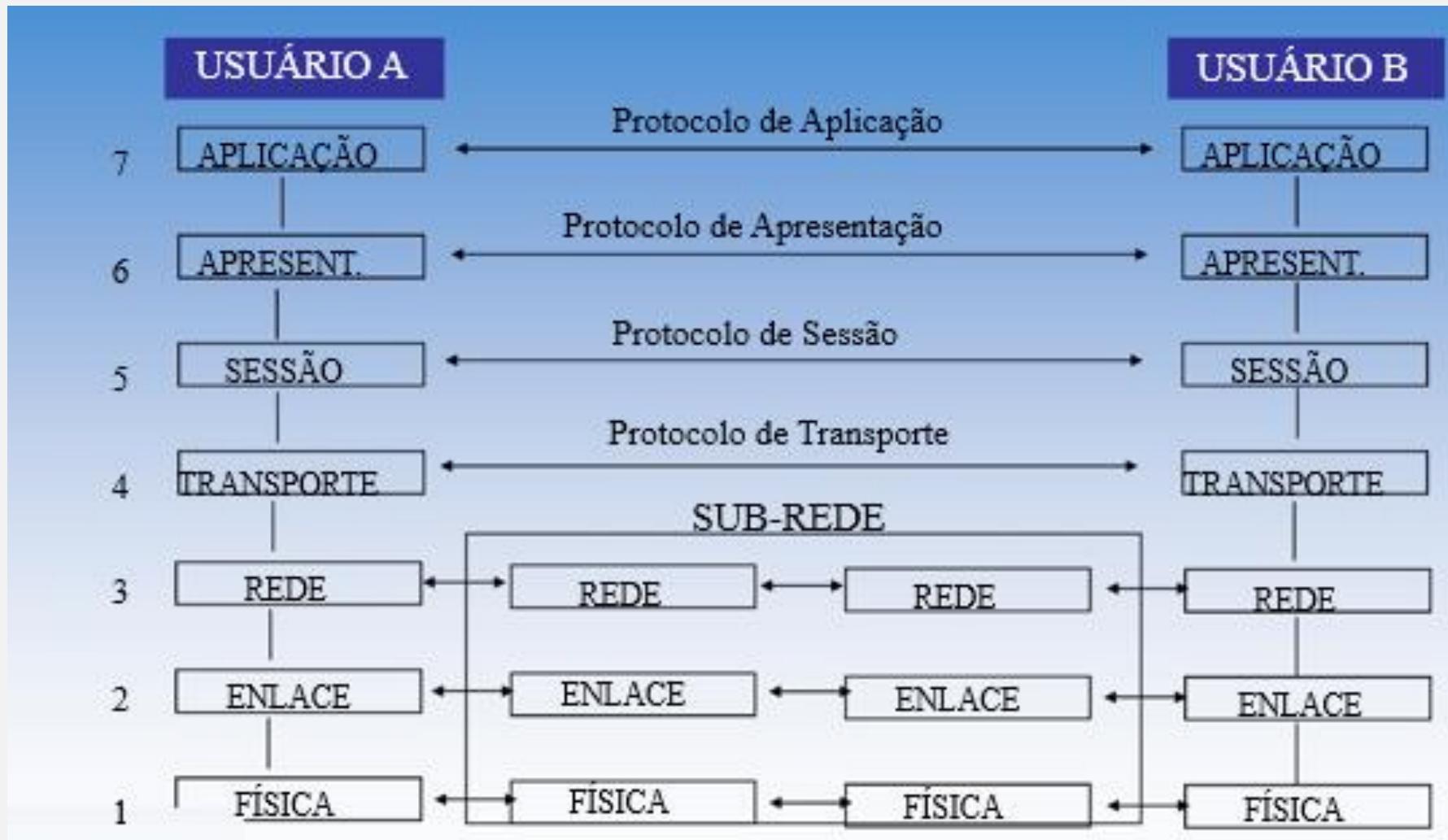
Arquitetura TCP/IP

TCP/IP X OSI



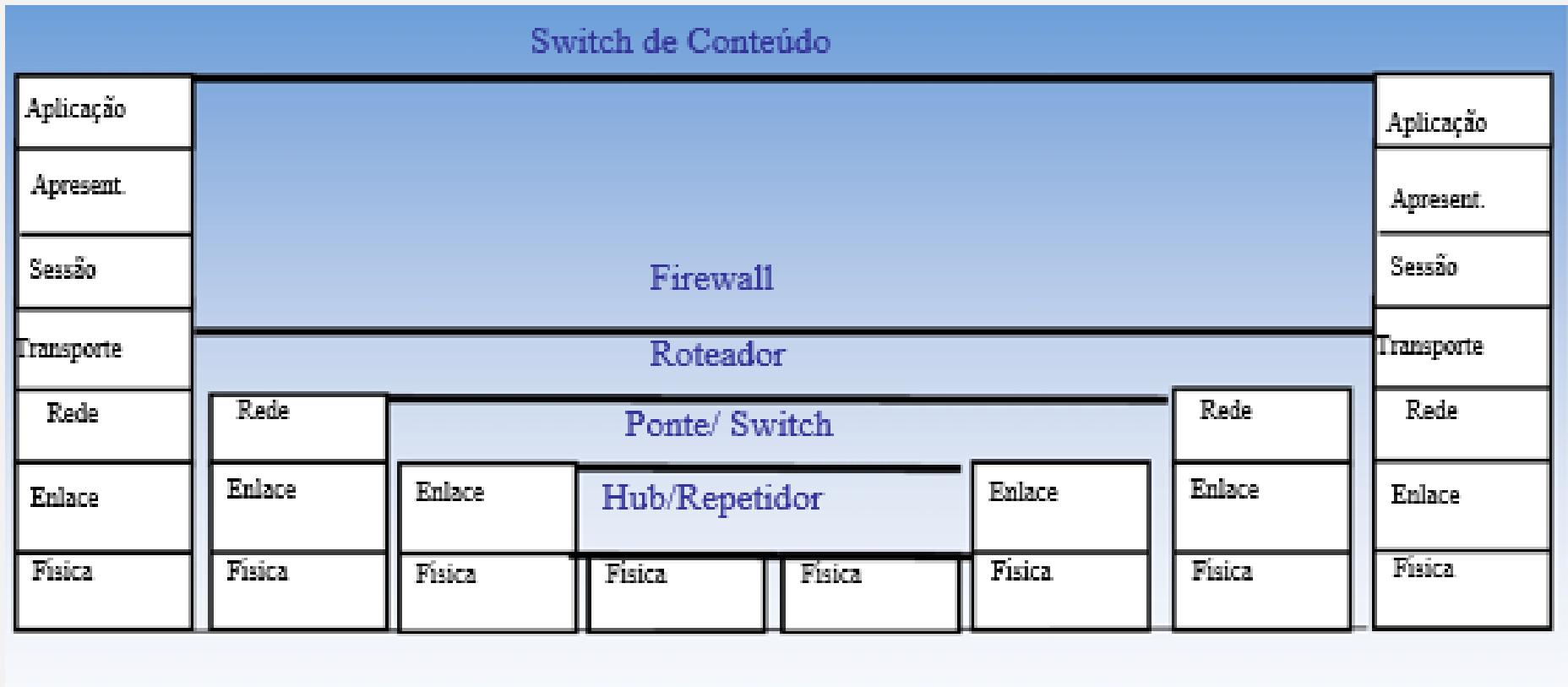
Arquitetura TCP/IP

Camadas do Modelo OSI

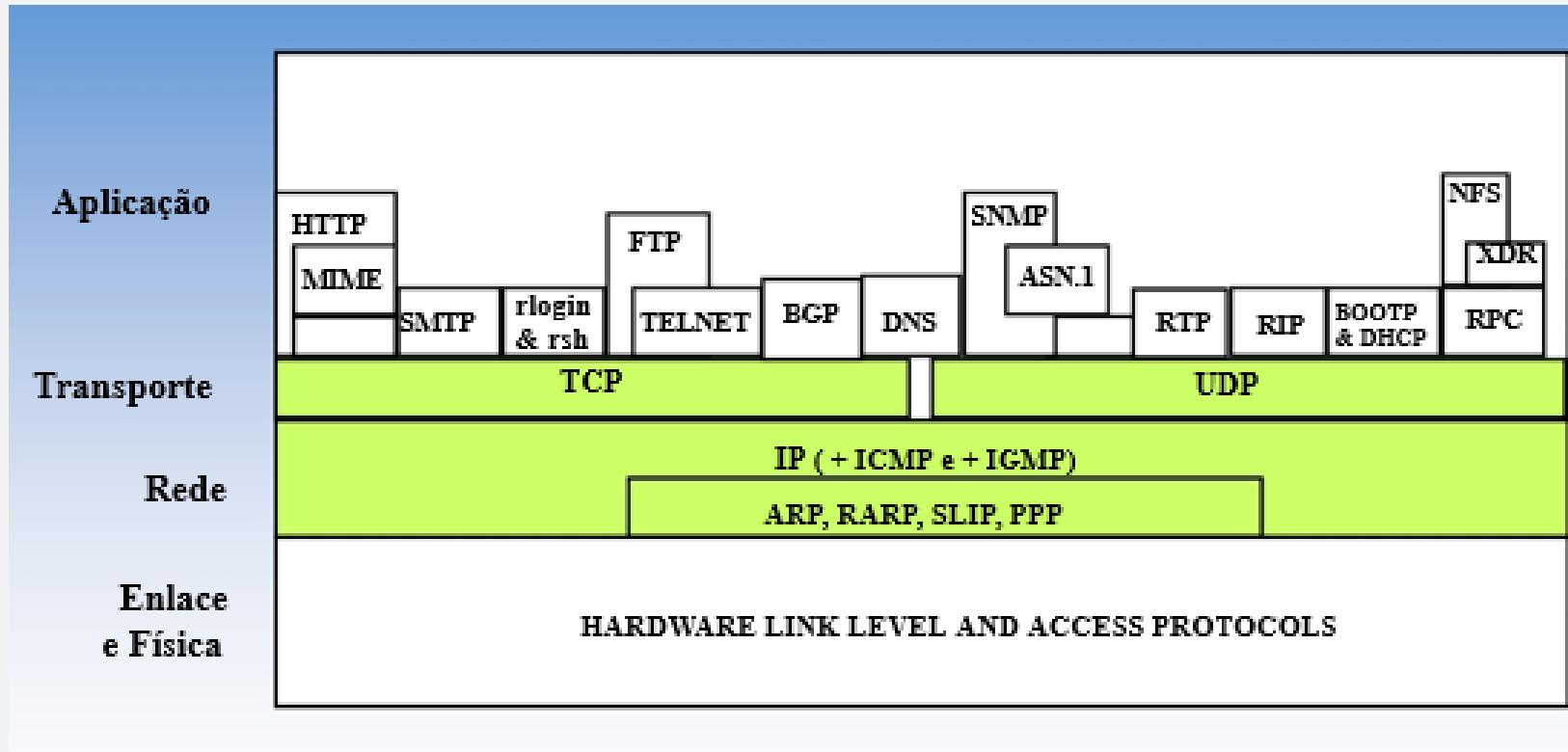


Arquitetura TCP/IP

Equipamentos de Redes

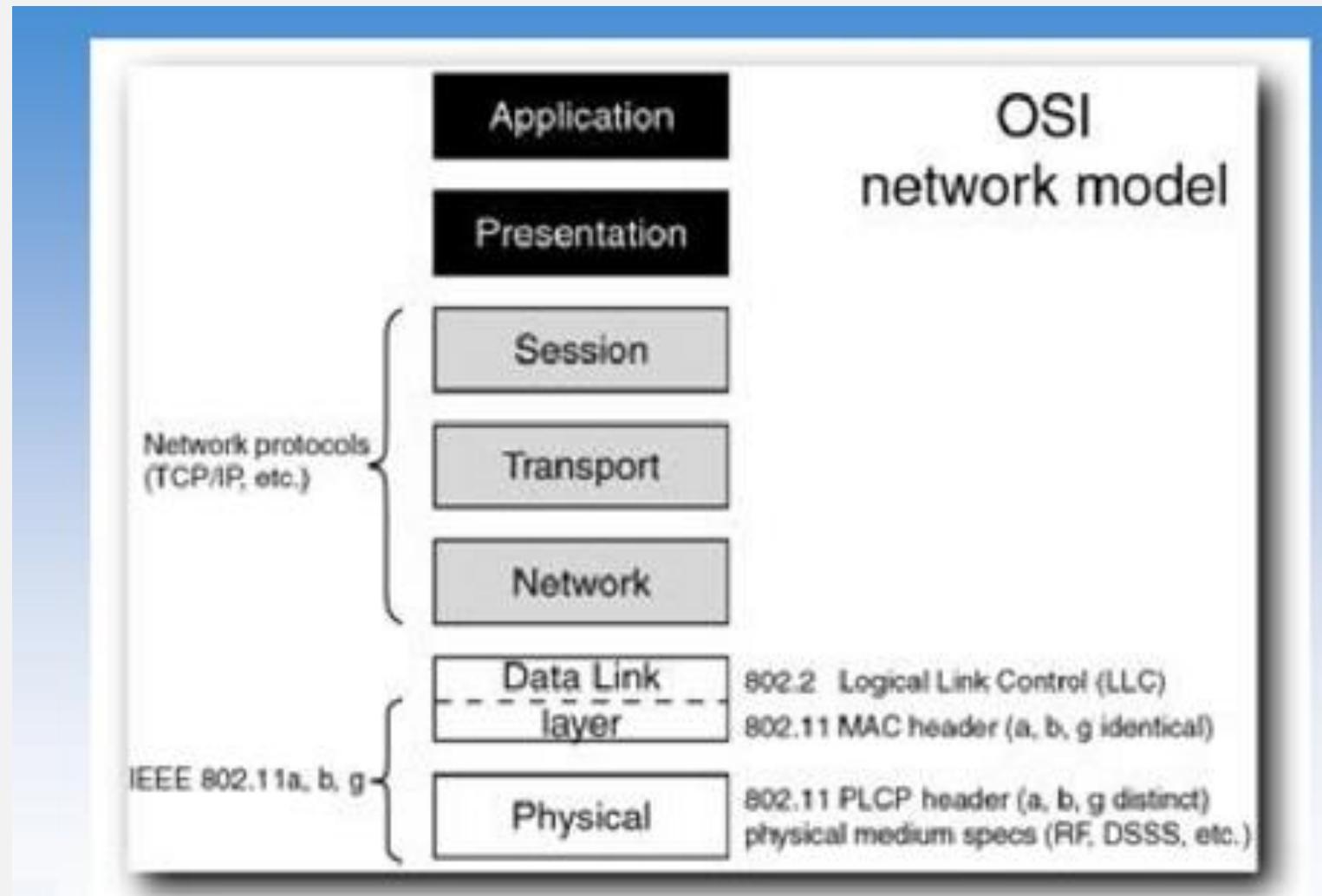


Arquitetura TCP/IP - Principais Protocols



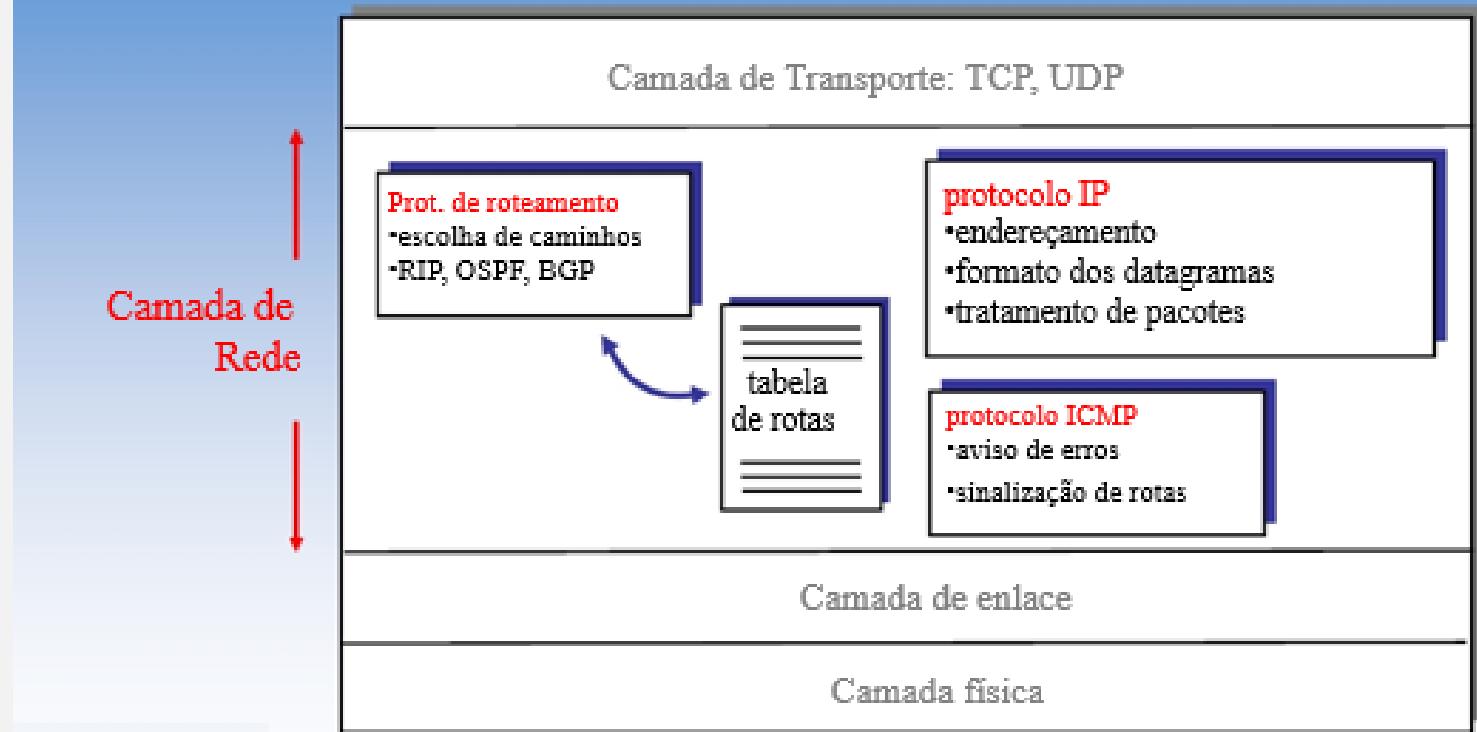
Arquitetura TCP/IP

Camada de Rede



Arquitetura TCP/IP

Entidade de rede implementada por roteadores e terminais:



Endereçamento IP

O endereço IP consiste de um número binário de 32 bits destinado a um host e usado para todas as comunicações com o host

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129.52.6.0
11000000 00000101 00110000 00000011	192.5.48.3
00001010 00000010 00000000 00100101	10.2.0.37
10000000 00001010 00000010 00000011	128.10.2.3
10000000 10000000 11111111 00000000	128.128.255.0

Arquitetura TCP/IP

Classes de endereçamento

Class	Range of Values
A	0 through 127
B	128 through 191
C	192 through 223
D	224 through 239
E	240 through 255

O intervalo de valores do primeiro octeto define a classe

Arquitetura TCP/IP

Classes de endereçamento

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

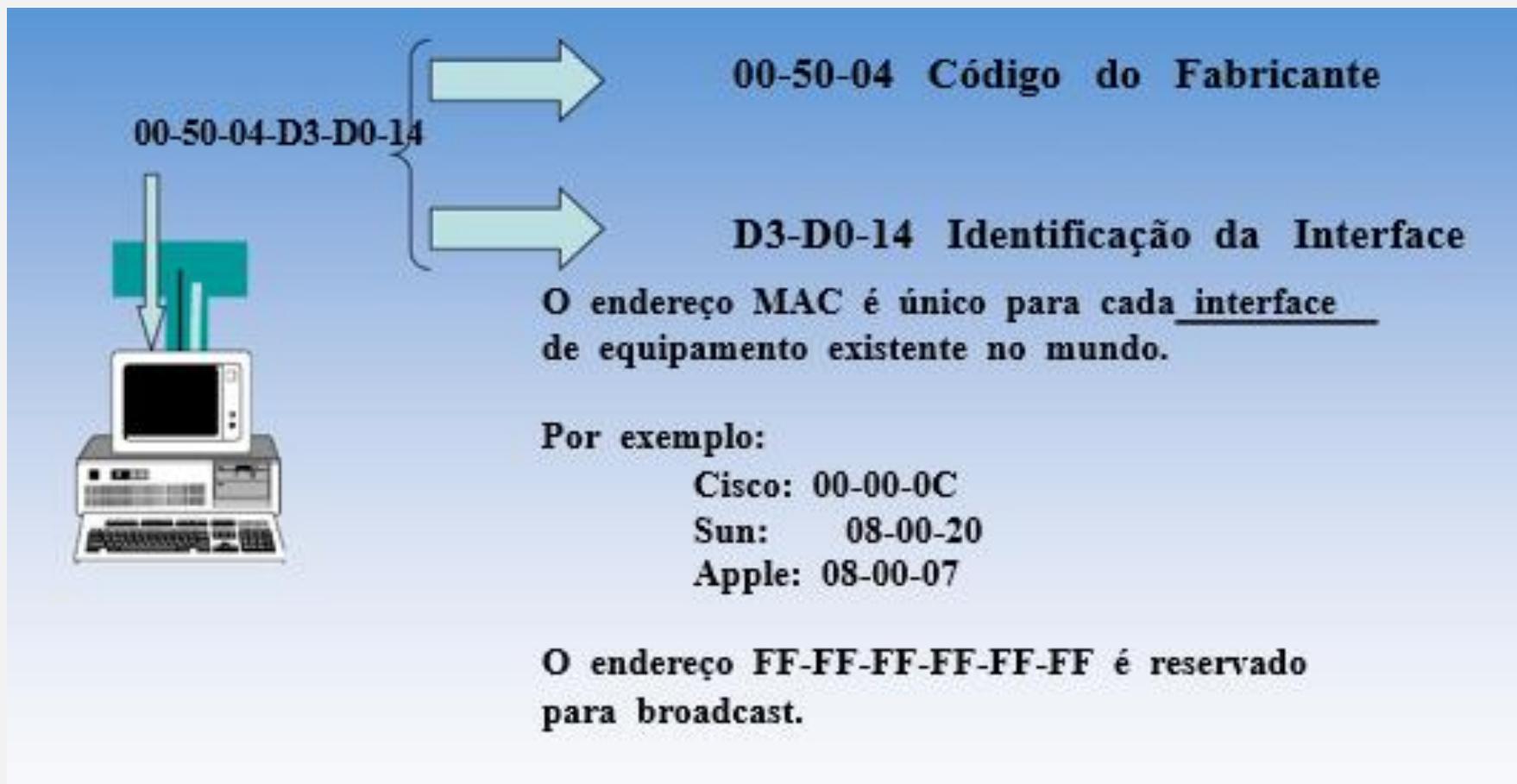
Arquitetura TCP/IP

Sub-redes e Computadores - Classe C

# de bits	Máscara - Decimal	Máscara - Hexadecimal	Qtd. Sub-redes	IP's válidos / sub-rede	IPs usados - total	Perda de IPs - total
0	255.255.255.0	FF.FFFF.00	0	254	254	2
1	255.255.255.128	FF.FFFF.80	2	126	252	4
2	255.255.255.192	FF.FFFF.C0	4	62	248	8
3	255.255.255.224	FF.FFFF.E0	8	30	240	16
4	255.255.255.240	FF.FFFF.F0	16	14	224	32
5	255.255.255.248	FF.FFFF.F8	32	6	192	64
6	255.255.255.252	FF.FFFF.FC	64	2	128	128
7	255.255.255.254	FF.FFFF.FE	Invalido	Invalido	Invalido	Invalido

Arquitetura TCP/IP

Endereço MAC



Serviços das Camadas

Transporte

- Entrega de dados “confiável” pelo protocolo TCP
- Suporte a aplicações
- Controle de fluxo e de erros fim a fim

Rede

- Entrega de dados “sem conexão” pelo protocolo IP
- Endereçamento lógico universal
- Roteamento
- Independência da Plataforma de Hardware

Protocolos de Camada de Rede

Internet Protocol (IP)

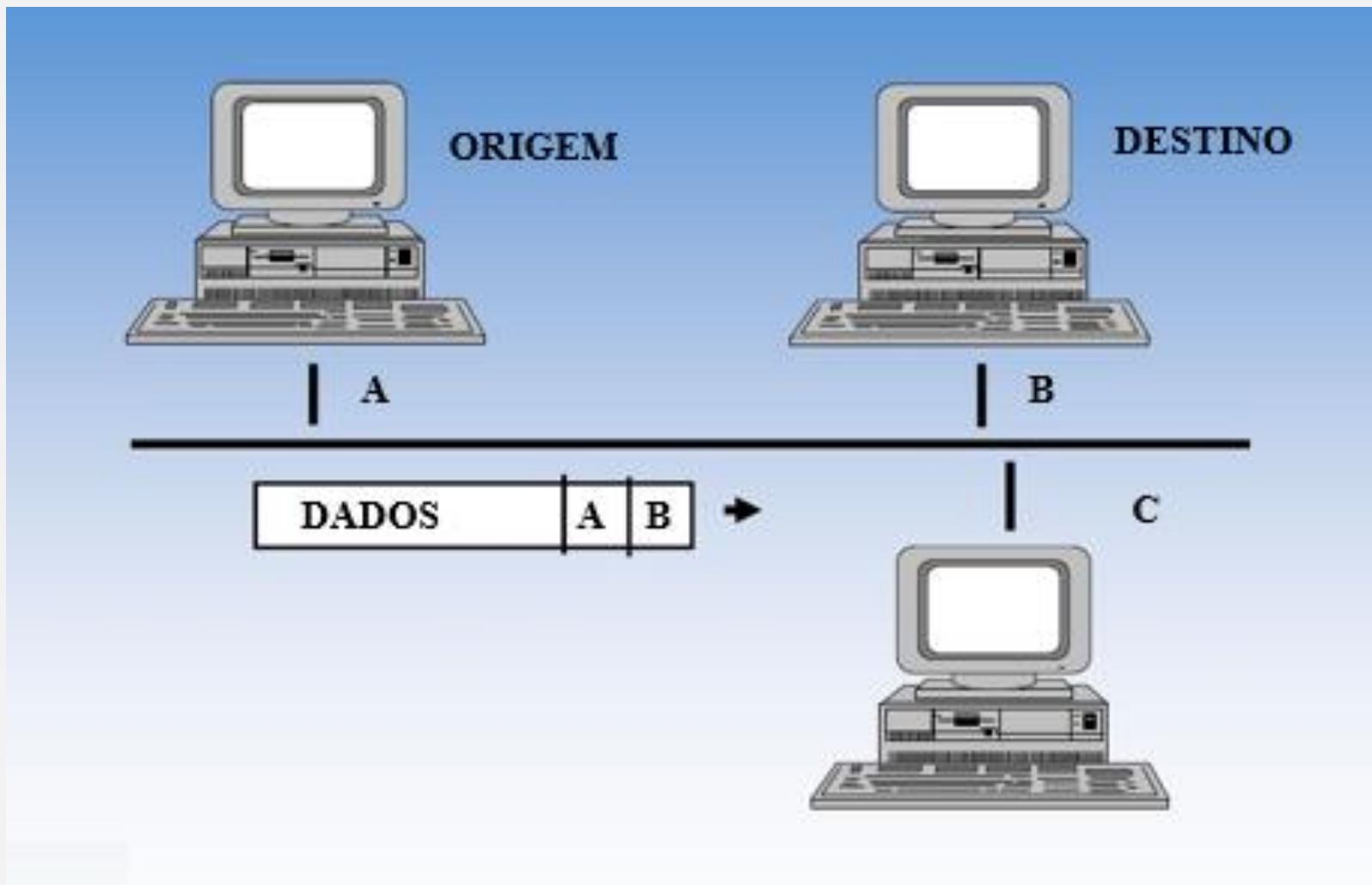
Responsável pela transmissão de blocos de dados (segmentos) através de um conjunto de redes

Esses dados são recebidos das camadas superiores (transporte), que usam protocolos tais como TCP ou UDP
O cabeçalho de cada datagrama IP define os seguintes campos:

- Endereçamento Internet
- Roteamento
- Time to Live (TTL)
- Type of Service (TOS)
- Demultiplexação
- Fragmentação
- Opções

Protocolos de Camada de Rede

Forma de endereçamento



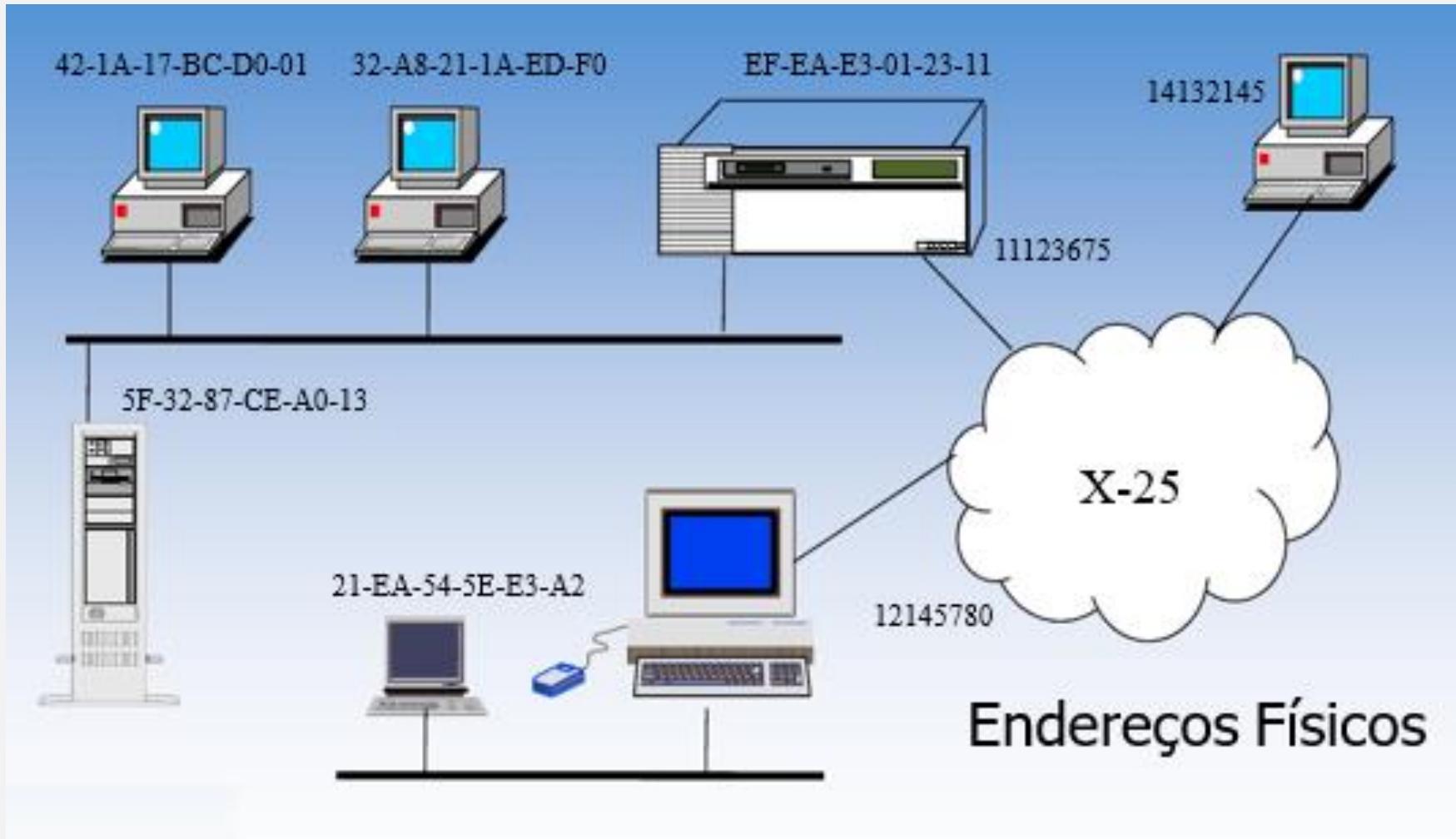
Protocolos de Camada de Rede

Forma de endereçamento

- ENDEREÇO FÍSICO
 - Utilizado abaixo do ip
 - Não configurável
 - Dependente do hard-ware ou do prestador de serviço
 - Não roteável fora da sua sub-rede
 - Formato variável
 - Necessário para o envio de mensagens na sub-rede
- ENDEREÇO LÓGICO
 - Utilizado pelo ip
 - Determinável pelo administrador de rede
 - Dependente do plano de numeração
 - Roteável
 - Formato único
 - Necessário para o envio de mensagens na internet

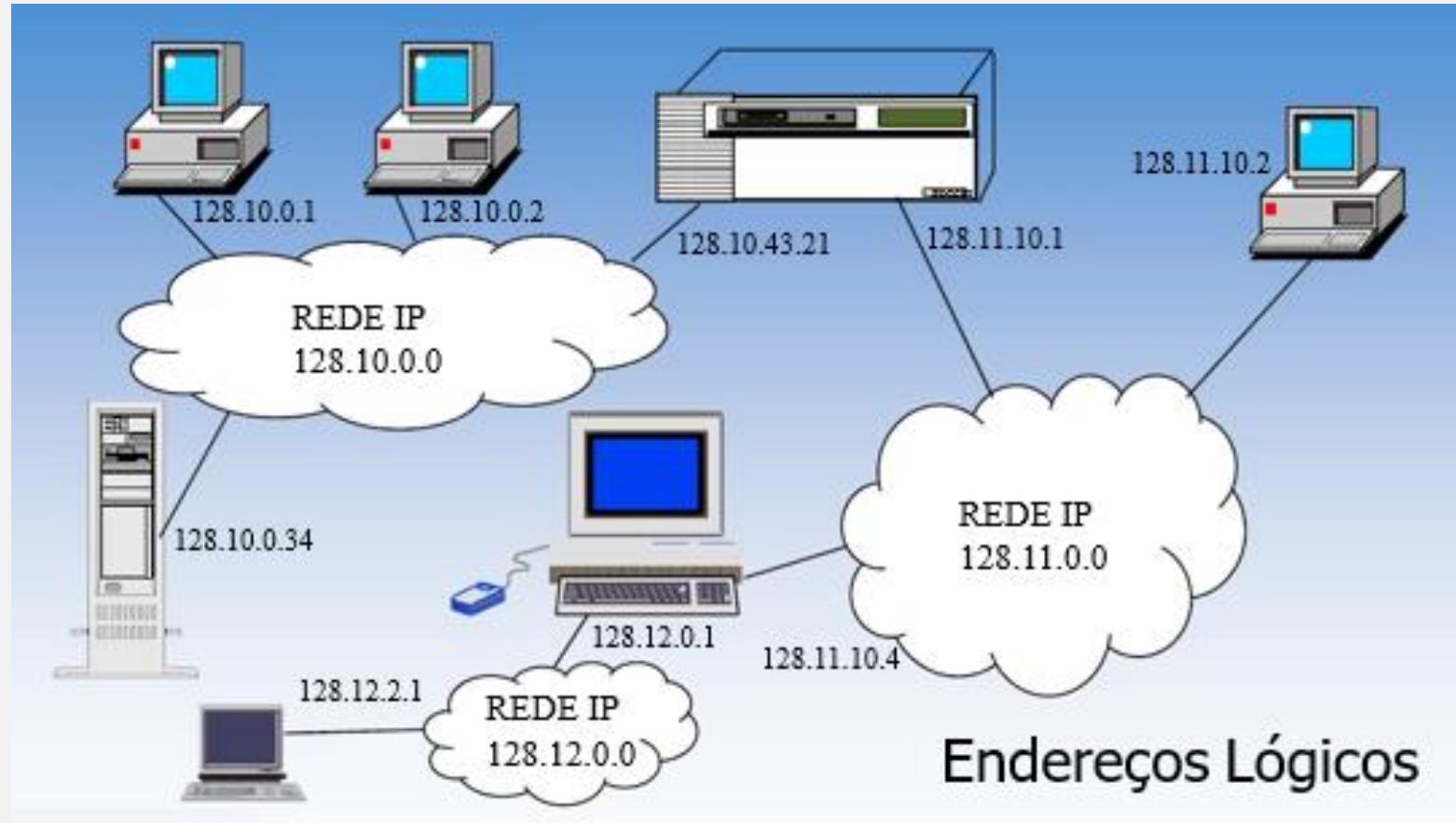
Protocolos de Camada de Rede

Forma de endereçamento



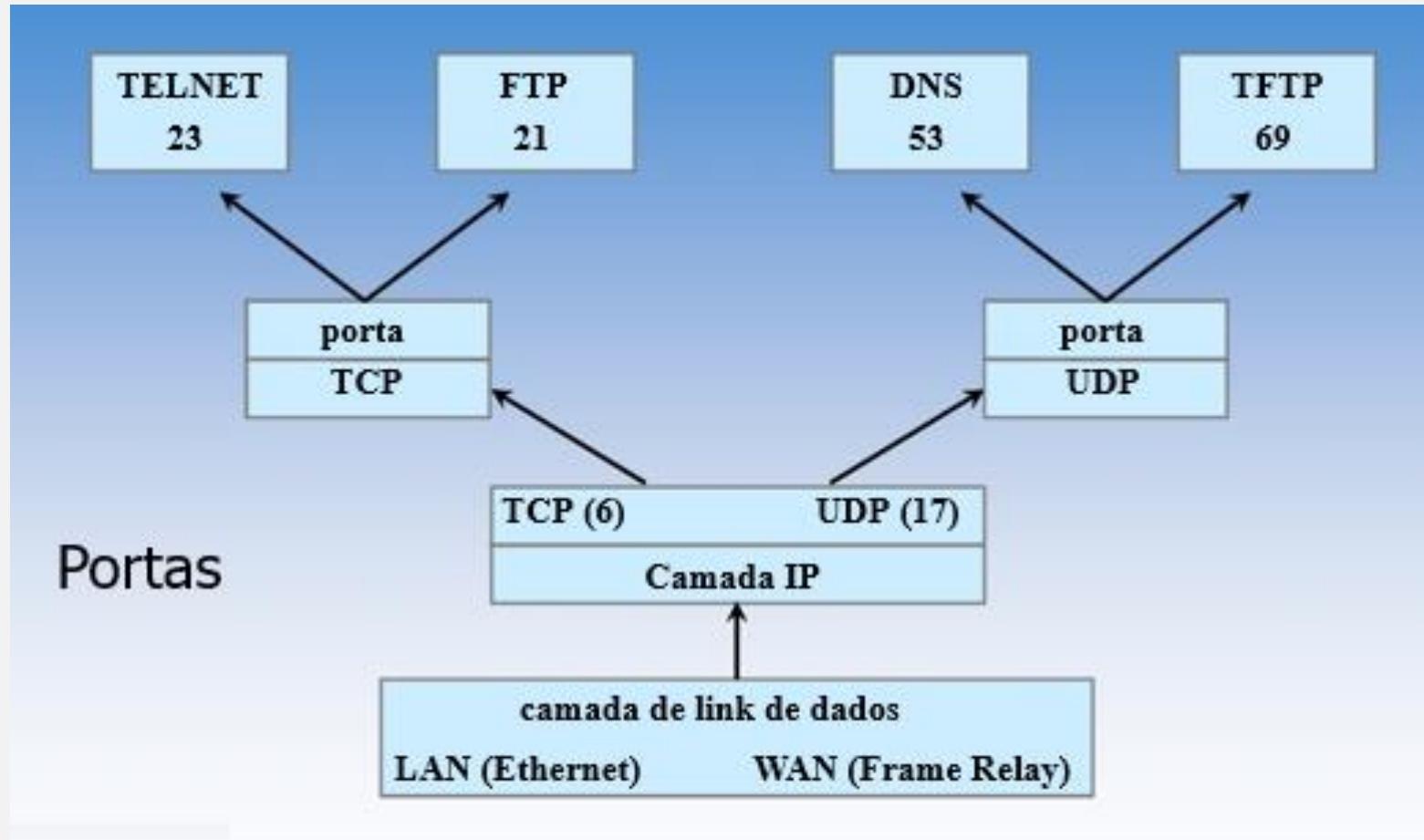
Protocolos de Camada de Rede

Forma de endereçamento



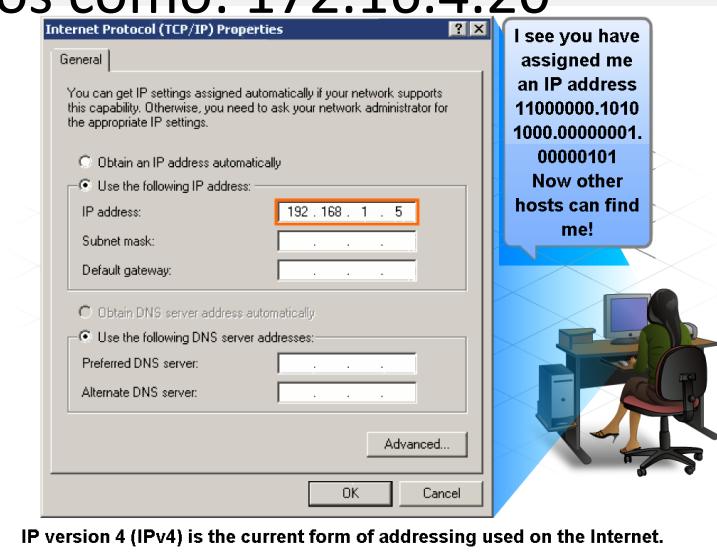
Protocolos de Camada de Rede

Forma de endereçamento

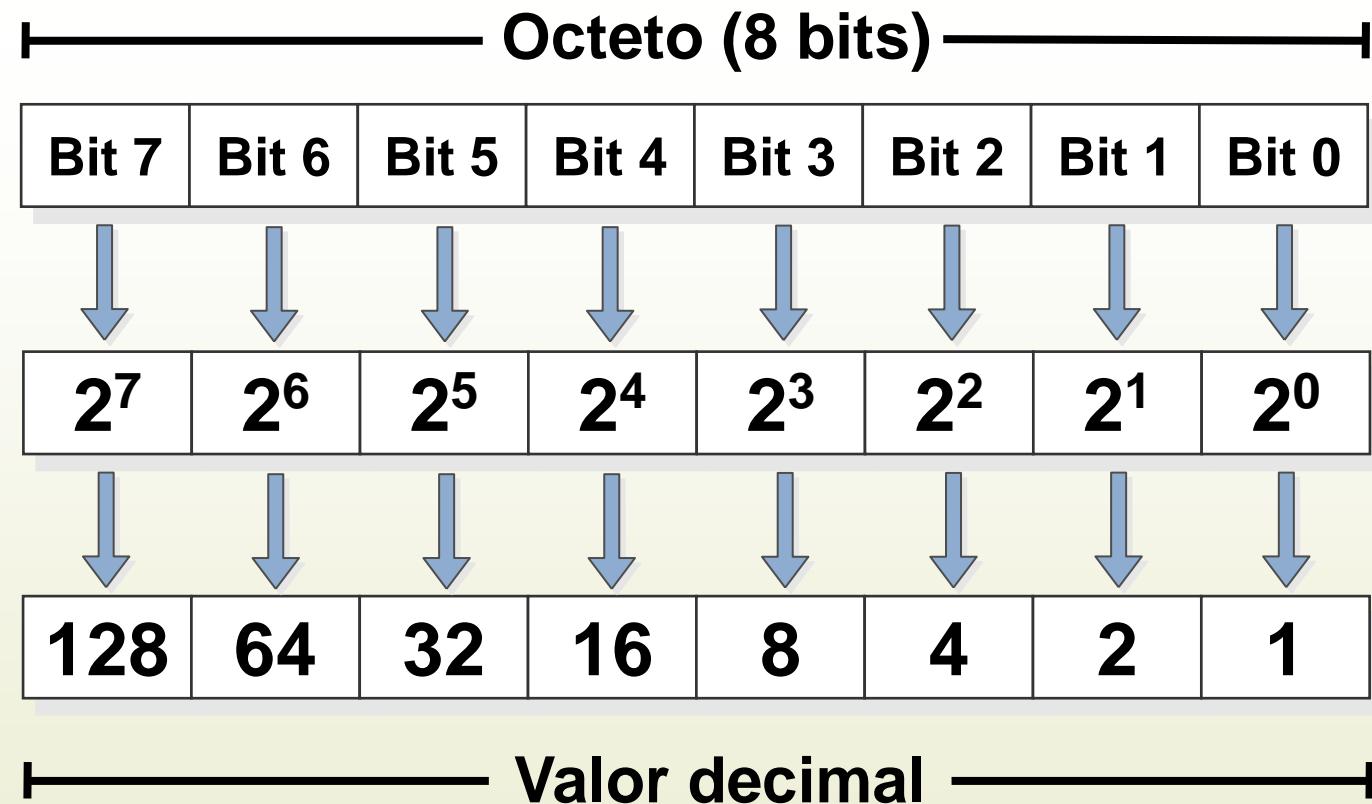


Estrutura do Endereço IP

- Endereço binário de 32 Bits
- Representado utilizando a forma decimal pontuada
 - Cada byte do padrão binário, chamado de octeto, é separado com um ponto
 - Por exemplo, o endereço:
 - 10101100000100000000010000010100 é expresso no formato decimal com pontos como: 172.16.4.20

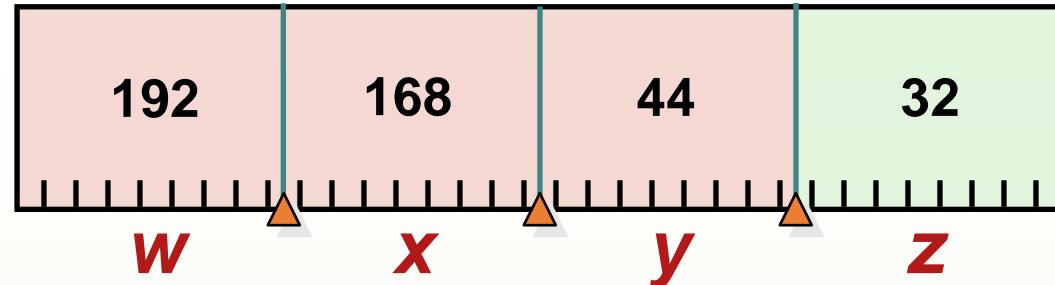


A relação entre notação decimal com ponto e números binários

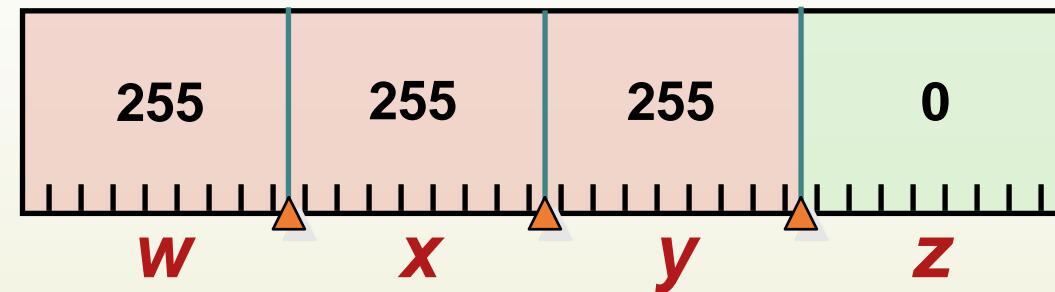


Máscara de sub-rede

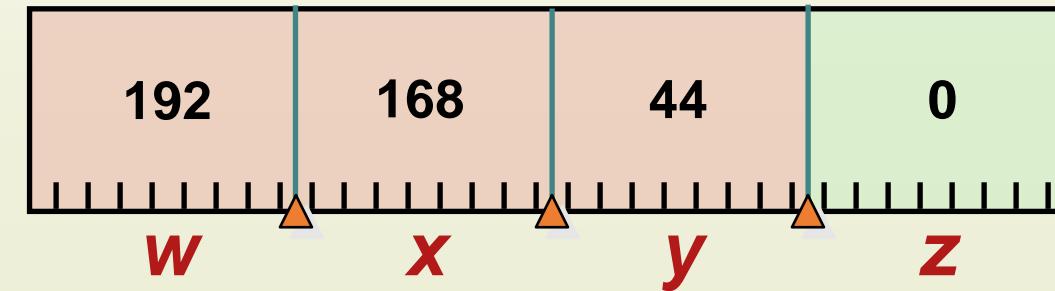
IP



Máscara

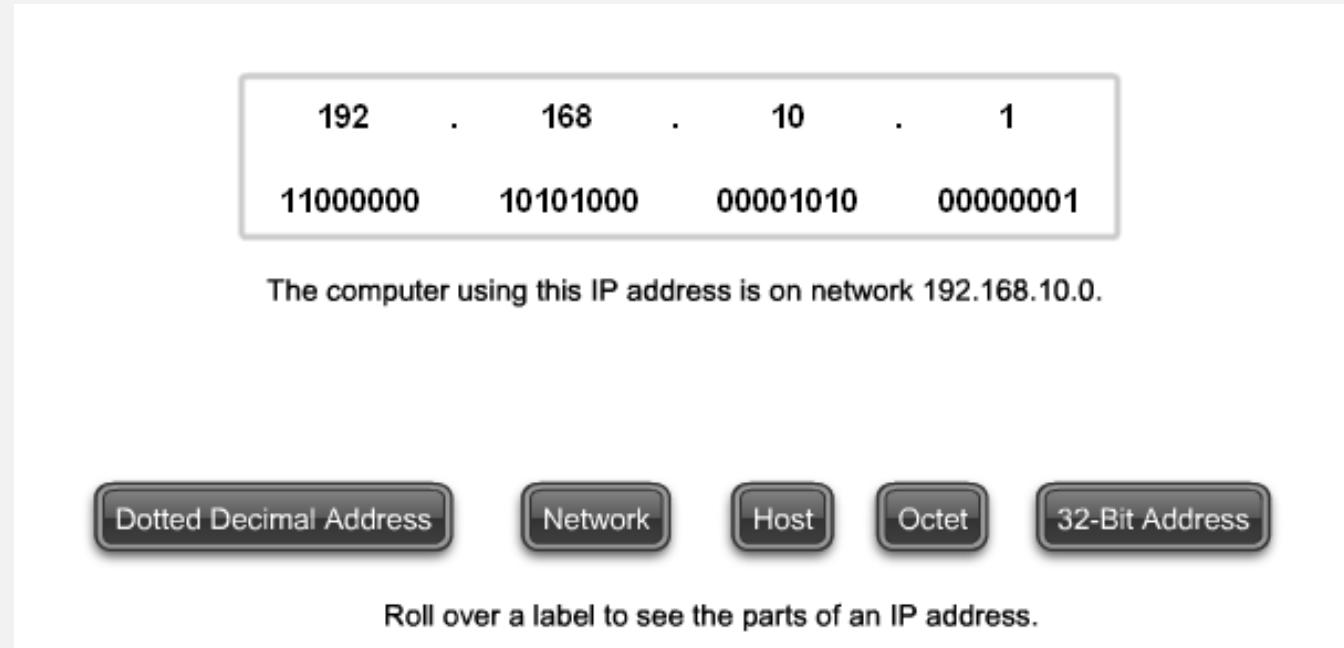


Network ID



Estrutura do Endereço IP

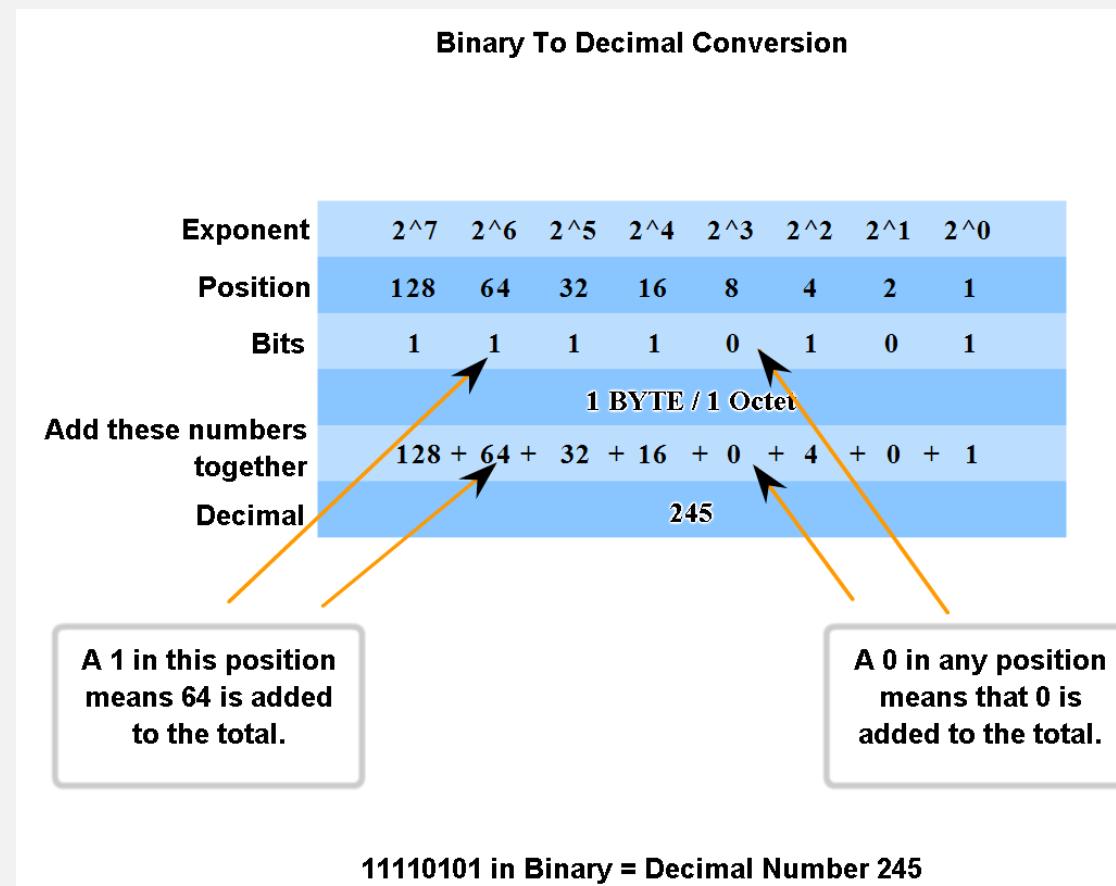
- A porção de bits mais significativa representa o endereço de rede
- Um número variável de bits chamado de **porção de host** e determina o número de hosts que pode-se ter na rede



Estrutura do Endereço IP

- Conversão Binário para Decimal

Analisaremos cada byte (octeto) como um número decimal no intervalo de 0 a 255



Classifique e Defina Endereços IPv4

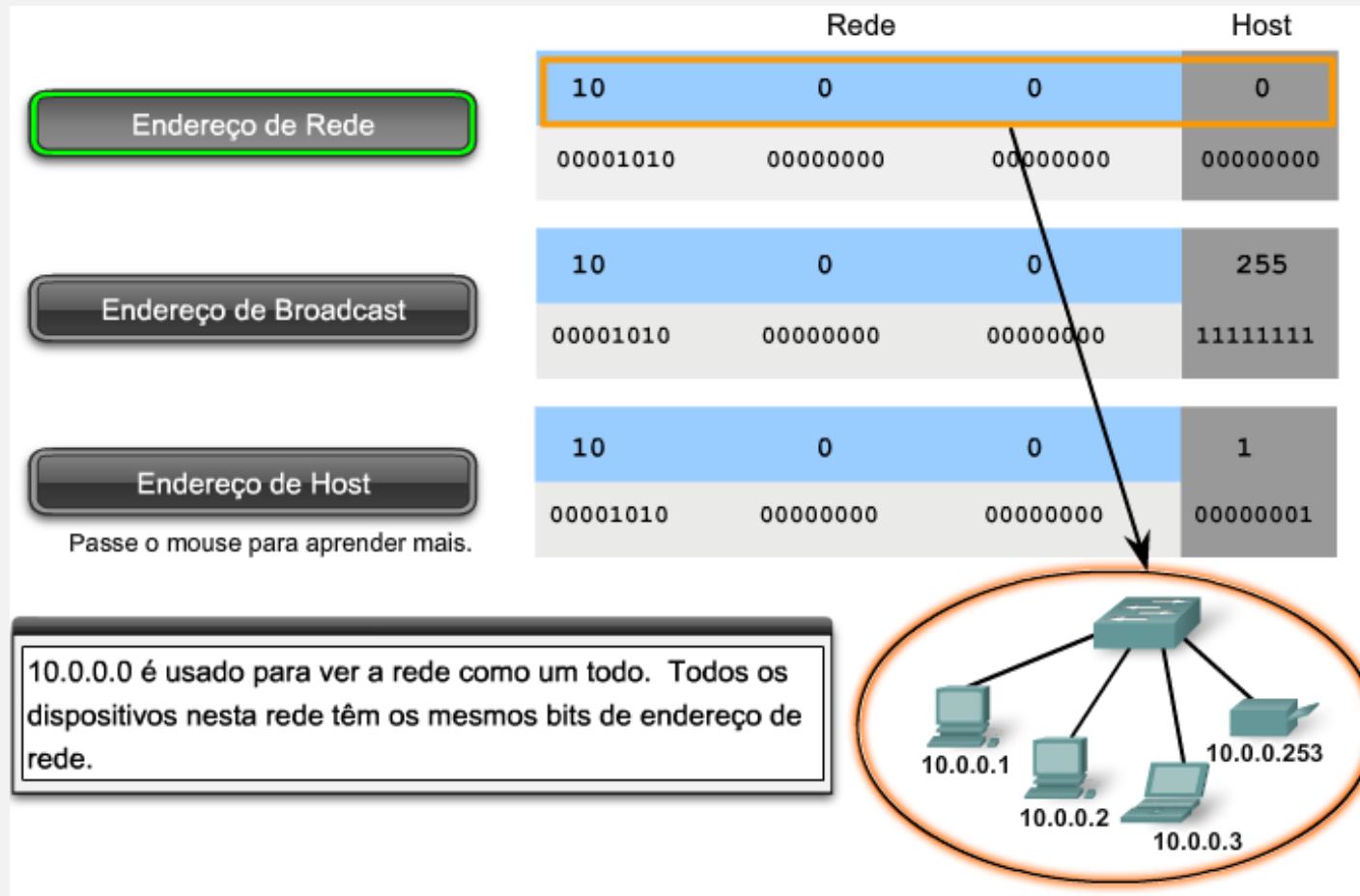
- Três tipos de endereço:

Tipos de Endereços			
	Rede		Host
Endereço de Rede	10	0	0
	00001010	00000000	00000000
Endereço de Broadcast	10	0	255
	00001010	00000000	11111111
Endereço de Host	10	0	1
	00001010	00000000	00000001

Classifique e Defina Endereços IPv4

- Endereço de Rede

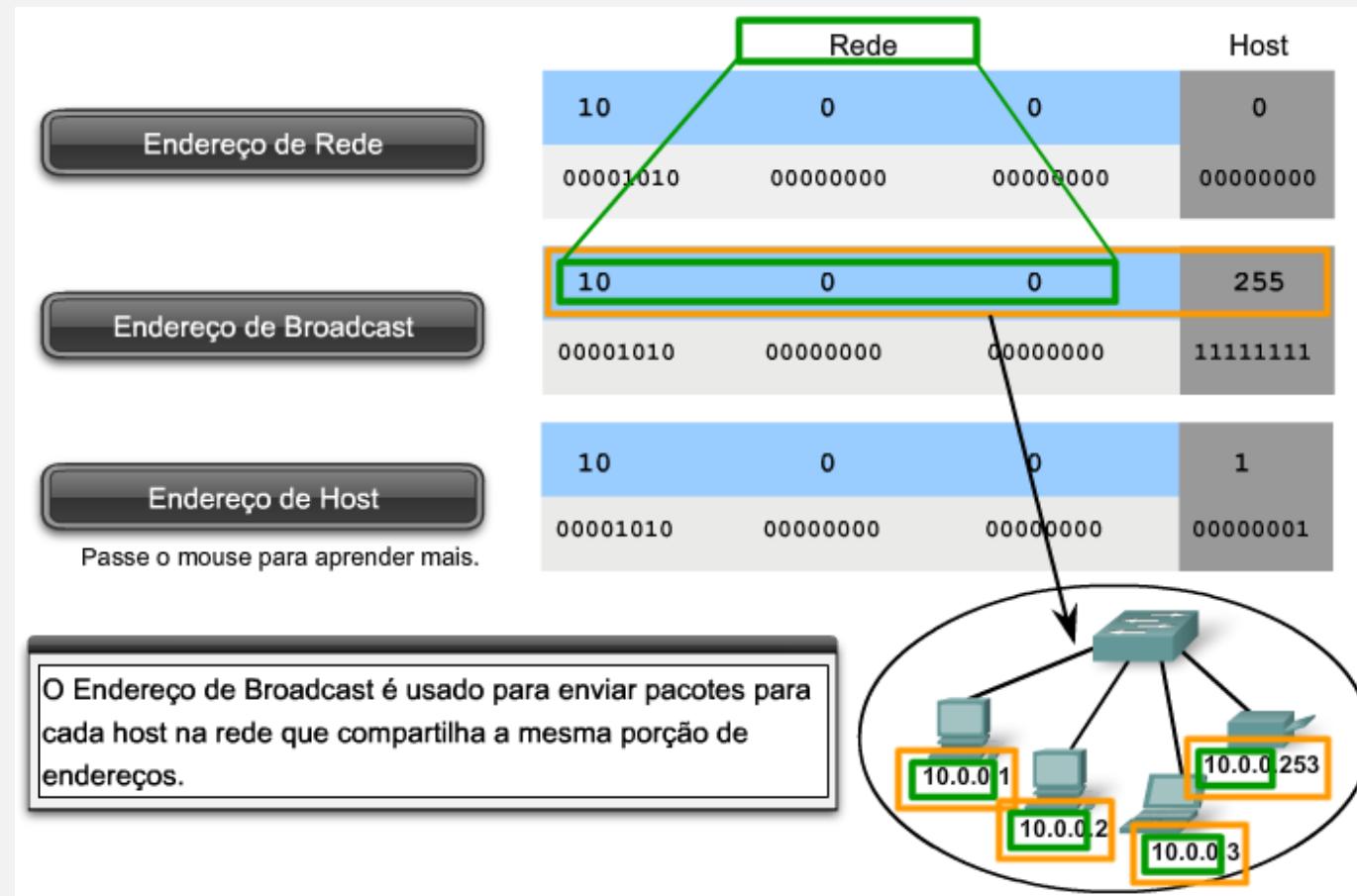
O primeiro endereço é reservado para o endereço de rede



Classifique e Defina Endereços IPv4

- Endereço de Broadcast

O endereço de broadcast usa o último endereço do intervalo de rede



Classifique e Defina Endereços IPv4

- Endereço de Host

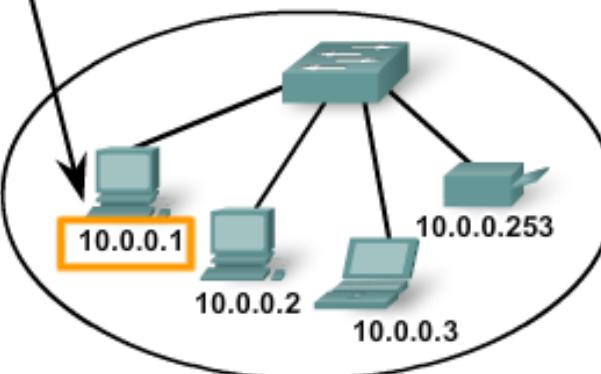
Rede			Host
10	0	0	0
00001010	00000000	00000000	00000000

Rede			Host
10	0	0	255
00001010	00000000	00000000	11111111

Rede			Host
10	0	0	1
00001010	00000000	00000000	00000001

Passe o mouse para aprender mais.

Cada host nesta rede tem um único endereço.



The slide illustrates three examples of IPv4 address classification based on their binary representations:

- Endereço de Rede:** An address where the Host portion is all zeros (00000000). This is shown for a Class C address (10.0.0.0).
- Endereço de Broadcast:** An address where the Host portion is all ones (11111111). This is shown for a Class C address (10.0.0.255).
- Endereço de Host:** An address where the Host portion contains a unique value (1 in this case). This is shown for a Class C address (10.0.0.1).

A callout box states: "Cada host nesta rede tem um único endereço." (Each host in this network has a unique address.)

Classifique e Defina Endereços IPv4

- Prefixo de Rede

- O tamanho do prefixo é o número de bits no endereço que nos dá a porção de rede.
- Para o endereço de exemplo 172.16.4.0/24 o **/24** é o tamanho do prefixo
- Indica que os 24 bits mais significativos são o endereço de rede deixando 8 bits para a porção de host

Uso de Prefixos Diferentes para a Rede 172.16.4.0

Rede	Endereço de Rede	Intervalo do Host	Endereço de Broadcast
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

Classifique e Defina Endereço IPv4

- Determine o endereço de rede, broadcast e host.

Given address/prefix of **183.26.103.215 /30**

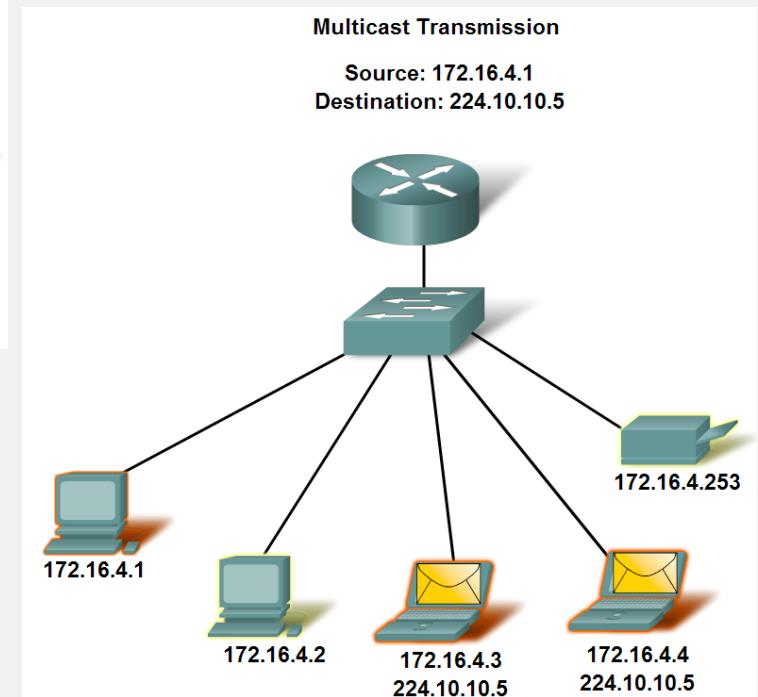
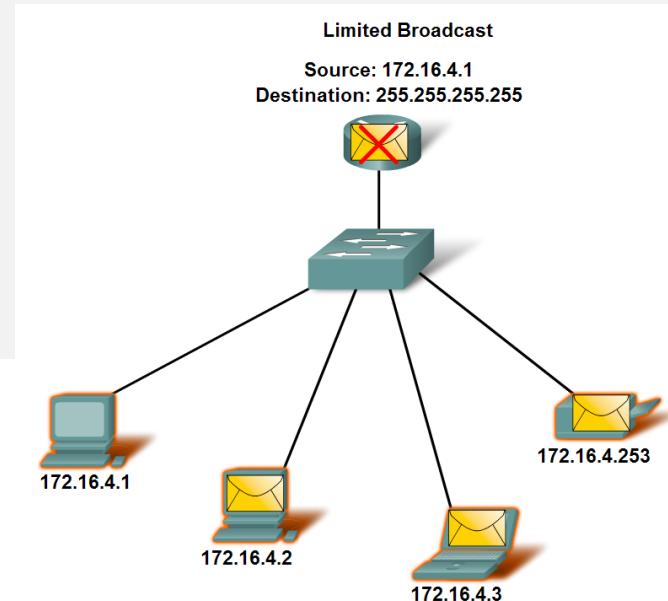
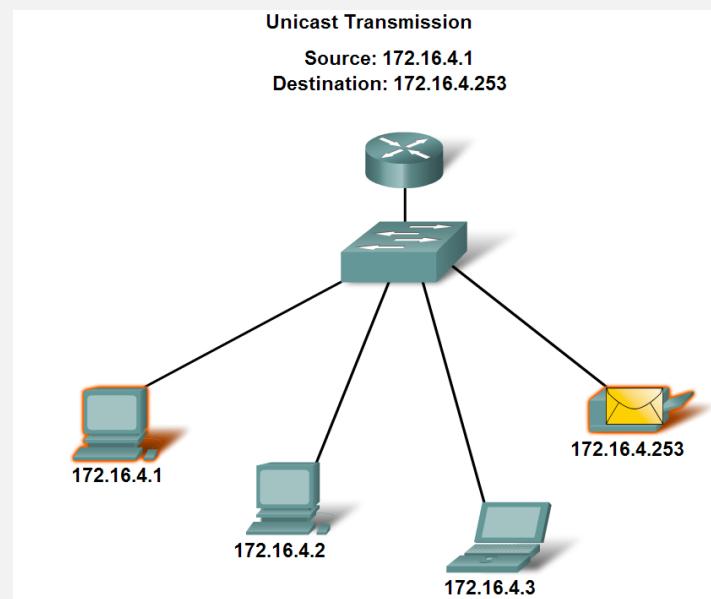
For each row, enter the values ...

Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
→ Network			
→ Broadcast			
→ First Usable Host Address			
→ Last Usable Host Address			

Classifique e Defina Endereços IPv4

- Tipos de Comunicação

- Unicast
- Broadcast
 - ✓ Limitado
 - ✓ Direcionado
- Multicast



Classifique e Defina Endereços IPv4

- Intervalos de Endereços IPv4 Reservados

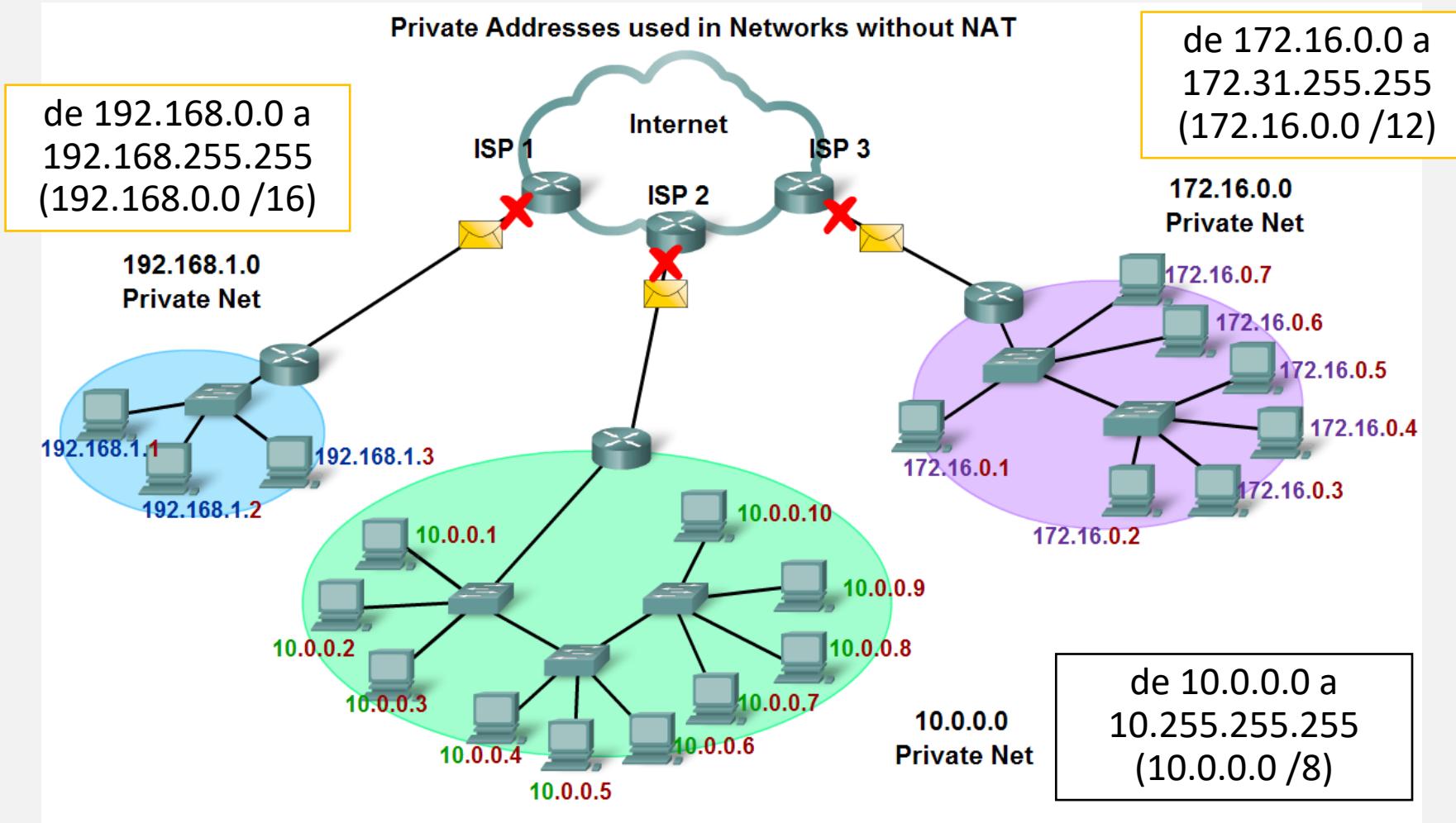
Tipos de Endereço	Uso	Faixa de Endereços IPv4 Reservados	RFC
Endereço de Host	Usado por hosts com endereço IPv4	0.0.0.0 até 223.255.255.255	790
Endereço Multicast	Usados por grupos multicast em uma rede local	224.0.0.0 até 239.255.255.255	1700
Endereço Experimental	<ul style="list-style-type: none">• Usado para pesquisa e experimentação• Atualmente não podem ser usados por hosts em redes IPv4	240.0.0.0 até 255.255.255.254	1700 3330

Faixa de endereços IP em uma rede

- O 1º endereço é o **Endereço da Rede**
- O último endereço é o **Endereço de Broadcast**
- Os Endereços de Rede e de Broadcast **não podem** ser usados em hosts.
- Assim, se uma rede possui **n** endereços, pode possuir no máximo **n-2** hosts.
- Veja os exemplos no próximo slide

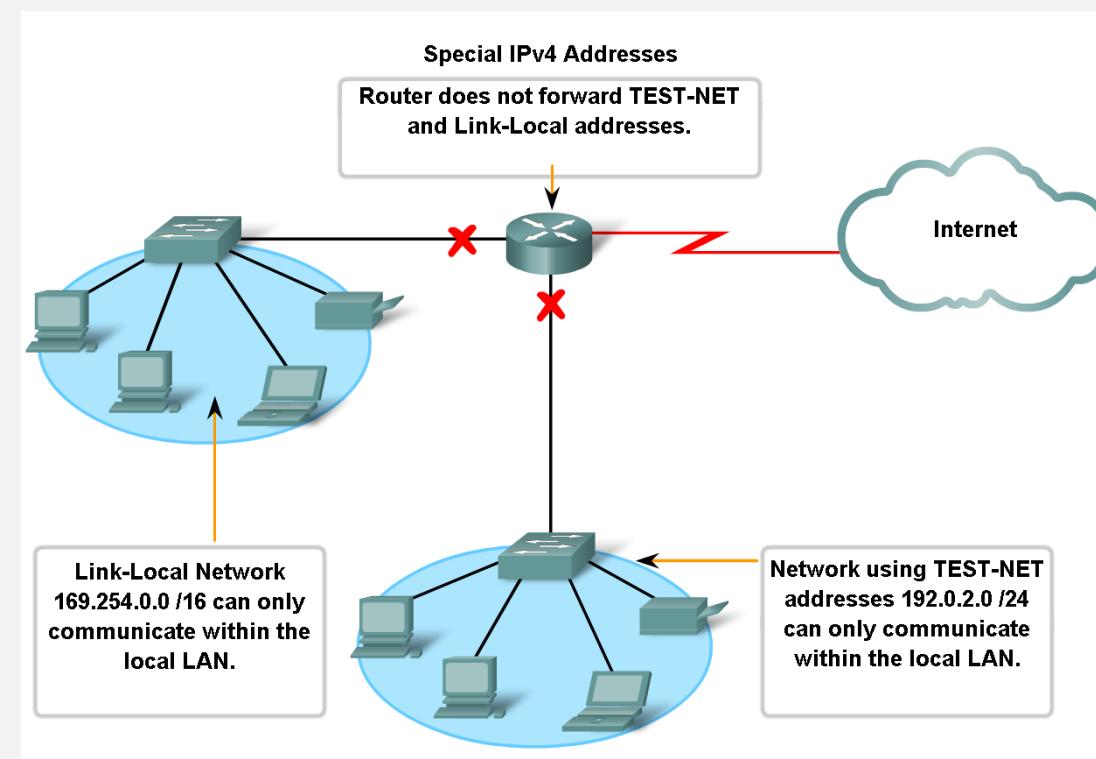
Classifique e Defina Endereços IPv4

- Endereços Públicos e Privados

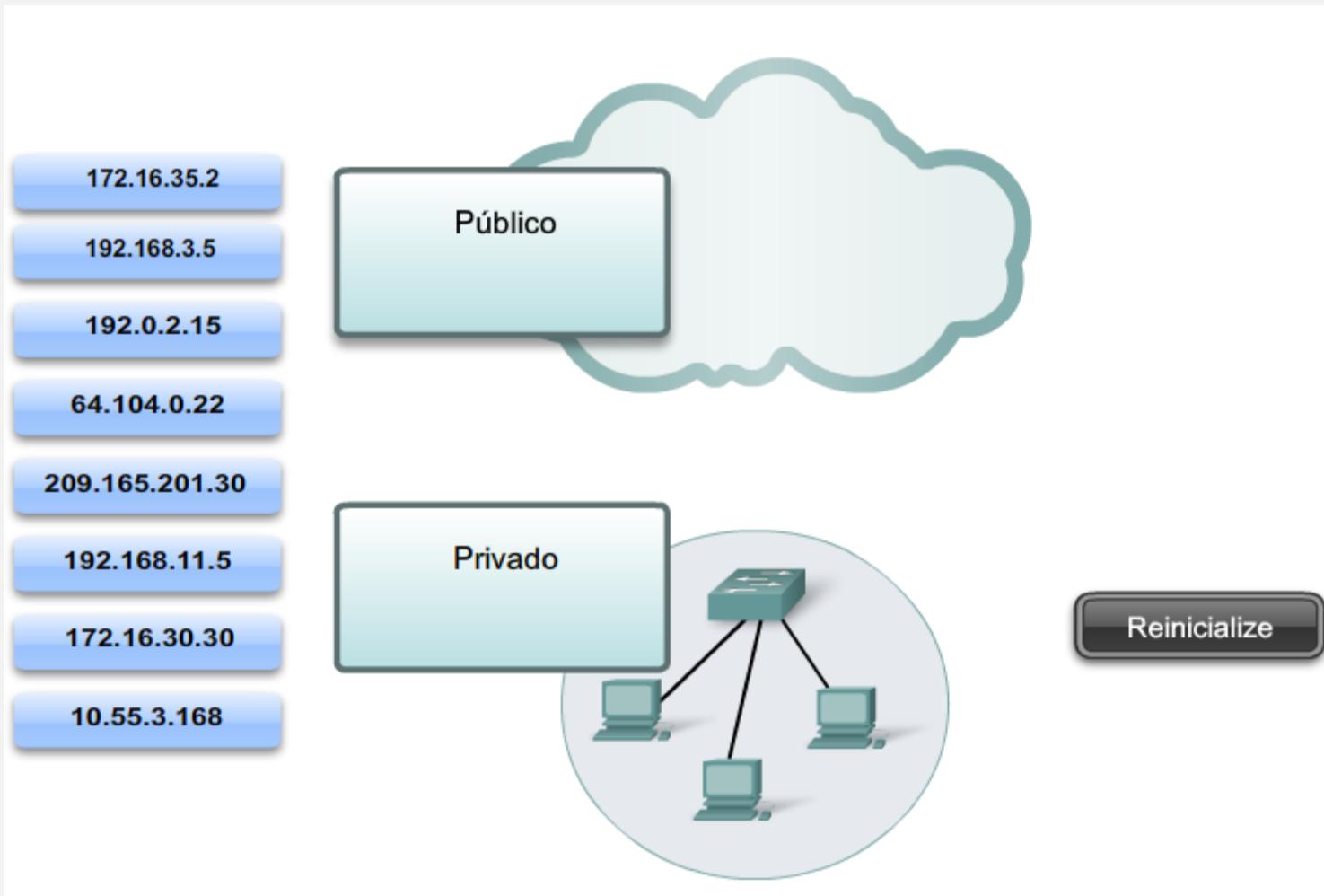


Classifique e Defina Endereços IPv4

- Endereços IPv4 Especiais
 - Endereço de Rede e de Broadcast
 - Rota padrão 0.0.0.0 / 0.0.0.0
 - Loopback (127.0.0.1 [127.0.0.0 a 127.255.255.255])
 - Endereços Locais de Link (169.254.0.0/16)
 - Endereços TEST-NET (192.0.2.0/24)



Pratique em Laboratório



Classifique e Defina Endereços IPv4

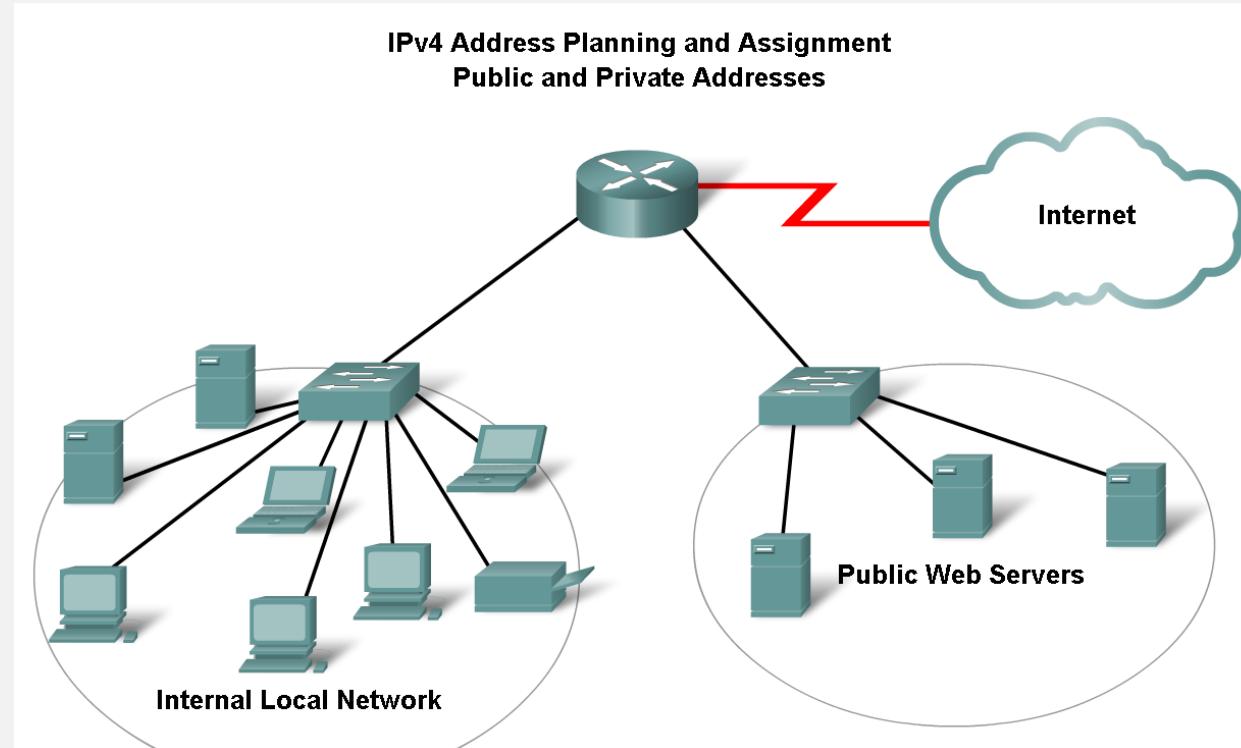
- Histórico de Endereçamento IPv4
 - Dividido em Classes – Chamado endereçamento Classful
 - Despediçava muitos endereços
- Endereços Classless

Classes de Endereço IP

Classe de Endereços	Faixa do primeiro octeto (decimal)	Bits do primeiro octeto (bits verdes não mudam)	Rede(N) e Host(H) partes do endereço	Máscara de sub-rede padrão (decimal e binário)	Número de redes possíveis e hosts por rede
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 redes (2^7) 16,777,214 hosts por rede (2^{24-2})
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 redes (2^{14}) 65,534 hosts por rede (2^{16-2})
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 redes (2^{21}) 254 hosts por rede (2^{8-2})
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

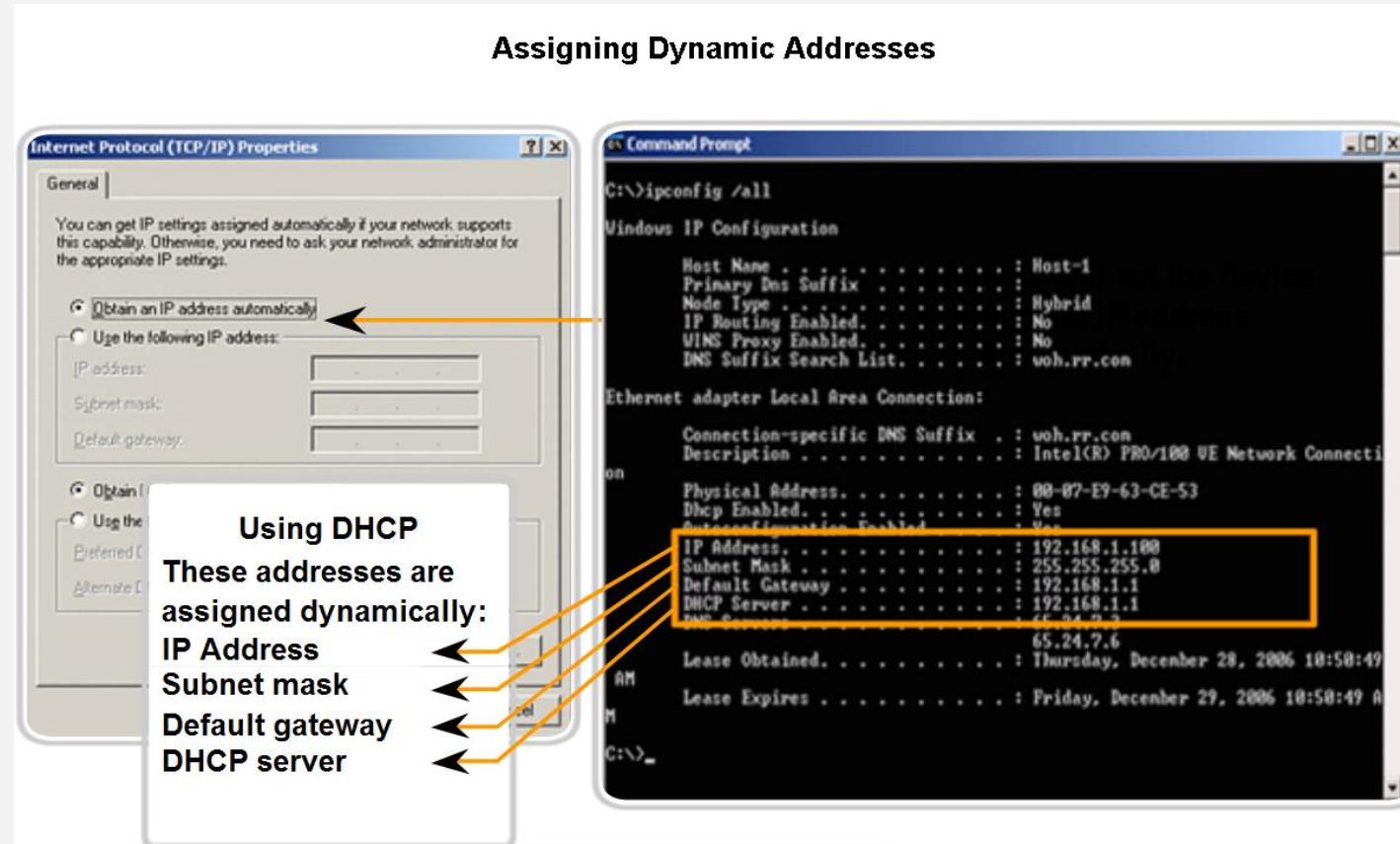
Atribuindo Endereços

- Planejamento do Endereçamento de Rede
 - Evitar a duplicação de endereços
 - Fornecer e controlar o acesso
 - Monitorar a segurança e o desempenho
- Endereço Público x Privado



Atribuindo Endereços

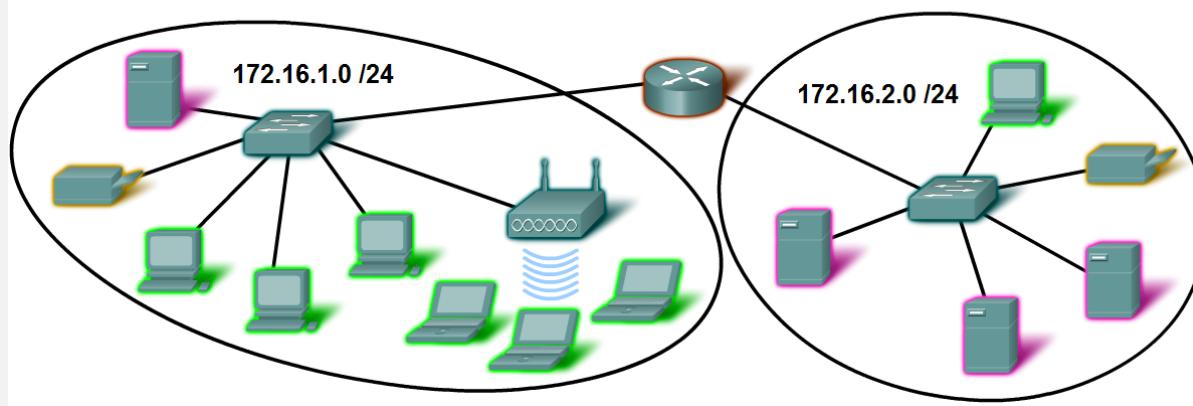
- Endereçamento de Dispositivos Finais
 - Estático – Atribuído manualmente
 - Dinâmico – Atribuído através do Protocolo DHCP



Atribuindo Endereços

- Endereço Estático
 - Servidores e Impressoras
 - Hosts acessíveis pela Internet
 - Dispositivos intermediários
 - Roteadores e Firewalls

Devices IP Address Ranges			
Use	First Address	Last Address	Summary Address
Network Address	172.16.x.0	172.16.x.0 /25
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	
Servers	172.16.x.128	172.16.x.191	172.16.x.128 /26
Peripherals	172.16.x.192	172.16.x.223	172.16.x.192 /27
Networking devices	172.16.x.224	172.16.x.253	
Router (gateway)	172.16.x.254	172.16.x.224 /27
Broadcast	172.16.x.255	



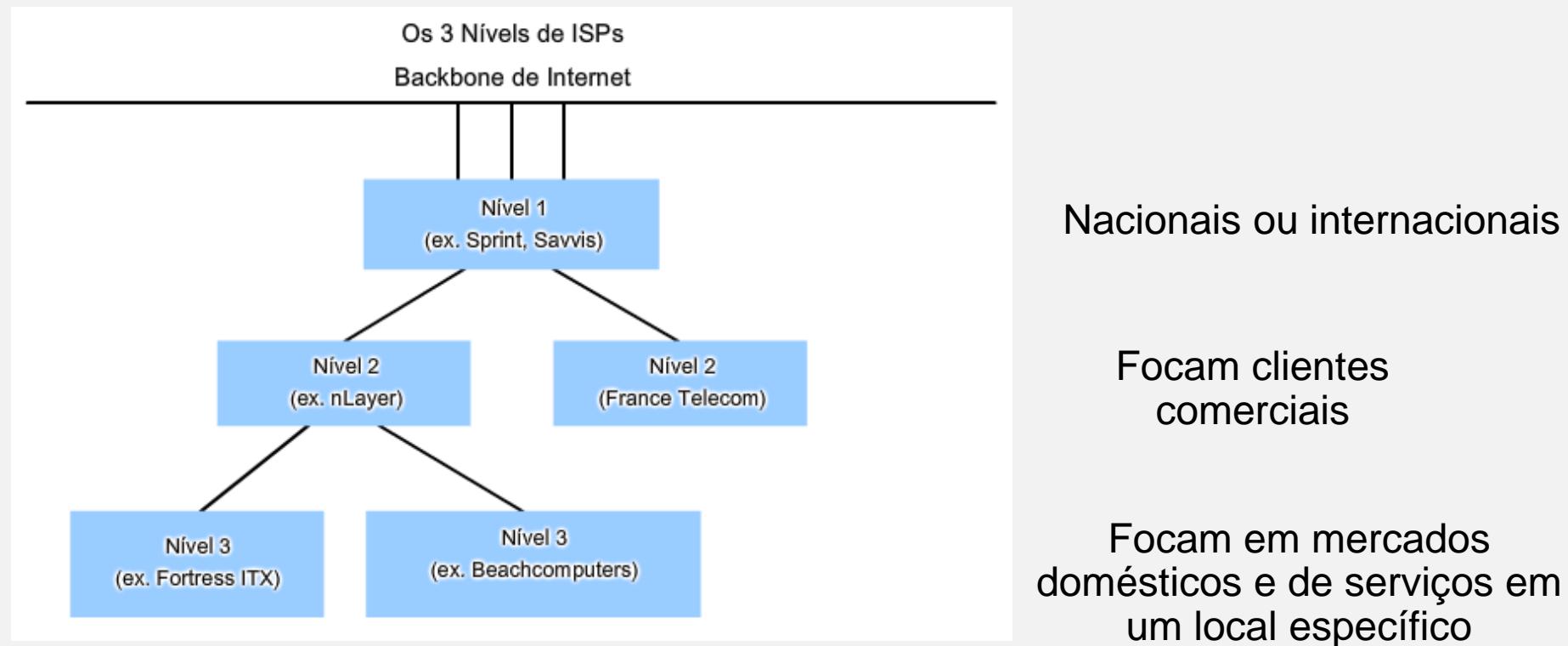
Atribuindo Endereços

- O uso de endereços públicos é regulado
- Uma organização deve ter um intervalo alocado
- IANA – Internet Assigned Numbers Authority é a detentora dos endereços IP

IANA					
Global	AfriNIC	APNIC	LACNIC	ARIN	RIPE NCC
Registros Regionais de Internet	Região da África	Região da Ásia/ Pacífico	Região da América Latina e Caribe	Região da América do Norte	Região da Europa, Oriente Médio e Ásia Central

Atribuindo Endereços

- Provedores de Internet
 - Fornecem pequeno número de endereços aos clientes
 - Níveis de ISP



Determinar a Porção de Rede do Endereço de Host e o Papel da Máscara de Sub-rede

- Máscara de Sub-rede – Definição da Rede e das Porções de Host
 - Prefixo e a máscara de sub-rede são modos diferentes de representar a mesma coisa - a porção de rede de um endereço.

Endereço IP	172	.	16	.	4	.	1
	10101100		00010000		00000100		00000001
Máscara de Sub-rede	255	.	255	.	255	.	0
	11111111		1111111111		11111111		00000000
Prefixo /24 (24 bits mais significativos)							

Determinar a Porção de Rede do Endereço de Host e o Papel da Máscara de Sub-rede

- Operação lógica AND
 - Utilizada para determinar o endereço de rede
 - Roteadores usam para determinar uma rota
 - Hosts usam para determinar se o pacote é direcionado para rede local ou gateway

1 AND 1 = 1
1 AND 0 = 0
0 AND 1 = 0
0 AND 0 = 0

	Bits mais significativos				Bits menos significativos	
	Prefixo /16					
	192	.	0	.	0	.
Host Endereço	11000000	00000000	00000000	00000001		
Sub-rede Máscara	255	255	0	0		
	11111111	11111111	00000000	00000000		
Endereço de Rede	11000000	00000000	00000000	00000000		
Rede	192	.	0	.	0	.

Determinar a Porção de Rede do Endereço de Host e o Papel da Máscara de Sub-rede

- Utilizando o AND lógico.

Applying the Subnet Mask						
A device with address 192.0.0.1 belongs to network 192.0.0.0						
	High order bits Prefix /16			Low order bits		
	192	.	0	.	0	.
Host	11000000		00000000		00000000	00000001
Subnet	255		255		0	0
	11111111		11111111		00000000	00000000
Network	11000000		00000000		00000000	00000000
Network	192	.	0	.	0	.

Determinar a Porção de Rede do Endereço de Host e o Papel da Máscara de Sub-rede

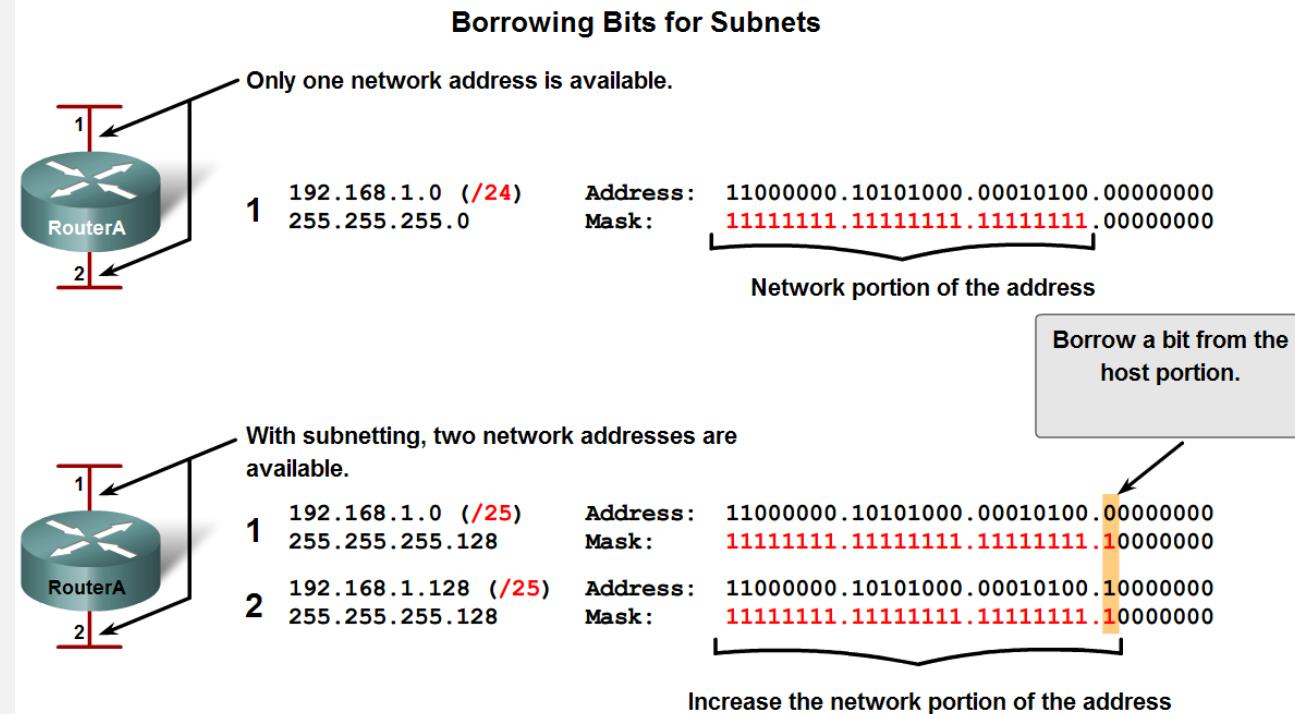
- Observe os passos para a conversão
 1. Converter o endereço de host para binário
 2. Converter o prefixo /20 em máscara de sub-rede binária
 3. Realizar o AND lógico da máscara com o host
 4. Converta o endereço obtido em decimal

Usando a máscara de sub-rede para determinar o endereço para o host 172.16.132.70/20

Endereço de Host	172	16	132	70
Endereço de Host Binário	10101100	00010000	10000100	01000110
Máscara de sub-rede binária	11111111	11111111	11110000	00000000
Endereço de Host Binário	10101100	00010000	10000000	00000000
Endereço de Rede	172	16	128	0

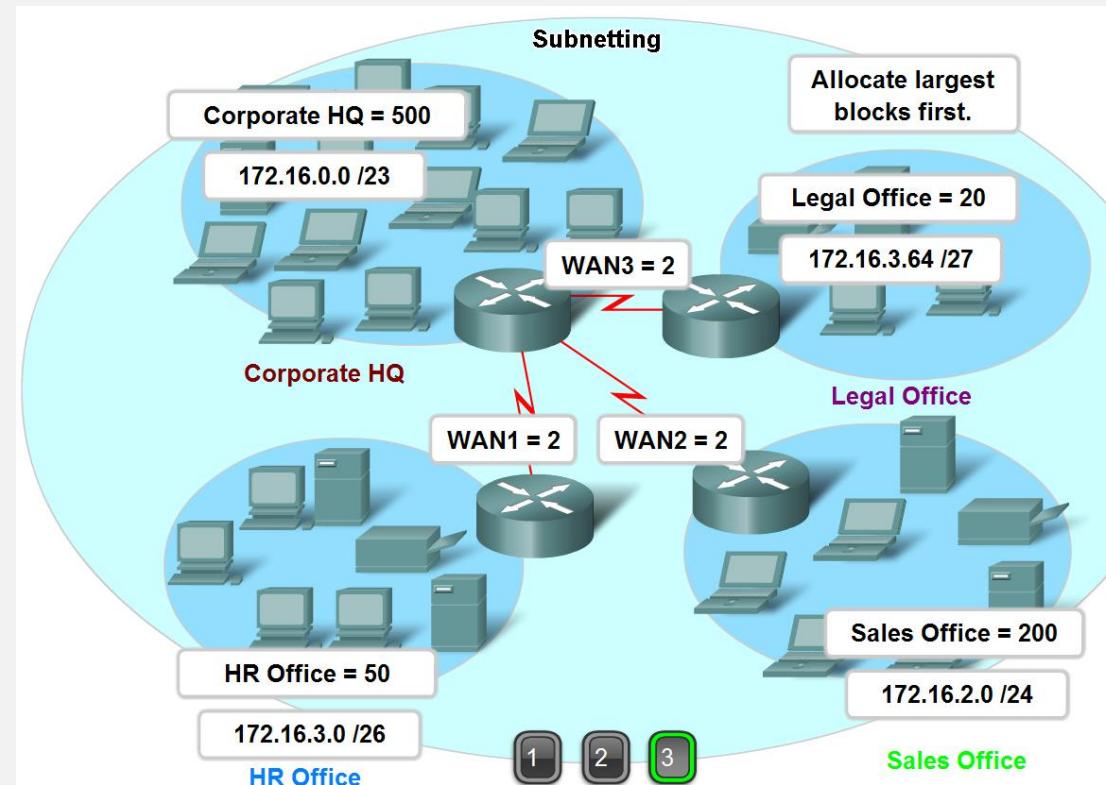
Calculando Endereços

- Criação de sub-redes
 - Permite criar múltiplas redes lógicas
 - Pega-se bits emprestados da porção de host
 - 2^n = número de sub-redes
 - $2^n - 2$ = número de hosts



Calculando Endereços

- Divisão de redes no tamanho correto
 - Determine o nº total de hosts
 - Determine o nº e tamanho das redes



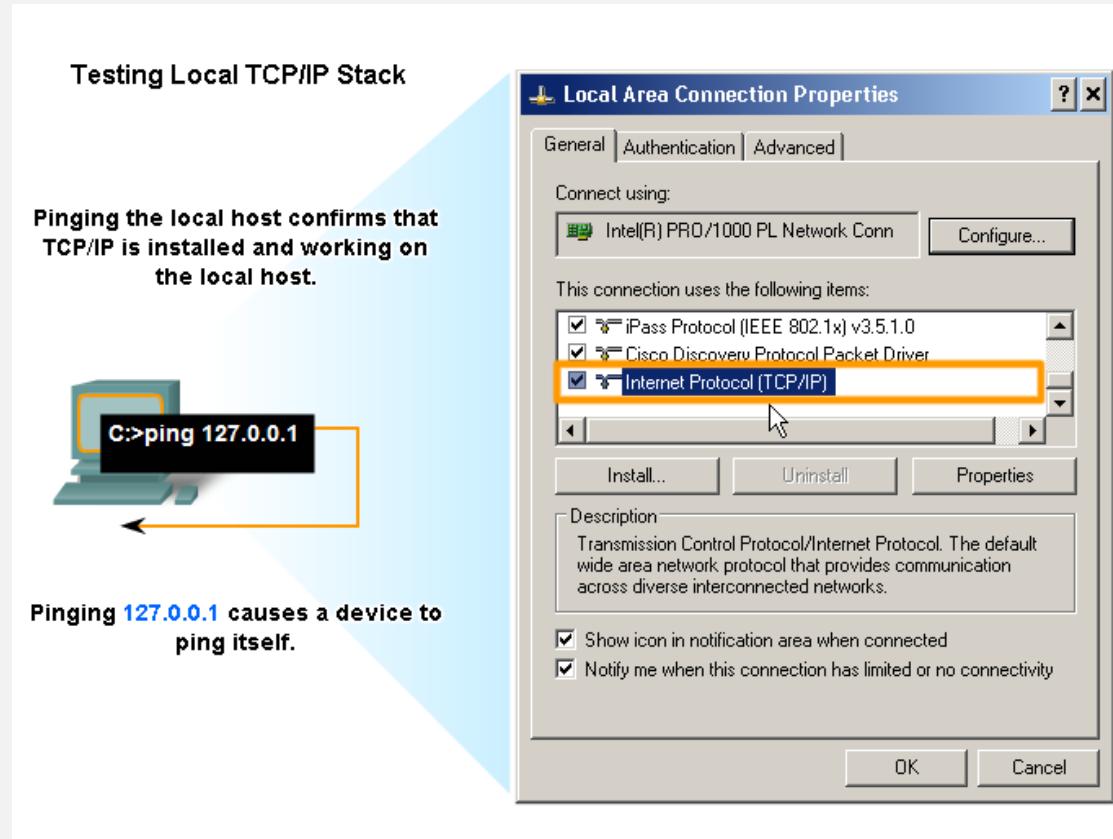
Diretrizes para endereçamento IP

Ao atribuir identificações de rede e host:

- Não usar 127 como identificação de rede
- Somente usar endereços registrados públicos onde for essencial fazê-lo
- Usar a faixa de endereços privados do IANA para endereços privados
- Não usar todos os números 1 binários para a identificação do host em uma rede baseada em classes
- Não usar todos os números 0 binários para a identificação de rede em uma rede baseada em classes
- Não repetir identificações de host

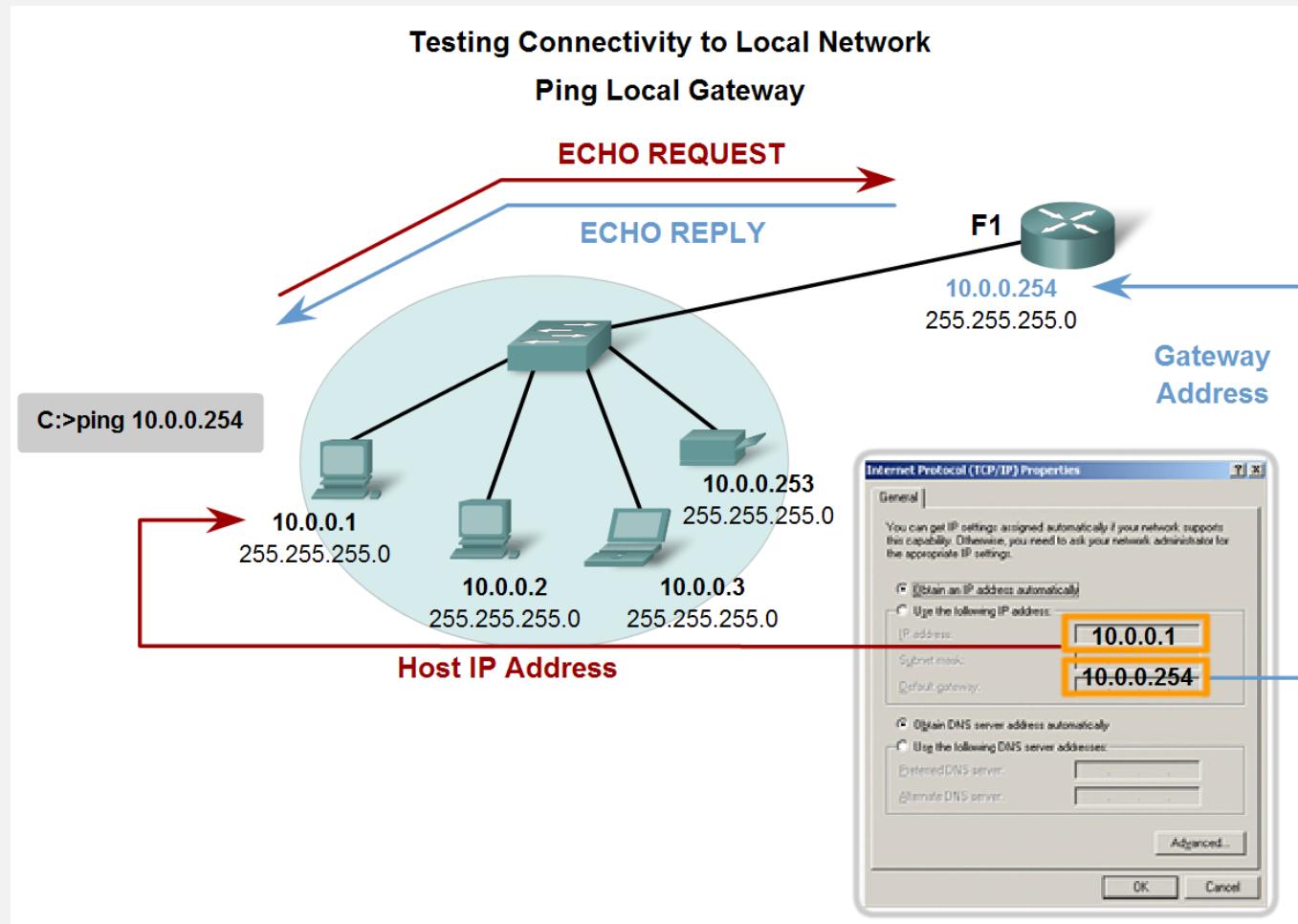
Testando a Camada de Rede

- PING – utilitário para testar conectividade entre hosts
- Utiliza um protocolo de camada 3, o Internet Control Message Protocol (ICMP)



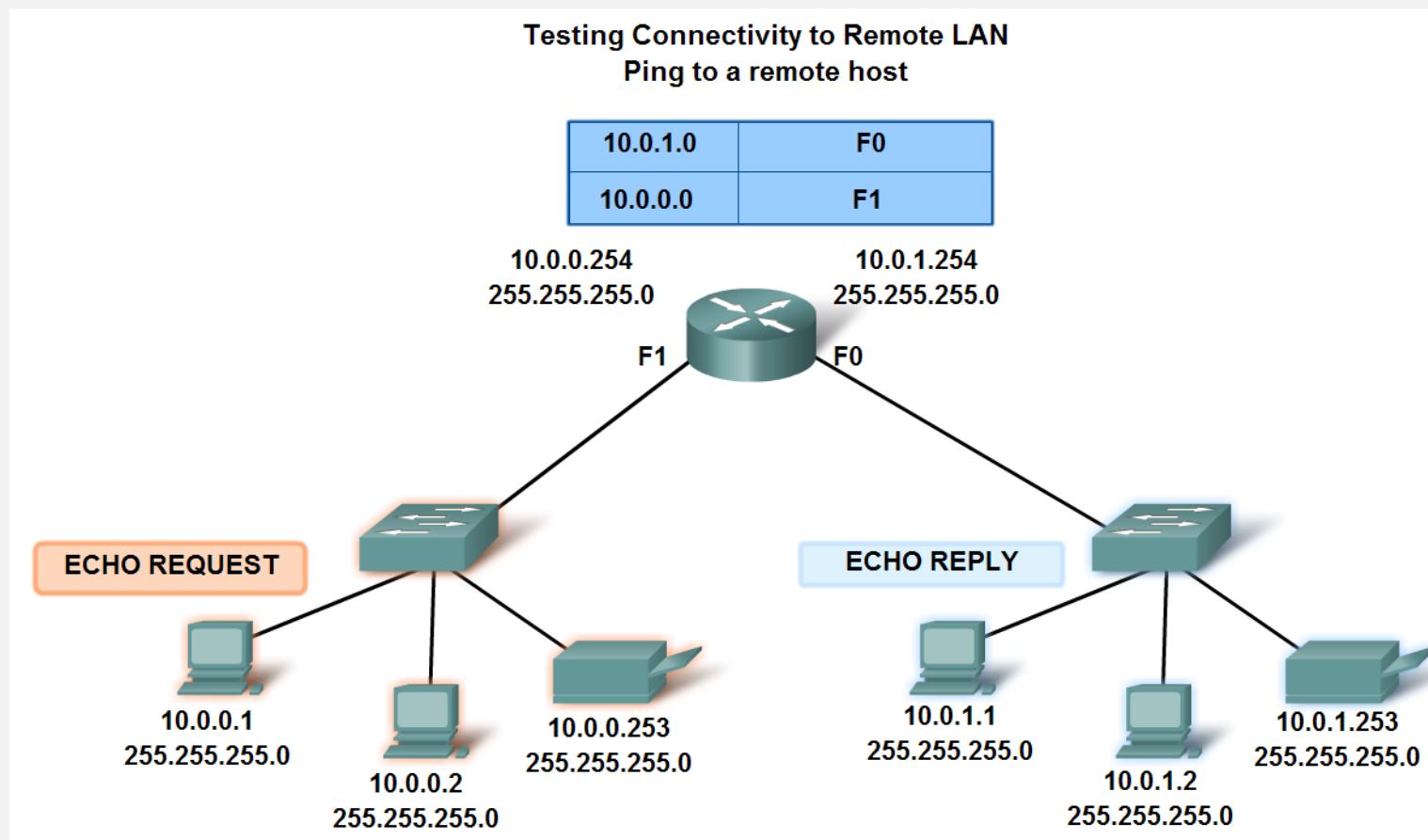
Testando a Camada de Rede

- Use o ping para verificar que o host pode se comunicar com o gateway através da rede local



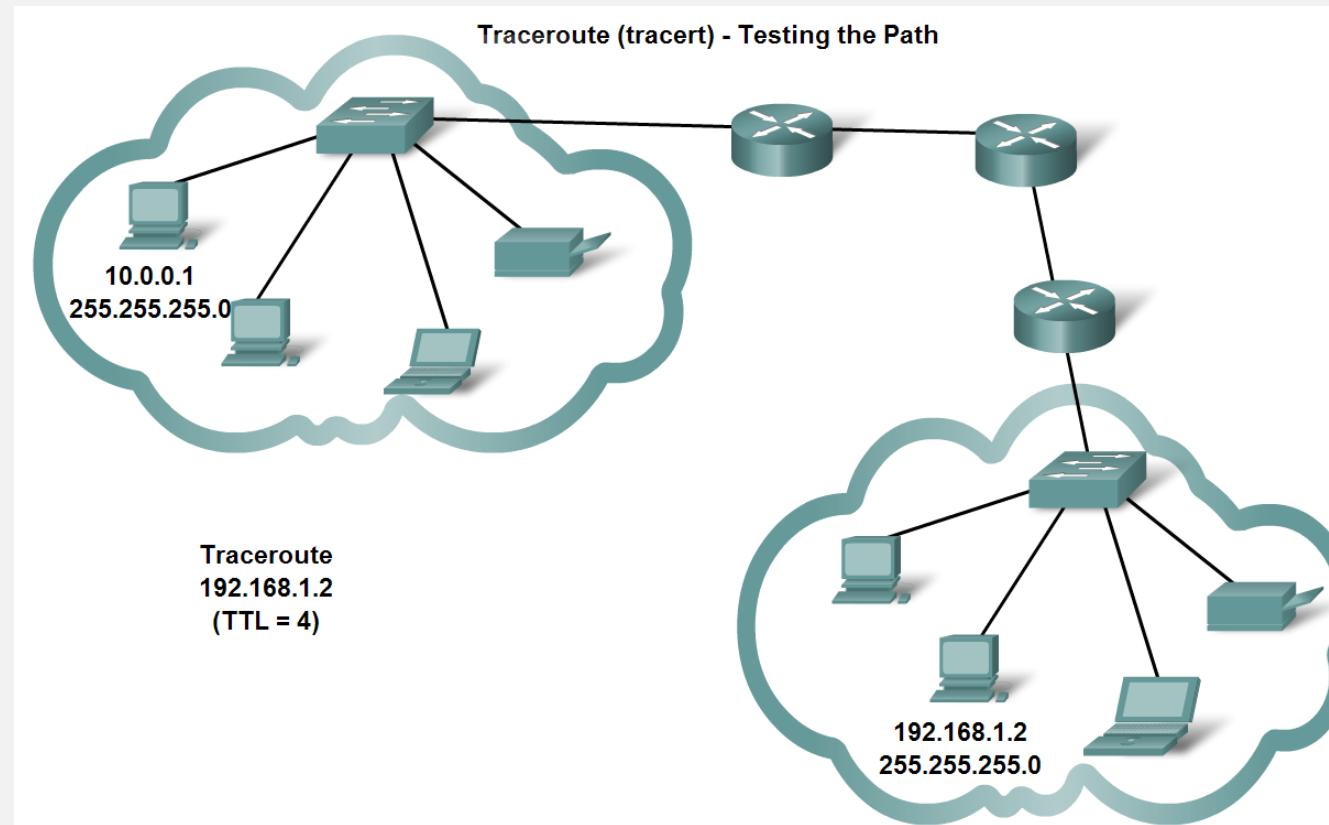
Testando a Camada de Rede

- Use o ping para verificar que o host pode se comunicar através do gateway com um dispositivo em outra rede

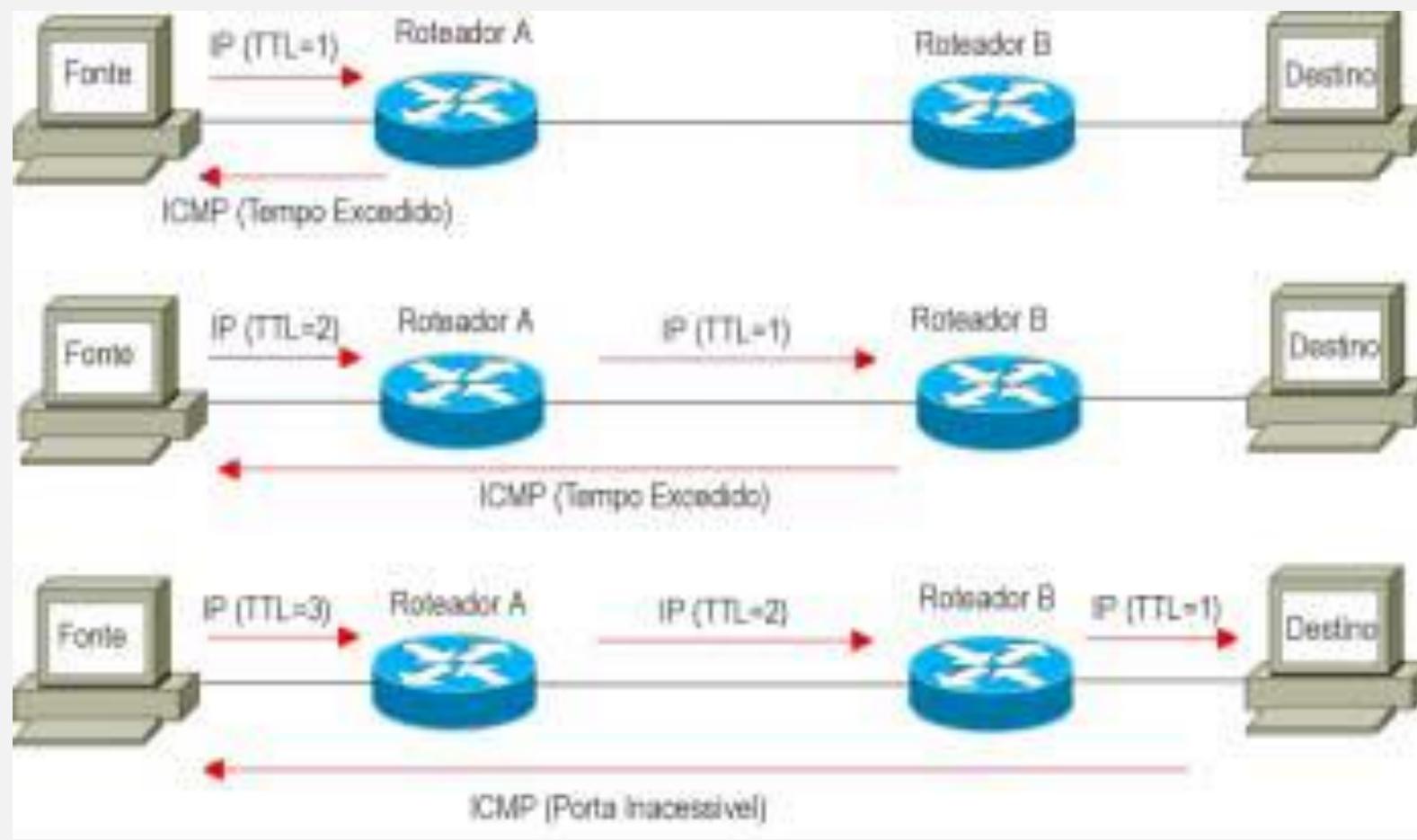


Testando a Camada de Rede

- Use o tracert/traceroute para observar o caminho entre dois dispositivos que se comunicam através da rede

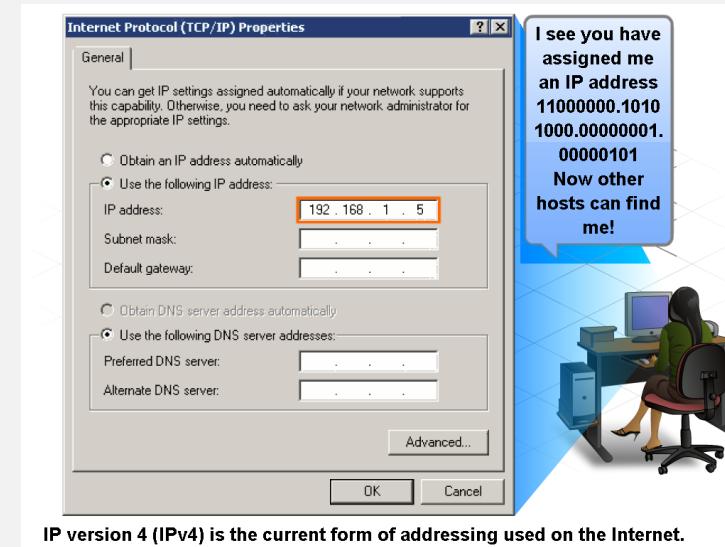


Funcionamento Traceroute

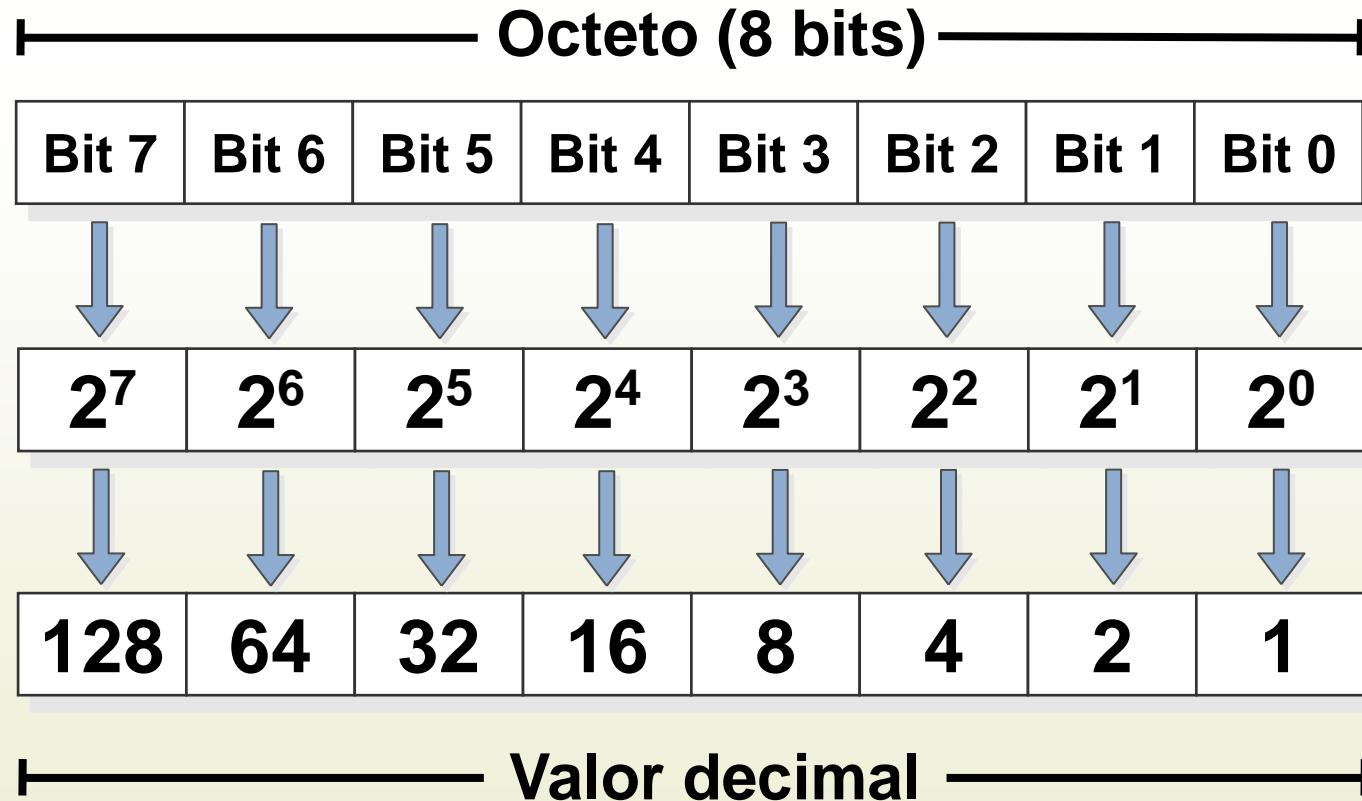


Estrutura do Endereço IP

- Endereço binário de 32 Bits
- Representado utilizando a forma decimal pontuada
 - Cada byte do padrão binário, chamado de octeto, é separado com um ponto
 - Por exemplo, o endereço:
 - 10101100000100000000010000010100 é expresso no formato decimal com pontos como: 172.16.4.20

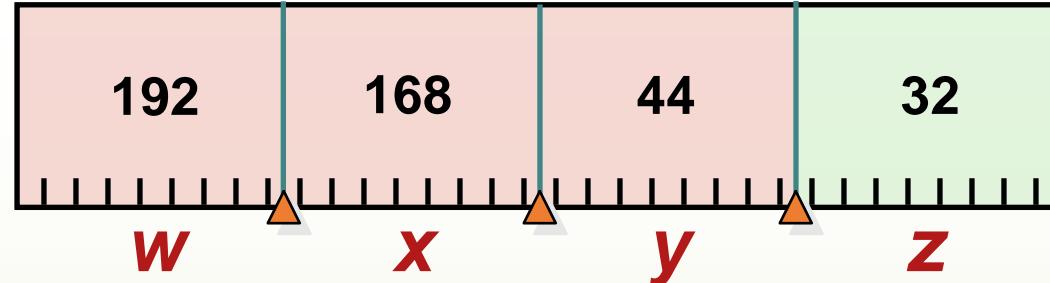


A relação entre notação decimal com ponto e números binários

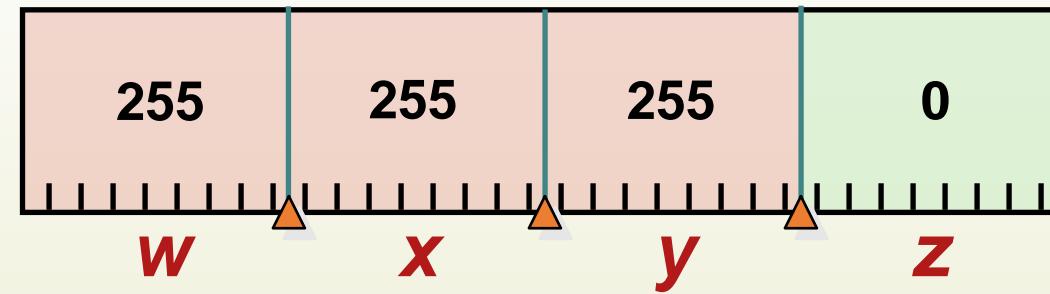


Máscara de sub-rede

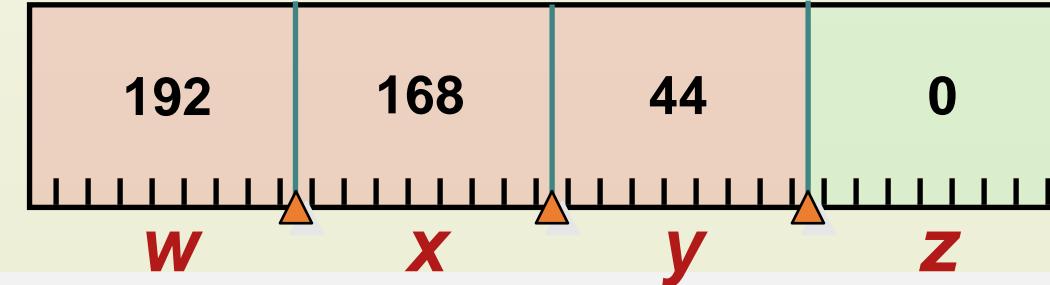
IP



Máscara



Network ID



Estrutura do Endereço IP



Mascara de Sub-Rede

Exemplo

Se você recebeu o endereço /16: 130.5.0.0 e você deseja usar o terceiro byte para representar o endereço de sub rede, então devemos usar a máscara: 255.255.255.0

		Prefixo de rede	Número de subrede	Número do host
Endereço IP:	130.5.5.25	10000010.00000101.	00000101.	00011001
Máscara de subrede:	255.255.255.0	11111111.11111111.	11111111.	00000000

← prefixo estendido de rede →

Notação CIDR

Classless Interdomain Routing

Ao invés de usar o endereço IP mais a máscara de sub rede como acima, podemos escrever apenas: 130.5.5.25/24. O número 24 designa o número de bits no prefixo de rede.

Embora a notação de endereço acima seja a mais moderna, os protocolos da Internet ainda exigem a máscara de subrede.

Exemplo - Notação

Exemplo

Uma organização possui o endereço 193.1.1.0/24 e necessita de 6 subredes. O número máximo de hosts a serem suportados é 25.

Número de bits para subredes: 3

Número de bits para hosts: 5

193.1.1.0/24 = 11000001.00000001.00000001.00000000

Máscara: 11111111.11111111.11111111.11100000 =
255.255.255.224

Endereço estendido: 193.1.1.0/27

Base Net: 11000001.00000001.00000001 .00000000 = 193.1.1.0/24

Subnet #0:	11000001.00000001.00000001. 000 00000 = 193.1.1.0/27
Subnet #1:	11000001.00000001.00000001. 001 00000 = 193.1.1.32/27
Subnet #2:	11000001.00000001.00000001. 010 00000 = 193.1.1.64/27
Subnet #3:	11000001.00000001.00000001. 011 00000 = 193.1.1.96/27
Subnet #4:	11000001.00000001.00000001. 100 00000 = 193.1.1.128/27
Subnet #5:	11000001.00000001.00000001. 101 00000 = 193.1.1.160/27
Subnet #6:	11000001.00000001.00000001. 110 00000 = 193.1.1.192/27
Subnet #7:	11000001.00000001.00000001. 111 00000 = 193.1.1.224/27

Exemplo - Notação

- Definido o endereço de broadcast para cada subnet:
 - O endereço de broadcast da subnet é o endereço estendido da subnet com todos os bits de host setados para 1.
 - Exemplo
 - Endereço de broadcast para subnet 6:
 - Subnet #6:
 - $11000001.00000001.00000001.11011111 = 193.1.1.223/27$

Redes IP – Classe A

Redes Classe A

Cada endereço de rede da classe A possui 8 bits de prefixo de rede com o bit mais significativo definido para 0 e um número de rede de 7 bits, seguido por um número de *host* de 24 bits. Mais modernamente redes de Classe A são chamadas de /8 (pronuncia-se barra 8) porque apresentam prefixo de rede 8 bits.

Redes /8	
Número máximo de redes *	$2^7 - 2 = 126$
Número máximo de <i>Hosts</i> por rede **	$2^{24} - 2 = 16\ 777\ 214$
Espaço IPv4	50%

	Prefixo	Sufixo	Significado
*	tudo 0	0.0.0.0 /8	este computador (usado para <i>bootstrap</i>)
	127	127.0.0.0 /8	reservado para função <i>loopback</i>
**	Rede	tudo 0s	Esta rede
	Rede	tudo 1s	<i>Broadcast</i>

Endereços especiais

Redes IP – Classe B

Redes Classe B

Cada endereço de rede da classe B possui 16 bits de prefixo de rede com os dois bits mais significativos definidos para 10 e um número de rede de 14 bits, seguido por um número de host de 16 bits. Mais modernamente redes de Classe B são chamadas de /16 porque apresentam prefixo de rede 16 bits. Os endereços de classe B tem-se esgotado rapidamente.

Redes /16	
Número máximo de redes	$2^{14} = 16384$
Número máximo de <i>Hosts</i> por rede **	$2^{16}-2 = 65534$
Espaço IPv4	25%

Redes IP – Classe C

Redes Classe C

Cada endereço de rede da classe C possui 24 bits de prefixo de rede com os três bits mais significativos definidos para 110 e um número de rede de 21 bits, seguido por um número de host de 8 bits. Mais modernamente redes de Classe C são chamadas de /24 porque apresentam prefixo de rede 24 bits.

Redes /24	
Número máximo de redes	$2^{21} = 2\ 097\ 152$
Número máximo de <i>Hosts</i> por rede **	$2^8 - 2 = 254$
Espaço IPv4	12.5%

Endereços Especiais

Endereço do computador

O endereço 0.0.0.0/8 significa “*este computador*”. Este endereço é usado pelo protocolo de *start up* de um computador para obter o endereço IP do próprio host. Como o próprio protocolo IP é utilizado para este fim e este protocolo exige um endereço fonte o endereço 0.0.0.0/8 é utilizado.

Endereço de loopback

O endereço cujo prefixo é 127/8 é utilizado para testar uma aplicação TCP/IP no próprio computador. Dois programas que querem se comunicar via rede podem ser testados desta forma. Toda mensagem enviada para o endereço de prefixo 127, por exemplo, 127.0.0.1 é roteado para o outro programa tentando receber do mesmo endereço.

Endereço da rede

O endereço que começa com um prefixo de rede e é seguido de zeros serve para designar o prefixo atribuído à rede e não os computadores da rede. Por exemplo, o endereço 150.164.0.0/16 serve para designar a rede da UFMG, que recebeu o prefixo 150.164.

Endereço de broadcast

O endereço prefixo seguido de 1s serve para enviar um pacote para todos os *hosts* de uma rede (endereço de *broadcast*).

Endereços Especiais

Redes privadas

Num rede privada, isto é, não acessível via Internet como a rede de micros em uma casa que se conecta ao ambiente externo por um router, os endereços podem ser escolhidos arbitrariamente dentro do range de endereços especificados pela RFC 1918:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Estes endereços não podem ser usados externamente para uso na Internet.

Endereçamento IP

Em notação decimal, as faixas de endereço das diversas classes ficam:

Classe de Endereços	Faixa de Endereços em notação decimal		
A (prefixo /8)	1.xx.xx.xx	a	126.xx.xx.xx
B (prefixo /16)	128.0.xx.xx	a	191.255.xx.xx
C (prefixo /24)	192.0.0.xx	a	223.255.255.xx

Problemas do endereçamento por classes puras:

- a) Esgotamento do endereços IP, principalmente os da classe B.
- b) Aumento do tamanho das tabelas de roteamento nos roteadores.

Como as tabelas de roteamento estavam crescendo e os administradores tinham que pedir novos números de rede à Internet toda vez que necessitavam instalar uma nova rede em seu site, foi criado um segundo nível na hierarquia de endereços IP. Esta arquitetura em 3 níveis se chamou de *subnetting*. *Subnetting* divide um único endereço de rede em vários endereços de subrede de tal forma que cada rede física tenha seu próprio endereço.

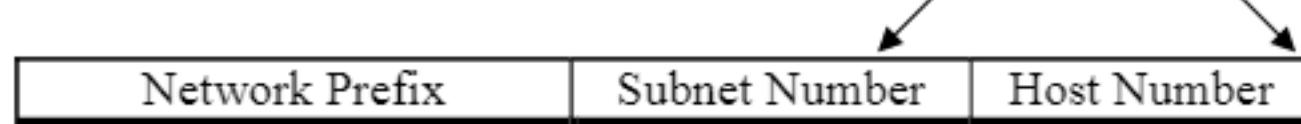
Endereçamento IP

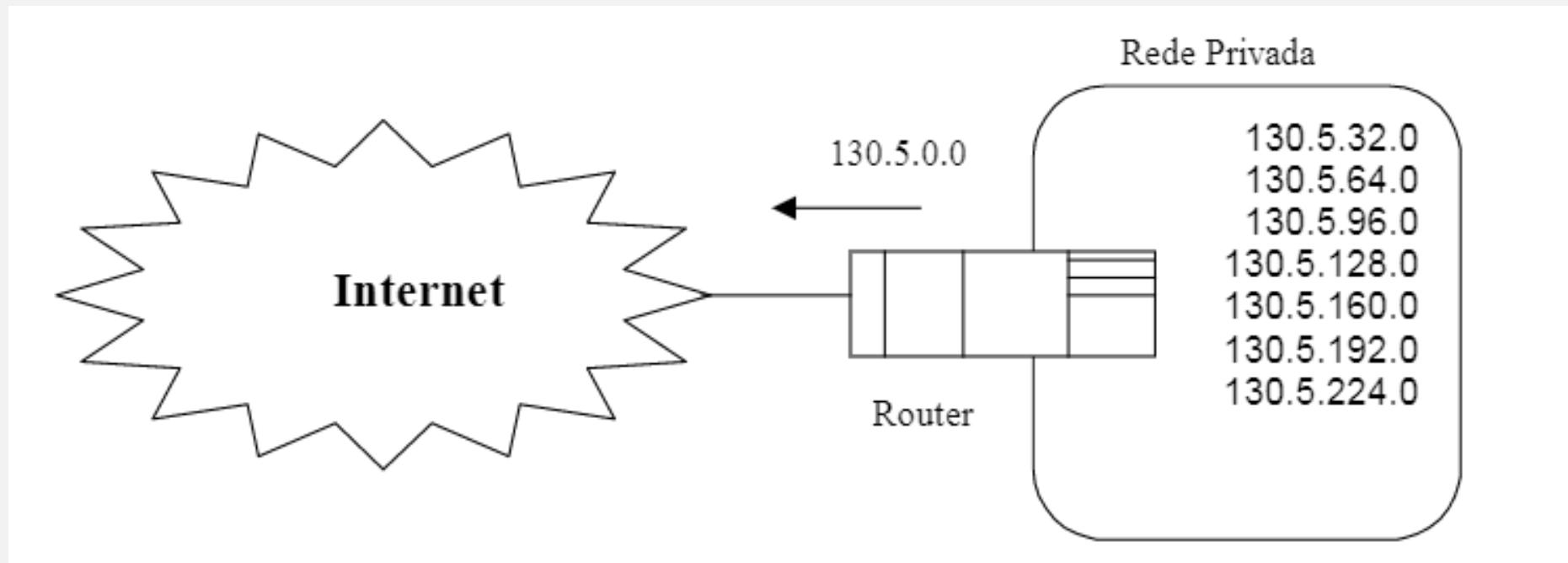
Como as tabelas de roteamento estavam crescendo e os administradores tinham que pedir novos números de rede à Internet toda vez que necessitavam instalar uma nova rede em seu site, foi criado um segundo nível na hierarquia de endereços IP. Esta arquitetura em 3 níveis se chamou de *subnetting*. *Subnetting* divide um único endereço de rede em vários endereços de subrede de tal forma que cada rede física tenha seu próprio endereço.

Hierarquia de 2-níveis (*Classful*):

Network Prefix	Host Number
----------------	-------------

Hierarquia em três níveis (Subnet):





Roteamento através de Gateways

Exemplo

Host fonte	
Aplicação	
Transporte	
Destino	Gateway
128.66.1.0	128.66.12.3
128.66.12.0	128.66.12.2
default	128.66.12.1
Acesso à Rede	
128.66.12.2	

Gateway

Destino	Gateway
128.66.1.0	128.66.1.5
128.66.12.0	128.66.12.3
default	128.66.12.1
Acesso à rede	
128.66.12.3	128.66.1.5

Host destino

Aplicação	
Transporte	
Destino	Gateway
128.66.1.0	128.66.1.2
default	128.66.1.5
Acesso à rede	
128.66.1.2	

128.66.12.0

128.66.1.0

Roteamento de mensagens através de um gateway

Atividade

- Responda as seguintes questões do Capítulo 5 “A Camada de Rede” do livro “Redes de Computadores” de Andrew Tanenbaum:
 - Questões de Revisão 37, 38, 42, 51 e 52.
 - O trabalho poderá ser realizado em duplas ou individualmente e entregue até o final da aula.

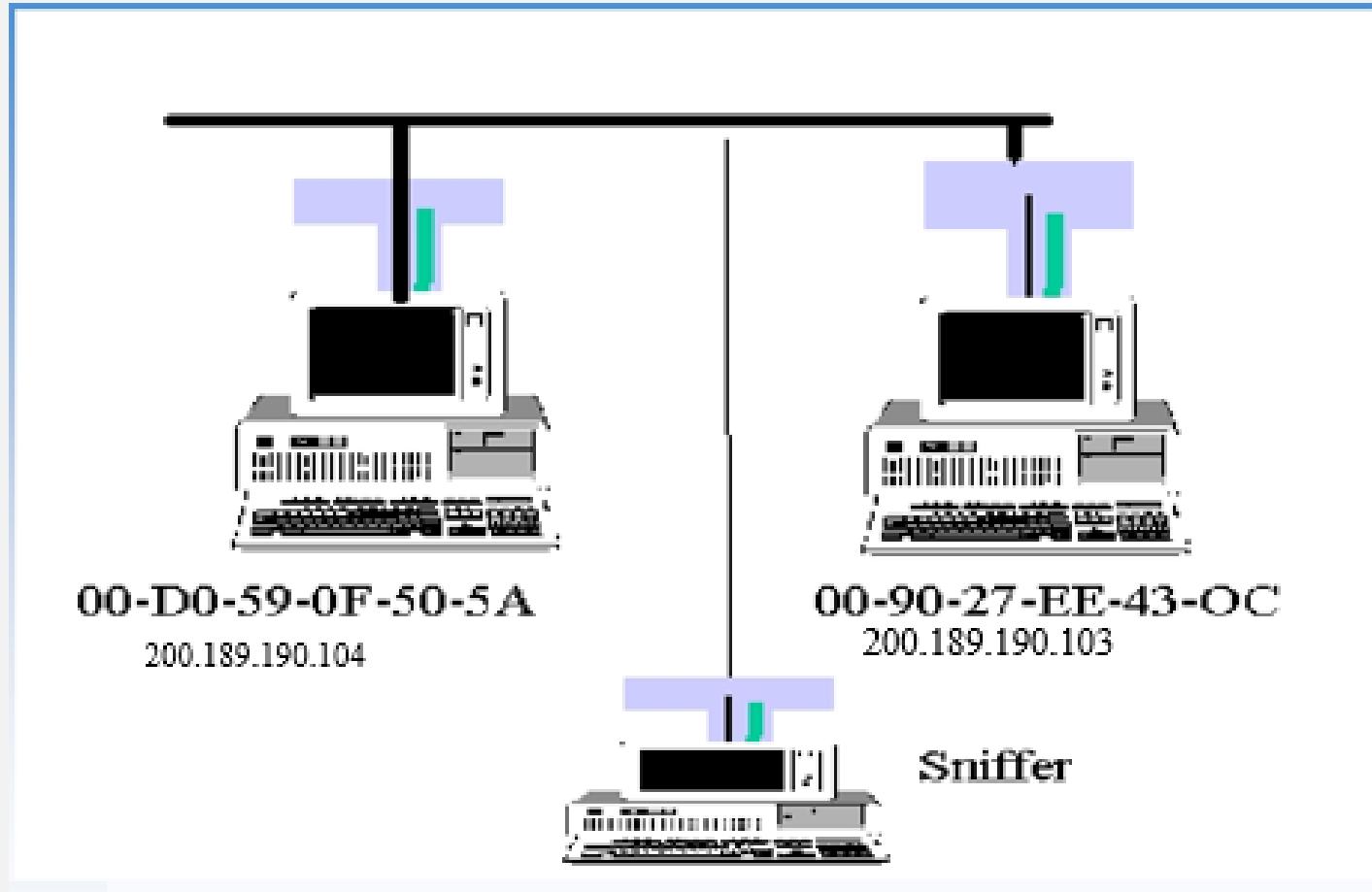


Analisador de redes

- Analisador de Rede, Monitor de Rede ou simplesmente “Sniffer” é um dispositivo que pode ser configurado para contar ou mostrar quadros conforme eles passam por uma rede compartilhada.

Redes Locais

Laboratório Sniffer

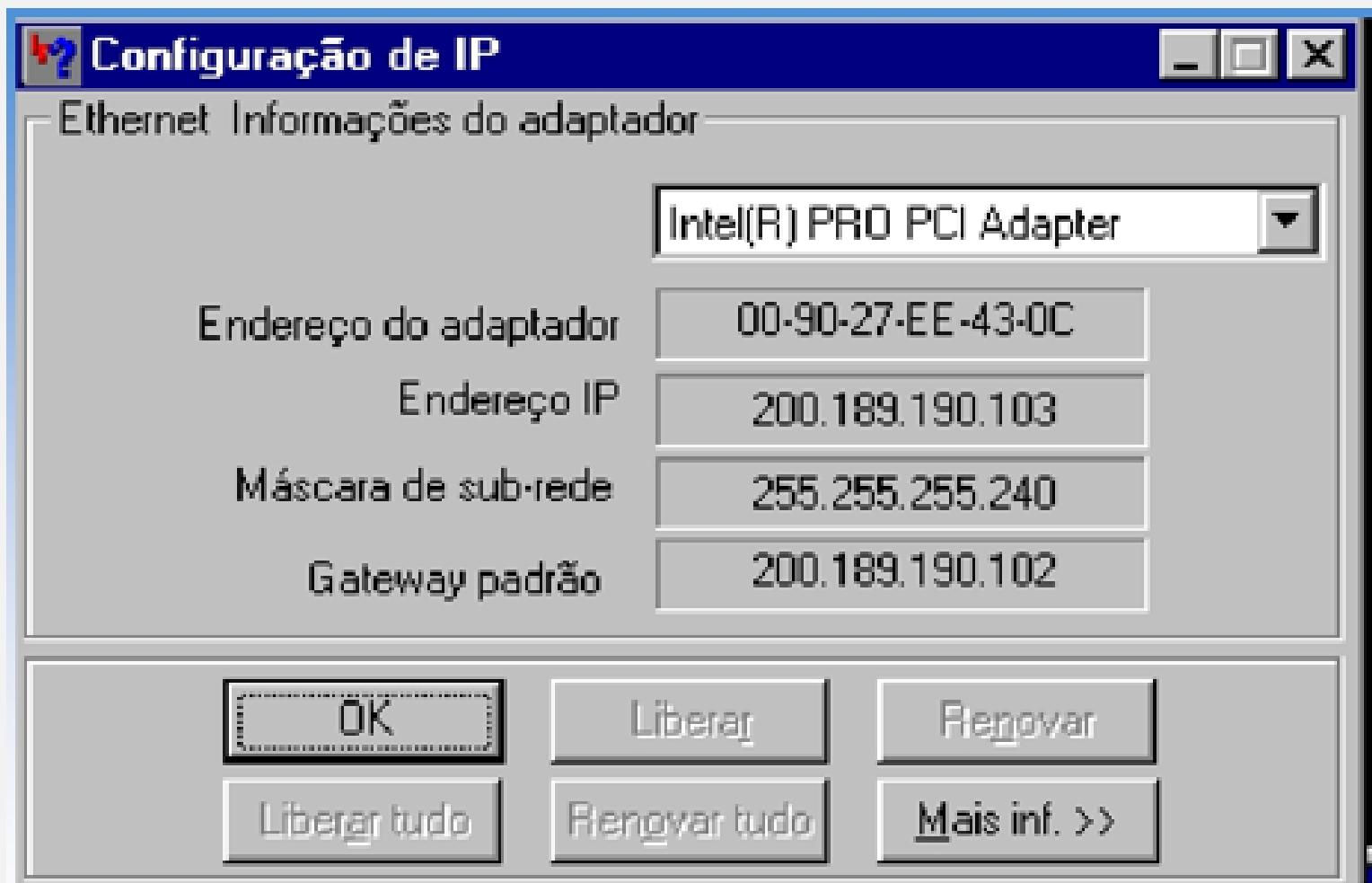


Redes Locais

ipconfig

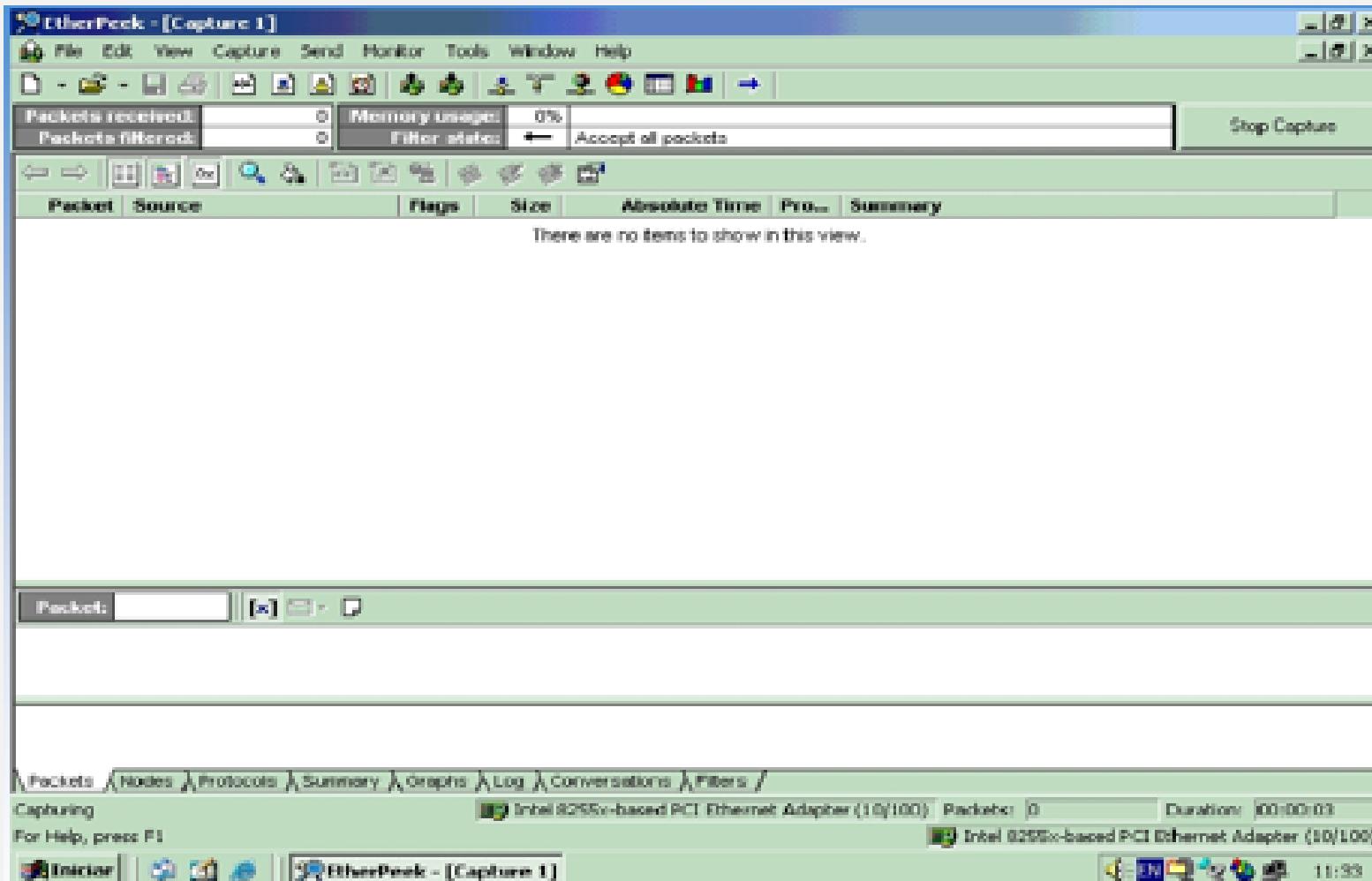
Redes Locais

winipcfg



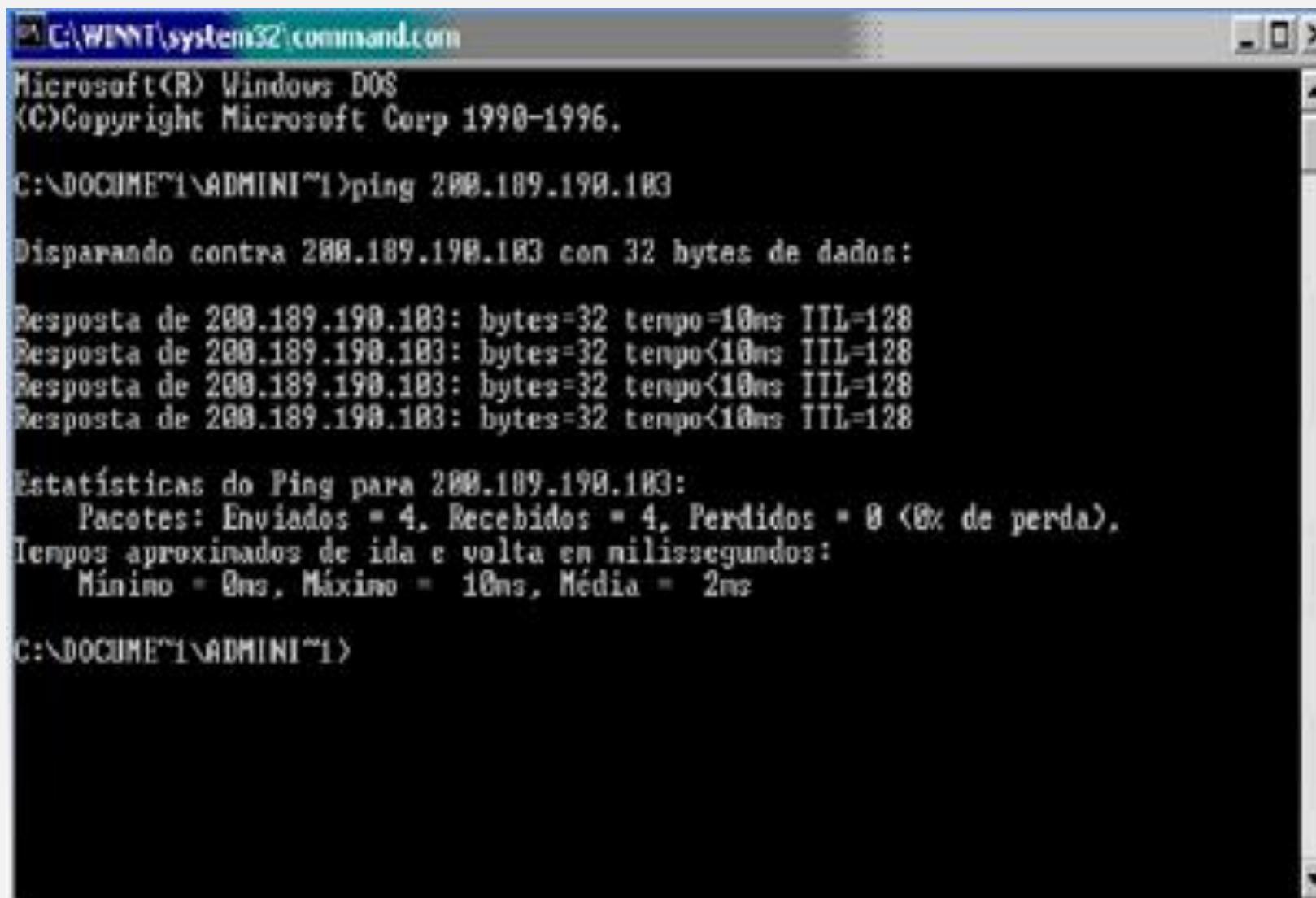
Redes Locais

Sniffer



Redes Locais

Testando- ping



A screenshot of a Windows DOS command window titled 'C:\WINNT\system32\command.com'. The window displays the output of a 'ping' command. The text in the window is as follows:

```
Microsoft (R) Windows DOS  
(C)Copyright Microsoft Corp 1990-1996.  
C:\DOCUMENTOS\ADMINISTRADOR>ping 200.189.198.183  
Disparando contra 200.189.198.183 com 32 bytes de dados:  
Resposta de 200.189.198.183: bytes=32 tempo=10ms TTL=128  
Resposta de 200.189.198.183: bytes=32 tempo<10ms TTL=128  
Resposta de 200.189.198.183: bytes=32 tempo<10ms TTL=128  
Resposta de 200.189.198.183: bytes=32 tempo<10ms TTL=128  
  
Estatísticas do Ping para 200.189.198.183:  
Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),  
Tempos aproximados de ida e volta em milissegundos:  
Mínimo = 0ms, Máximo = 10ms, Média = 2ms  
C:\DOCUMENTOS\ADMINISTRADOR>
```

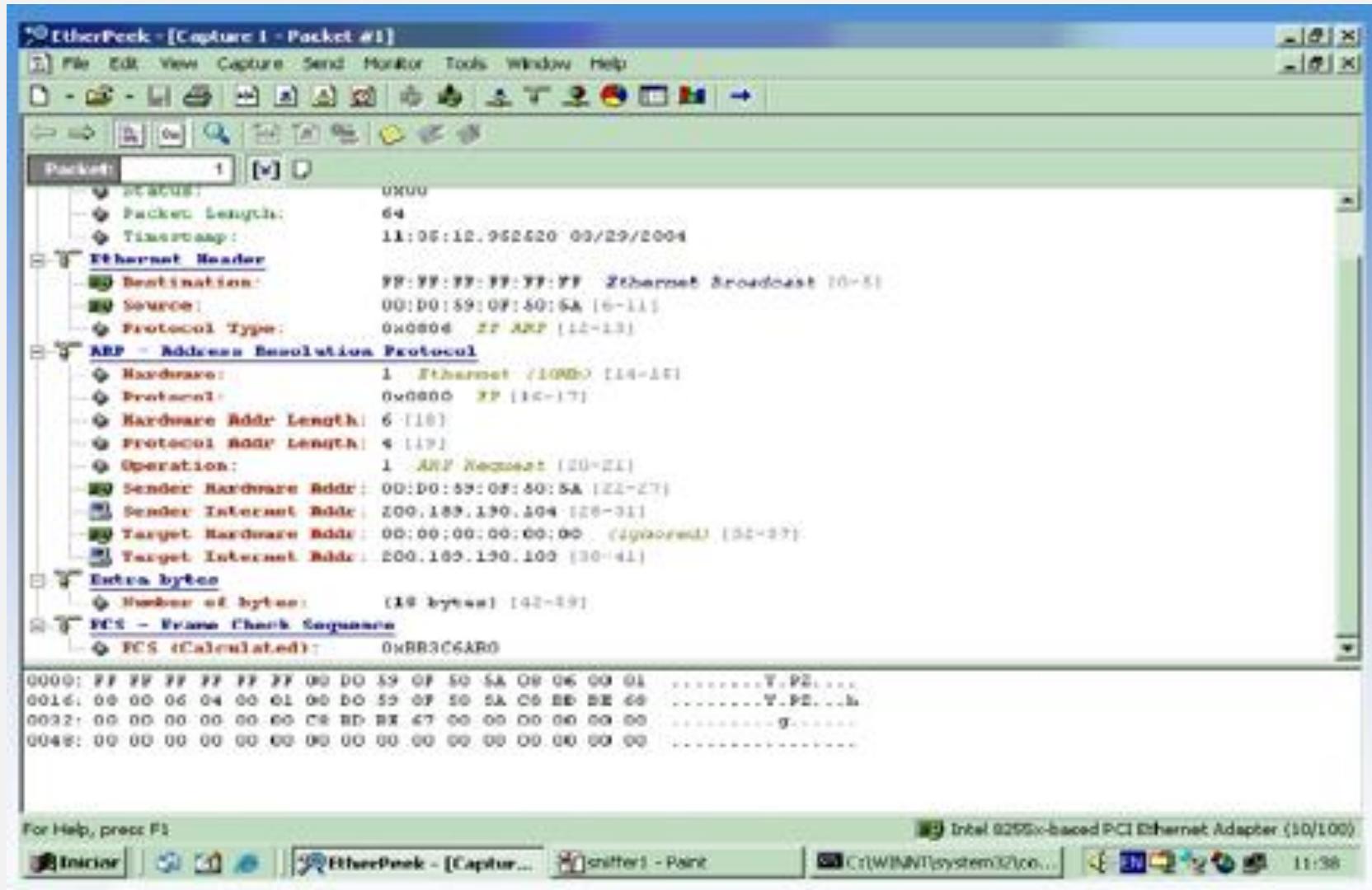
Redes Locais

Sniffer

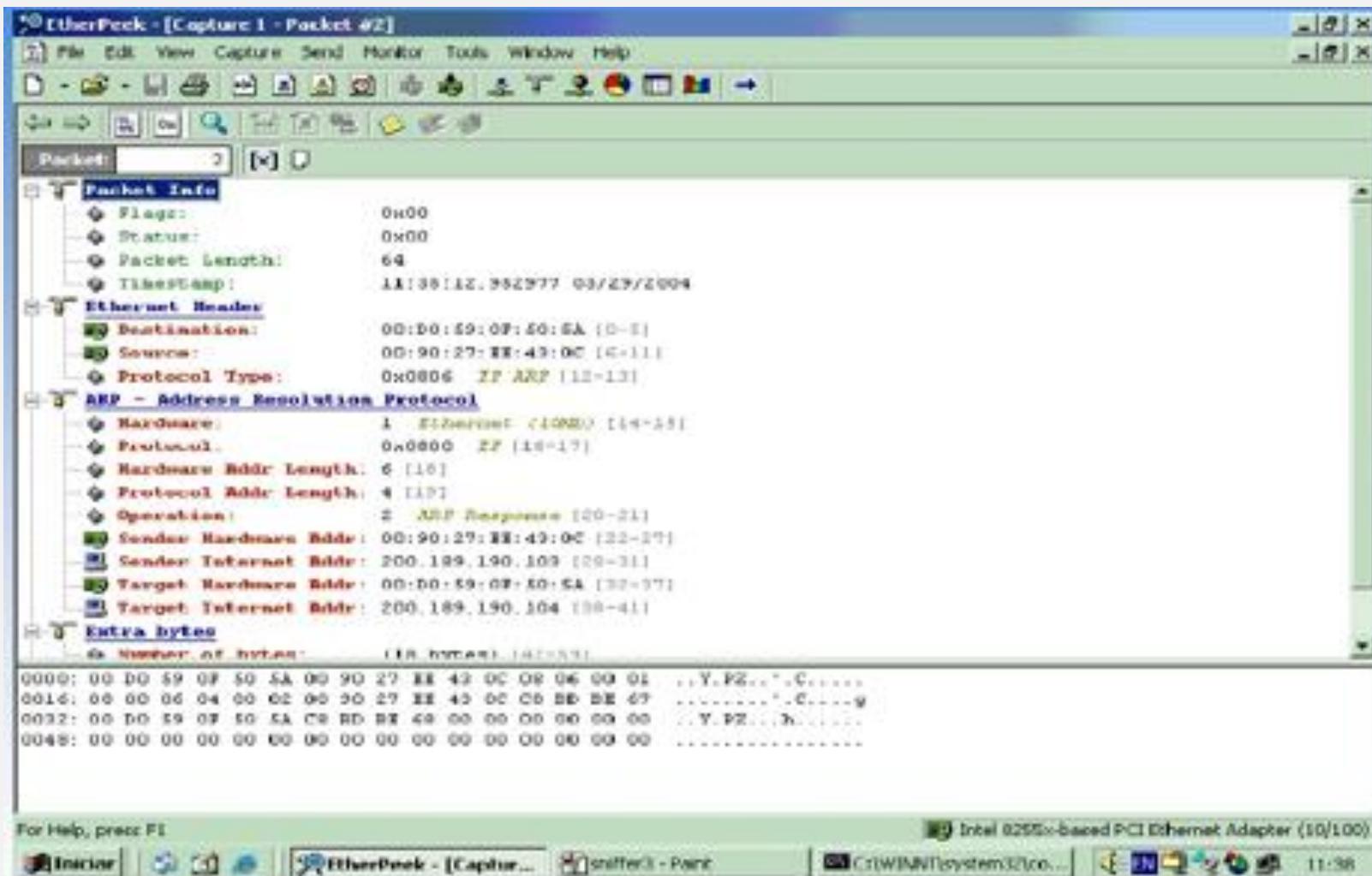
Packet	Source	Flags	Size	Absolute Time	Protocol	Summary
1	00:D0:59:0F:50:5A		64	11:35:12.952520	ARP Request	200.189.190.103 = ?
2	00:90:27:EE:43:0C		64	11:35:12.952977	ARP Response	00:90:27:EE:43:0C = 20
3	IP-200.189.190.104		78	11:35:12.952994	PING Req	Echo: 200.189.190.103
4	IP-200.189.190.103		78	11:35:12.953151	PING Reply	Echo Reply: 200.189.190.104
5	IP-200.189.190.104		78	11:35:13.944722	PING Req	Echo: 200.189.190.103
6	IP-200.189.190.103		78	11:35:13.945045	PING Reply	Echo Reply: 200.189.190.104
7	IP-200.189.190.104		78	11:35:14.946291	PING Req	Echo: 200.189.190.103
8	IP-200.189.190.103		78	11:35:14.946588	PING Reply	Echo Reply: 200.189.190.104
9	IP-200.189.190.104		78	11:35:15.948612	PING Req	Echo: 200.189.190.103
10	IP-200.189.190.103		78	11:35:15.948931	PING Reply	Echo Reply: 200.189.190.104

Redes Locais

quadro-Sniffer

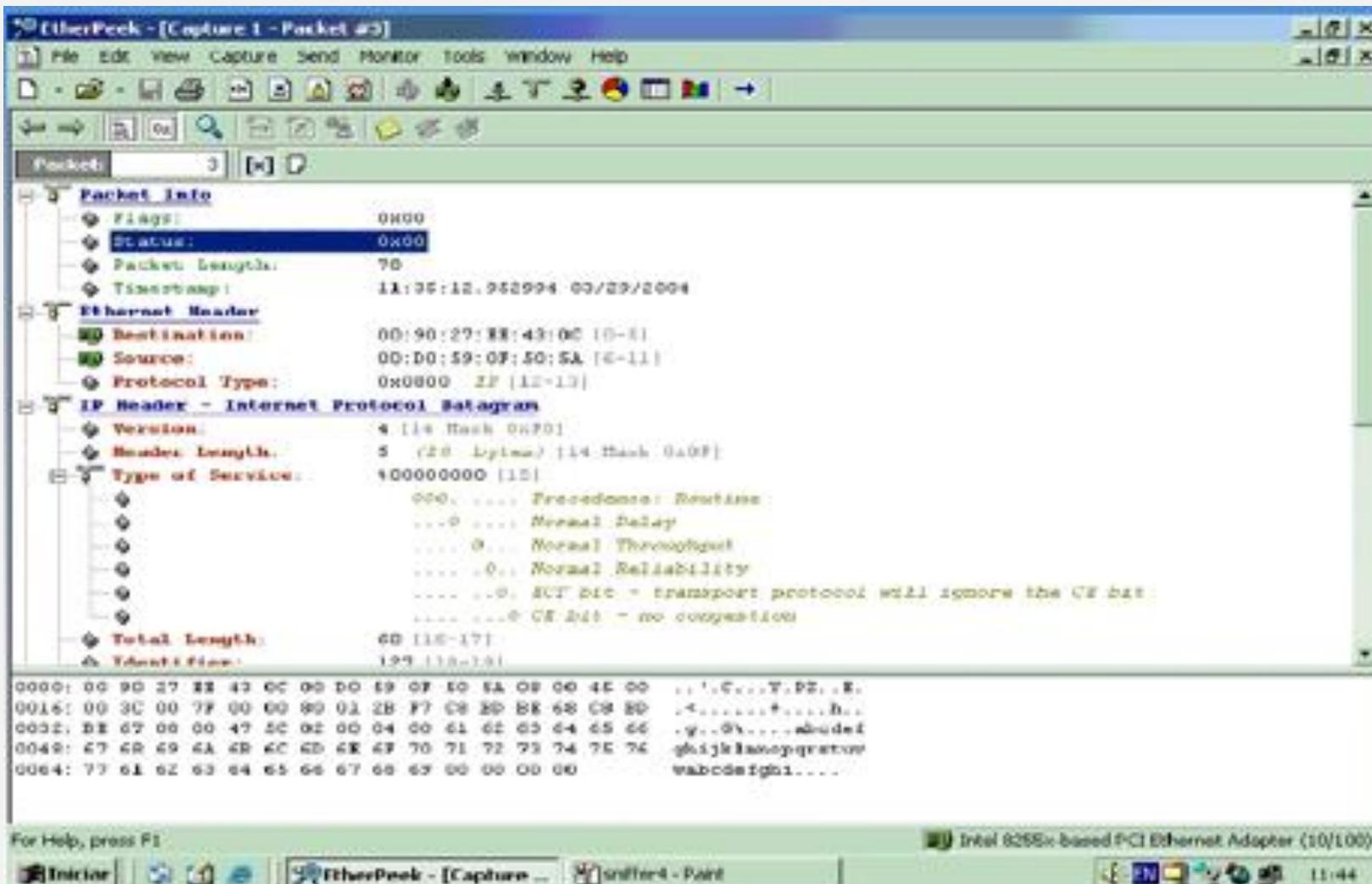


Redes Locais quadro- Sniffer



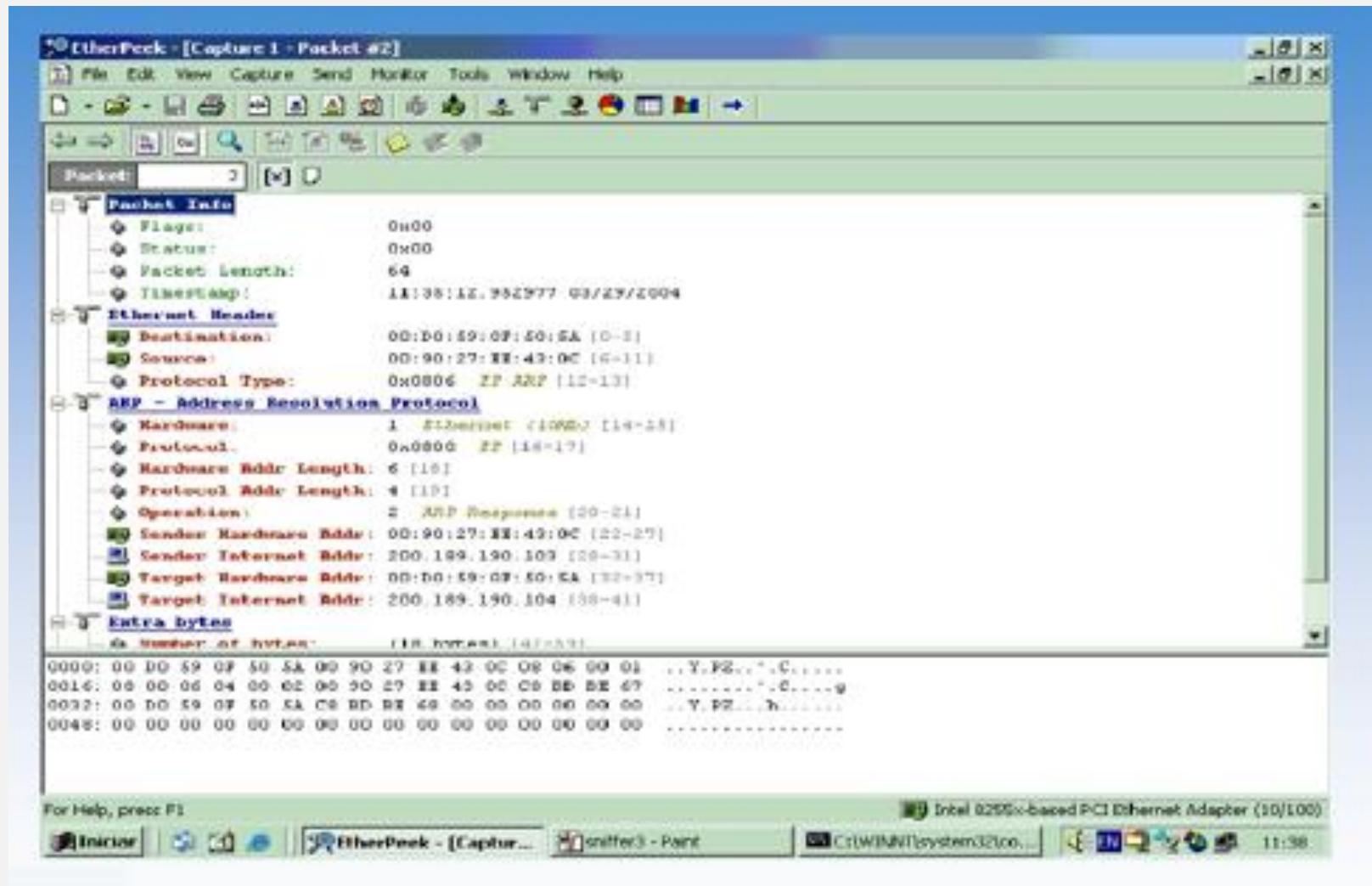
Redes Locais

quadro- Sniffer



Redes Locais

quadro- Sniffer



Exercícios de Fixação

Dada a tabela de endereços de estações abaixo e dado que o endereço do default gateway é o endereço do primeiro host e de suas redes , preencha a tabela abaixo:

Endereço IP	Endereço de rede	Default Gateway	Broadcast
200.215.189.3/27			
172.16.9.4.3/29			
192.168.5.1/28			
172.16.9.2/30			
172.16.10.67/27			
200.30.0.20/28			

Exercícios de Fixação

Para atender uma empresa com as seguintes características :

- 2 localidades
- 20 estações em cada localidade

1. Escolha um endereço privado e uma sub-rede adequada para atender as estações
2. Escolha um endereço privado e as sub-redes para atender os links entre as localidades
3. Indicar quais são os endereços de rede, broadcast e válidos para cada localidade
4. O que seria necessário para as estações acessarem a Internet ?

Laboratório

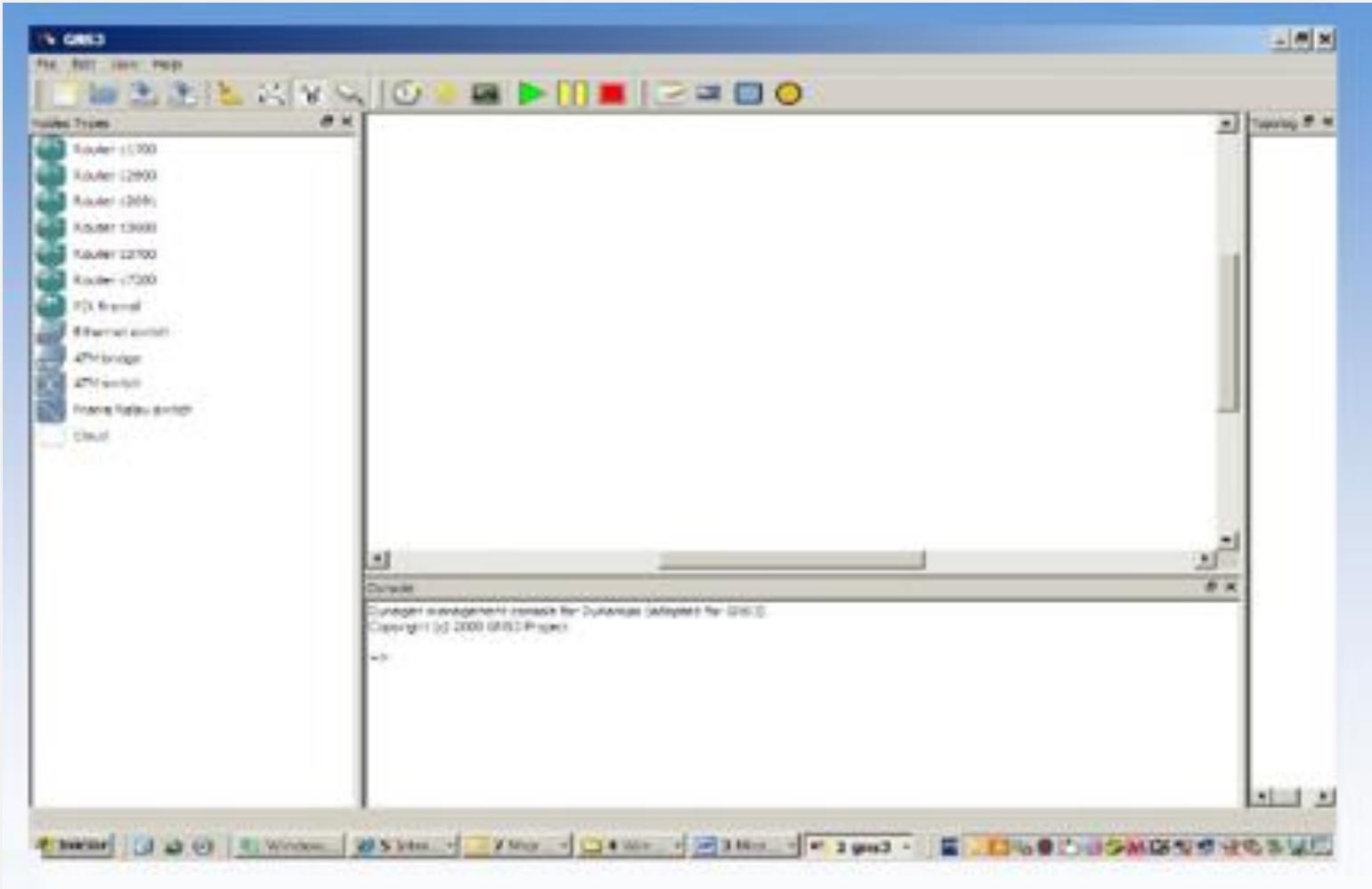
Simulador de redes

GNS3

Simulador de ambiente gráfico de redes que permite desenvolver a topologia de uma rede complexa e fazer simulações de envio de pacotes, conexão, entre outras. Pode ser usado para estudo de protocolos.

Laboratório Simulador de redes

Aspecto do ambiente GNS3



Laboratório Analizador de redes

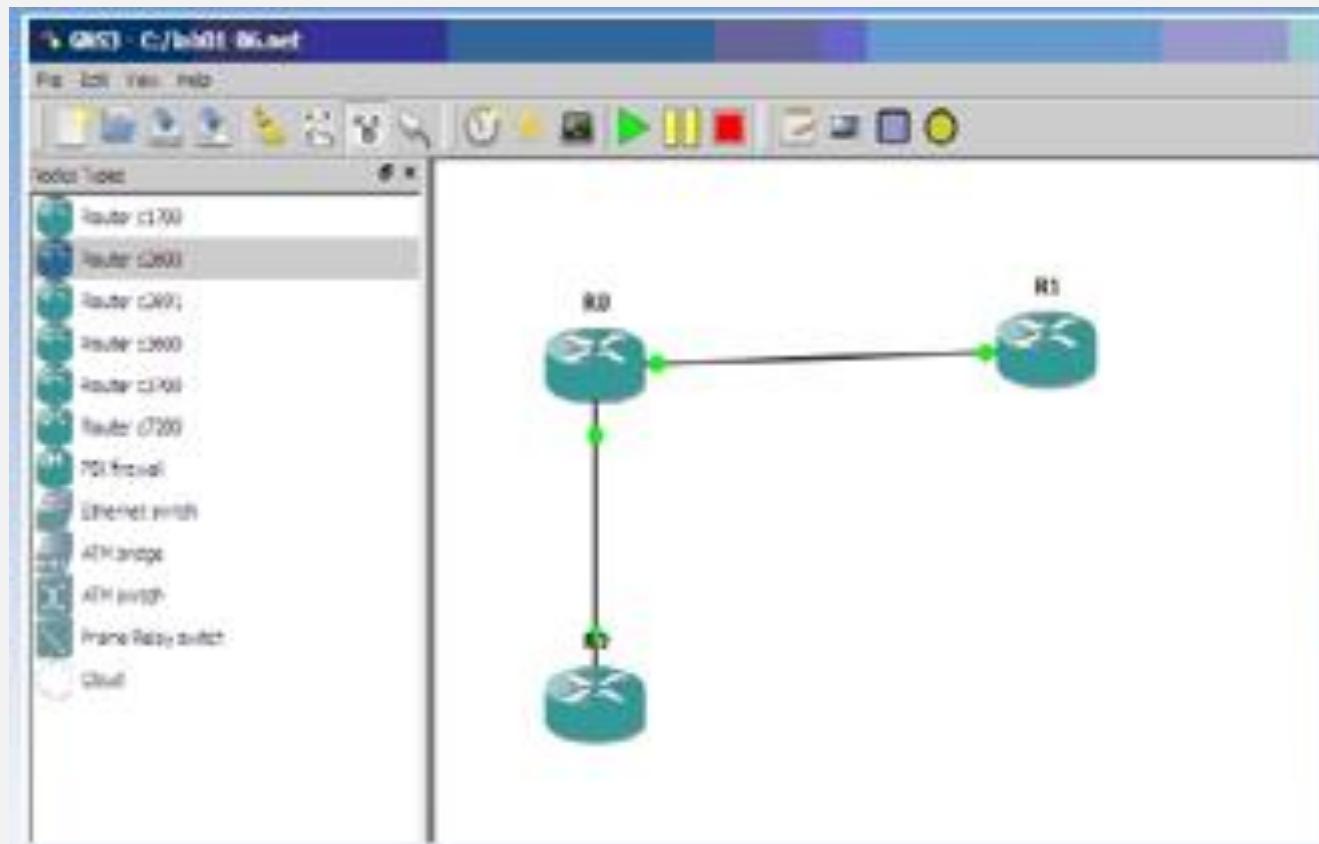
Wireshark é um programa de código aberto para analisar pacotes de rede IP. Possui versões para Unix, Linux e MAC. Pode-se utilizá-lo como analisador de protocolo para:

- Detecção de problemas na rede;
- Análise de segurança de redes;
- Desenvolvimento de novos protocolos ou aplicações;
- Treinamento em aspectos funcionais e da dinâmica de rede.

Laboratório

Atividade Laboratório GNS3

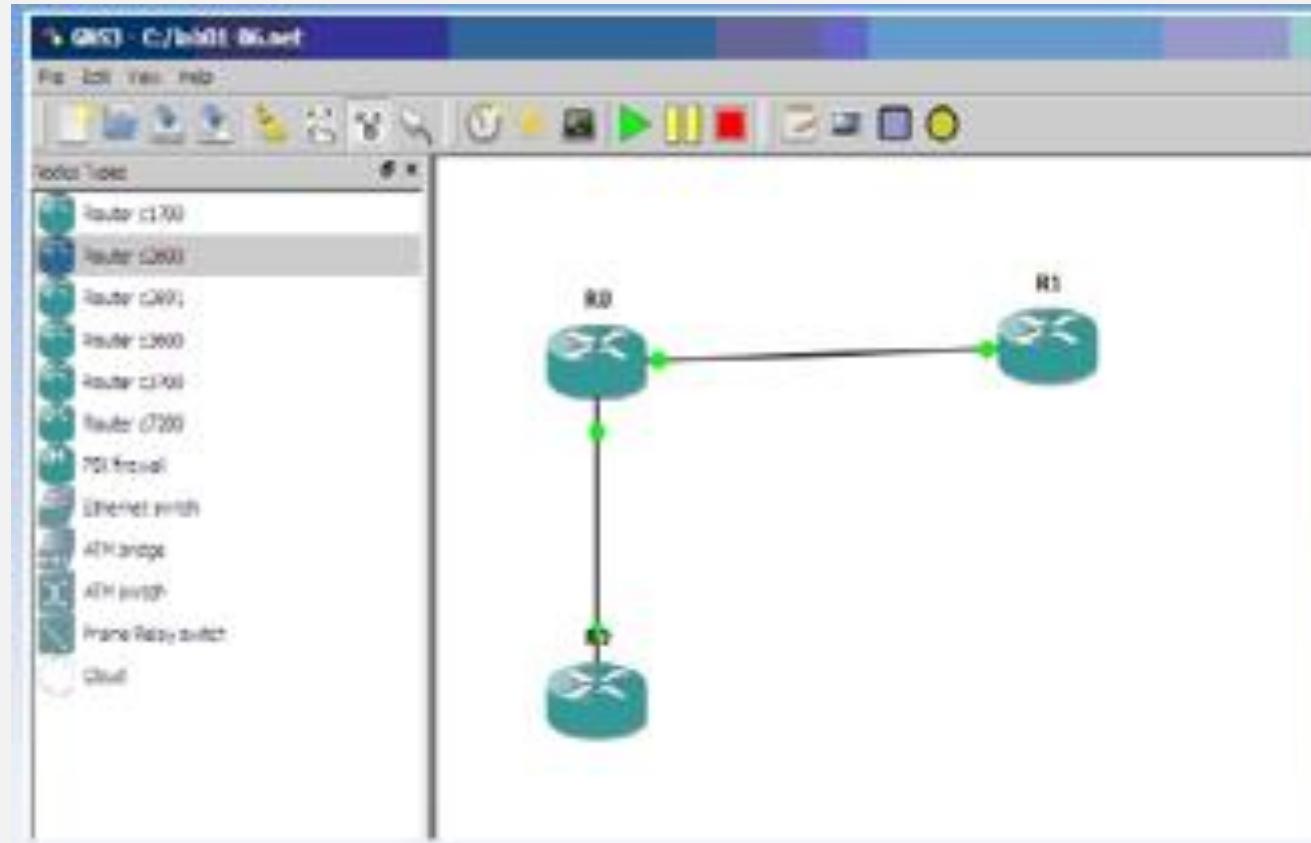
Configurar a topologia com o roteador 7200



Laboratório

Atividade Laboratório GNS3

Configurar os endereços ponto a ponto
usando o bloco (172.16.10.0/ 24)



Laboratório GNS3

ANEXOS COMANDOS

Senhas

```
line con 0  
password portoalegre  
Login
```

```
line vty 0 4  
password portoalegre1
```

```
enable password saopaulo2
```

Laboratório GNS3

ANEXOS COMANDOS

Configurações de interfaces

```
interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.252
No shutdown
!
interface FastEthernet0/1
ip address 192.168.10.1 255.255.255.252
duplex auto
speed auto
!
```

Laboratório

Atividade Laboratório

Identificar roteadores com
hostnames e senhas conforme tabela:

Roteador	Hostname	Senha Console	Senha Telnet	Senha Ebable
R0	SP-CoreIPT14MESTRADO			REDES
R1	SP-LANIPT14MESTRADO			REDES

Laboratório

Atividade Laboratório

Incluir mais um roteador ,
testar conectividade com o protocolo ICMP

<u>Roteador</u>	<u>R0</u>	<u>R1</u>	<u>R2</u>
<u>R0</u>			
<u>R1</u>			
<u>R2</u>			

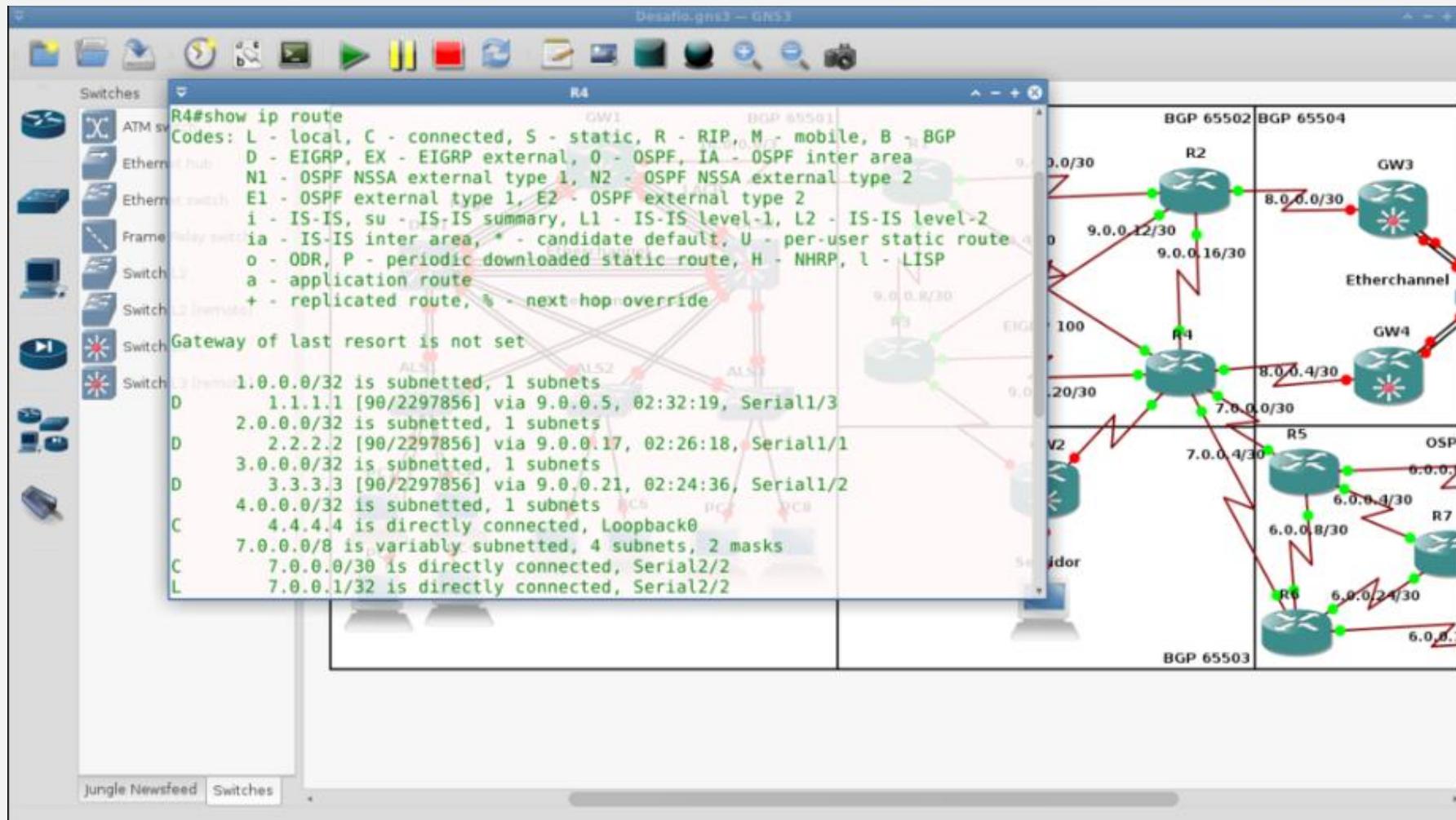
Observar o pacote ICMP no Wireshark

GNS3 – Simulador de Redes

The screenshot shows the official GNS3 website. At the top, there is a dark navigation bar with the GNS3 logo (a stylized green and blue lizard), followed by links for Software, Documentation, Community, Marketplace, and Training. To the right of the navigation bar are a search icon and a "Sign In" button. The main content area has a dark background featuring a network diagram in the bottom right corner. In the center, the GNS3 logo is displayed above the tagline "The software that empowers network professionals". Below the tagline, a sub-tagline reads "Join the world's largest community of network professionals who rely on GNS3 to build better networks, share ideas and make connections." At the bottom of the main section are two buttons: "Free Download" (green) and "Watch Video" (dark grey).

<https://www.gns3.com/>

GNS3 - Exemplo



O que é o GNS3?

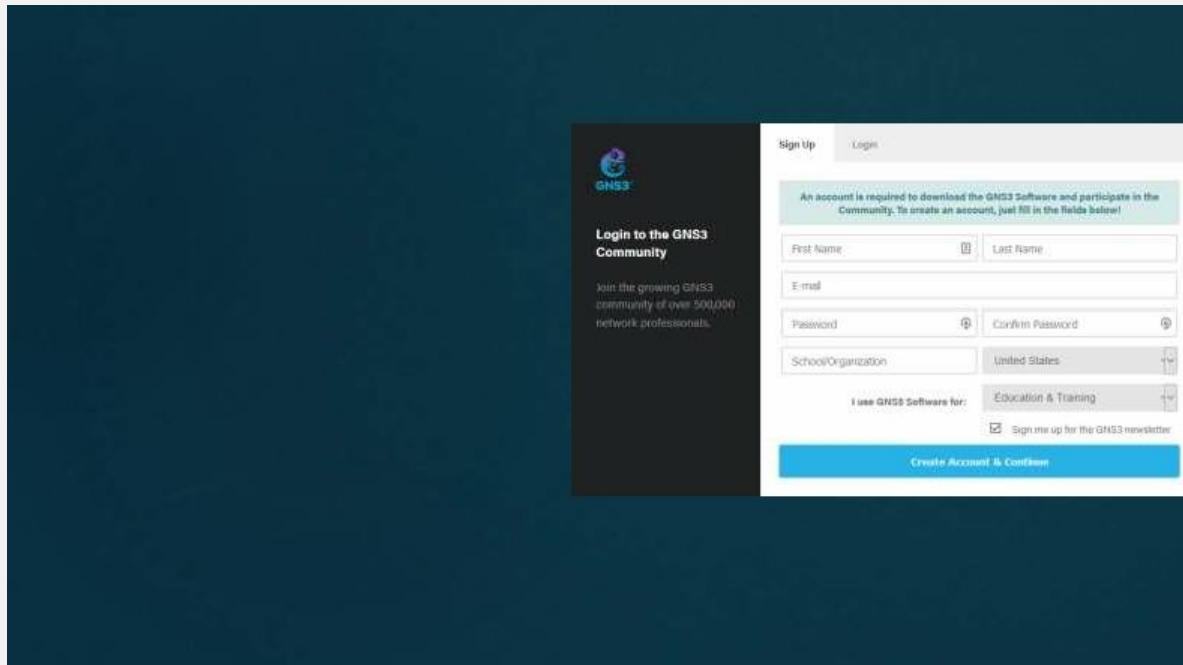
- O GNS3 é um simulador de rede que fornece a capacidade de visualizar, planejar, testar e solucionar problemas de ambientes de rede em qualquer plataforma de fornecedor em escala - sem a necessidade de interagir diretamente com o hardware da rede.
- Os usuários podem conectar todos os tipos de interfaces virtuais para compor uma representação real de redes.
- O GNS3 é executado no Windows, Linux e MacOS X usando o PC tradicional hardware.
- O GNS3 é GRÁTIS

Configuração Mínima

OS	Windows 7 (64 bit) and later, Mavericks (10.9) and later, Any Linux Distro - Debian/Ubuntu are provided and supported
Processor	4 or more Logical cores - AMD-V / RVI Series or Intel VT-X / EPT - virtualization extensions present and enabled in the BIOS. More resources allows for larger simulation
Memory	8 GB RAM
Storage	SSD - 35 GB available space
Additional Notes	Additional RAM up to 16 gigs and i7 or equivalent for optimal usage. Virtualizing devices is processor and memory intensive. More is better but properly configured device trumps RAM and Processing power.

Instalação

- ▶ Crie uma conta GRATUITA no GNS3 em <https://gns3.com/>
- ▶ Clique no link "Inscreva-se" no canto superior esquerdo
 - ▶ Preencha as informações necessárias

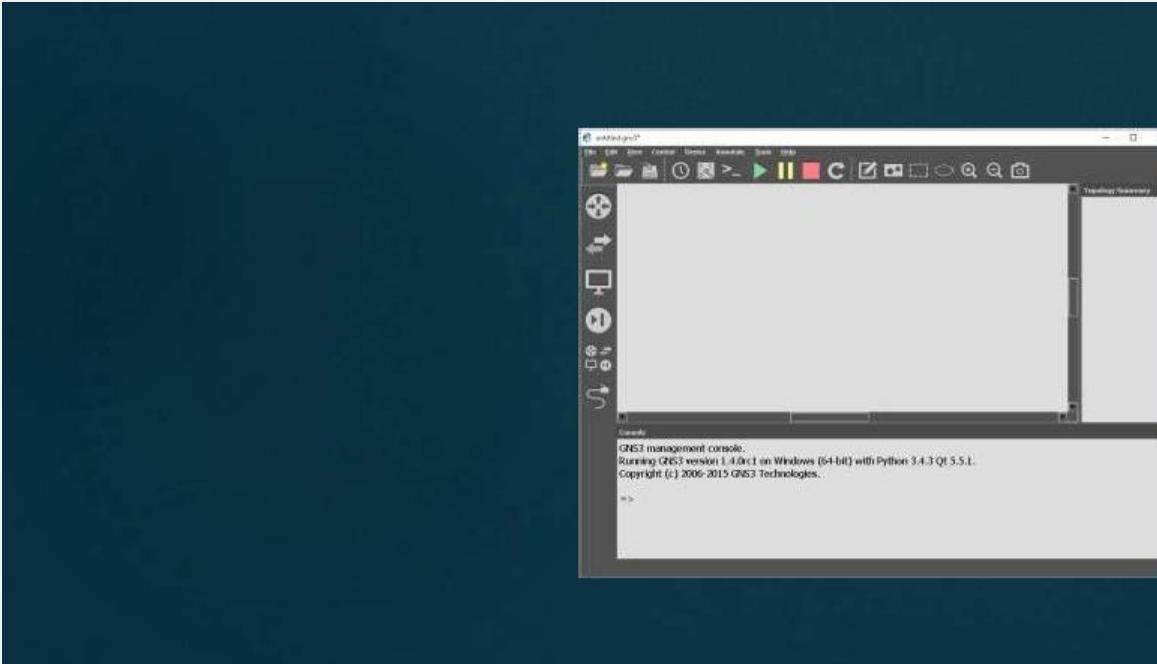


Instalação

- ▶ O GNS3 depende de vários outros programas para operar.
 - ▶ Essas dependências de software incluem
 - ▶ WinPcap
 - ▶ Dynamips
 - ▶ Qemu to name a few
- ▶ Esses componentes principais junto com o GNS3 são todos escolhidos por padrão para instalação. O local padrão para instalar o GNS3 também é escolhido por padrão
- ▶ Observe que, se necessário, o Assistente de Configuração do WinPcap será iniciado para você instalar. Essa dependência é necessária para o GNS3 se comunicar com redes reais por meio de um controlador interno de rede física. Certifique-se de que a caixa de seleção "Iniciar automaticamente o driver do WinPcap na inicialização" está marcada.

Instalação no Windows

Selecionar o botão “Download” fará o download do instalador “tudo em um”. Quando a instalação estiver concluída, clique no botão Iniciar, Todos os Programas, GNS3 e, em seguida, escolha GNS3 fora da lista de aplicativos instalados. A interface gráfica do GNS3 será iniciada.



Não é obrigatório, mas ALTAMENTE Recomendado para o Windows

Download the GNS3 VM from <https://github.com/GNS3/gns3-gui/releases>

The VM is distributed in three different flavors:*

VMware Workstation to be used with Workstation Pro/Player and Fusion (Recommended)

VMware ESXi (For experts only)

VirtualBox (No nested virtualization support)

We highly recommend VMware because VirtualBox doesn't support nested virtualization, this means any VM running inside the GNS3 VM will be slow because the guest VM cannot access to your CPU virtualization instructions (VT-x or AMD-V).

Please note that VMware Workstation Player is free and you can get [20% off VMware Workstation Pro and VMware Fusion thanks to our deal with VMware.](#)

* <https://www.gns3.com/support/docs/download-the-gns3-vm>

Por que usar a VM do GNS3? *

For Linux users, some dependencies are hard to install, like the requirements for IOU (you need specific libraries and 32-bit support).

Using VMware, you can use KVM acceleration for Qemu allowing to run Qemu based appliances with excellent performances on Windows and Mac.

Dynamips and Qemu tend to work a lot better on Linux (less random issues with ASA for example).

Full IOU support (you just need the license file + IOU images).

Future version of the VM will include full Docker support.

No antivirus getting in the way or firewall inside the VM blocking network traffic.

The VM is isolated from your computer and a lot less likely to break something important.

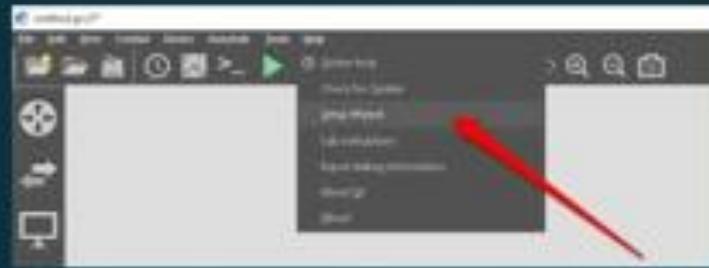
A virtual machine that GNS3 can use to upload images to and control CPU and memory usage by confining the running image in a single virtual machine instance.

It's intended for Windows users who want to use more IOS and IOU images that cannot be supported natively in a Windows environment.

*<https://www.gns3.com/support/docs/-what-is-the-gns3-vm>

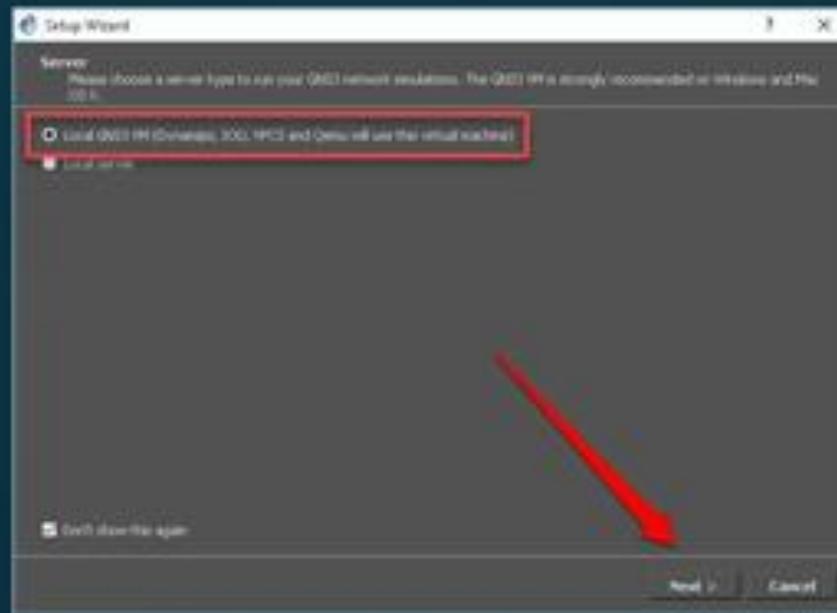
O Assistente de Configuração

- ▶ <https://www.gns3.com/support/docs/the-new-setup-wizard-for-gns3--4>
 - ▶ Note: You can use the traditional local GNS3 server **Or** the GNS3 VM server, not both the setup Wizard.
 - ▶ To locate the Setup Wizard at any time, go to Help → Setup Wizard



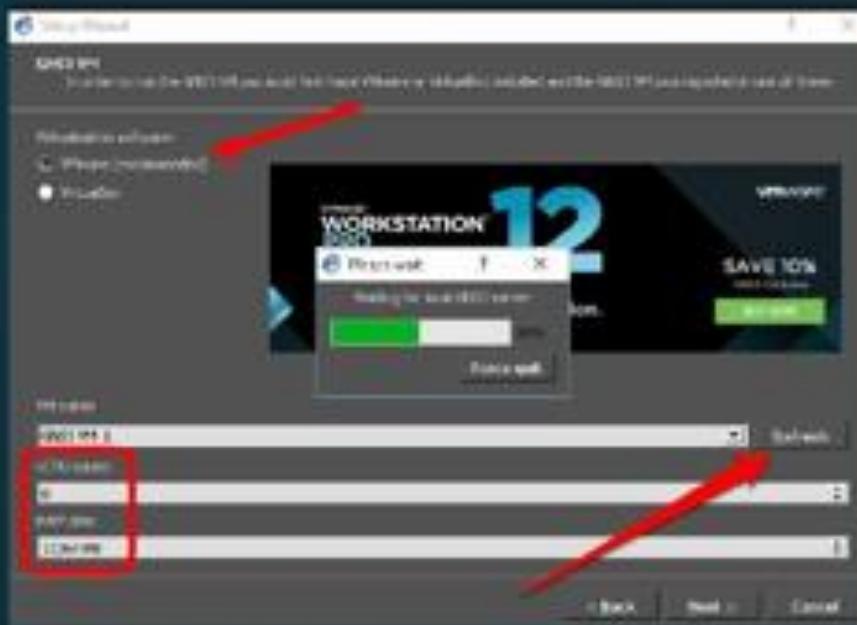
O Assistente de Configuração

► Use the GNS3 VM



O Assistente de Configuração

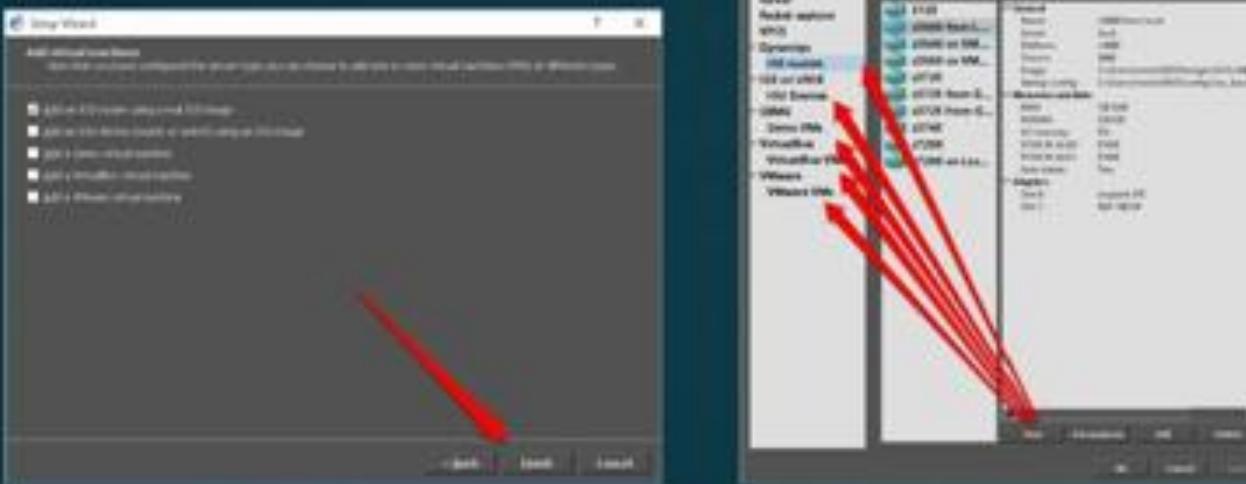
- ▶ Use VMWare



- ▶ Notice the default vCPU cores for this image.
 - ▶ It is recommended to run a minimum of 2 virtual CPU cores, but more is better.
 - ▶ The default value of RAM is half of the available physical memory rounded to a multiple of 4, be careful not to set too much RAM.

O Assistente de Configuração

- ▶ Can use this screen to add images or use Edit | Preferences from the GUI

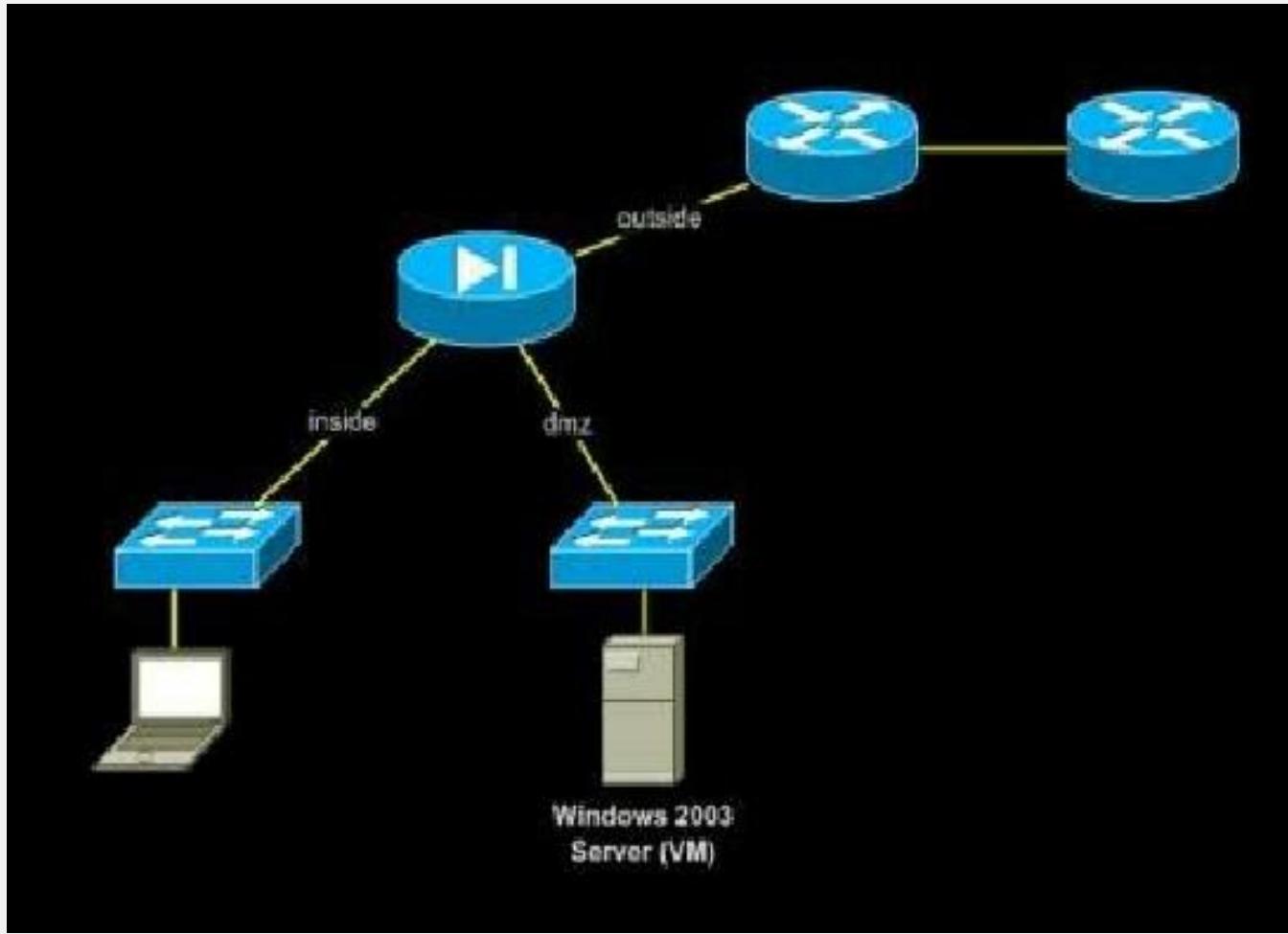


GNS3

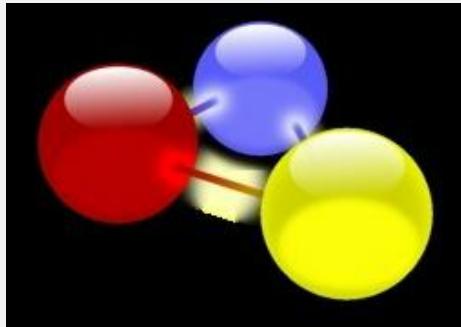
<http://www.gns3.net>

The screenshot shows the official website for GNS3, a graphical network simulator. At the top, there is a logo featuring three colored spheres (red, blue, and yellow) connected by lines, followed by the text "GNS3" in large letters and "Graphical Network Simulator" below it. To the right of the logo is a search bar with a "Search" button. A navigation menu bar at the top has links for Home, News, RSS, Docs, Team, Screenshots, Forum, Blog, and Download. Below the menu, there are several ads from Google, including links for "Practice CCNA", "CCNP Simulator", "Cisco 1841", and "LAN Diagram". A section titled "What is GNS3 ?" contains text about the software's purpose and its integration with other tools like Dynamips, Dynagen, and Pemu. Another section discusses its use for Cisco certification preparation and real lab simulations. A prominent "DOWNLOAD" button with a green arrow icon is located on the right side. Below it, a "Sponsored Link" section for "CCTF Labs Solutions" is shown, along with a small "Ads by Google" banner.

Simulador Gráfico de Redes de Computadores



GNS3



=

Dynamips

Programa que permite emular IOS Cisco

Dynagen

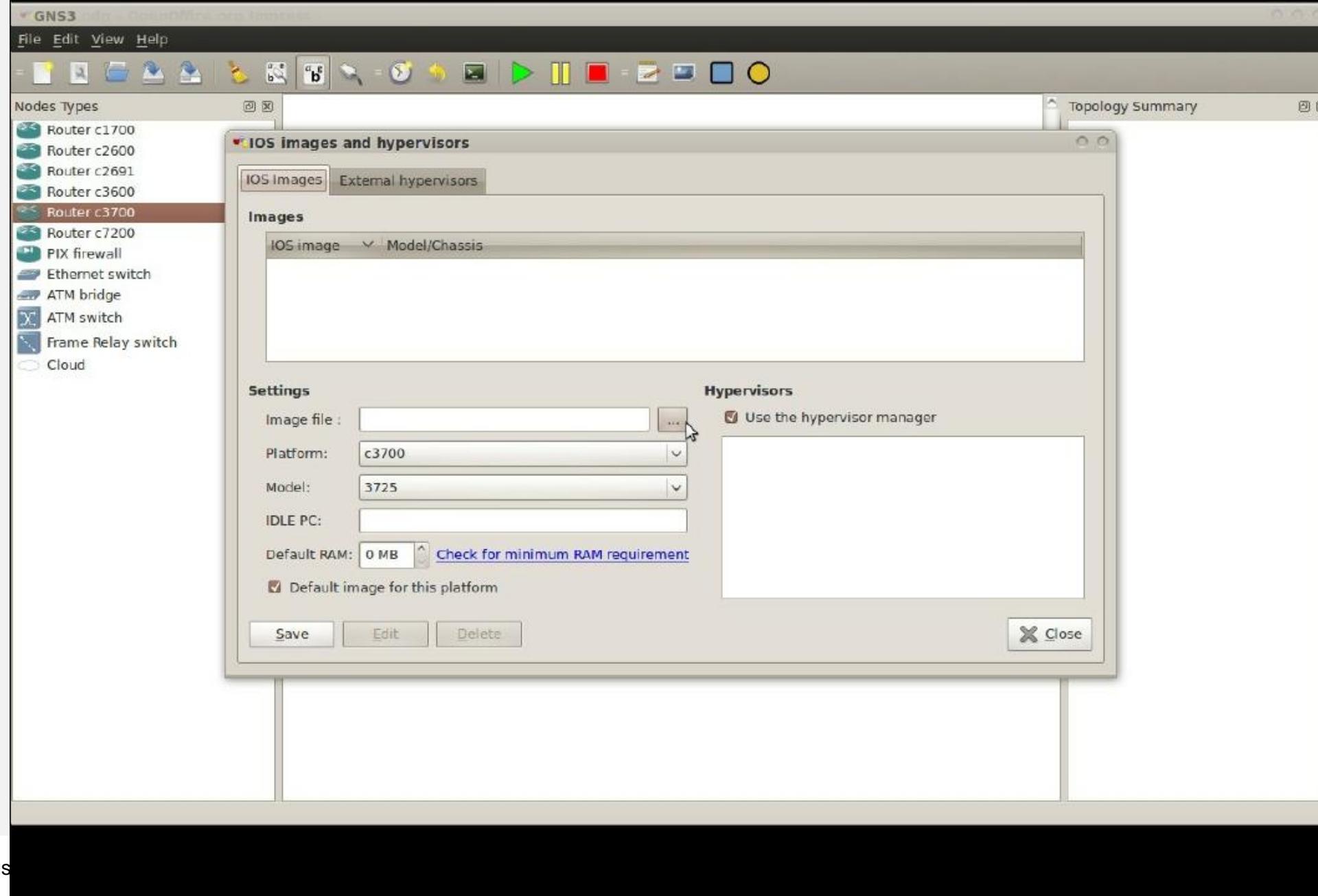
Ferramenta baseada em texto que permite configuração para uso gráfico do Dynamips

Pemu

Emulador de firewall Cisco PIX

GNS3

Além de simular um ambiente de rede,
o GNS3 é capaz de emular os equipamentos CISCO
utilizando o **mesmo** Sistema Operacional
embarcado nos hardwares.



DMVPN lab

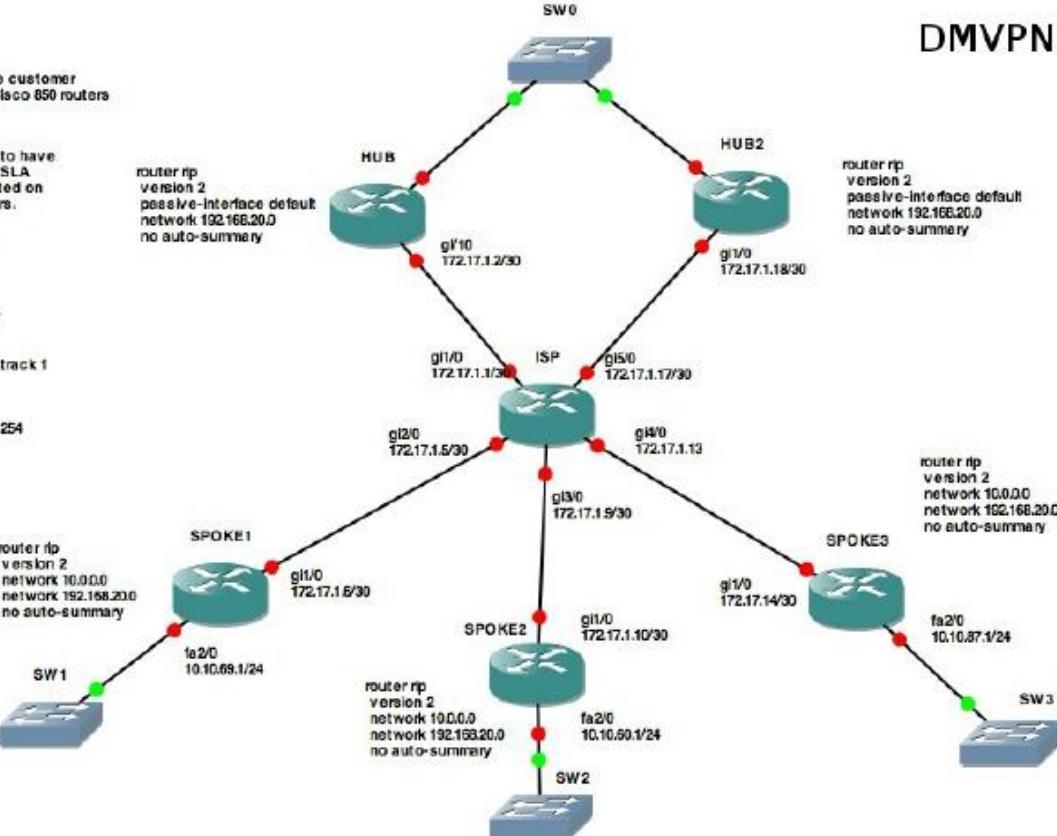
Comments:

I used RIP as routing protocol because the customer for which I need DMVPN phase3 we have Cisco 850 routers on remote sites

On all remote sites, I'm using static routes to have redundancy towards the two hubs with IP SLA features (tracking...) This one is not supported on Cisco 850 routers, just from Cisco 870 routers.

```
ip sil 1
udpecho 192.168.20.1 2000 control disable
timeout 1000
threshold 21000
frequency 1
ip sil schedule 1 life forever start-time now
track 1 itrl1 reachability

ip route 192.168.20.0 255.255.255.0 192.168.20.1 track 1
ip route 10.0.0.0 255.0.0.0 192.168.20.1 track 1
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0
ip route 10.0.0.0 255.0.0.0 192.168.20.2 254
ip route 192.168.20.0 255.255.255.0 192.168.20.2 254
```



DMVPN config on hub:

```
interface Tunnel0
bandwidth 10000
ip address 192.168.20.x 255.255.255.0
no ip redirects
ip mtu 1400
ip nhop authentication 71nhrp
ip nhop map multicast dynamic
ip nhop network-id 1
ip nhop redirect
tunnel source GigabitEthernet1/0
tunnel mode gre multipoint
tunnel key 1234
tunnel protection ipsec profile DMVPN
```

hub1: 192.168.20.1
hub2: 192.168.20.2

DMVPN config on remote site:

```
interface Tunnel0
bandwidth 10000
ip address 192.168.20.x 255.255.255.0
no ip redirects
ip mtu 1400
ip nhop authentication 71nhrp
ip nhop map multicast 172.17.1.2
ip nhop map 192.168.20.1 172.17.1.2
ip nhop map multicast 172.17.1.18
ip nhop map 192.168.20.2 172.17.1.18
ip nhop network-id 1
ip nhop nha 192.168.20.1
ip nhop nha 192.168.20.2
ip nhop shortcut
tunnel source GigabitEthernet1/0
tunnel mode gre multipoint
tunnel key 1234
tunnel protection ipsec profile DMVPN
```

Funcionalidades

- Projeto de topologias complexas e de alta qualidade
- Emulação de diversas plataformas de roteadores CISCO e firewalls PIX
- Simulação de switches Ethernet, ATM e Frame Relay
- Conexão da rede simulada ao mundo real!
- Captura de pacotes usando Wireshark

Vantagens

Empresas / Laboratórios

Pode ser utilizado como ferramenta complementar por oferecer roteamento real

Experimentar funcionalidades de novas versões de CISCO IOS

Testar configurações antes de implantar em ambiente real

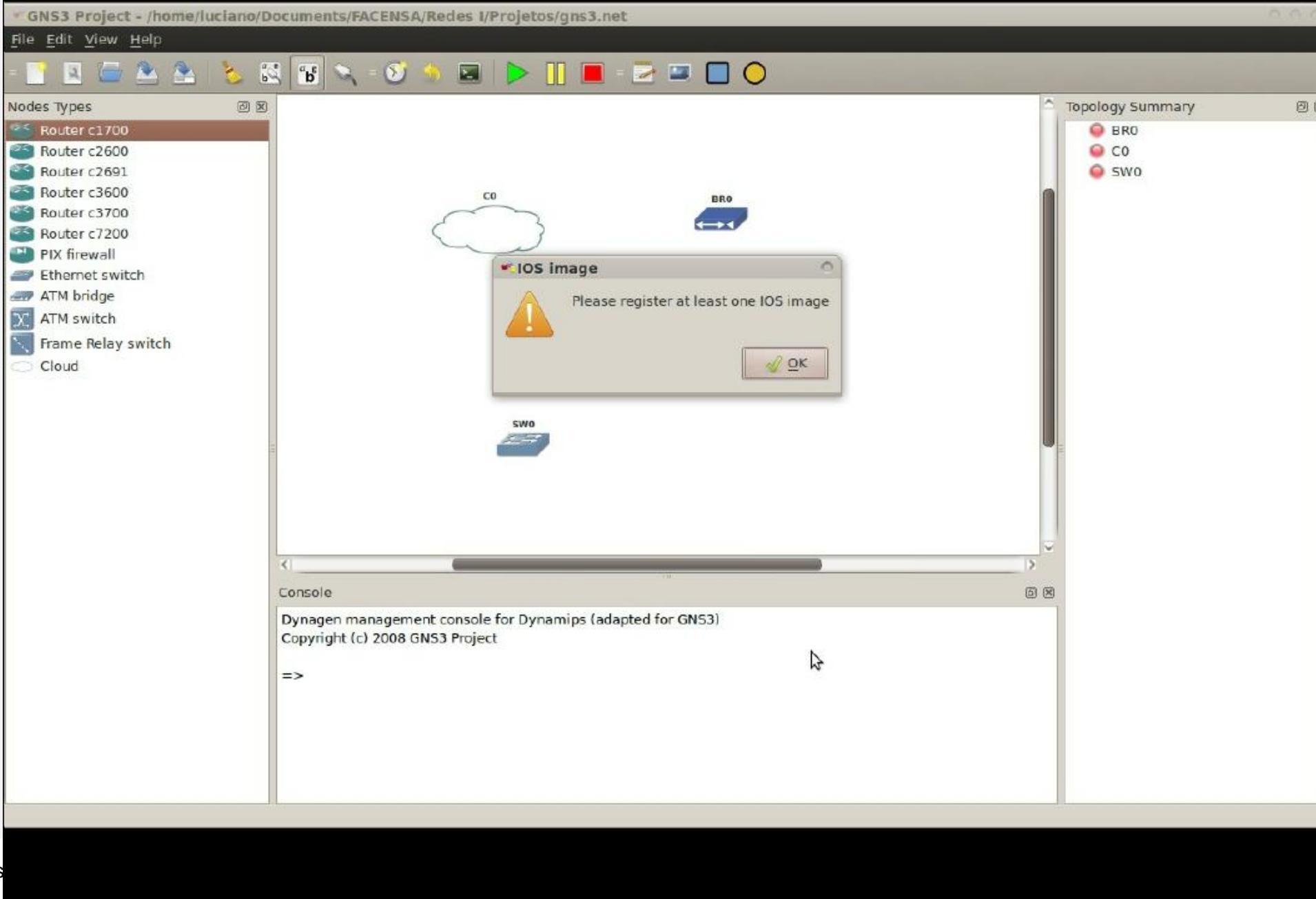
Profissionais

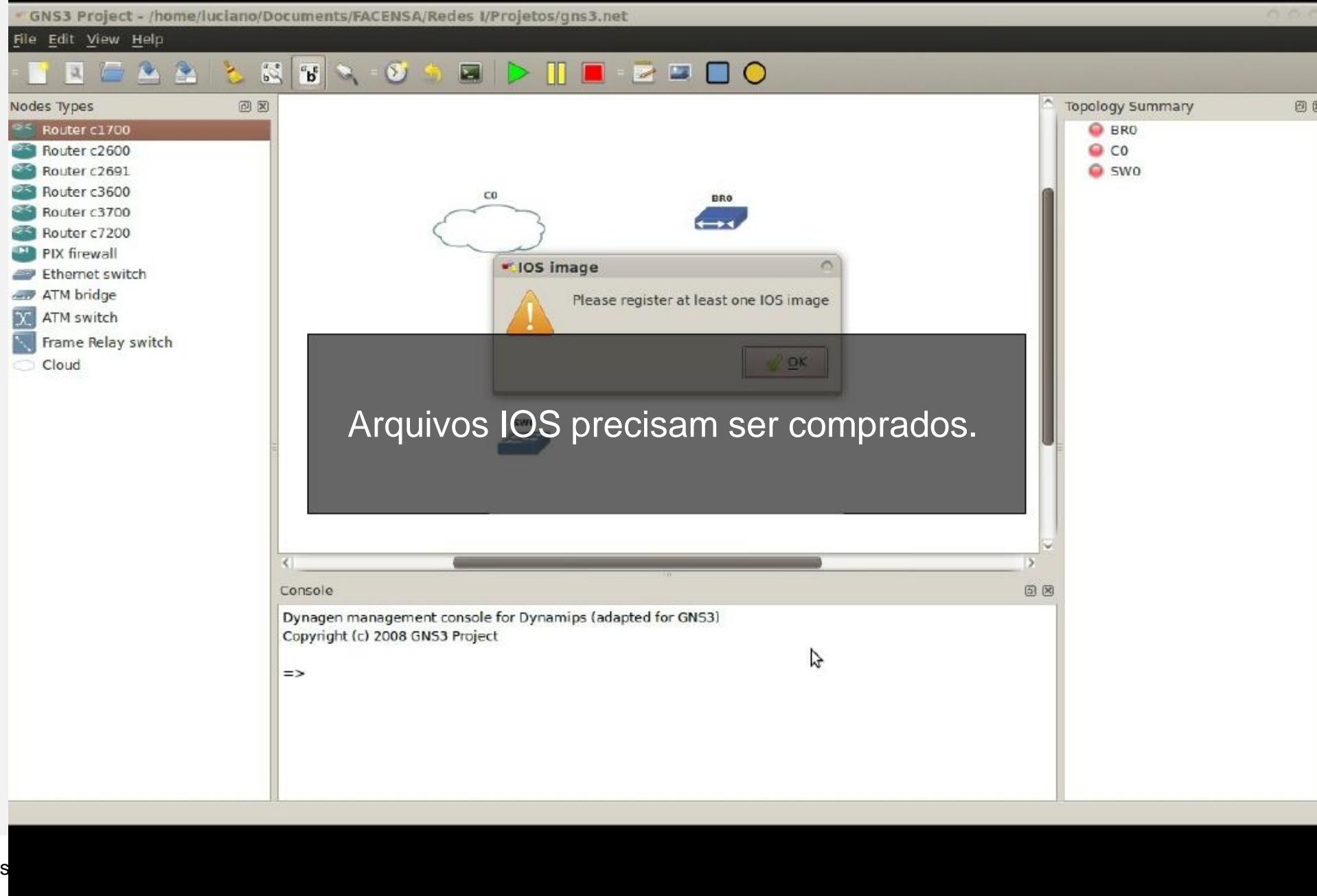
Pode ser utilizado como material de apoio para quem estuda para obter certificações como CCNA, CCNP, CCIP ou CCIE

Portabilidade

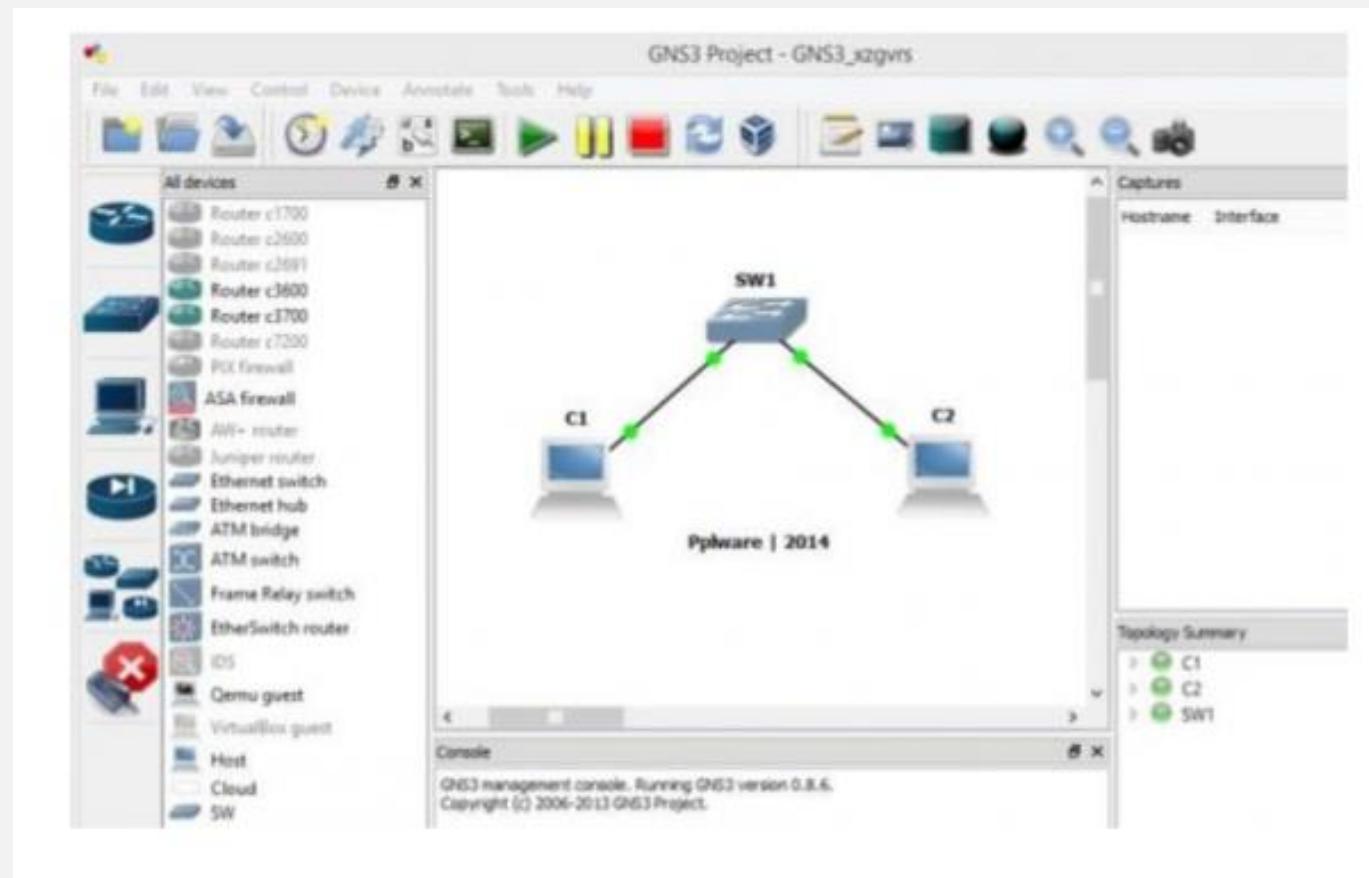
Por ser escrito em Python, pode rodar em qualquer plataforma que suporte esse ambiente de execução. Ex.: Windows, Linux e MacOS X

Desvantagens ?



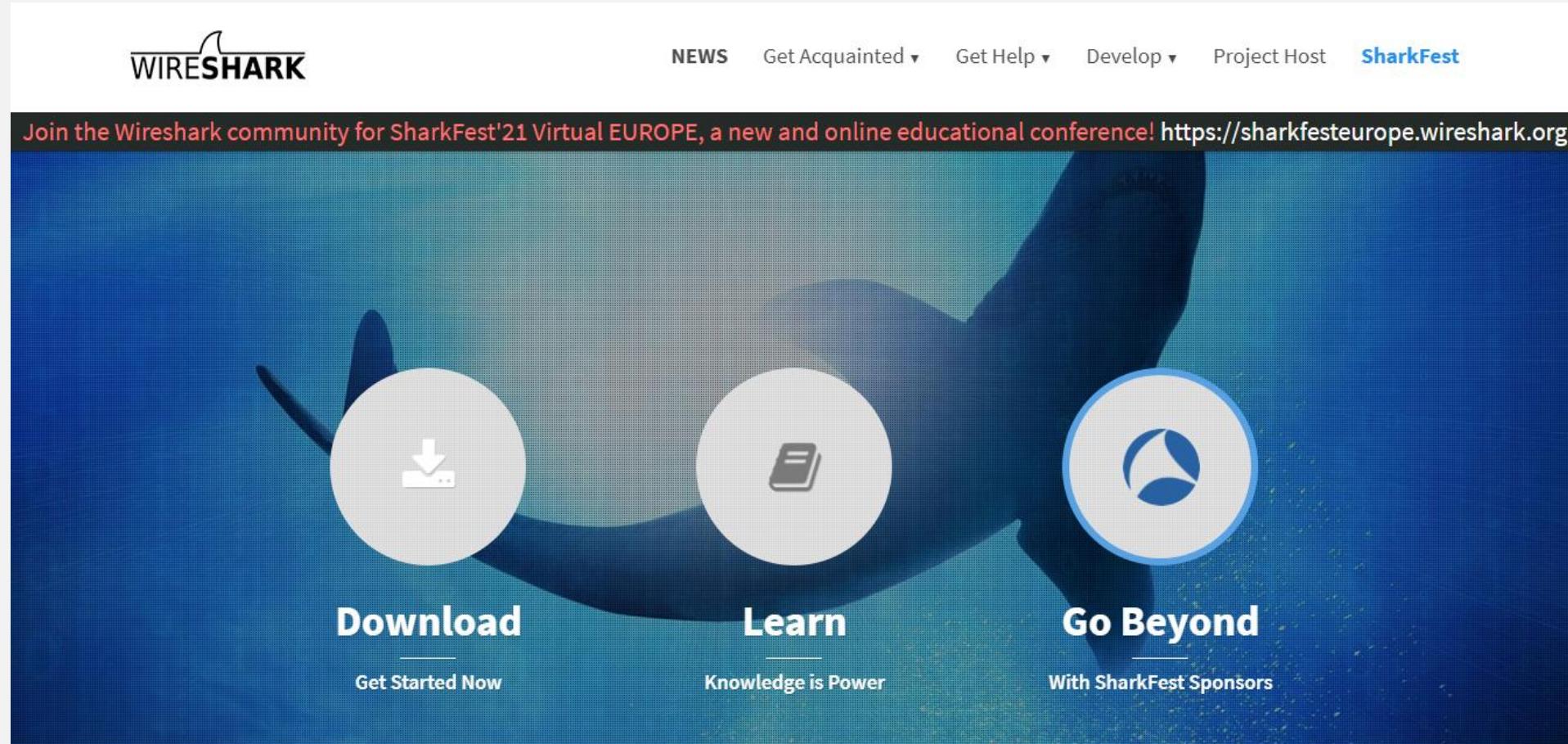


Exercício



<https://www.dropbox.com/sh/ygovs5gygxefmuq/AABmAnlWe0B3MI6OhN8S9RnRa?dl=0>

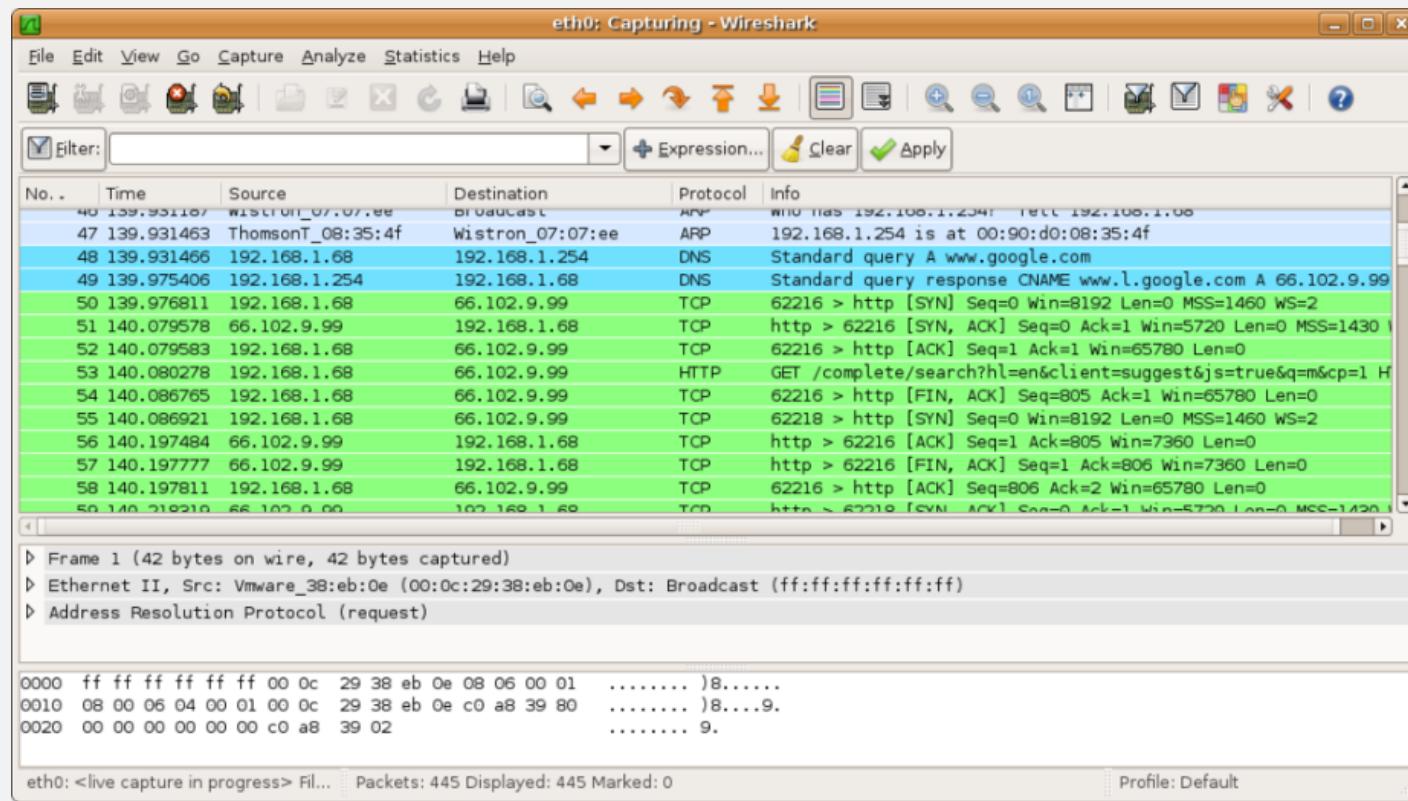
Wireshark



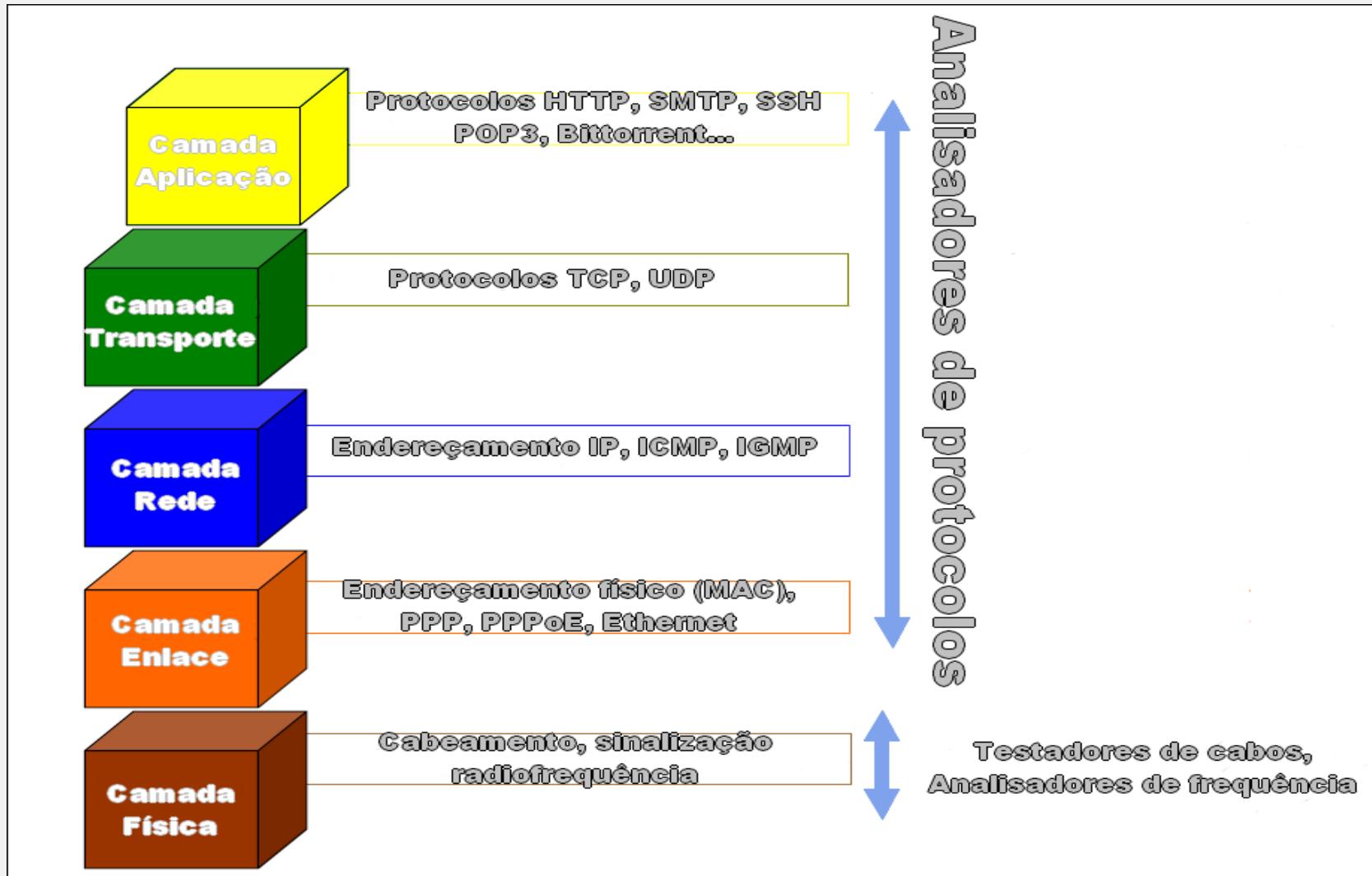
<https://www.wireshark.org/>

Wireshark

O **Wireshark** (anteriormente conhecido como Ethereal) é um programa que analisa o tráfego de rede, e o organiza por protocolos. ... Também é possível controlar o tráfego de um determinado dispositivo de rede numa máquina que pode ter um ou mais desses dispositivos.



Camada de atuação de um analisador de protocolos/tráfego



Ferramentas

- **Tcpdump**
- **Ngrep**
- **Snort**
- **Ethereal**
- **Wireshark**

Ferramentas: Tcpdump

- **Tcpdump (<http://www.tcpdump.org/>)**
 - **Analizador de tráfego padrão no sistema operacional UNIX/Linux**
 - **Código-fonte aberto**
 - **Linha de comando**
 - **Utiliza a biblioteca libpcap**
 - **Por padrão, somente o usuário root tem acesso**

```
19:23:55.180920 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 62264 win 13440 <nopt,nop,timestamp 3328114 652846572>
19:23:55.180927 IP 177.159.181.162.80 > 192.168.201.117.51372: . ack 2484 win 661 <nopt,nop,timestamp 652848076 787018173>
19:23:55.180936 IP 187.7.117.12.80 > 192.168.200.185.57207: . 62264:63712(1448) ack 1 win 108 <nopt,nop,timestamp 652846572 3327502>
19:23:55.180940 IP 177.159.181.162.80 > 192.168.201.117.51405: . ack 1690 win 406 <nopt,nop,timestamp 652848076 787018173>
19:23:55.180943 IP 189.11.250.136.00 > 192.168.201.117.51344: . ack 2520 win 215 <nopt,nop,timestamp 652848058 787018102>
19:23:55.180946 IP 189.11.250.131.80 > 192.168.201.117.51448: . ack 2520 win 272 <nopt,nop,timestamp 652848070 787018152>
19:23:55.180949 IP 177.159.181.163.80 > 192.168.201.117.51408: . ack 2520 win 723 <nopt,nop,timestamp 652847396 787017221>
19:23:55.180951 IP 192.168.201.117.51410: . 12396:15232(2896) ack 1 win 723 <nopt,nop,timestamp 652847396 787017221>
19:23:55.180954 IP 177.159.181.163.80 > 192.168.201.117.51410: . ack 15232 win 8011 <nopt,nop,timestamp 787018274 652847986>
19:23:55.180955 IP 192.168.201.117.51410 > 177.159.181.163.80: . ack 15232 win 8192 <nopt,nop,timestamp 787018274 652847986>
19:23:55.180956 IP 187.7.117.12.80 > 192.168.200.185.57207: . 63712:66609(2896) ack 1 win 108 <nopt,nop,timestamp 652846665 3327540>
19:23:55.180958 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 65160 win 13440 <nopt,nop,timestamp 3328117 652846572>
19:23:55.180960 IP 192.168.200.185.57207 > 192.168.201.117.51408: . F 15232:15432(2200) ack 1 win 723 <nopt,nop,timestamp 652847396 787017221>
19:23:55.180963 IP 192.168.200.185.57207 > 177.159.181.163.80: . ack 1691 win 817 <nopt,nop,timestamp 787018321 652847986>
19:23:55.180964 IP 192.168.200.185.57207 > 192.168.201.117.51372: . 3670:3672(1448) ack 2484 win 406 <nopt,nop,timestamp 652848108 787018173>
19:23:55.180965 IP 187.7.117.12.80 > 192.168.200.185.57207: . 66054:68054(1448) ack 1 win 108 <nopt,nop,timestamp 652846666 3327540>
19:23:55.180966 IP 187.7.117.12.80 > 192.168.200.185.57207: . 66054:68054(1448) ack 1 win 108 <nopt,nop,timestamp 652846666 3327540>
19:23:55.180967 IP 187.7.117.12.80 > 192.168.200.185.57207: . 66054:68054(1448) ack 1 win 108 <nopt,nop,timestamp 652846666 3327540>
19:23:55.180968 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 66605 win 13440 <nopt,nop,timestamp 3328121 652846665>
19:23:55.180969 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 68592 win 13440 <nopt,nop,timestamp 3328123 652846665>
19:23:55.180970 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 68592 win 13440 <nopt,nop,timestamp 3328123 652846665>
19:23:55.180971 IP 177.159.181.163.80 > 192.168.201.117.51408: . 16432:16522(2896) ack 1 win 723 <nopt,nop,timestamp 652847987 787017221>
19:23:55.180972 IP 192.168.201.117.51408 > 177.159.181.163.80: . ack 19328 win 8101 <nopt,nop,timestamp 787018373 652847987>
19:23:55.180973 IP 192.168.200.185.57207 > 192.168.200.185.57207: . 70952:72400(1448) ack 1 win 108 <nopt,nop,timestamp 652846666 3327540>
19:23:55.180974 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 70952 win 13440 <nopt,nop,timestamp 3328127 652846665>
19:23:55.180975 IP 177.159.181.162.80 > 192.168.201.117.51408: . F 1795:2707(912) ack 1690 win 406 <nopt,nop,timestamp 652848118 787018173>
19:23:55.180976 IP 187.7.117.12.80 > 192.168.200.185.57207: . 72400:72598(2896) ack 1 win 108 <nopt,nop,timestamp 652846666 3327540>
19:23:55.180977 IP 177.159.181.162.80 > 192.168.201.117.51372: . F 5124:5172(48) ack 2484 win 641 <nopt,nop,timestamp 652848108 787018173>
19:23:55.180978 IP 192.168.201.117.51408 > 19328:2052(1200) ack 1 win 723 <nopt,nop,timestamp 652847987 787017221>
19:23:55.180979 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 73891 win 13440 <nopt,nop,timestamp 3328129 652846665>
19:23:55.180980 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 2707 win 8135 <nopt,nop,timestamp 787018417 652848118>
19:23:55.180981 IP 192.168.201.117.51372 > 177.159.181.162.80: . ack 5172 win 8189 <nopt,nop,timestamp 787018417 652846666>
19:23:55.180982 IP 192.168.201.117.51408 > 177.159.181.163.80: . ack 20529 win 8117 <nopt,nop,timestamp 787018417 652847987>
19:23:55.180983 IP 192.168.201.117.51372 > 177.159.181.162.80: . ack 6620 win 8101 <nopt,nop,timestamp 787018435 652848108>
19:23:55.180984 IP 192.168.201.117.51408 > 192.168.200.185.57207: . 75296:76744(1448) ack 1 win 108 <nopt,nop,timestamp 652846666 3327540>
19:23:55.180985 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 75296 win 13440 <nopt,nop,timestamp 787018435 652846666>
19:23:55.180986 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 25828:25844(1448) ack 1 win 108 <nopt,nop,timestamp 652847987 787017221>
19:23:55.180987 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 75296:76744(1448) ack 1 win 108 <nopt,nop,timestamp 652846666 3327540>
19:23:55.180988 IP 192.168.200.185.57207 > 187.7.117.12.80: . ack 75296:76744(1448) ack 1 win 108 <nopt,nop,timestamp 652846666 3327540>
```



Ferramentas: Tcpdump

Exemplos de uso

- **tcpdump -nn -i eth1** - **captura e filtra o tráfego na interface eth1, sem usar resolução de endereços e portas**
- **tcpdump -nn -i eth1 port 80** - **captura e filtra o tráfego na interface eth1, sem usar resolução de endereços e portas, para pacotes com a porta 80 na origem ou no destino**
- **tcpdump -nn -i eth1 -w /tmp/arquivo.cap port 80** - **captura e filtra o tráfego na interface eth1, sem usar resolução de endereços e portas, para pacotes com a porta 80 na origem ou no destino e salva no arquivo /tmp/arquivo.cap**
- **tcpdump -nn -i eth1 dst port 80** - **captura e filtra o tráfego na interface eth1, sem usar resolução de endereços e portas, para pacotes com a porta 80 no destino. Para usar a porta 80 como origem, utilizar o parâmetro src**

Ferramentas: Tcpdump

Exemplos de uso

- **tcpdump -nn -i eth1 host 192.168.200.3 and host 192.168.200.1** - captura e filtra o tráfego na interface eth1, sem usar resolução de endereços e portas, para pacotes com os endereços 192.168.200.3 e 192.168.200.1
- **tcpdump -nn -i eth1 host 192.168.200.3 or host 192.168.200.1** - captura e filtra o tráfego na interface eth1, sem usar resolução de endereços e portas, para pacotes com os endereços 192.168.200.3 or 192.168.200.1
- **tcpdump -nn -i eth1 udp** - captura e filtra o tráfego na interface eth1, sem usar resolução de endereços e portas, para pacotes com o protocolo udp
- **tcpdump -nn -i eth1 tcp port 80 and not host 192.168.200.3** - captura e filtra o tráfego na interface eth1, sem usar resolução de endereços e portas, para pacotes que não tenham o endereço IP 192.168.200.3 e sejam para a porta 80 do protocolo TCP, de origem ou destino

Mais exemplos de uso:

<http://packetlife.net/media/library/12/tcpdump.pdf>

Ferramentas: Ngrep

Exemplos de uso:

•**ngrep -d eth0 “Bittorrent”**

(lista os pacotes que contenham a palavra Bittorrent)

•**ngrep -d eth0 “Bittorrent|GNUTELLA” not net 192.168.200.0 and not port 587**

(lista os pacotes que contenham as palavras Bittorrent ou GNUTELLA e que não sejam pertencentes a rede 192.168.200.0 e não usem a porta 587 em origem ou destino)

```
* ngrep -d eth0:7.70 -i "Globo" port 80
interface: eth0:7.70 (10.70.0.0/255.255.255.0)
filter: (ip or ipv6) and (port 80)
match: Globo
#####
T 10.70.1.51:52039 -> 198.96.57.6:80 [AP]
GET /urlis/count.json?url=https%3A%2F%2Fgloboesporte.globo.com%2Ffutebol%2Ffutebol-internacional%2Ffutebol-ingles%2Fnoticias%2F2014%2F05%2Fliverpool-apga-a-cede-empate-e-fica-mais-distante-do-titulo-ingles.html&callback=wttr.receiveCount HTTP/1.1..Host: cdn.api.twitter.com..Connection: keep-alive..Accept: */*.User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36..Referer: http://platfrom.twimgter.com/widgets/tweet_button.1399310891.html..Accept-Encoding: gzip,deflate,sdch..Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4...
#####
T 10.70.1.51:61460 -> 173.194.118.20:80 [AP]
GET /recapscha/api/challenge?challenge=6LcSOls5AAAj1bSfQuvuANCekBqKwVTTSB7dajax1cacheStamp=0.3701790149476078 HTTP/1.1..Host: www.google.com..Connection: keep-alive..Accept: */*.User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36..Referer: http://globoesporte.globo.com/futebol/internacional/futebol-ingles/noticias/2014/05/liverpool-apaga-cede-empate-e-fica-mais-distante-do-titulo-ingles.html..Accept-Encoding: gzip,deflate,sdch..Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4...
#####
T 10.70.1.51:518043 -> 198.192.82.194:80 [AP]
GET /comunicado/comunicado-421225/resultados-reuniao_jcpng HTTP/1.1..Host: interatividade.globo.com..Connection: keep-alive..Accept: */*.User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36..Referer: http://globoesporte.globo.com/futebol/futebol-internacional/futebol-ingles/noticias/2014/05/liverpool-apaga-cede-empate-e-fica-mais-distante-do-titulo-ingles.html..Accept-Encoding: gzip,deflate,sdch..Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4...Cookie: OX=jPSFM1NGewACCV; nav19574+10889075641_45; nvpossew_=C9$huudoxw1s888poor_glb_uid=jVYjz25ule4sPPhXs_0Oedzbf12xx1KwvIQNow"; _utma=100629313.1989331247.1399331247.1399331247.1399331247.1399331247; _utmb=100629313.9.1999331285039; _utmc=100629313; _utmx=100629313.1999331247.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)...
#####
#####Cexit
```

Ferramentas: Snort

- **Snort (<http://www.snort.org>)**
 - **Detector de intrusão com recursos poderosos**
 - **Procura por padrões nos pacotes detectando anomalias e as prevenindo**
 - **Assinaturas de aplicações e protocolos**
 - **Disponível para Linux e Windows**
 - **Código-fonte aberto**



```
C:\>WINNT\System32\cmd.exe
F:\$nort>snort
--- Initializing Snort ---
-> Snort! <-
Version 1.7-WIN32
By Martin Roesch <roesch@clark.net, www.snort.org>
WIN32 Port By Michael Davis <mike@datanerds.net, www.datanerds.net/~mike>
USAGE: snort [-options] <filter options>
Options:
  -A      Set alert mode: fast, full, or none  (alert file alerts only)
          "unsock" enables UNIX socket logging (experimental). *
  -a      Display ARP packets
  -b      Log packets in tcpdump format (much faster!)
  -c <rules> Use Rules File <rules>
  -C      Print out payloads with character data only (no hex)
  -d      Dump the Application Layer
  -D      Run Snort in background (daemon) mode
  -e      Display the second layer header info
  -E      Log alert messages to NT Eventlog.
  -F <bpf> Read BPF filters from file <bpf>
  -g <gname> Run snort gid as 'gname' user or uid after initialization *
  -h <hn> Home network = <hn>
  -i <if> Listen on interface <if>
  -I      Add Interface name to alert output
  -l <ld> Log to directory <ld>
  -n <cnt> Exit after receiving <cnt> packets
  -N      Turn off logging (alerts still work)
  -o      Change the rule testing order to Pass!Alert!Log
  -O      Obfuscate the logged IP addresses
  -p      Disable promiscuous mode sniffing
  -P <snap> set explicit snaplen of packet (default: 1514)
  -q      Quiet. Don't show banner and status report
  -r <tf> Read and process tcpdump file <tf>
  -s <server:port> Log alert messages to syslog server (default port: 514)
  -S <n=v> Set rules file variable n equal to value v
  -t <dir> Chroots process to <dir> after initialization
  -u <uname> Run snort uid as <uname> user (or uid) after initialization
  -U      Use UTC for timestamps
  -v      Be verbose
  -V      Lists available interfaces.
  -V      Show version number
  -X      Dump the raw packet data starting at the link layer
  -?      Show this information
<Filter Options> are standard BPF options, as seen in TCPDump
* denotes an option that is NOT SUPPORTED in this WIN32 port of snort.
Uh, you need to tell me to do something....
: Invalid argument
F:\$nort>
```

Wireshark

Desenvolvedor	Equipe de desenvolvimento do Wireshark
Versão estável	3.0.2 ^[1] (21 de maio de 2019; há 0 dia)
Idioma(s)	Inglês
Linguagem	C, C++ (Qt)
Sistema operativo	Linux, Solaris, FreeBSD, NetBSD, OpenBSD, DragonFly BSD, HP-UX, AIX, macOS e Windows
Gênero(s)	Analisador de rede
Licença	GNU General Public License
Estado do desenvolvimento	Ativo
Página oficial	wireshark.org ↗

Ferramenta: Wireshark

The screenshot shows the Wireshark interface with the following details:

- Title Bar:** msnms.pcap - Wireshark
- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Help
- Toolbar:** Standard file operations (Open, Save, Print, Copy, Paste, Find, etc.)
- Filter Bar:** Filter: Expression... Clear Apply
- Panels:**
 - Packet List:** Shows 18 captured frames. Frame 1 is selected, showing details for an Ethernet II frame from HonHaiPr_6e:8b:24 to D-Link_21:99:4c. The TCP segment contains a SYN from port 3331 to 1863.
 - Details:** Displays the selected frame's header information: Ethernet II, Internet Protocol, and Transmission Control Protocol.
 - Bytes:** Displays the raw hex and ASCII data for the selected frame.
 - Status Bar:** File: "C:\UCPel\redes\depende_2007\exe4\ppa_capture_files\msnms.pcap" 6635 Bytes 00:01:02 P: 50 D: 50 M: 0

Usando o Wireshark

- **Processo de instalação:**

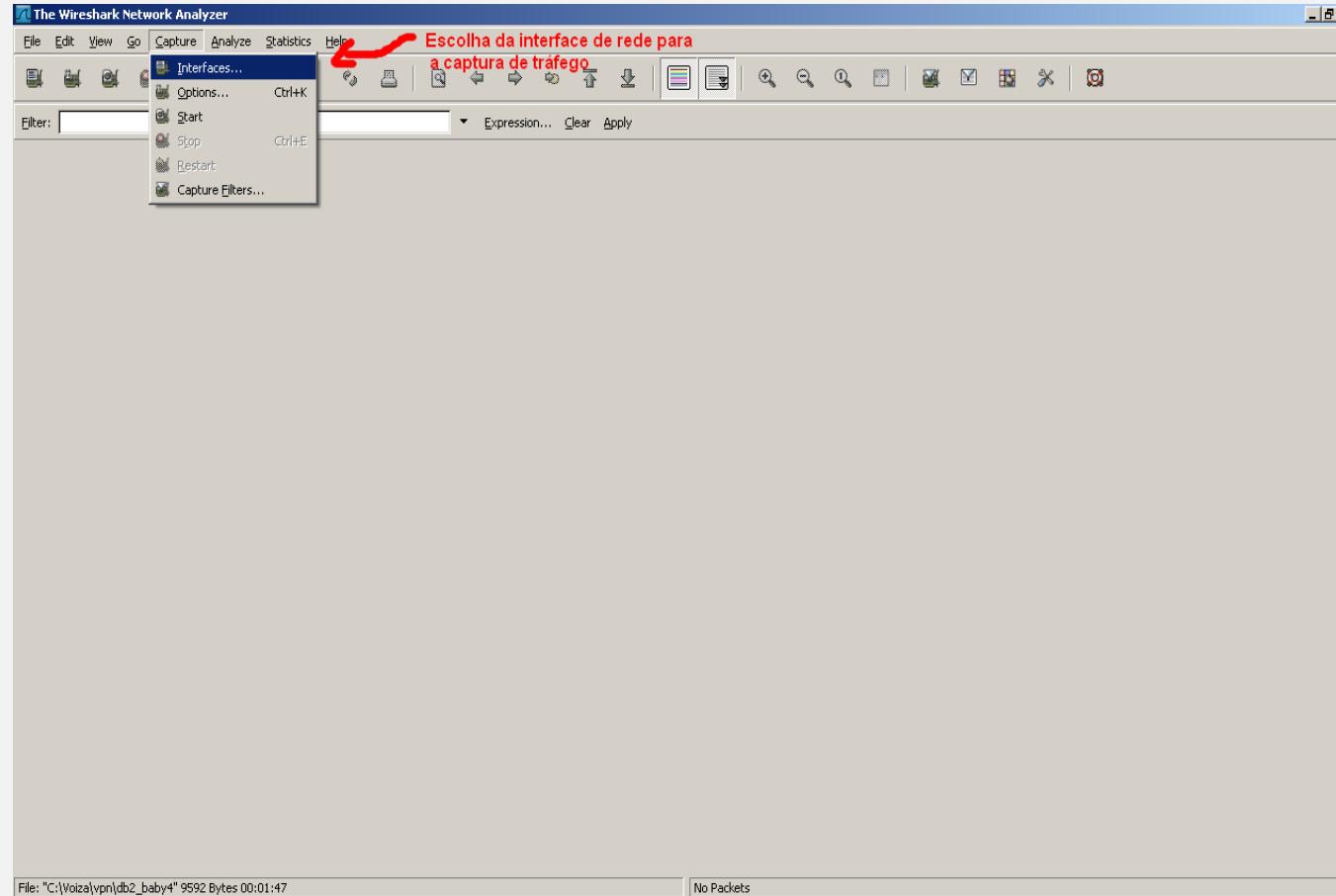
- **Fazer o download de:**

<http://www.wireshark.org/download.html>

- **O processo de instalação insere a biblioteca Winpcap no sistema operacional MS Windows;**
- **Procedimento “NEXT” de instalação**
- **Nas distribuições Linux, verificar os pacotes com o nome “wireshark”**

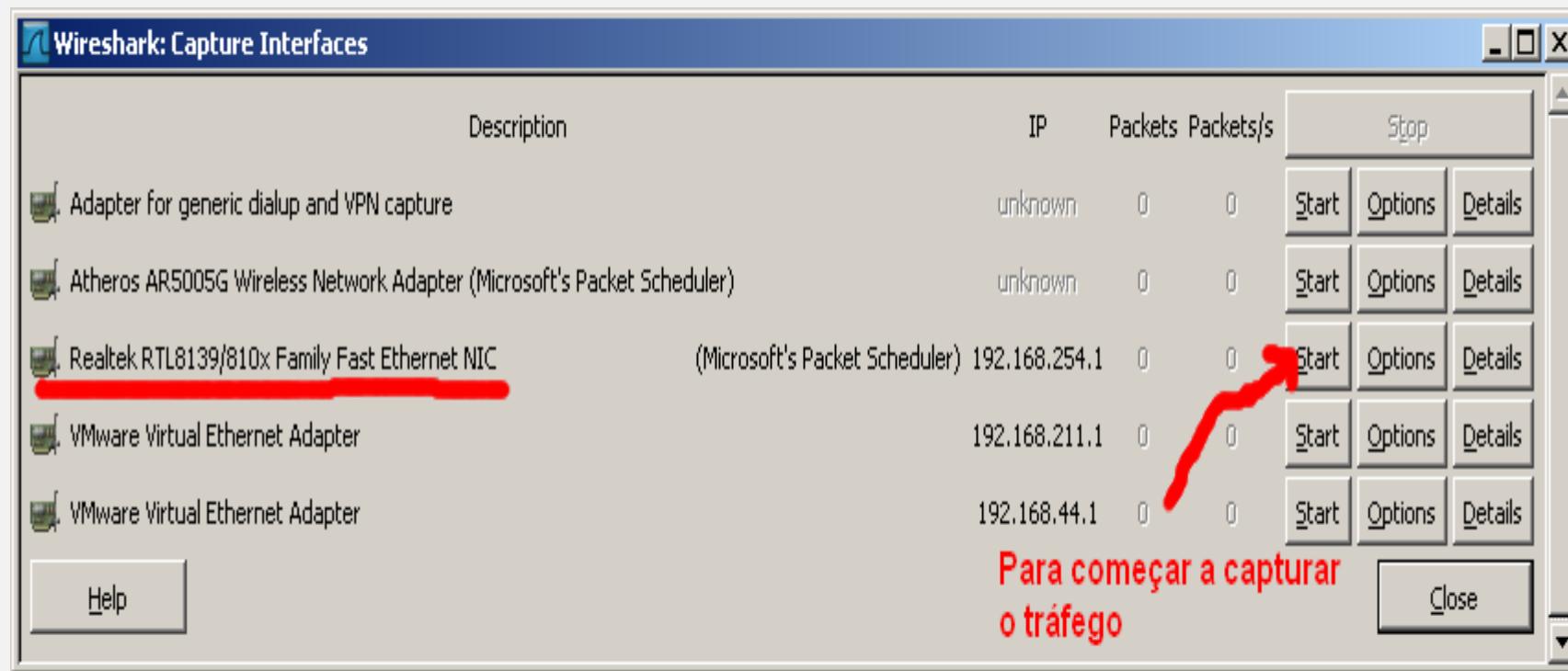
Usando o Wireshark

- **Executando a ferramenta e escolhendo a interface de rede:**



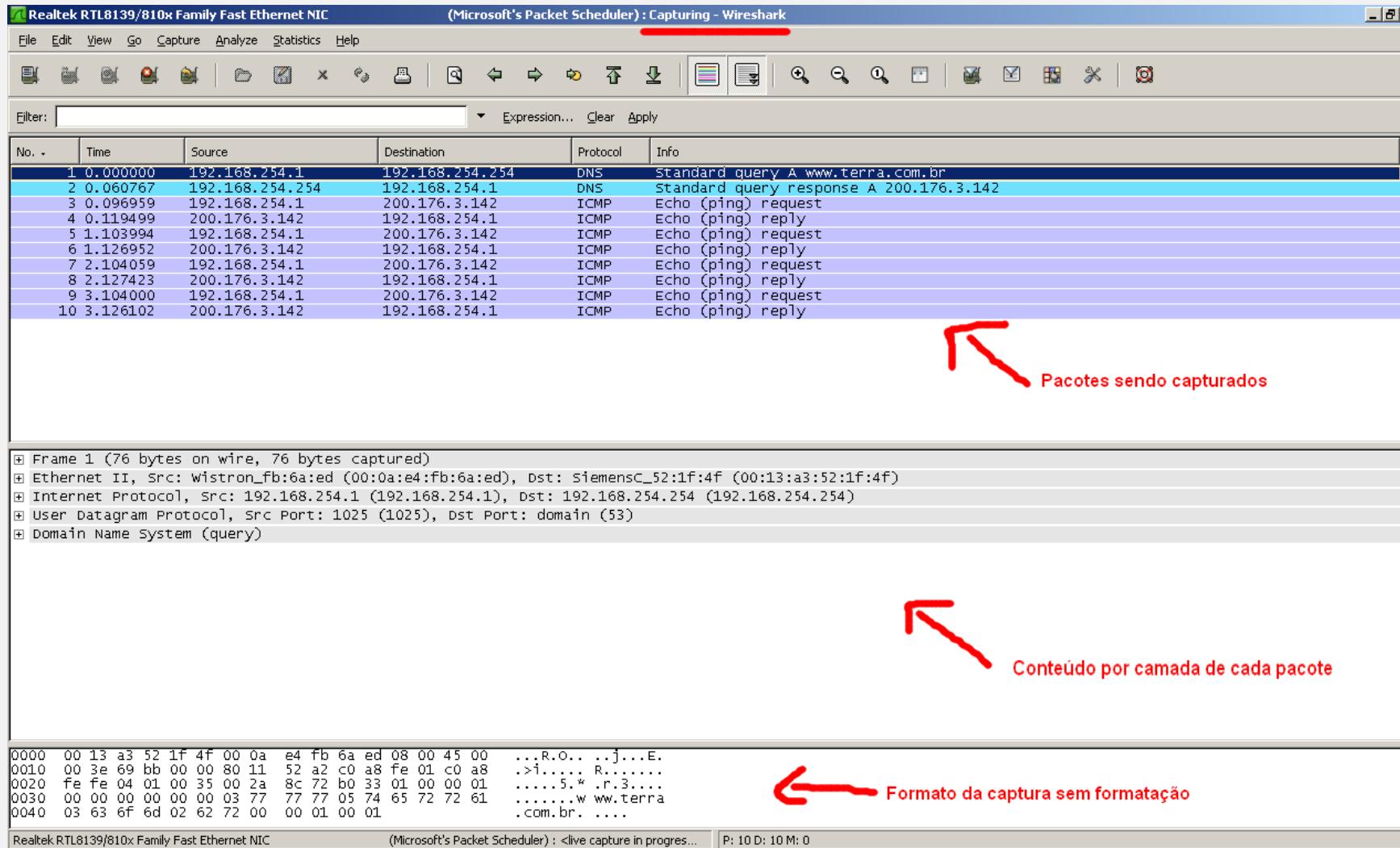
Usando o Wireshark

- Executando a ferramenta e escolhendo a interface de rede:



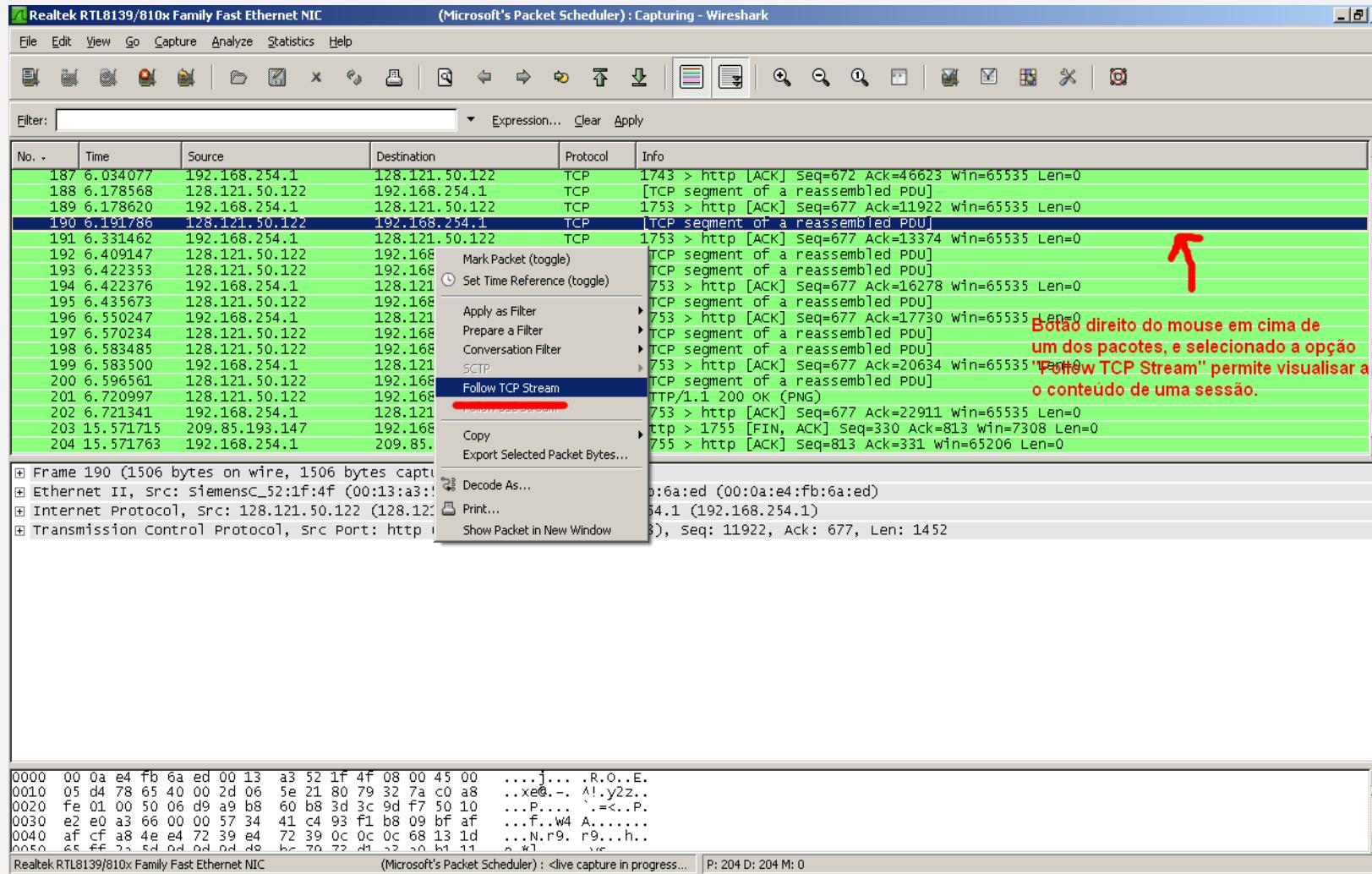
Usando o Wireshark

- Capturando pacotes:



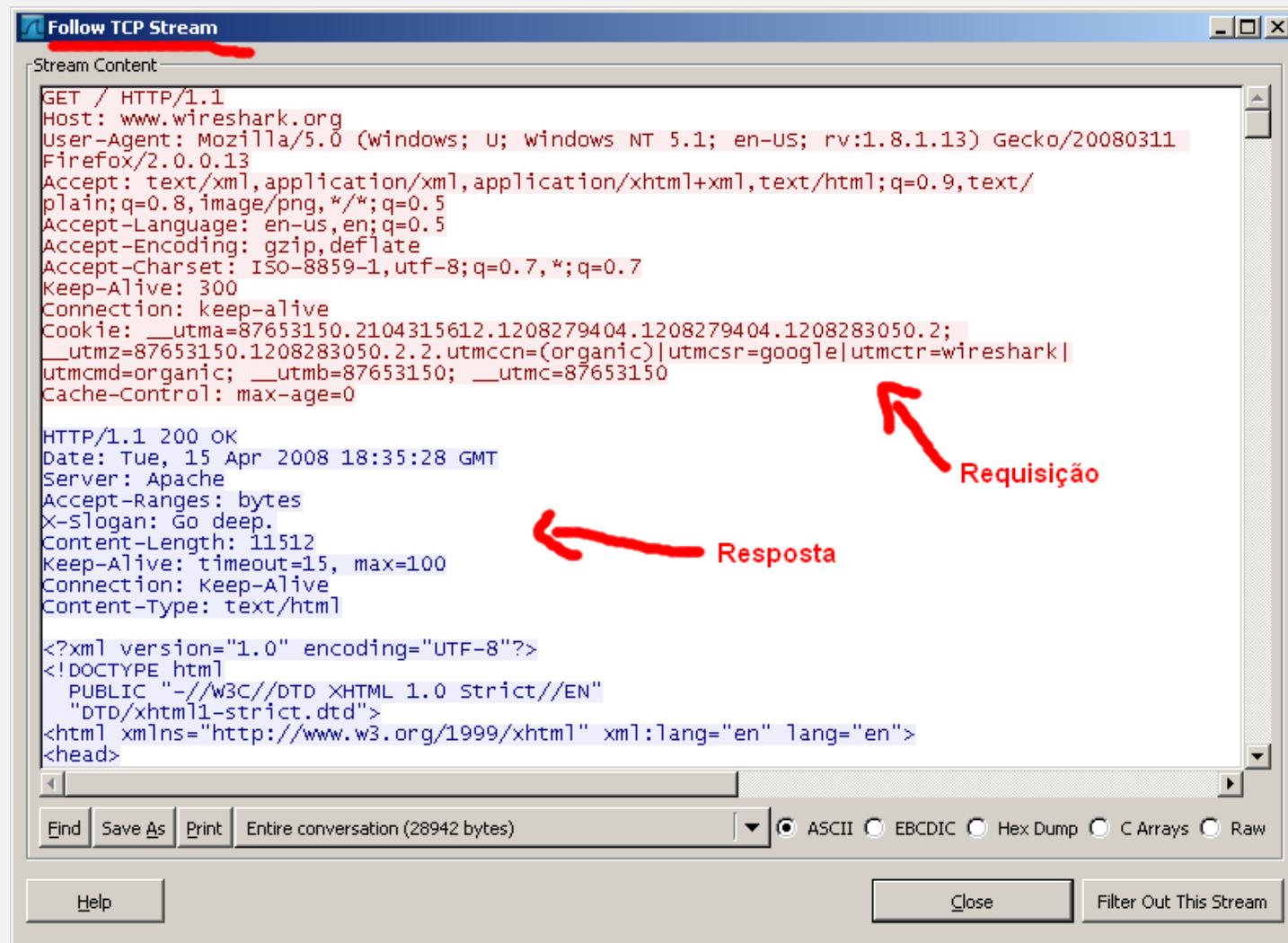
Usando o Wireshark

- **Analisando sessões:**



Usando o Wireshark

- **Analisando sessões:**



The screenshot shows the 'Follow TCP Stream' dialog in Wireshark. The title bar says 'Follow TCP Stream'. The main area is labeled 'Stream Content'.

Requisição (Request):

```
GET / HTTP/1.1
Host: www.wireshark.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.13) Gecko/20080311
Firefox/2.0.0.13
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: __utma=87653150.2104315612.1208279404.1208279404.1208283050.2;
__utmz=87653150.1208283050.2.2.utmccn=(organic)|utmcsr=google|utmctr=wireshark|
utmcmd=organic; __utmb=87653150; __utmc=87653150
Cache-Control: max-age=0
```

Resposta (Response):

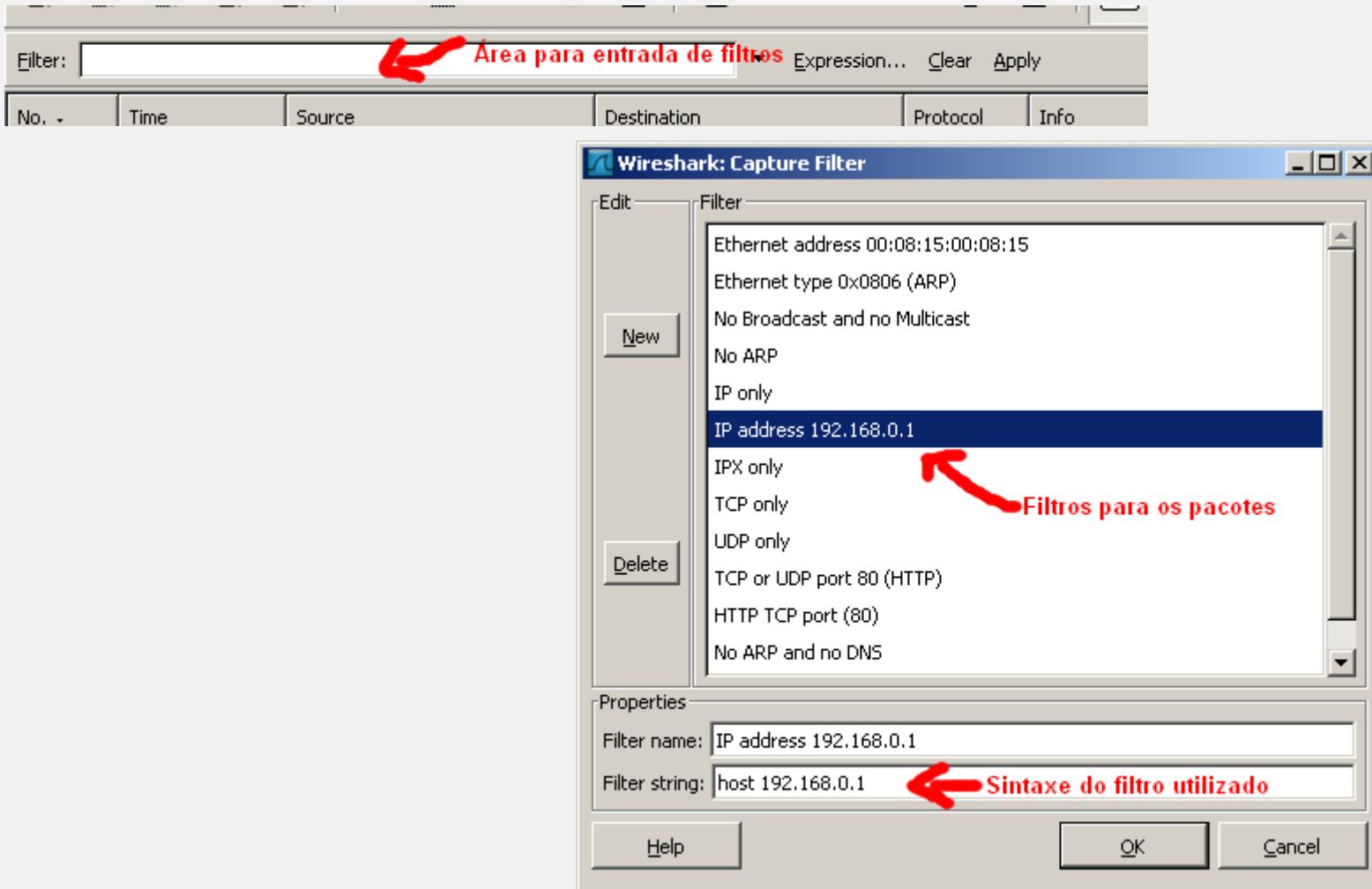
```
HTTP/1.1 200 OK
Date: Tue, 15 Apr 2008 18:35:28 GMT
Server: Apache
Accept-Ranges: bytes
X-Slogan: Go deep.
Content-Length: 11512
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html
  PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
```

At the bottom, there are buttons for 'Find', 'Save As', 'Print', and 'Entire conversation (28942 bytes)'. There are also radio buttons for ASCII, EBCDIC, Hex Dump, C Arrays, and Raw. The 'ASCII' button is selected.

Usando o Wireshark

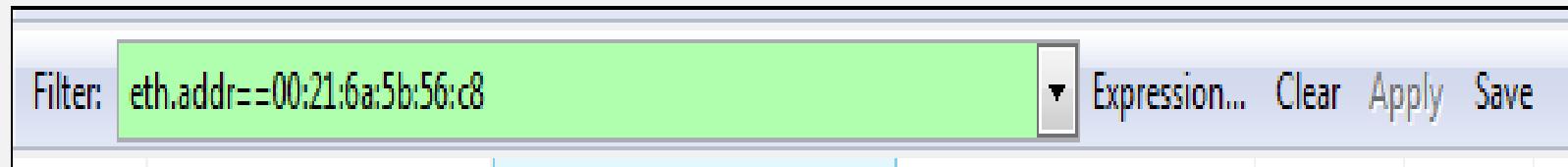
- **Filtros de pacotes:**



Usando o Wireshark

Exemplos de filtros (display filters):

- Todos os quadros Ethernet que contenham o endereço físico **00:22:64:7e:1a:3a**:
eth.addr==00:22:64:7e:1a:3a
- Todos os quadros Ethernet que contenham o endereço físico **00:22:64:7e:1a:3a** como origem:
eth.src==00:22:64:9e:0a:3a
- Todos os quadros Ethernet que contenham o endereço físico **ff:ff:ff:ff:ff:ff** como destino:
eth.dst==ff:ff:ff:ff:ff:ff
- Todos os quadros Ethernet que utilizem o protocolo ARP (tipo no campo Type 806):
eth.type==0x806



Usando o Wireshark

Exemplos de filtros (display filters):

- **Pacotes com o endereço IP 192.168.200.3:**
`ip.addr==192.168.200.3`
- **Pacotes com endereço IP de origem 192.168.200.3:**
`ip.src==192.168.200.3`
- **Pacotes com endereço IP de destino 192.168.200.3:**
`ip.dst==192.168.200.3`
- **Pacotes IP com campo TTL igual a 63:**
`ip.ttl==63`
- **Pacotes UDP com porta 4500:**
`udp.port==4500`
- **Pacotes UDP com porta de destino 53:**
`udp.dstport==53`
- **Pacotes UDP com porta de origem 789:**
`udp.srcport==789`
- **Pacotes UDP maiores do que 100 Bytes:**
`udp.length >= 100`

Usando o Wireshark

Exemplos de filtros (display filters):

- **Pacotes TCP com a porta 80:**

`tcp.port==80`

- **Pacotes TCP com a porta de destino 23:**

`tcp.dstport==23`

- **Pacotes TCP com a porta de origem 1098;**

`tcp.srcport==1098`

- **Pacotes TCP maiores ou iguais a 100 Bytes:**

`tcp.len >= 100`

- **Pacotes TCP com a *flag* SYN ativada:**

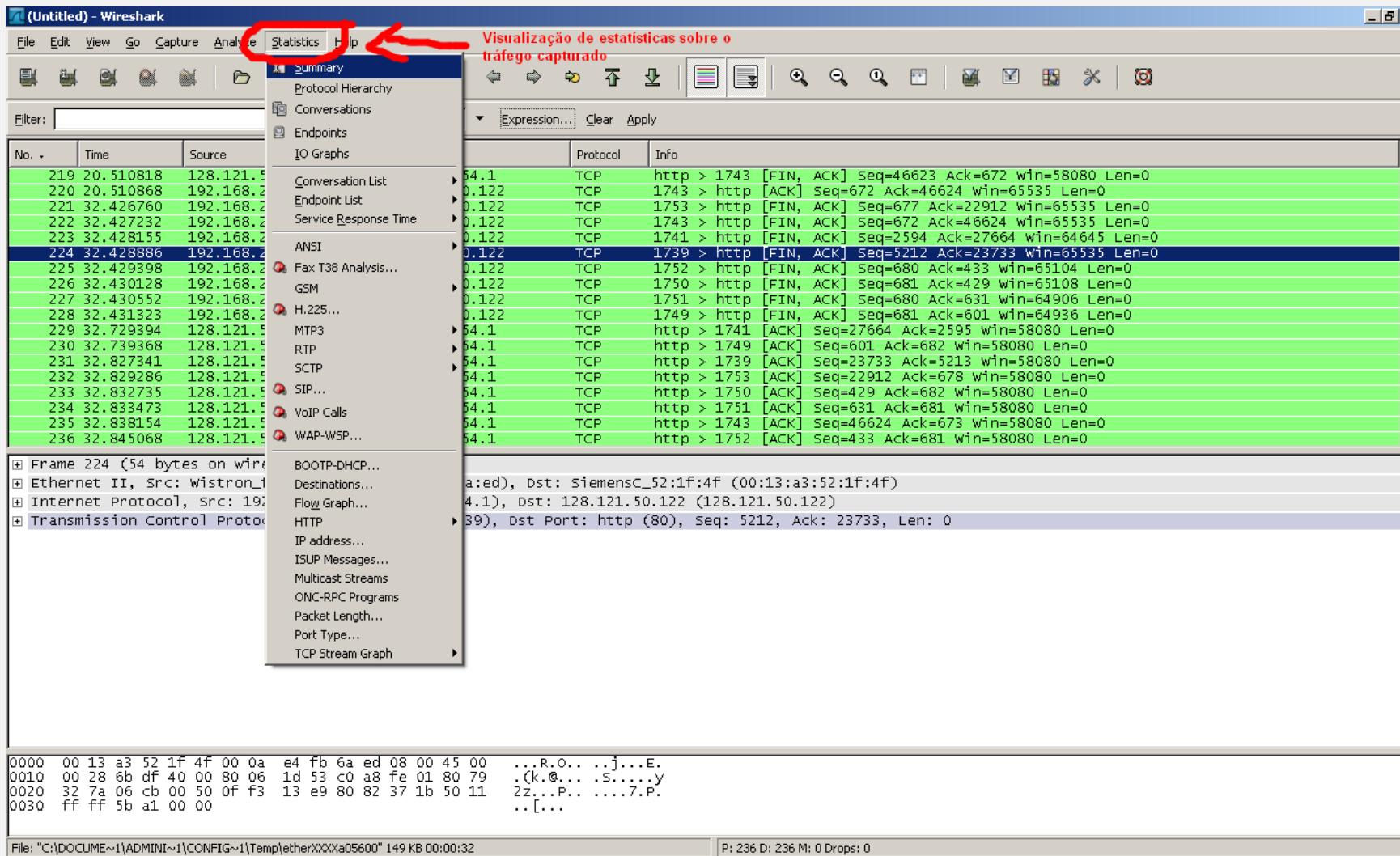
`tcp.flags.syn==1`

- **Pacotes TCP com a *flag* SYN ativada e a *flag* ACK desativada:**

`tcp.flags.syn==1 and tcp.flags.ack==0`

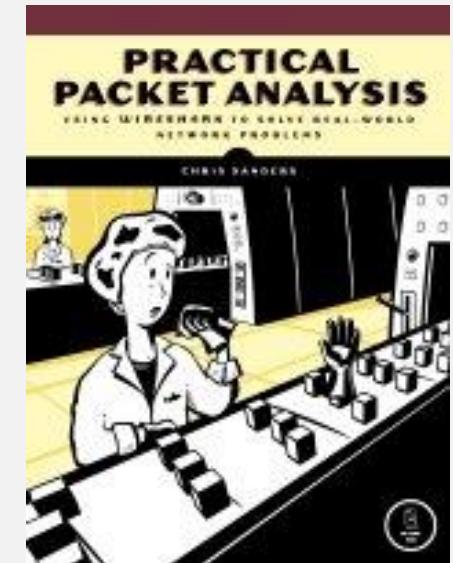
Usando o Wireshark

- **Estatísticas do tráfego de rede capturado**



Referências

- **Site do Wireshark:**
 - <http://www.wireshark.org>
- **Wireshark User's Guide:**
 - http://www.wireshark.org/docs/wsug_html_chunked/
- **Wireshark Wiki:**
 - <http://wiki.wireshark.org/>
- **SANDERS, Chris. Practical Packet Analysis Using Wireshark to Solve Real-World Network Problems. 2nd ed. No Starch Press, 2013.**
- **Livro: disponível no Dropbox**



Atividade III

1. Responder as questões da Lista de endereçamento IPV4:

<https://www.dropbox.com/s/se14901sxki41tn/Exercicio%20-%20Enderecamento%20Ipv41.pdf?dl=0>.

2. Assistir os vídeos de apoio a aprendizagem de IPV4:

- 1. Introduction to IPv4: <https://youtu.be/TqVTs9RjWcE>
- 2. Tipos de Endereços IPv4 e IPv6: <https://youtu.be/bihCH2fCRZI>
- 3. Curso de Redes - Endereço IPv4 e Classes de Endereçamento: https://youtu.be/65B_GENms18
- 4. Aprendendo a utilizar o GNS3: <https://youtu.be/z8z84zaYhxM>
- 5. Instalação e configuração do GNS3: <https://youtu.be/-wOQ6nTuyEU>
- 6. Instalando e Configurando o GNS3 e sua VM: <https://youtu.be/rV5GusJD-M4>
- 7. Setting up a basic network in GNS3: <https://youtu.be/ueNACHY10OM>
- 8. Como usar o Wireshark: <https://youtu.be/zp45Qv2nLWU>