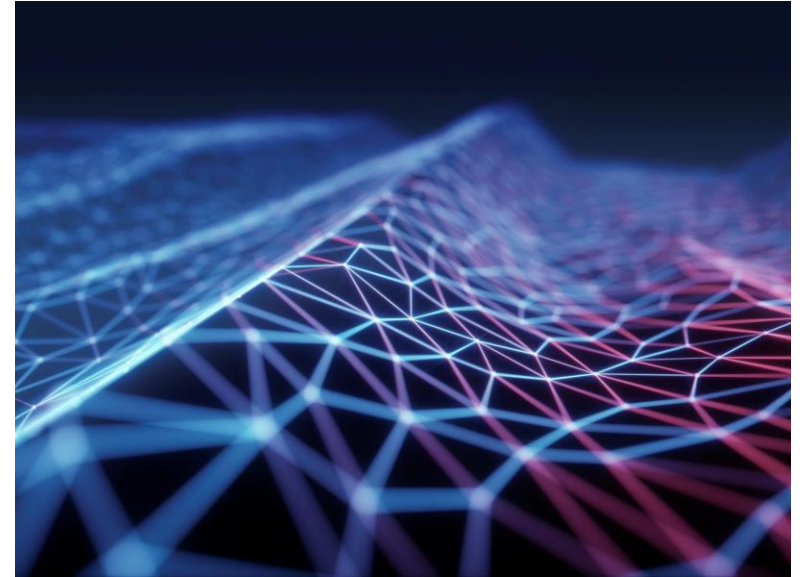


05 – PROJETO LÓGICO E FÍSICO DE REDES – PARTE I

PROFESSORES:

OSMAR DE OLIVEIRA BRAZ JUNIOR

RICHARD HENRIQUE DE SOUZA



OBJETIVOS

- Revisão dos conceitos relacionados ao Modelo OSI
- Compreender os elementos do quadro de enlace
- Compreender o funcionamento da camada de rede.
- Compreender o esquema de endereçamento IP.

MODELO EM CAMADAS OSI

- Baseia-se no conceito de camadas sobrepostas, com um conjunto de funções;
- Composto por 7 camadas: camada física, de enlace de dados, rede, transporte, sessão, apresentação e aplicação.

MODELO DE CAMADAS

- Dois modelos clássicos:
 - Modelo OSI (*Open System Interconnection*):
 - 7 camadas;
 - Modelo Internet:
 - 4 camadas;

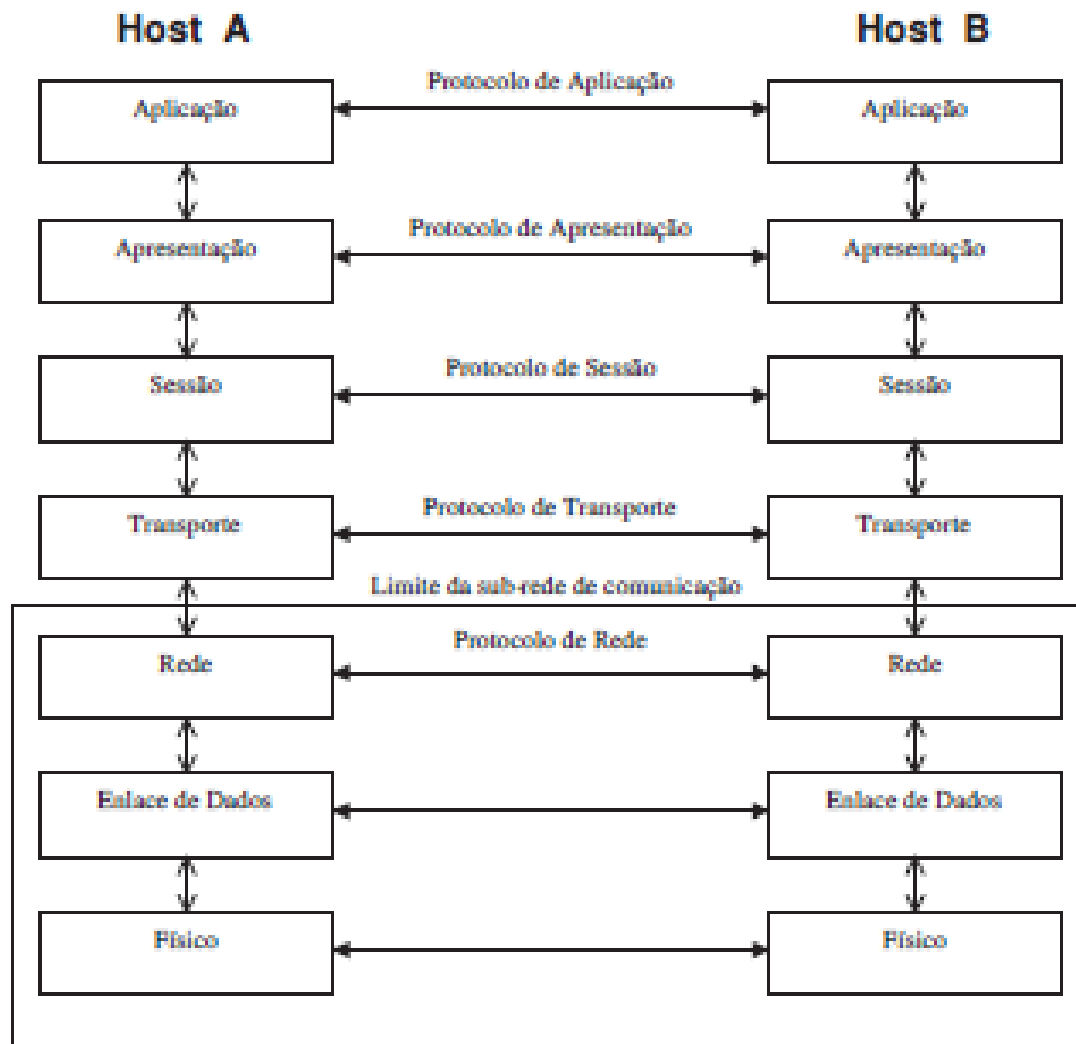


Figura 4.5: As 7 camadas do Modelo de Referência OSI [1]

COMUNICAÇÃO VERTICAL-HORIZONTAL


- No modelo de camadas, cada nível comunica-se apenas com a(s) camada(s) adjacente(s);
- Cada nível oferece um conjunto de *serviços* para a camada imediatamente superior e utiliza serviços do nível inferior;


TRANSMISSÃO – MODELO OSI



TRANSMISSÃO DE DADOS NO OSI

- Quando recebe dados para efetuar um serviço, uma camada N precisa incluir um cabeçalho, neste, são registradas informações relativas à camada.
- Os dados recebidos pela camada N, damos o nome de Unidade de dados do Serviço – SDU (Service Data Unit).

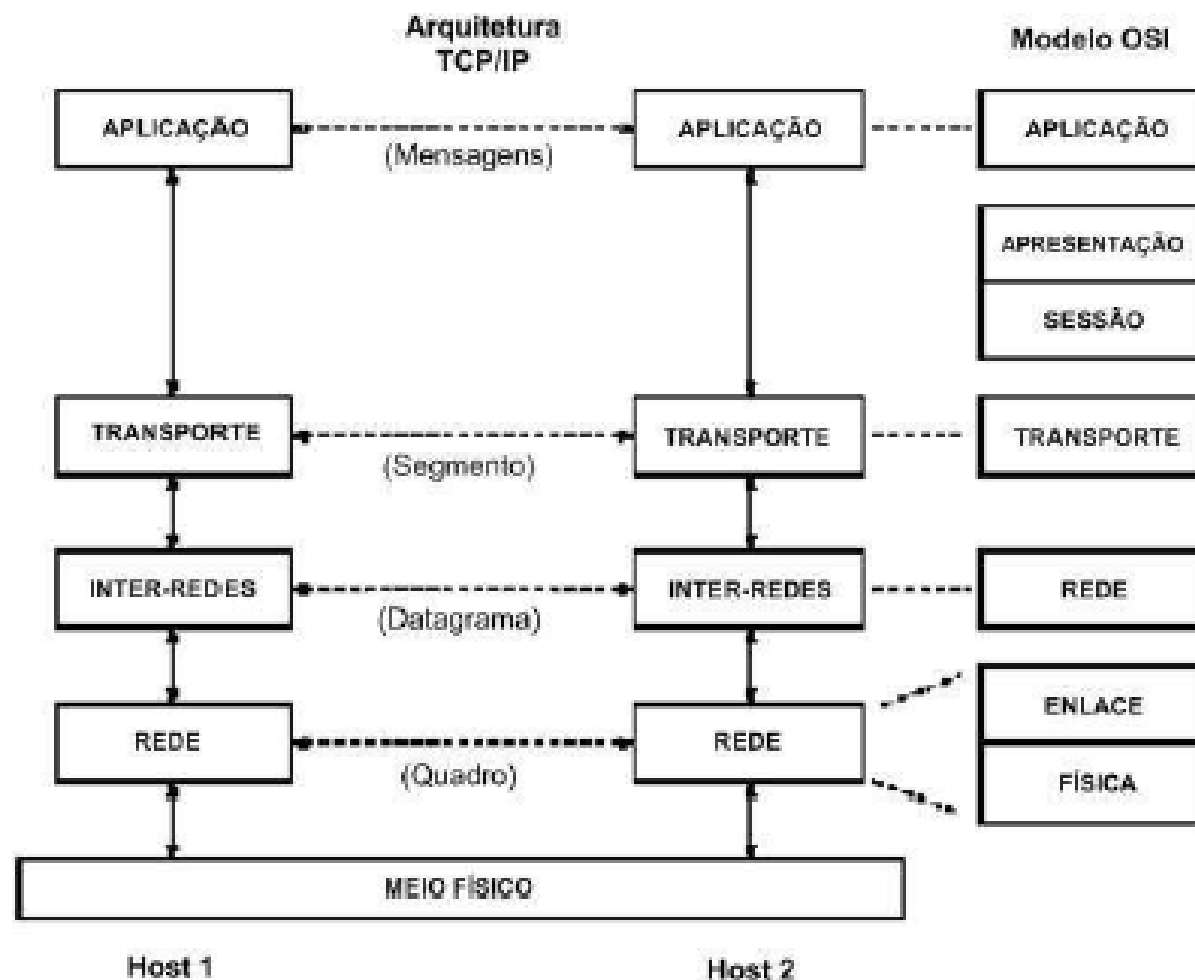
- 
- O conjunto formado pelo cabeçalho + SDU é denominado Unidade de Dados do Protocolo – PDU (Protocol Data Unit)
 - Neste momento dizemos que ocorreu um encapsulamento que é então passado para camada inferior.
 - A PDU do nível de aplicação é uma SDU no nível de apresentação.

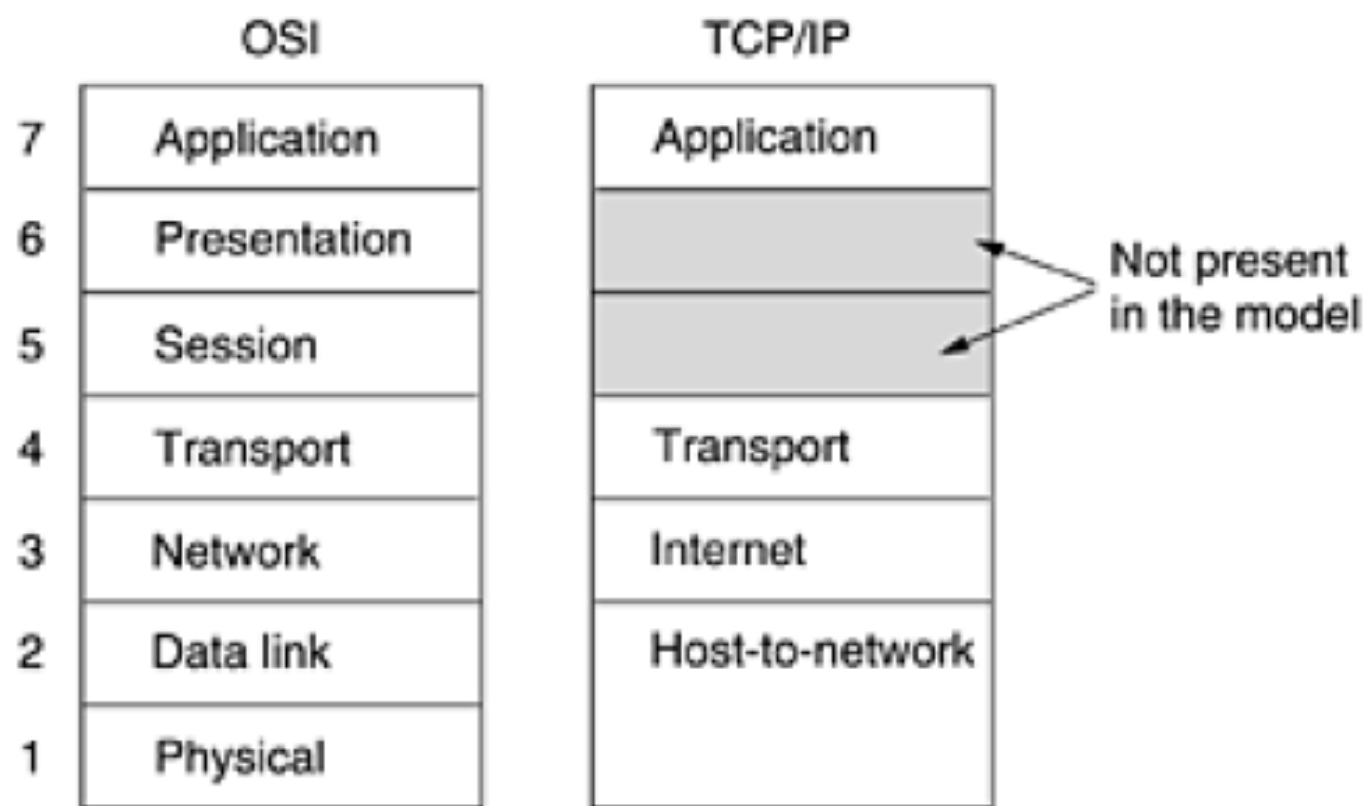
- 
- Esse processo continua até o nível de enlace, que geralmente acrescenta um cabeçalho e um fecho para detecção de erros.
 - A PDU do nível de enlace, é transmitida pelo nível físico através do meio de transmissão, depois de agregar ao quadro seu cabeçalho e seu fecho.
 - Quando o quadro é recebido pelo destinatário, o processo inverso ocorre.

MODELO TCP/IP

- É baseado em camadas sobrepostas;
- Apresenta quatro camadas:
 - Aplicação
 - Transporte
 - Inter-redes ou Internet
 - Rede

ARQUITETURA TCP/IP E MODELO OSI





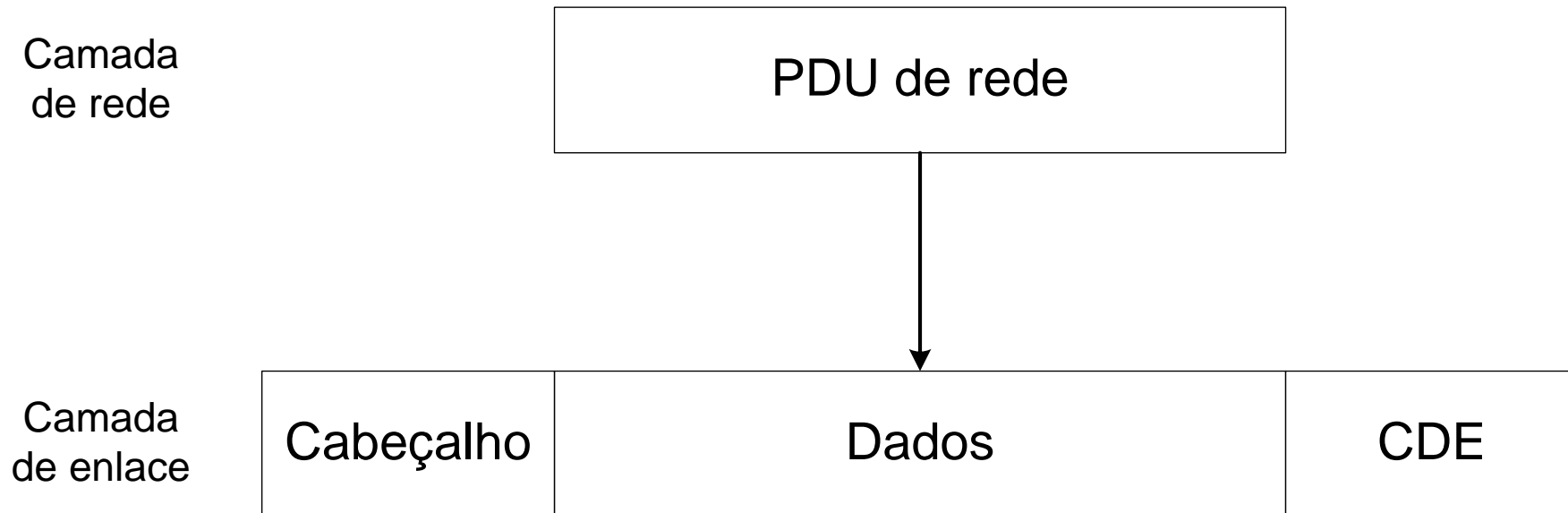


O QUE FAZ A INTERFACE DE REDE NESSE MODELO?

QUADROS

- Enquanto a camada física trabalha com bits, a camada de enlace trabalha com blocos de bits, chamados *quadros* ou *frames*.
- Quadros são formados por três estruturas básicas:
 - Cabeçalho – diversos campos para permitir a comunicação horizontal;
 - dados e;
 - CDE – código de detecção de erro;

ESTRUTURA DE UM QUADRO



ENDEREÇAMENTO

- O *endereçamento na camada de enlace* está associado à identificação da interface de comunicação, que conecta o dispositivo à rede,
- Cada interface possui um endereço único que permite identificá-la.
- O formato do endereço é definido pelo protocolo de enlace e deve ser seguido pelos fabricantes de interfaces de rede.

QUADRO ETHERNET

6	6	2	0-1500	4
End. destino	End. origem	Tam	Dados	CDE

ENDEREÇO FÍSICO

- O endereço da camada de enlace é também chamado de *endereço físico* ou *endereço MAC (Medium Access Control)*

```
c:\>ipconfig/all
```

```
Adaptador Ethernet Conexão local:
```

```
  Descrição . . . . . : Realtek RTL8169/8110 Family Gigabit Ethernet NIC  
  Endereço físico . . . . . : 00-08-54-46-4B-FA
```

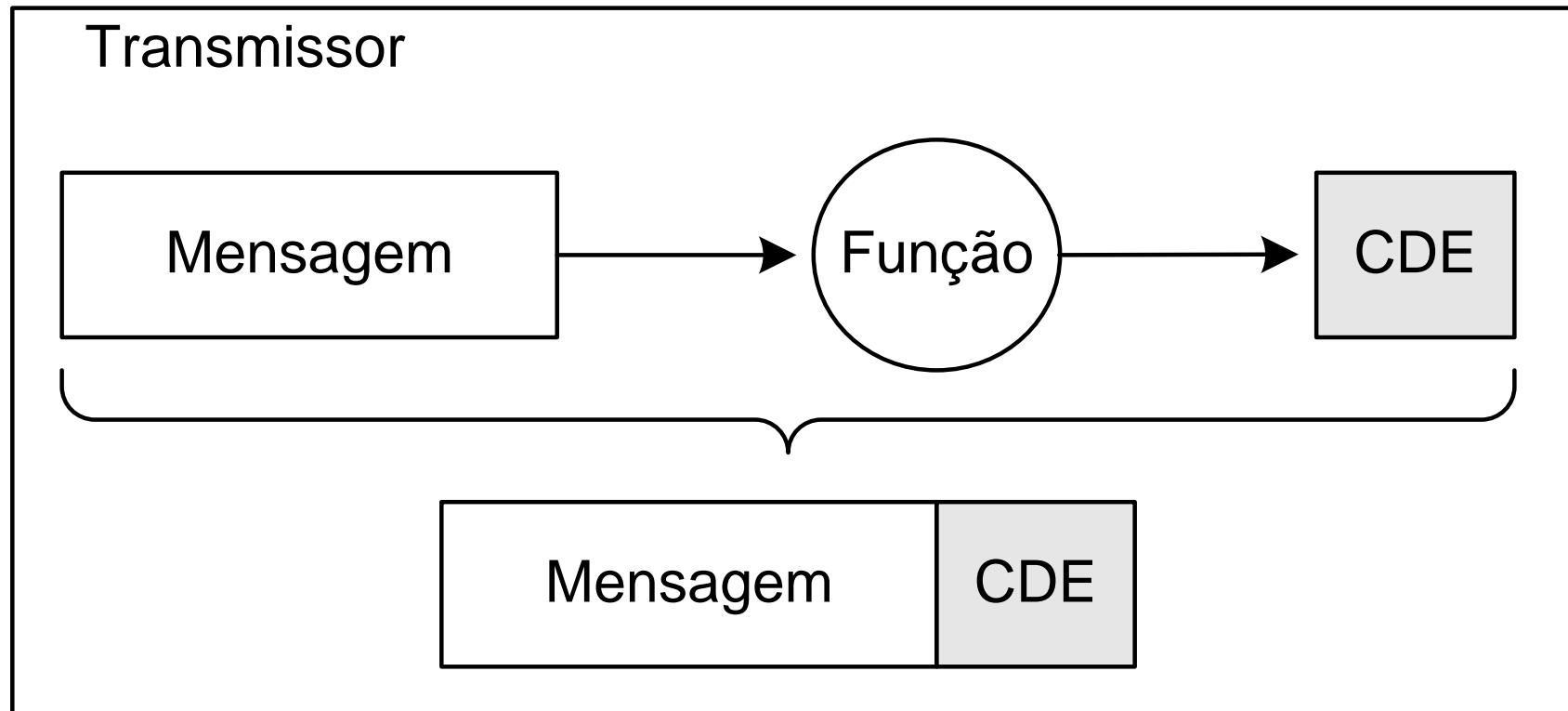
```
# ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:02:B3:B1:96:09  
          inet addr:10.10.0.50  Bcast:10.10.255.255  Mask:255.255.0.0
```

DETECÇÃO DE ERROS

- A detecção de erro é feita pelas informações de controle que são enviadas juntamente com os dados transmitidos.
 - Função para calcular um código de detecção de erro (CDE) a partir da mensagem a ser enviada (de forma a gerar uma espécie de dígito verificador).
 - O código gerado é anexado ao final da mensagem;

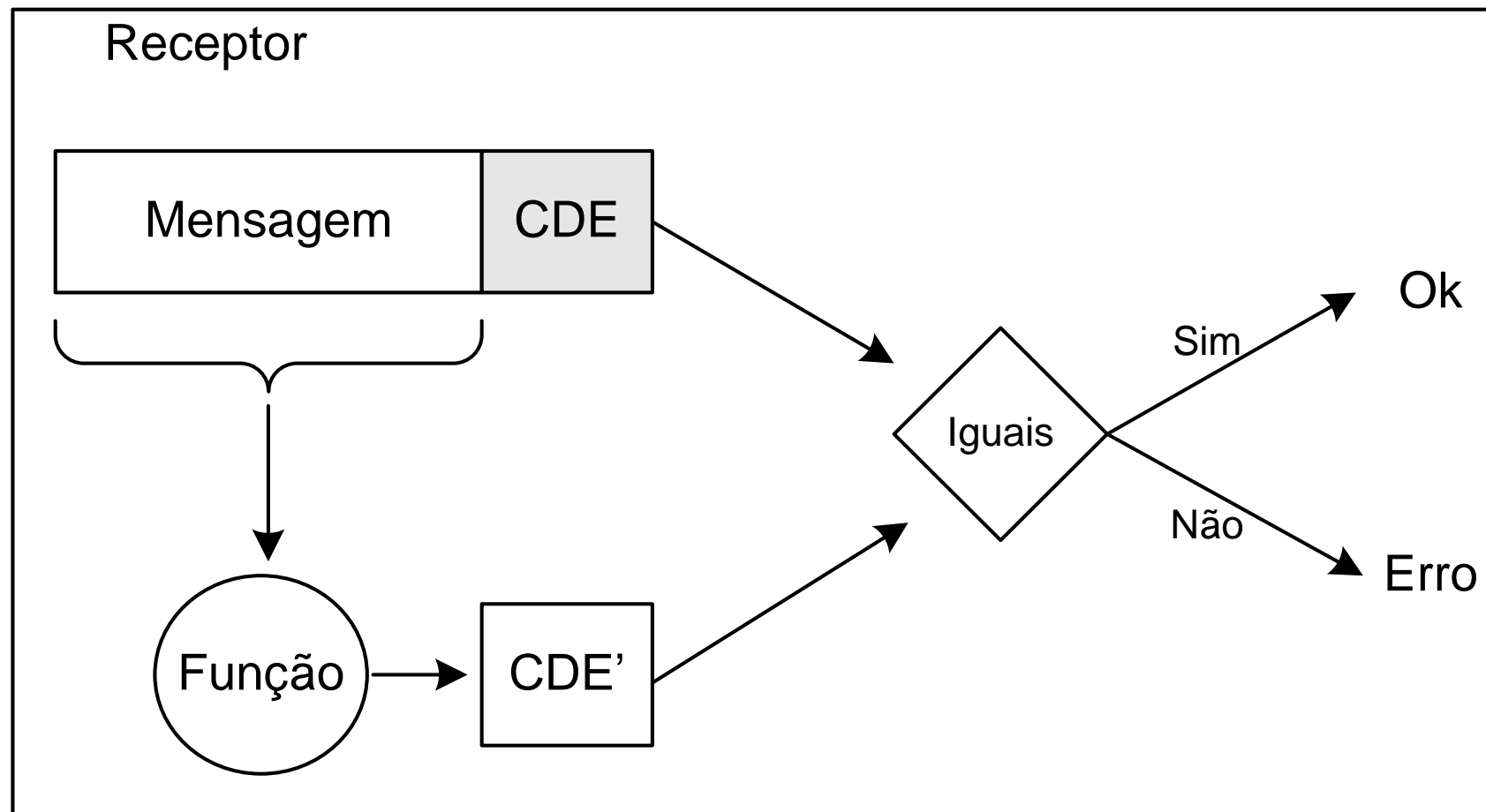
GERAÇÃO DO CÓDIGO DE DETECÇÃO DE ERRO



DETECÇÃO DE ERROS

- O destinatário, ao receber a mensagem, recalcula o código de detecção de erro (CDE') e o compara com o código recebido (CDE).
 - Se o código calculado no destino for igual ao transmitido, a mensagem está íntegra;
 - Caso contrário, houve algum erro;

VERIFICAÇÃO DO CÓDIGO DE DETECÇÃO DE ERRO



- 
- COMO FUNCIONA A CAMADA DE REDE?



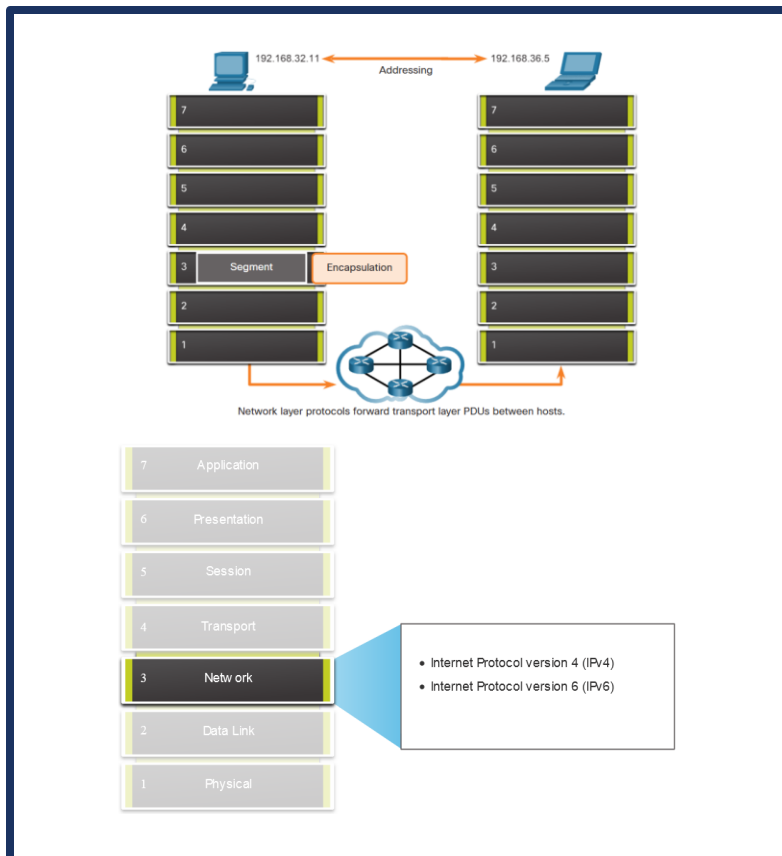
CAMADA DE REDE

A background image featuring a complex network of black nodes (spheres) connected by thin black lines, set against a light gray grid of thicker lines. The nodes are scattered across the frame, with some appearing larger and more prominent than others. The overall aesthetic is technical and digital.

CARACTERÍSTICAS DE CAMADA DE REDE

CARACTERÍSTICAS DE CAMADA DE REDE

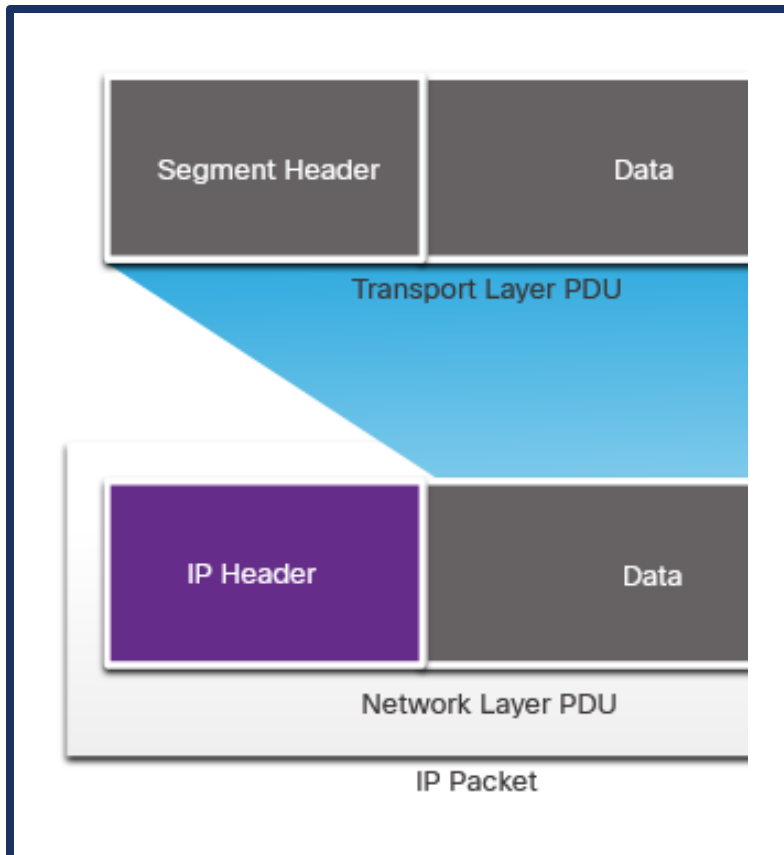
CAMADA DE REDE



- Fornece serviços para permitir que dispositivos finais troquem dados
- A camada de rede executa quatro operações básicas:
 - Endereça os dispositivos finais
 - Encapsulamento
 - Roteamento
 - Desencapsulamento

CARACTERÍSTICAS DE CAMADA DE REDE

ENCAPSULAMENTO IP



- O IP encapsula o segmento da camada de transporte.
- O pacote IP será examinado por todos os dispositivos de camada 3 à medida que atravessa a rede.

CARACTERÍSTICAS DE CAMADA DE REDE CONEXÕES

- IP não tem conexão
- Nenhuma conexão é estabelecida com o destino antes do envio dos pacotes de dados.
- Não há informações de controle necessárias (sincronizações, confirmações, etc.).
- O destino receberá o pacote quando ele chegar, mas nenhuma pré-notificação é enviada por IP.
- Se houver necessidade de tráfego orientado para conexão, outro protocolo irá lidar com isso (normalmente TCP na camada de transporte).



A letter is sent.



PACOTE IPV4

PACOTE IPV4

CABEÇALHO DO PACOTE IPV4

IPv4 é o principal protocolo de comunicação para a camada de rede.

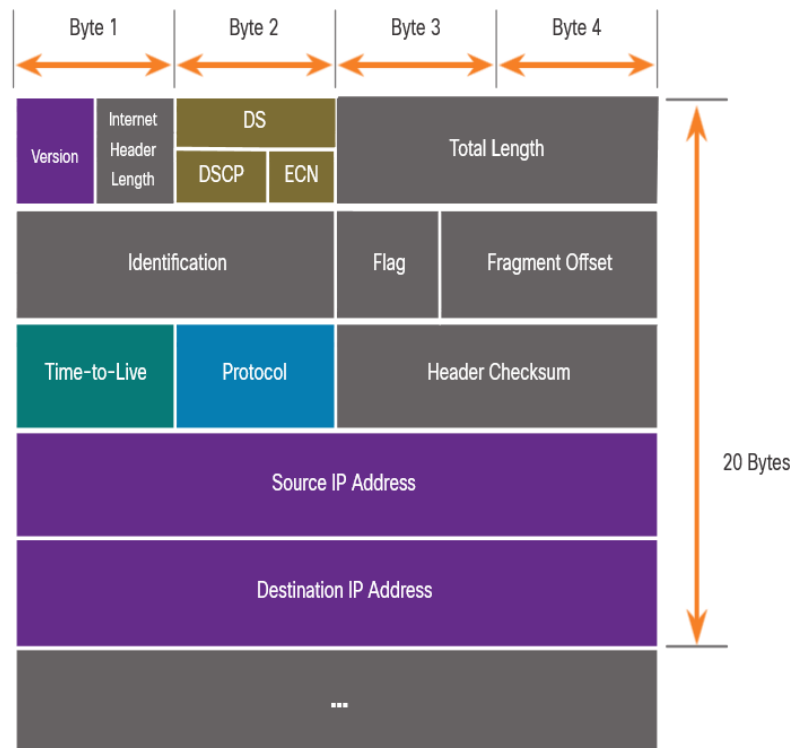
O cabeçalho de rede tem muitas finalidades:

- Ele garante que o pacote seja enviado na direção correta (para o destino).
- Ele contém informações para o processamento da camada de rede em vários campos.
- As informações no cabeçalho são usadas por todos os dispositivos de camada 3 que manipulam o pacote

CAMPOS DO CABEÇALHO DO PACOTE IPV4

Função	Descrição
Versão	Isso será para v4, ao contrário de v6, um campo de 4 bits = 0100
Serviços Diferenciados	Usado para QoS: campo DiffServ — DS ou o IntServ mais antigo — ToS ou Tipo de Serviço
Soma de verificação do cabeçalho	Detectar corrupção no cabeçalho IPv4
Tempo de vida (TTL)	Contagem de saltos de camada 3. Quando se tornar zero, o roteador descartará o pacote.
Protocolos	I.D.s protocolo de próximo nível: ICMP, TCP, UDP, etc.
Endereço IPv4 Origem	Endereço de origem de 32 bits
Endereço IPV4 de destino	Endereço de destino de 32 bits

CAMPOS DO CABEÇALHO DO PACOTE IPV4



- As características do cabeçalho de rede IPv4:
 - É em binário.
 - Contém vários campos de informação
 - O diagrama é lido da esquerda para a direita, 4 bytes por linha
 - Os dois campos mais importantes são a origem e o destino.
- Protocolos podem ter uma ou mais funções.

ESTRUTURA DE ENDEREÇO IPV4



REPRESENTAÇÃO DECIMAL

- Os dispositivos em uma rede possuem um endereçamento lógico composto de 32 bits, divididos em 4 dígitos de 8 bits, conhecidos como octetos e representados de forma decimal.

Valor da Posição	128	64	32	16	8	4	2	1
Base ^{Exponênc}	$2^7 = 128$		$2^3 = 8$					
	$2^6 = 64$		$2^2 = 4$					
	$2^5 = 32$		$2^1 = 2$					
	$2^4 = 16$		$2^0 = 1$					
Número de Símbolos	2							
Símbolos	0, 1							
Base lógica	Os sistemas de voltagem de dois-estados (discretos binários), formados por transistores, podem ser diversos, possantes, baratos, minúsculos e relativamente imunes ao ruído.							

SISTEMA NUMÉRICO BASE 10

- O Sistema Numérico de Base 10 é representado pelos símbolos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, os quais podem ser combinados para formar todos os valores numéricos.

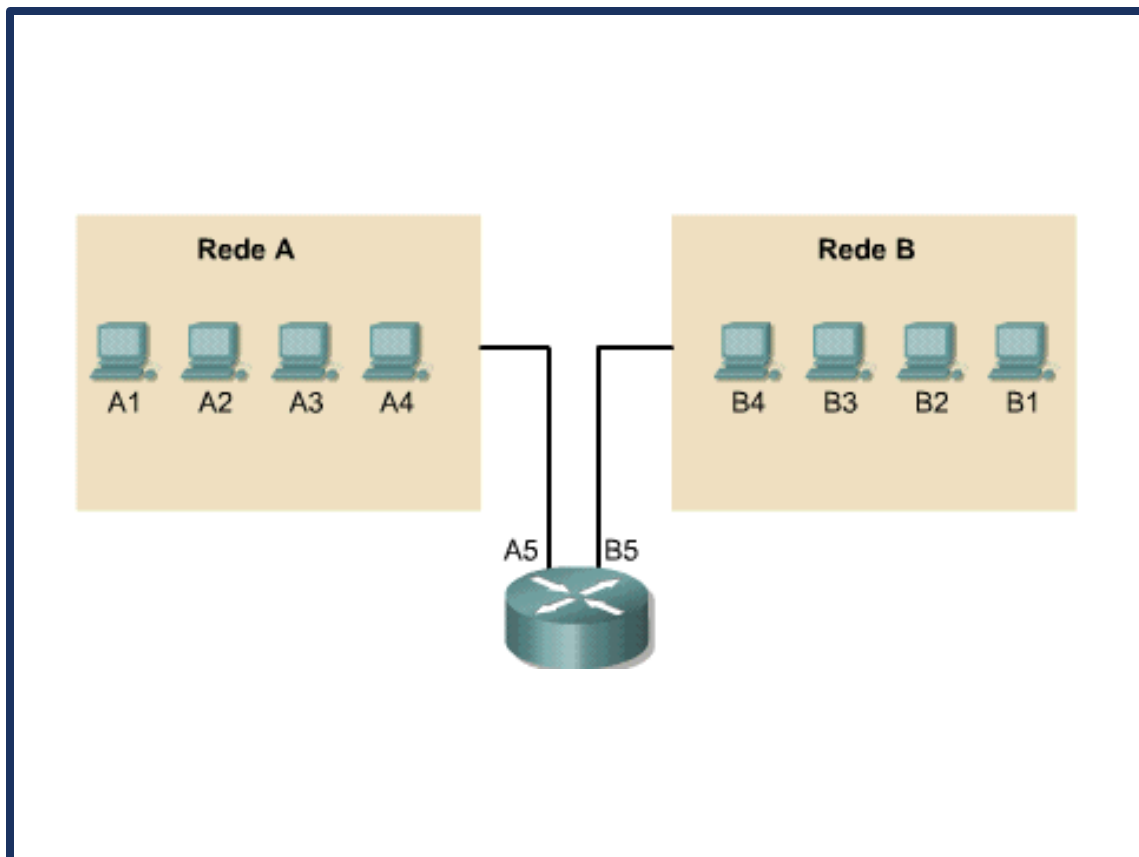
Valor da Posição	$\overline{1000}$ $\overline{100}$ $\overline{10}$ $\overline{1}$
Base ^{Expoente}	$10^3 = 1000$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$
Número de Símbolos	10
Símbolos	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Base lógica	O número típico de dedos equivale a dez

SISTEMA NUMÉRICO BASE 2

- O Sistema Numérico de Base 2 é representado pelos símbolos 0 e 1.
- Exemplo:
- $10110 = (1 \times 2^4 = 16) + (0 \times 2^3 = 0) + (1 \times 2^2 = 4) + (1 \times 2^1 = 2) + (0 \times 2^0 = 0) = 22$ (16 + 0 + 4 + 2 + 0)

Valor da Posição	128	64	32	16	8	4	2	1
Base ^{Exponente}	$2^7 = 128$		$2^3 = 8$					
	$2^6 = 64$		$2^2 = 4$					
	$2^5 = 32$		$2^1 = 2$					
	$2^4 = 16$		$2^0 = 1$					
Número de Símbolos	2							
Símbolos	0, 1							
Base lógica	Os sistemas de voltagem de dois-estados (discretos binários), formados por transistores, podem ser diversos, possantes, baratos, minúsculos e relativamente imunes ao ruído.							

ENDEREÇAMENTO IP



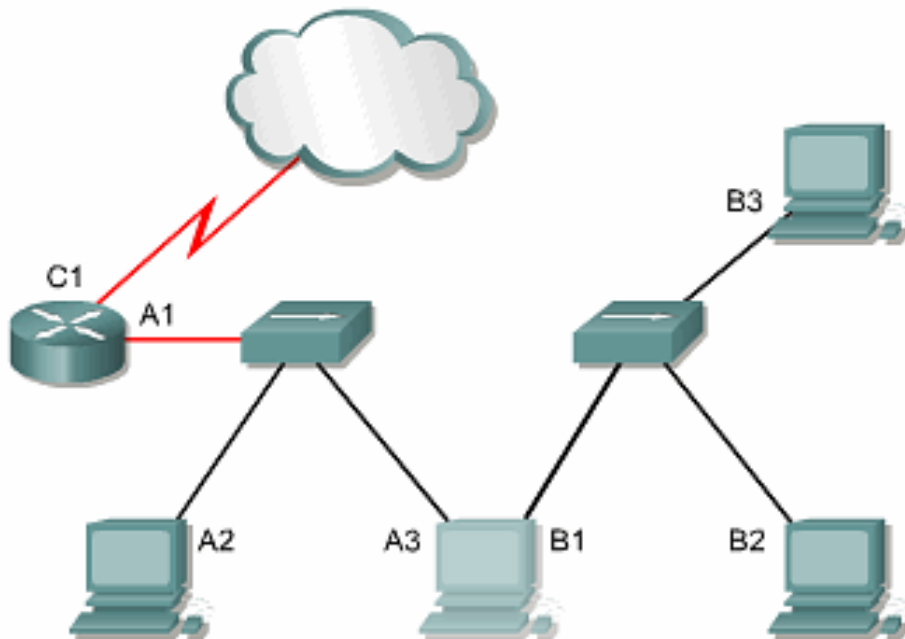
O IP é o endereço da Camada 03 (Rede), que tem a função de identificar a localização da rede e do host.

O endereçamento IP é composto de 32 bits divididos em 04 octetos, exibidos em 04 números decimais separados por pontos.

Cada endereço IP tem 32 bits ou 4 BYTES ou 4 Octetos.

Cada campo tem 8 bits - 00000000 (Zero) até 11111111 (255)

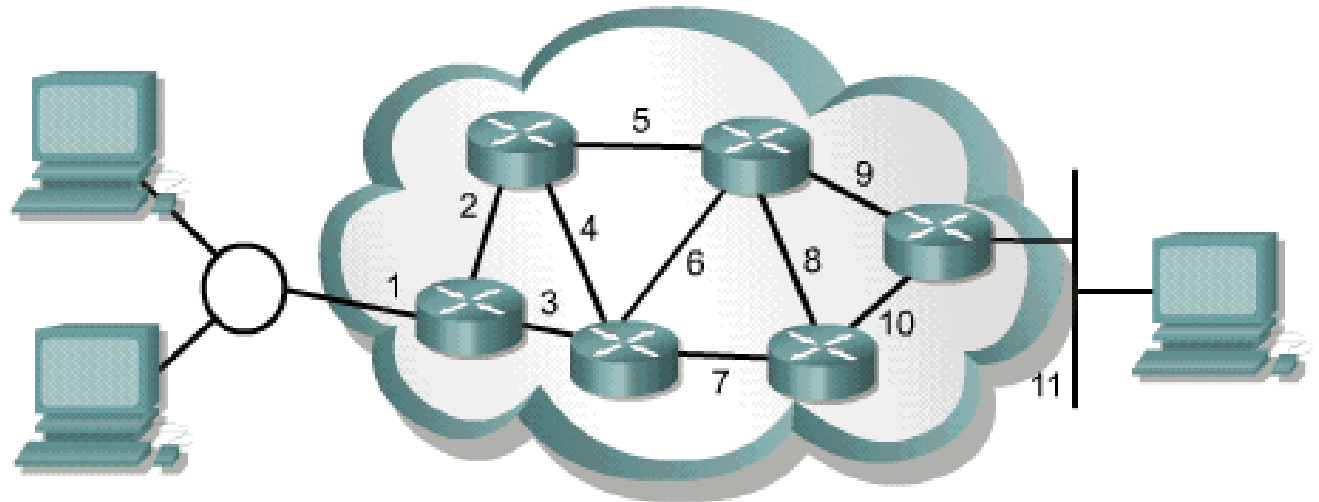
ENDEREÇAMENTO IP



- O valor máximo para cada um dos números é 255 (2^8).
- 11111111 (128+64+32+16+8+4+2+1)

ENDEREÇAMENTO IPV4

- Usando o endereço IP da rede de destino, um roteador pode entregar um pacote para a rede correta.
- Quando o pacote chega a um roteador conectado à rede de destino, esse roteador usa o endereço IP para localizar o computador específico conectado a essa rede.

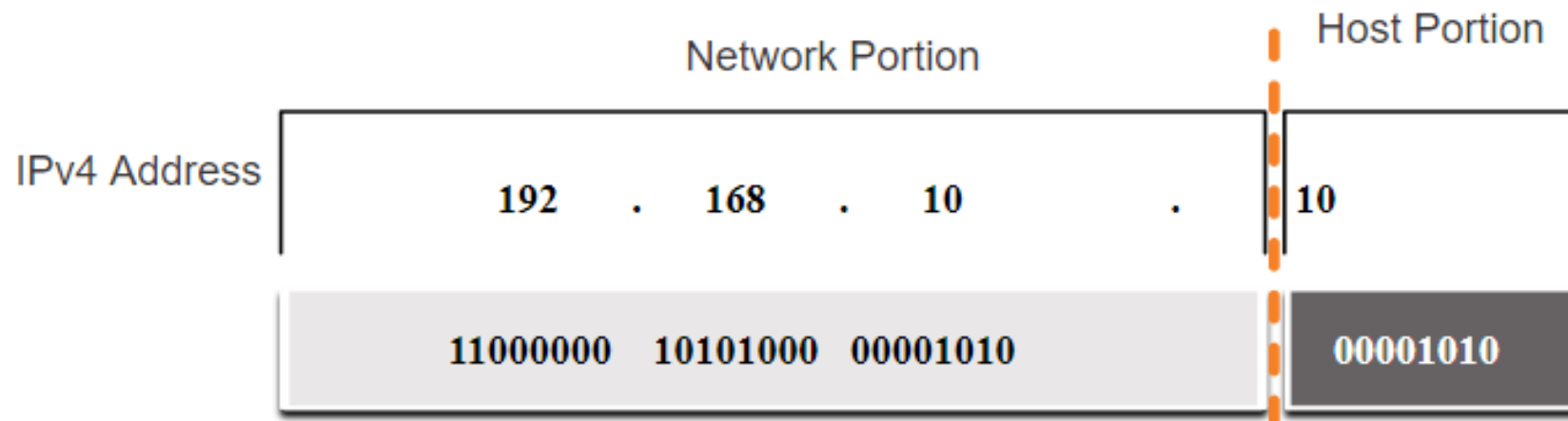


O endereço representa o caminho das conexões dos meios

ESTRUTURA DO ENDEREÇO IPV4

PARTES DE REDE E HOST

- Um endereço IPv4 é um endereço hierárquico de 32 bits, composto por uma parte da rede e uma parte do host.
- Ao determinar a parte da rede versus a parte do host, você deve observar o fluxo de 32 bits.
- Uma máscara de sub-rede é usada para determinar as partes da rede e do host.

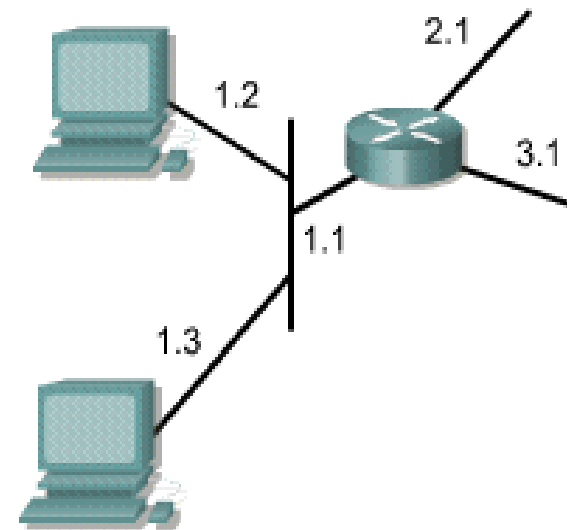


ENDEREÇAMENTO IPV4

O endereço IP tem duas partes:

- **rede:** identifica a rede a qual o sistema está conectado;
- **host:** identifica o sistema específico na rede.

O limite entre a parte de host e de rede, é definido pela máscara.



Rede	Host
1	1 2 3
2	1
3	1

ESTRUTURA DE ENDEREÇO IPV4

A MÁSCARA DE SUB-REDE

- Para identificar as partes da rede e do host de um endereço IPv4, a máscara de sub-rede é comparada com o endereço IPv4 bit por bit, da esquerda para a direita.

- O processo real usado para identificar as partes da rede e do host é chamado AND.

	Network Portion			Host Portion
IPv4 Address	192	. 168	. 10	. 10
	11000000	10101000	00001010	00001010
Subnet Mask	255	. 255	. 255	. 0
	11111111	11111111	11111111	00000000

O COMPRIMENTO DO PREFIXO

Um comprimento de prefixo é um método menos complicado usado para identificar um endereço de máscara de sub-rede.

- O comprimento do prefixo é o número de bits definido como 1 (um) na máscara de sub-rede.
- Está escrito em "notação de barra", portanto, conte o número de bits na máscara de sub-rede e adicione-a com uma barra.

Máscara de Sub-Rede	Endereço de 32 bits	Prefixo Duração
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

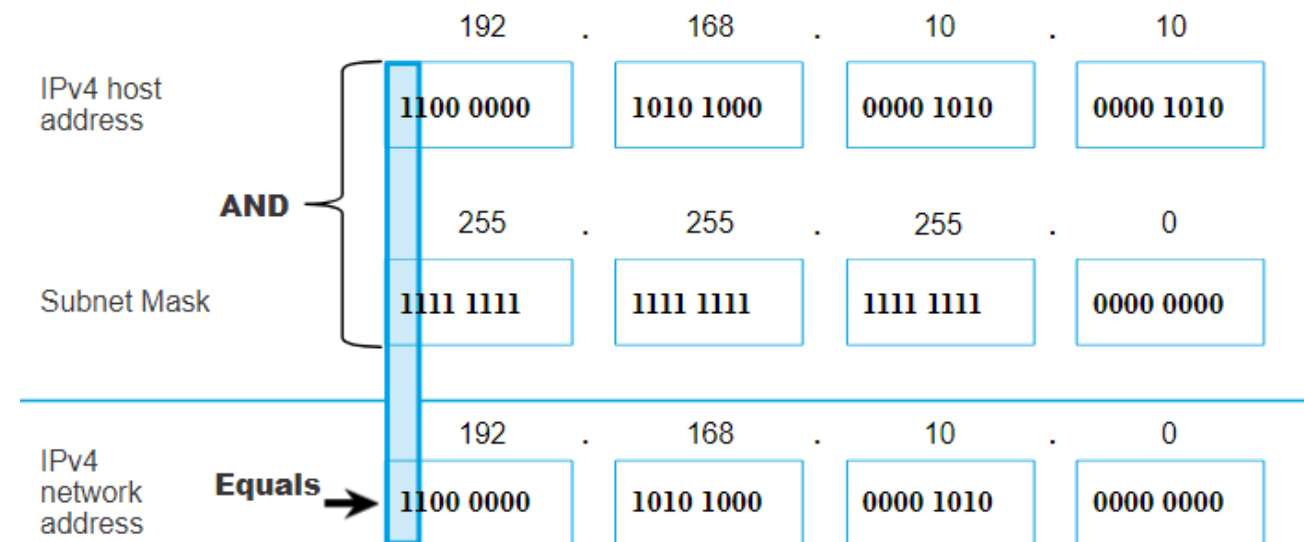
ESTRUTURA DE ENDEREÇOS IPV4

DETERMINANDO A REDE: LÓGICA E

■ Uma operação lógica AND booleana é usada na determinação do endereço de rede.

- Lógico AND é a comparação de dois bits onde apenas um 1 e 1 produz um 1 e qualquer outra combinação resulta em um 0.
- 1 e 1 = 1, 0 e 1 = 0, 1 e 0 = 0, 0 e 0 = 0
- 1 = Verdadeiro e 0 = Falso

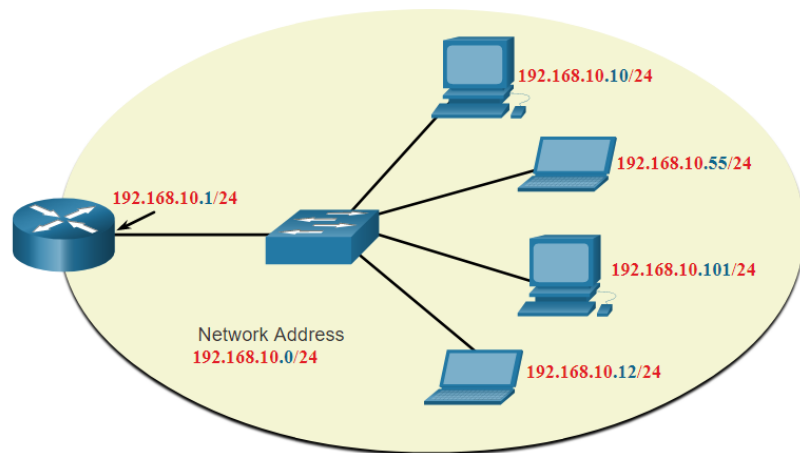
- Para identificar o endereço de rede, o endereço IPv4 do host é AND logicamente, bit a bit, com a máscara de sub-rede para identificar o endereço de rede.



ESTRUTURA DE ENDEREÇO IPV4

ENDEREÇOS DE REDE, HOST E TRANSMISSÃO

- Dentro de cada rede há três tipos de endereços IP:
 - Endereço de rede
 - Endereços de host
 - Endereço de broadcast



	Parte de rede	Parte de host	Bits de host
Máscara de sub-rede 255.255.255.0 ou /24	255 255 255 11111111 111111 111111 111111	0 00000000	
Endereço de rede 192.168.10.0 ou /24	192 168 10 11000000 10100000 00001010	0 00000000	Todos os 0
Primeiro endereço 192.168.10.1 ou /24	192 168 10 11000000 10100000 00001010	1 00000001	Todos os 0s e um 1
Último endereço 192.168.10.254 ou /24	192 168 10 11000000 10100000 00001010	254 11111110	Todos os 1s e um 0
Endereço de broadcast 192.168.10.255 ou /24	192 168 10 11000000 10100000 00001010	255 11111111	Todos os 1s

TIPOS DE ENDEREÇOS IPV4

ENDEREÇOS IPV4 DE USO ESPECIAL

- Endereços de loopback
 - 127.0.0.0 / 8 (127.0.0.1 a 127.255.255.254)
 - Comumente identificado como apenas 127.0.0.1
 - Usado em um host para testar se o TCP / IP está operacional.

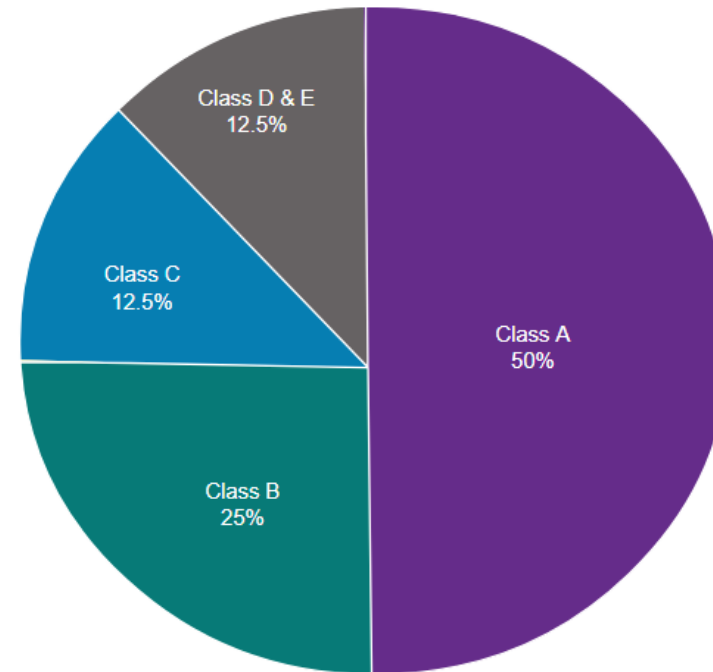
```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

TIPOS DE ENDEREÇOS IPV4

ENDEREÇAMENTO CLASSIFICADO LEGADO

■ RFC 790 (1981) alocado endereços IPv4 em classes

- Classe A (0.0.0/8 a 127.0.0.0/8)
- Classe B (128.0.0.0 /16 — 191.255.0.0 /16)
- Classe C (192.0.0.0 /24 — 223.255.255.0 /24)
- Classe D (224.0.0.0 a 239.0.0.0)
- Classe E (240.0.0.0 — 255.0.0.0)



Class A

Total Networks: 128
Total Hosts/Net: 16,777,214

Class B

Total Networks: 16,384
Total Hosts/Net: 65,534

Class C

Total Networks: 2,097,152
Total Hosts/Net: 254

Endereços de classe desperdiçaram muitos endereços IPv4.

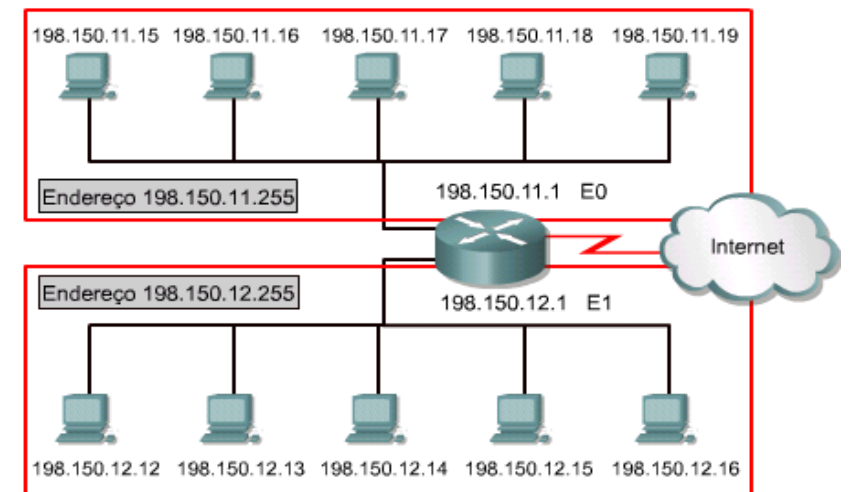
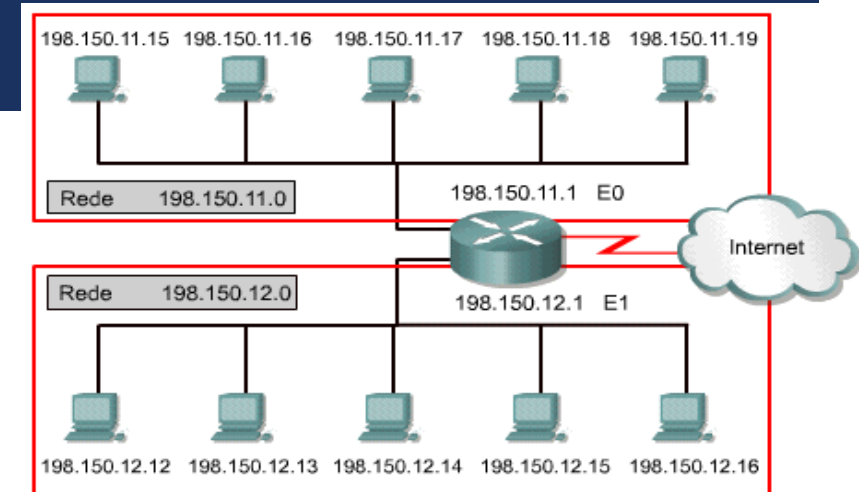
A alocação de endereços de classe foi substituída por endereçamento sem classe que ignora as regras das classes (A, B, C).

ENDEREÇOS IP RESERVADOS

Existem **endereços reservados** que não podem ser atribuídos a nenhum dispositivo na rede, tais

Endereço de rede: endereço utilizado para identificar a rede;

Endereço de broadcast: endereço utilizado para uma origem enviar dados para todos os hosts em uma rede.



ENDEREÇO DE BROADCAST

- Endereço com todos os bits destinados à identificação da máquina, iguais a 1: Um endereço com valor 1 em todos os bits de identificação da máquina, representa o endereço de broadcast.
- Exemplo:
 - 200.100.10.3
 - 255.255.255.0
 - Endereço de BroadCast - 200.100.10.255



COMO DESCOBRIR O NÚMERO DE HOSTS POR REDE OU SUB-REDE?

- Para descobrir o número de hosts possíveis por sub-rede, é dado pela equação genérica:
 - $2^n - 2$,
- onde n é igual ao número de bits do host.

CLASSE C

192 -223

- Exemplo de IP : 200.100.10.100 /24
- Máscara padrão em decimal: 255.255.255.0
- Máscara padrão em binário: 11111111.11111111.11111111.00000000
- Função da Máscara: REDE.REDE.REDE.HOST
- Quantidade de hosts por rede: 254 ($2^n - 2$)
 - Rede: 200.100.10.0
 - 1º Host: 200.100.10.1
 - Último Host: 200.100.10.254
 - BroadCast: 200.100.10.255

CLASSE B

128-191

- Exemplo de IP : 170.70.7.10 /16
- Máscara padrão em decimal: 255.255.0.0
- Máscara padrão em Binário: 11111111.11111111.00000000.00000000
- Função da Máscara: REDE.REDE. HOST.HOST
- Quantidade de Hosts por REDE: 65.534 Hosts ($2^n - 2$)
- Exemplo:
 - REDE: 170.70.0.0
 - 1º Host: 170.70.0.1
 - Último Host: 170.70.255.254
 - BroadCast: 170.70.255.255

CLASSE A

1-127

- Exemplo de IP: 11.200.12.200 /8
- Máscara padrão em decimal: 255.0.0.0
- Máscara padrão em Binário: 11111111.00000000.00000000.00000000
- Função da Máscara: REDE.HOST.HOST.HOST
- Quantidade de Hosts por REDE: 16.777.214 Hosts ($2^n - 2$)
- Exemplo:
 - REDE: 11.0.0.0
 - 1º Host: 11.0.0.1
 - Último Host: 11.255.255.254
 - BroadCast: 11.255.255.255

MÁSCARAS E SUB-REDES

- Serve para definir a classe de endereçamento, especificando que parte do endereço IP representa a rede e que parte representa o host (computador).
- O número 255 na máscara, confirma que o respectivo byte (octeto de bits) do endereço IP faz parte do endereço de rede.

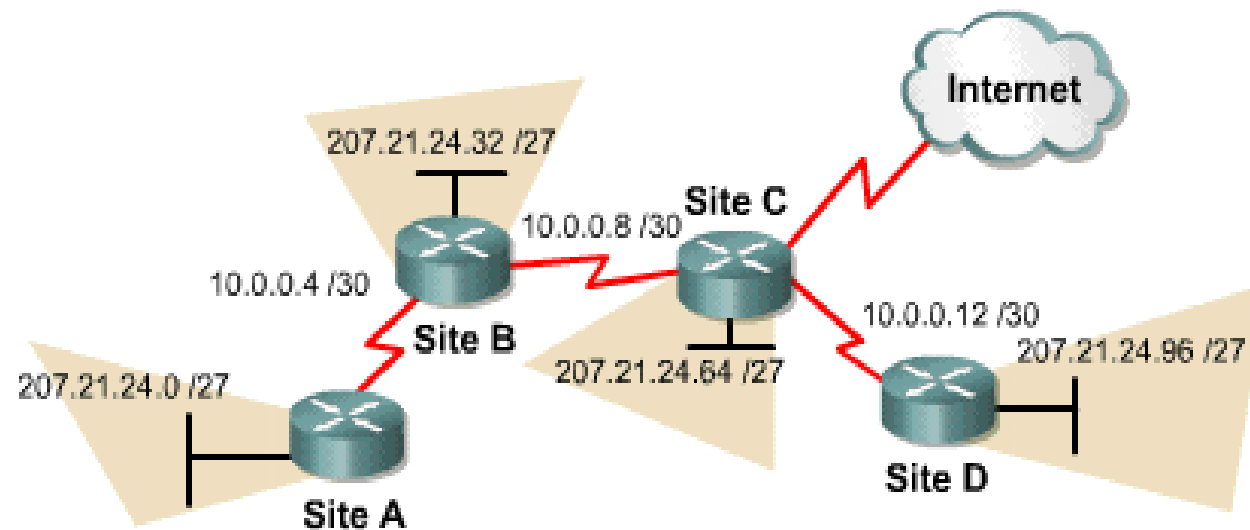
EXEMPLO


- Dado o endereço IP 143.106.12.37 e a máscara 255.255.0.0, o endereço de rede é 143.106.0.0 e broadcast nesta rede dá-se através do endereço 143.106.255.255.

ENDEREÇOS IP PÚBLICOS E PRIVADOS

Os hosts que estiverem conectados a rede pública (Internet) precisam de um endereço IP exclusivo.

Endereços IP são administrados sob a autoridade do IANA/ ICANN – *Internet Corporation for Assigned Names and Numbers*.





TIPOS DE ENDEREÇOS IPV4

ENDEREÇOS IPV4 PÚBLICOS E PRIVADOS

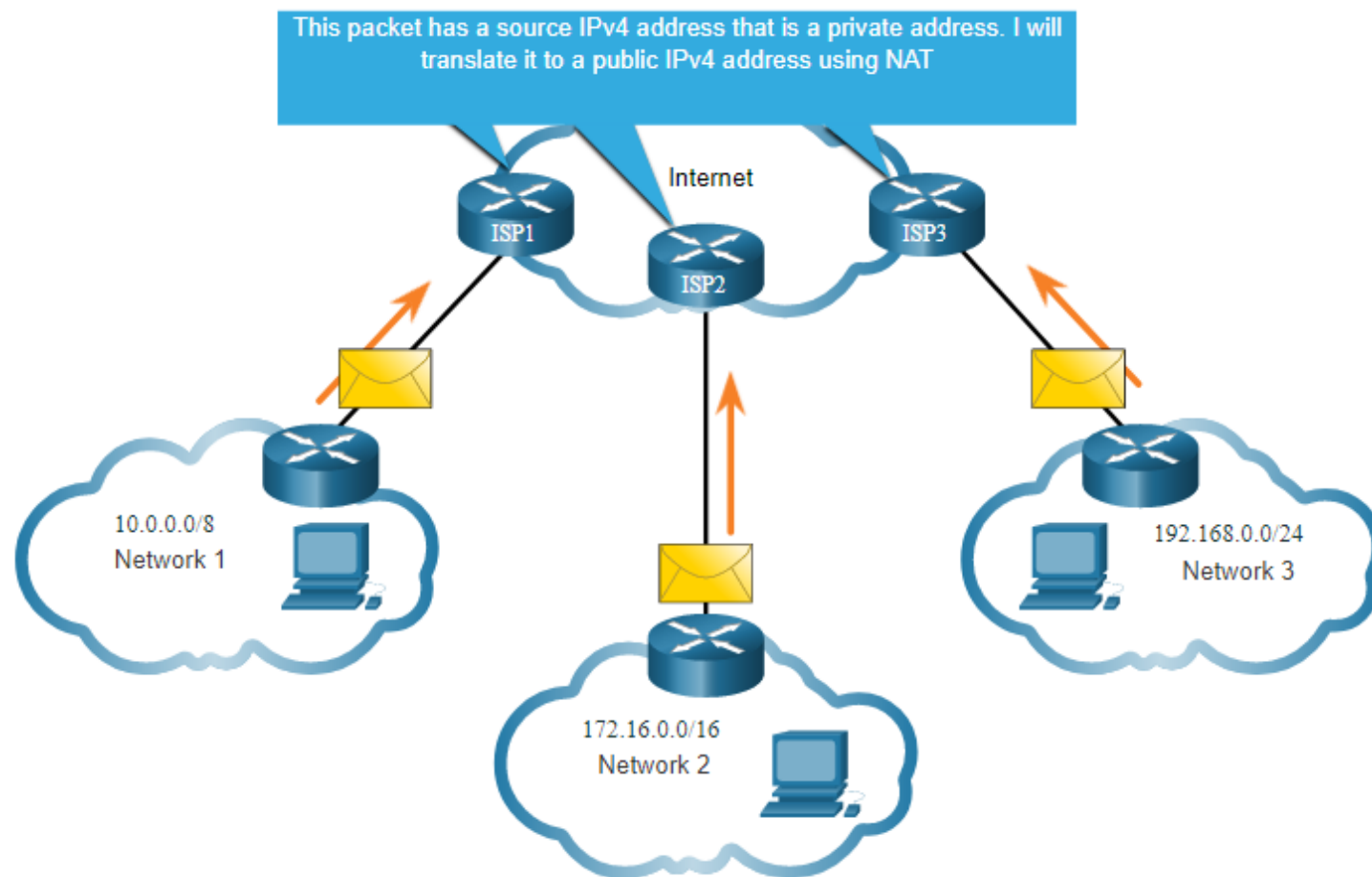
Conforme definido na RFC 1918, os endereços IPv4 públicos são roteados globalmente entre os roteadores do provedor de serviços de Internet (ISP).

- Endereços privados são blocos comuns de endereços usados pela maioria das organizações para atribuir endereços IPv4 a hosts internos.
- Os endereços IPv4 privados não são exclusivos e podem ser usados internamente em qualquer rede.
- No entanto, os endereços privados não são globalmente roteáveis.

Endereço de rede e prefixo	RFC 1918 Intervalo de endereços privados
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

ROTEAMENTO PARA A INTERNET

- A conversão de endereços de rede (NAT) converte endereços IPv4 privados em endereços IPv4 públicos.
- Normalmente, o NAT é habilitado no roteador de borda que se conecta à Internet.
- Ele converte o endereço privado interno em um endereço IP global público.



ESTRUTURA DE ENDEREÇO IPV6



IPv6

Necessidade de IPv6

1. A redução do espaço do endereço IPv4 era o fator de motivação para migrar para IPv6.
2. Na segunda-feira, 31 de janeiro de 2011, a IANA atribuiu os últimos dois blocos de /8 um endereço IPv4 para os registros regionais (RIRs) da Internet.
3. Os endereços privados RFC 1918 em combinação com a Network Address Translation (NAT) foi imprescindível para retardar a redução do espaço de endereços IPv4. A NAT tem limitações que impedem a comunicação ponto-a-ponto.

IPV6

- 1.O IPv6 é projetado para ser o sucessor do IPv4.
- 2.O IPv6 tem um maior espaço de endereços de 128 bits, fornecendo 340 endereços de undecilhão. (O número 340, seguido de 36 zeros.)
- 3.O IPv6 usou essa oportunidade de corrigir as limitações de IPv4 e incluir aprimoramentos adicionais.
- 4.Um exemplo é a versão 6 do Internet Control Message Protocol (ICMPv6), incluindo a resolução de endereço e a configuração automática de endereços não encontradas no ICMP para IPv4 (ICMPv4).

IPv6

Necessidade de IPv6

1. A redução do espaço do endereço IPv4 era o fator de motivação para migrar para IPv6.
2. Na segunda-feira, 31 de janeiro de 2011, a IANA atribuiu os últimos dois blocos de /8 um endereço IPv4 para os registros regionais (RIRs) da Internet.
3. Os endereços privados RFC 1918 em combinação com a Network Address Translation (NAT) foi imprescindível para retardar a redução do espaço de endereços IPv4. A NAT tem limitações que impedem a comunicação ponto-a-ponto.

IPv6

Nome do número	Notação científica	Número de zeros
1 mil	10^3	1.000
1 milhão	10^6	1.000.000
1 bilhões	10^9	1,000,000,000
1 trilhão	10^{12}	1,000,000,000,000
1 Quadrilhão	10^{15}	1,000,000,000,000,000
1 Quintilhão	10^{18}	1,000,000,000,000,000,000
1 Sextilhão	10^{21}	1,000,000,000,000,000,000,000
1 setilhão	10^{24}	1,000,000,000,000,000,000,000,000
1 octilhão	10^{27}	1,000,000,000,000,000,000,000,000,000
1 nonilhão	10^{30}	1,000,000,000,000,000,000,000,000,000,000
1 decilhão	10^{33}	1,000,000,000,000,000,000,000,000,000,000,000
1 undecilhão	10^{36}	1,000,000,000,000,000,000,000,000,000,000,000,000

Legenda



Há 4 bilhões de endereços IPv4



Há 340 undecilhões de endereços IPv6

IPV6

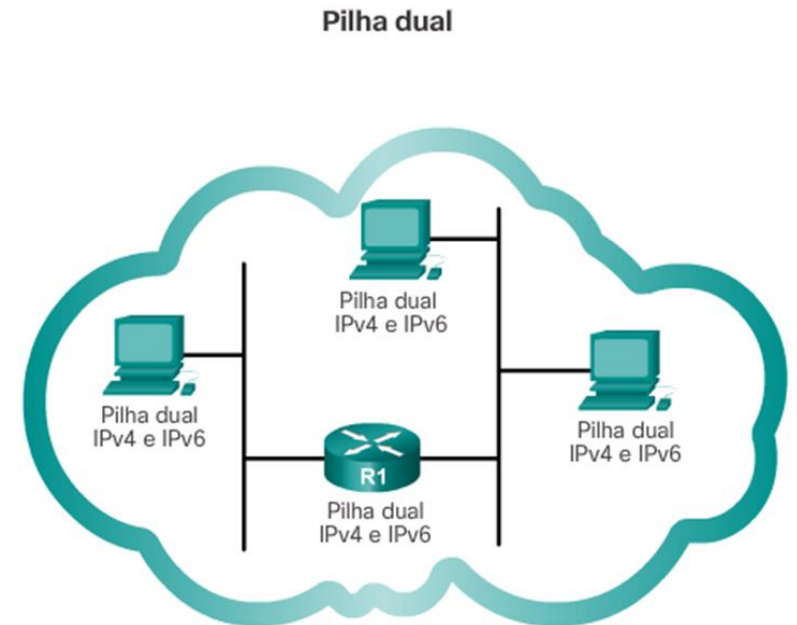
Coexistência de IPv4 e IPv6

O IETF criou vários protocolos e ferramentas para ajudar os administradores de rede a migrar as redes para IPv6.

As técnicas de migração podem ser divididas em três categorias:

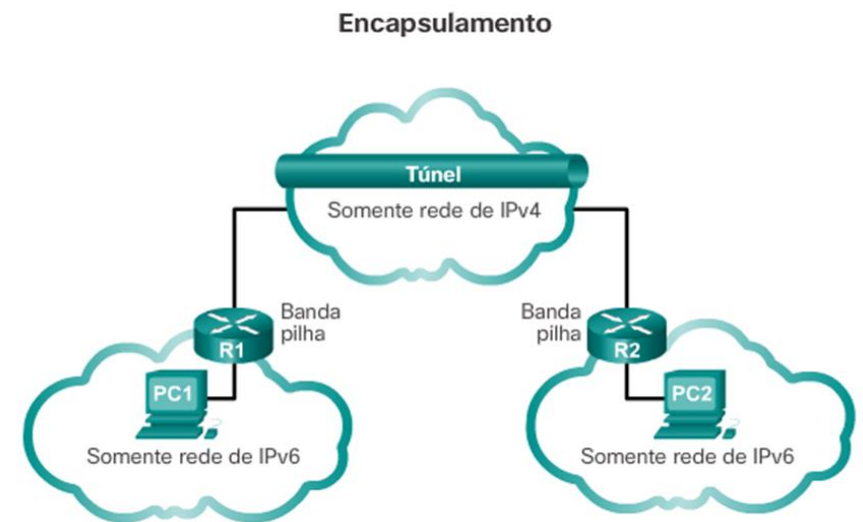
IPv6

Pilha dupla – Como mostrado na figura, a pilha dupla permite que o IPv4 e IPv6 coexistam na mesma rede. Os dispositivos de pilha dupla executam o protocolo IPv4 e o IPv6 simultaneamente.



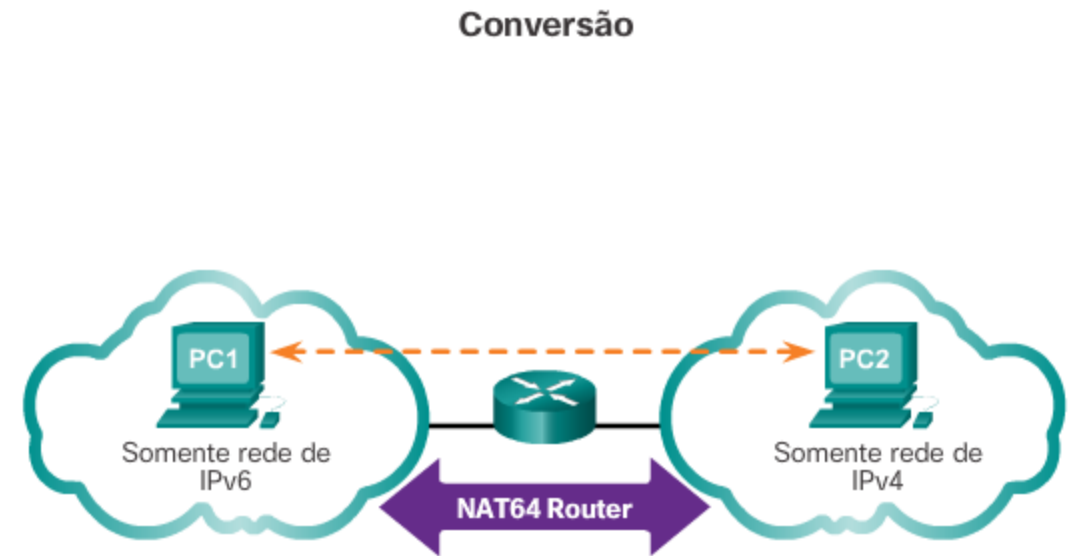
IPV6

Encapsulamento – Como mostrado na figura 2, o encapsulamento é um método de transportar um pacote de IPv6 em uma rede IPv4. O pacote IPv6 é encapsulado dentro de um pacote IPv4, semelhante a outros tipos de dados.



CONVERSÃO

Conversão – Como mostrado na figura, a Network Address Translation 64 (NAT64) permite que dispositivos com IPv6 ativo se comuniquem com dispositivos com IPv4 ativo usando uma técnica de conversão semelhante à NAT para IPv4. Um pacote IPv6 é traduzido em um pacote IPv4, e vice-versa.



CONVERSÃO

Pilha dupla

IPv4

Encapsulamento

IPv6

Conversão

Período

Descrição

Endereço de 128 bits/endereços de 340 undecilhões.

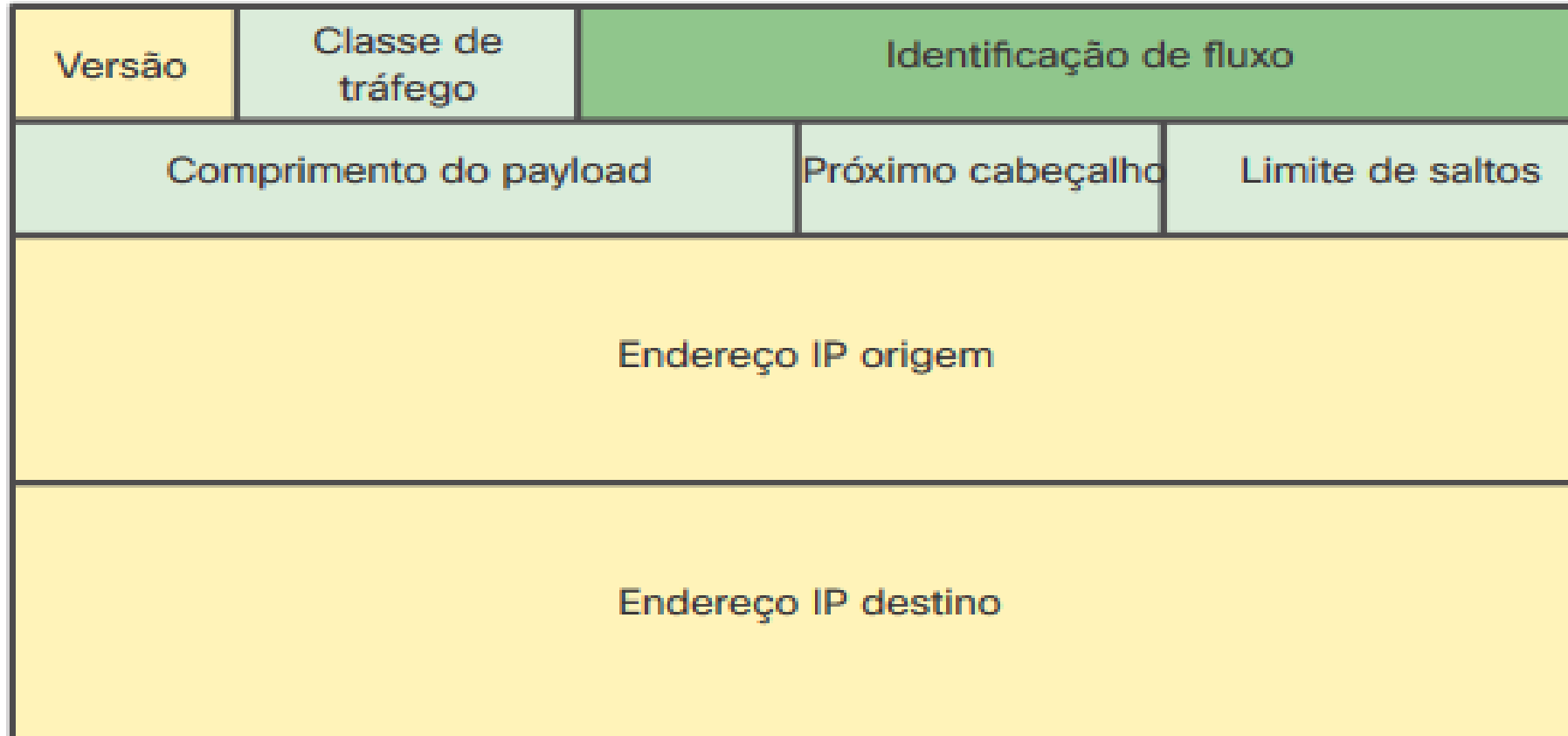
Endereço de 32 bits/endereços de 4,3 bilhões.

Transmite um pacote de IPv6 nas redes IPv4.




Permite que o NAT seja usado em redes IPv6 e IPv4.

Permite que o IPv4 e IPv6 coexistam na mesma rede.

Cabeçalho IPv6



Legenda

-  - Nomes de campo mantidos de IPv4 para IPv6
-  - Nome e posição alterados no IPv6
-  - Novo campo no IPv6

CABEÇALHO

- 1. Versão** - Esse campo contém um valor binário de 4 bits que identifica a versão do pacote IP. Em pacotes IPv6, esse campo é sempre definido como 0110.
- 2. Classe de tráfego** - Esse campo de 8 bits é equivalente ao campo Serviços Diferenciados (DS) do IPv4. Ele também contém um valor diferenciado de 6 bits do valor do Differentiated Services Code Point (DSCP) usado para classificar pacotes e um Explicit Congestion Notification (ECN) de 2 bits usado para controle de congestionamento de tráfego.
- 3. Identificação de fluxo** - Esse campo de 20 bits fornece um serviço especial para aplicações em tempo real. Ele pode ser usado para informar roteadores e switches para manter o mesmo caminho para o fluxo de pacotes de modo que os pacotes não sejam reordenados.

CABEÇALHO

4. Comprimento da payload - Esse campo de 16 bits é equivalente ao campo Comprimento total no cabeçalho IPv4. Ele define o tamanho total do pacote (fragmento), incluindo cabeçalho e extensões opcionais.

5. Próximo cabeçalho - Esse campo de 8 bits é equivalente ao campo do protocolo IPv4. Ele exibe o tipo de payload de dados que o pacote está carregando, permitindo que a camada de rede passe os dados para o protocolo apropriado das camadas superiores. Esse campo também é usado se houver cabeçalhos de extensão opcionais adicionados ao pacotes IPv6.

REPRESENTAÇÃO DO ENDEREÇO IPV6

Representação

1. Os endereços IPv6 têm 128 bits de comprimento e são escritos como uma sequência de valores hexadecimais.
2. Cada 4 bits são representados por um único dígito hexadecimal; para um total de 32 valores hexadecimais.
3. Os endereços IPv6 não diferenciam maiúsculas e minúsculas e podem ser escritos em minúsculas ou em maiúsculas.

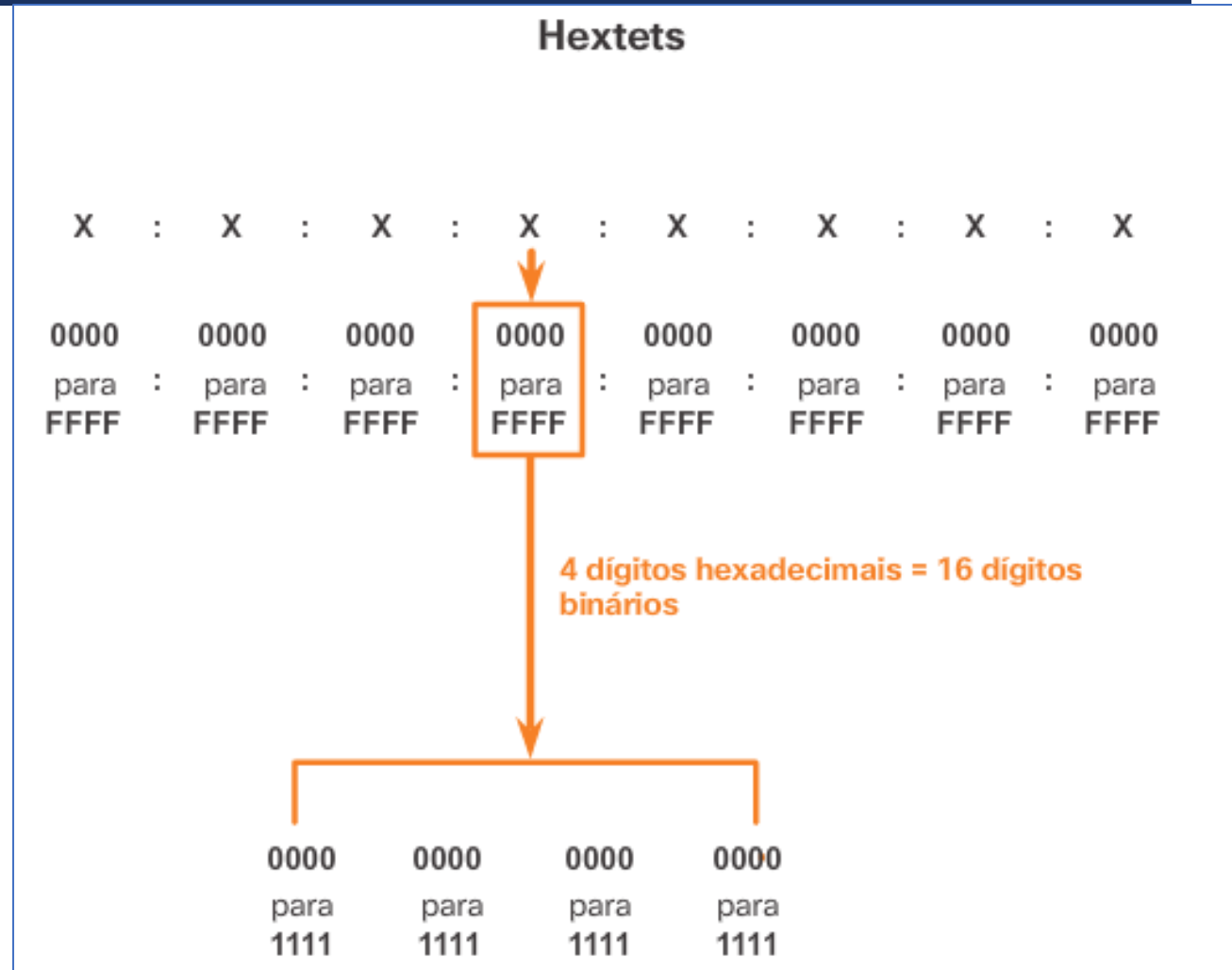
Por exemplo:

- 2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1
- 8 grupos de 4 caracteres em hexadecimal

FORMATO REFERÊNCIA

O formato de preferência para gravar um endereço IPv6 é x:x:x:x:x:x:x:x, com cada “x” que consiste em quatro valores hexadecimais.

Por exemplo, o endereço **2001:0DB8:0000:0000:130F:0000:0000:140B** pode ser escrito como **2001:DB8:0:0:130F::140B** ou **2001:DB8::130F:0:0:140B**



ABREVIANDO

A primeira regra para ajudar a reduzir a notação de endereços IPv6 é 0s principal (zero) em qualquer seção de 16 bits ou o hextet pode ser omitido. Por exemplo:

- 01AB pode ser representado como 1AB
- 09F0 pode ser representado como 9F0
- 0A00 pode ser representado como A00
- 00AB pode ser representado como AB

Essa regra se aplica somente a 0s da frente, NÃO 0s de trás, se não o endereço seria ambíguo. Por exemplo, o hextet “ABC” poderia ser “0ABC” ou “ABC0”.

A figura mostram um exemplo de como omitir os 0s da frente ou podem ser usados para reduzir o tamanho de um endereço IPv6.

Regra 1 – Omitindo o 0s condutor

Preferência de	2001:0DB8:0000:1111:0000:0000:0000:0200
Nenhum 0 à esquerda	2001: DB8: 0:1111: 0: 0: 0: 200

ABREVIANDO

A segunda regra para ajudar a reduzir a notação de endereços IPv6 é que os dois pontos em dobro (::) podem substituir uma única, sequência contígua de um ou mais segmentos de 16 bits (hextets) que consistem em 0s.

Os dois pontos em dobro (::) podem ser usados apenas uma vez em um endereço, se não houvesse mais do que um endereço resultante possível. Quando usado com a técnica de omissão dos 0s na frente, a notação de endereço IPv6 pode normalmente ser bastante reduzido. Isso é comumente conhecido como o formato compactado. endereço incorreto:

- 2001:0DB8::ABCD::1234

Expansões possíveis de endereços ambíguos compactados:

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

A figura mostra um exemplo de como utilizar os dois pontos em dobro (::) e omitir 0s na frente pode reduzir o tamanho de um endereço IPv6.

Regra 2 – Omissão de os segmentos 0

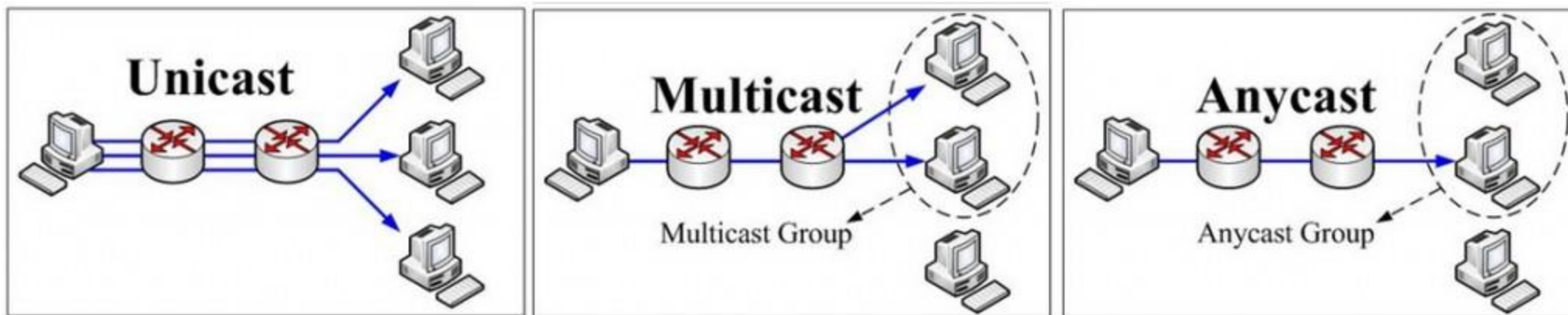
Preferência de	2001:0DB8:0000:1111:0000:0000:0000:0200
Nenhum 0 à esquerda	2001: DB8: 0:1111: 0: 0: 0: 200
Compactado	2001:DB8:0:1111::200

TIPOS DE ENDERENÇO

■ Tipos de Endereços

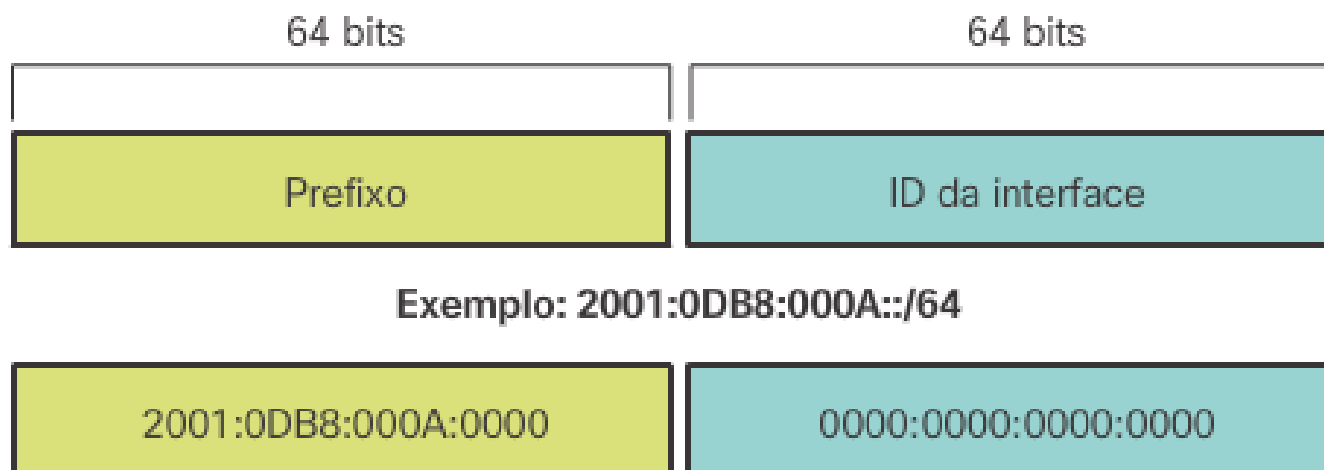
■ Existem no IPv6 três tipos de endereços definidos:

1. **Unicast** – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço unicast é entregue a uma única interface;
2. **Anycast** – identifica um conjunto de interfaces. Um pacote encaminhado a um endereço anycast é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço anycast é utilizado em comunicações de um-para-um-de-muitos.
3. **Multicast** – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço multicast é entregue a todas as interfaces associadas a esse endereço. Um endereço multicast é utilizado em comunicações de um-para-muitos.

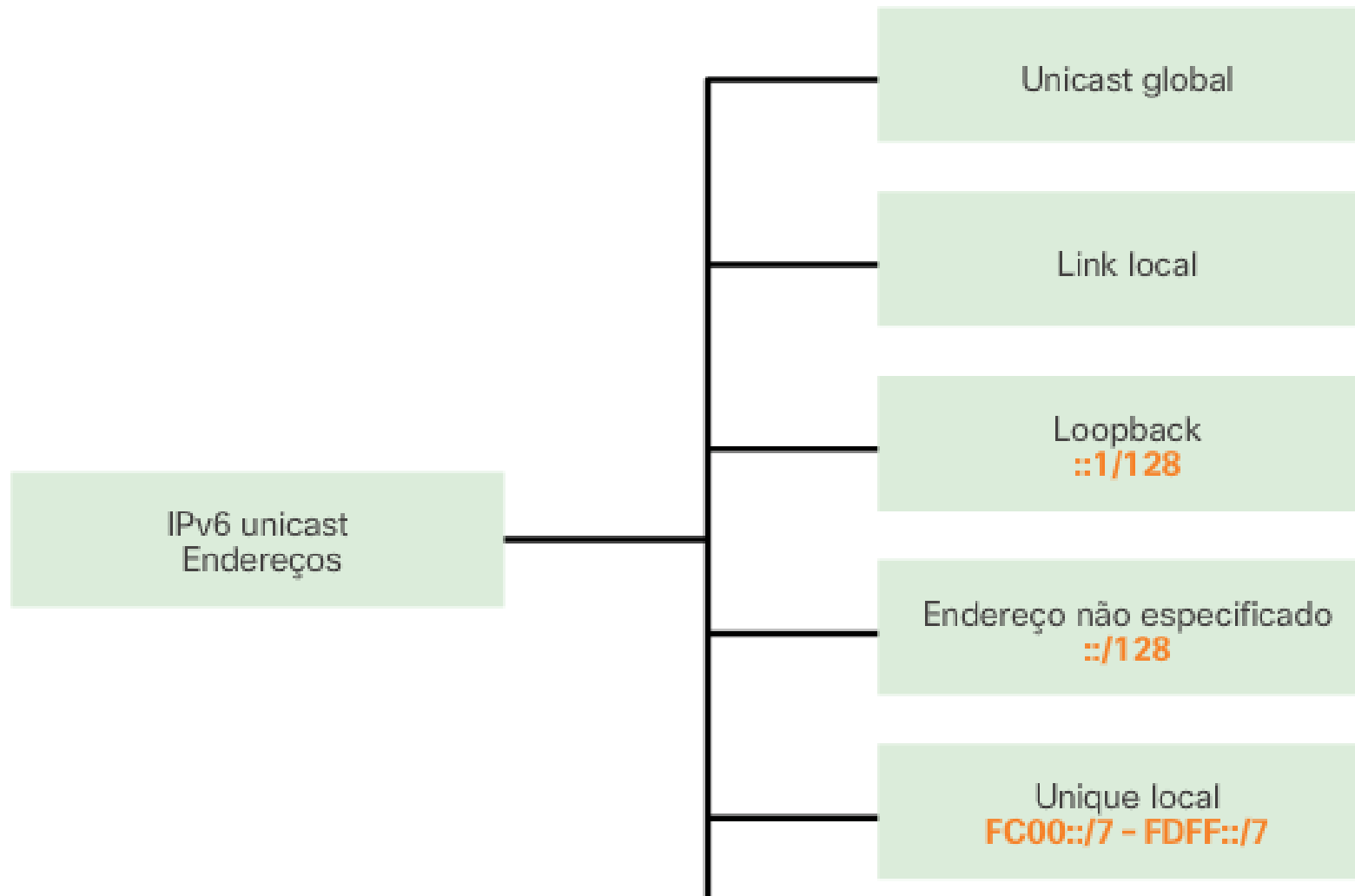


COMPRIMENTO DO PREFIXO IPV6

- ❑ Lembre-se de que o prefixo, ou porção de rede, de um endereço IPv4 pode ser identificado pela máscara de sub-rede decimal com ponto ou pelo tamanho do prefixo (notação de barra). Por exemplo, o endereço IP de 192.168.1.10 com máscara de sub-rede decimal com ponto 255.255.255.0 é equivalente a 192.168.1.10/24.
- ❑ O IPv6 usa o comprimento do prefixo para representar a porção de prefixo do endereço. O IPv6 não usa a notação de máscara de sub-rede decimal com ponto. O comprimento do prefixo é usado para indicar a porção de rede de um endereço IPv6 usando o endereço IPv6/tamanho do prefixo.
- ❑ O tamanho do prefixo pode variar de 0 a 128. Um tamanho típico de prefixo IPv6 de LANs e a maioria dos outros tipos de redes é /64. Isso significa que porção de prefixo ou de rede do endereço é de 64 bits, deixando outros 64 bits para o ID da interface (porção de host) do endereço.



ENDEREÇOS UNICAST IPV6



ENDEREÇOS UNICAST IPV6

Unicast global

Um endereço global unicast é semelhante a um endereço IPv4 público. Eles são endereços roteáveis da Internet globalmente únicos. Os endereços globais unicast podem ser configurados estaticamente ou atribuídos de forma dinâmica. Há algumas diferenças importantes em como um dispositivo recebe o endereço IPv6 dinamicamente em comparação ao DHCP do IPv4.

Link local

Os endereços locais de conexão são usados para a comunicação com outros dispositivos na mesma conexão local. Com o IPv6, o link do termo se refere a uma sub-rede. Os endereços locais de conexão são limitados a uma única conexão. A exclusividade só deve ser confirmada nessa conexão porque não são roteáveis além da conexão. Em outras palavras, os roteadores não encaminham pacotes com um endereço origem ou destino de conexão local.

Loopback

O endereço de loopback é usado por um host para enviar um pacote para ele mesmo e não pode ser atribuído a uma interface física. Semelhante a um endereço de loopback IPv4, você pode fazer ping em um endereço de loopback IPv6 para testar a configuração do TCP/IP no host local. O endereço de loopback IPv6 é tudo 0 com exceção do último bit, representados como ::1/128 ou apenas ::1 em formato compactado.

ENDEREÇOS UNICAST IPV6

Endereço não especificado

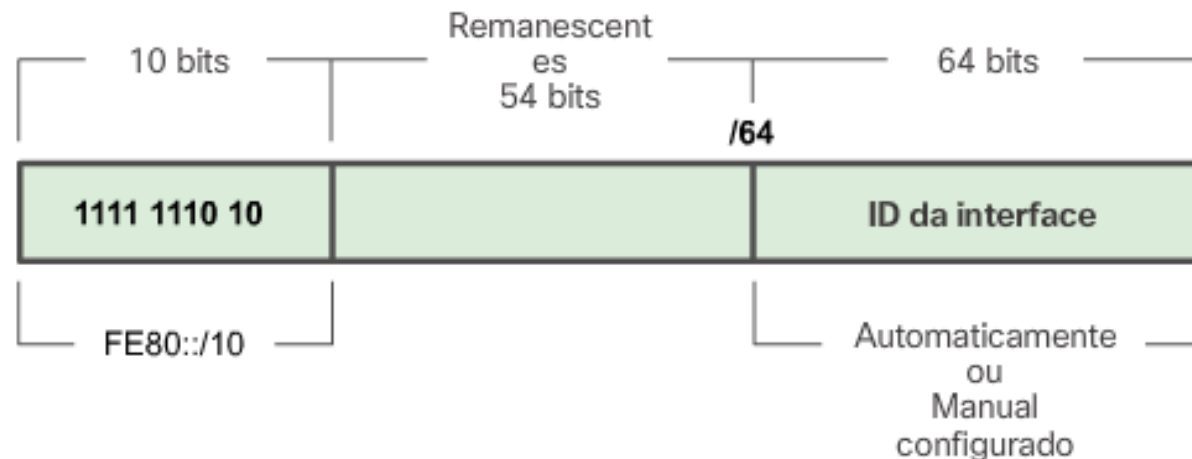
Um endereço não especificado é um endereço de all-0s representado em formato compactado como `::/128` ou apenas `::` em formato compactado. Ele não pode ser atribuído a uma interface e só pode ser usado como um endereço origem em um pacote IPv6. Um endereço não especificado será usado como o endereço origem quando o dispositivo ainda não possuir um endereço permanente IPv6 ou quando a origem do pacote for irrelevante ao destino.

Unique local

Os endereços unique local de IPv6 têm alguma similaridade com os endereços privados RFC 1918 de IPv4, mas há diferenças significativas também. Os endereços unique local são utilizados para endereçamento local dentro de um local ou entre um número limitado de unidades. Esses endereços não devem ser roteáveis no IPv6 global. Os endereços unique local estão no intervalo de `FC00::/7` a `FDFF::/7`.

ENDEREÇOS UNICAST LOCAIS DE CONEXÃO IPV6 (LINK-LOCAL)

- ❑ Um endereço de link local IPv6 permite que um dispositivo se comunique com outros dispositivos habilitados com IPv6 no mesmo link e somente nesse link (sub-rede). Os pacotes com um endereço de link local de origem ou de destino não podem ser roteados além do link de onde o seu pacote se originou.
- ❑ Diferentemente dos endereços locais de conexão IPv4, os endereços locais de conexão IPv6 têm um papel fundamental em vários aspectos de rede. O endereço global unicast não é obrigatório; entretanto, cada interface de rede habilitada com IPv6 é necessária para ter um endereço local de conexão.
- ❑ Se um endereço local de conexão não estiver configurado manualmente a uma interface, o dispositivo criará automaticamente o seu próprio sem se comunicar com um servidor DHCP. Os hosts habilitados com IPv6 criam um endereço local de conexão IPv6 mesmo se o dispositivo não tiver sido atribuído a um endereço global IPv6 unicast. Isso permite que os dispositivos habilitados com IPv6 se comuniquem com outros dispositivos habilitados com IPv6 na mesma sub-rede. Isso inclui a comunicação com o gateway padrão (roteador).
- ❑ Os endereços de link local IPv6 estão no intervalo FE80::/10. O /10 indica que os primeiros 10 bits são 1111 1110 10xx xxxx. O primeiro hexetec tem um intervalo de 1111 1110 1000 0000 (FE80) a 1111 1110 1011 1111 (FEBF).



Endereço IPv6 exclusivo roteável pela Internet (dinâmico ou estático)

Endereço IPv6 representado como:: 1 (formato compactado)

Endereço IPv6 representado como:: (formato compactado) - não pode ser atribuído a uma interface

Prefixo IPv6 típico usado para indicar a porção de rede do endereço

Usado para se comunicar com outros dispositivos na mesma sub-rede IPv6

/64

Link local

Unicast global

Não especificado

Loopback

ESTRUTURA DE UM ENDEREÇO GLOBAL UNICAST IPV6

O endereço global unicast IPv6 é globalmente exclusivo e roteável na Internet IPv6. Esses endereços são equivalentes aos endereços públicos de IPv4. O Internet Committee for Assigned Names and Numbers (ICANN), o operador de Internet Assigned Numbers Authority (IANA), aloca os blocos de endereço IPv6 para os cinco RIRs. Atualmente, somente endereços globais unicast com os primeiros três bits de 001 ou 2000::

Observação: o endereço 2001:0DB8::

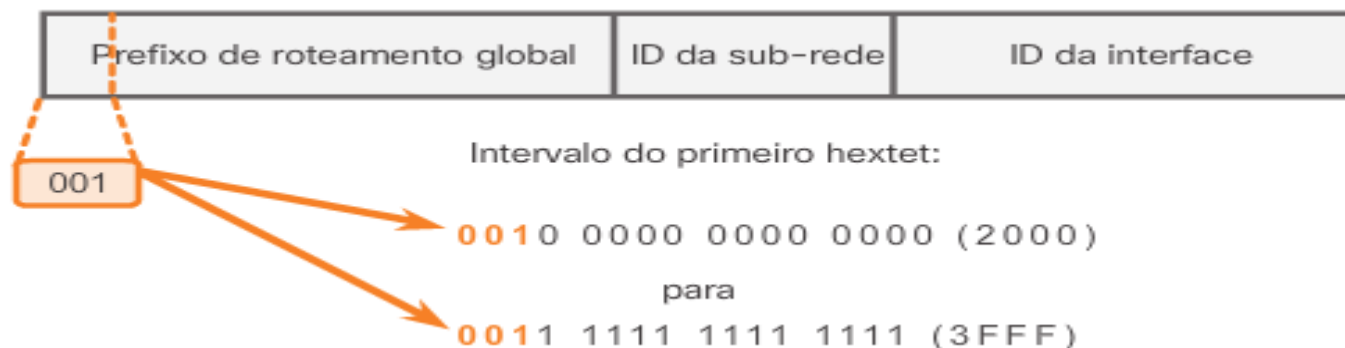
A figura mostra a estrutura e o alcance de um endereço global unicast.

Um endereço unicast global tem três partes:

- Prefixo de roteamento global
- ID da sub-rede
- ID da interface

Prefixo de roteamento global

O prefixo global de roteamento é porção do endereço do prefixo, ou da rede, atribuída pelo provedor, como um ISP, a um cliente ou para um local. Atualmente, RIRs atribuem um prefixo global de roteamento /48 a clientes. Isso inclui todas as redes corporativas da empresa para residências individuais. Isso é mais do que o espaço de endereço suficiente para a maioria dos clientes.



ESTRUTURA DE UM ENDEREÇO GLOBAL UNICAST IPV6

A Figura mostra a estrutura de um endereço unicast global usando um prefixo global de roteamento de /48. Os prefixos de /48 são o roteamento global mais comum atribuídos e serão usados na maioria dos casos ao longo deste curso.

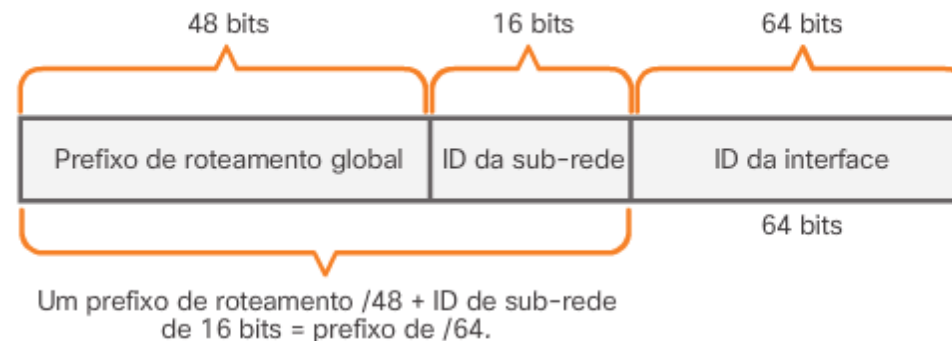
Por exemplo, o endereço IPv6 2001:0DB8:ACAD::/48 têm um prefixo que indica que os primeiros 48 bits (3 hextets) (2001:0DB8:ACAD) são a porção de prefixo ou de rede do endereço. Os dois pontos duplos (::) antes do tamanho do prefixo de /48 significa que o restante do endereço contém todos os 0s.

ID da sub-rede

O ID da sub-rede é usado por uma organização para identificar sub-redes dentro da sua localização.

ID da interface

O ID da interface IPv6 é equivalente à porção de host de um endereço IPv4. O ID de interface do termo é usado porque um único host pode ter várias interfaces, cada um com um ou mais endereços IPv6.



ENDEREÇOS MULTICAST

Os endereços multicast não devem ser utilizados como endereço de origem de um pacote. Esses endereços derivam do bloco **FF00::/8**, onde o prefixo **FF**, que identifica um endereço multicast, é precedido por quatro bits, que representam quatro flags, e um valor de quatro bits que define o escopo do grupo multicast. Os 112 bits restantes são utilizados para identificar o grupo multicast.

As flags são definidas da seguinte forma:

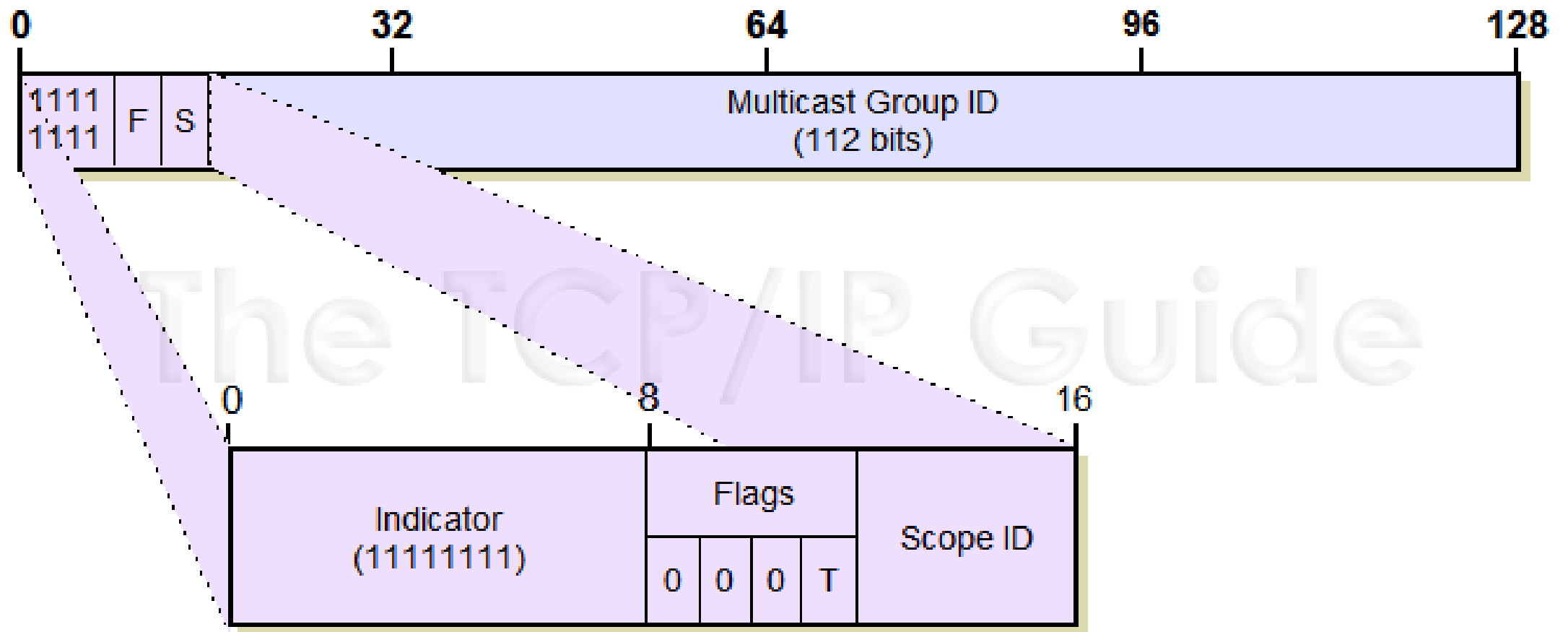
1. O primeiro bit mais a esquerda é reservado e deve ser marcado com 0;
2. **Flag R:** Se o valor for 1, indica que o endereço multicast “carrega” o endereço de um Ponto de Encontro (Rendezvous Point). Se o valor for 0, indica que não há um endereço de Ponto de Encontro embutido;
3. **Flag P:** Se o valor for 1, indica que o endereço multicast é baseado em um prefixo de rede. Se o valor for 0, indica que o endereço não é baseado em um prefixo de rede;
4. **Flag T:** Se o valor for 0, indica que o endereço multicast é permanente, ou seja, é atribuído pela IANA. Se o valor for 1, indica que o endereço multicast não é permanente, ou seja, é atribuído dinamicamente.

ENDEREÇOS MULTICAST

Os **quatro bits** que representam o escopo do endereço multicast, são utilizados para delimitar a área de abrangência de um grupo multicast. Os valores atribuídos a esse campo são o seguinte:

- a) 1 - abrange apenas a interface local;
- b) 2 - abrange os nós de um enlace;
- c) 3 - abrange os nós de uma sub-rede
- d) 4 - abrange a menor área que pode ser configurada manualmente;
- e) 5 - abrange os nós de um site;
- f) 8 - abrange vários sites de uma mesma organização;
- g) E - abrange toda a Internet;
- h) 0, F - reservados;
- i) 6, 7, 9, A, B, C, D - não estão alocados.

ENDEREÇOS MULTICAST

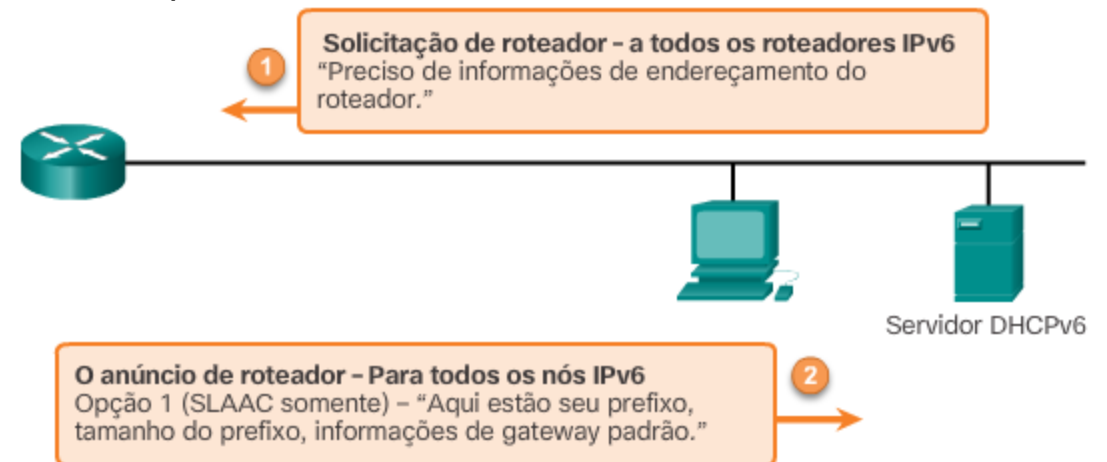


CONFIGURAÇÃO DINÂMICA DE UM ENDEREÇO UNICAST GLOBAL USANDO SLAAC

- ❑ Configuração automática do endereço de vida curta (SLAAC) é um método que permite que um dispositivo obtenha o prefixo, tamanho do prefixo, e informações do endereço do gateway padrão de um roteador IPv6 sem o uso de um servidores DHCPv6. Usando a SLAAC, os dispositivos dependem do Anúncio do roteador (RA) ICMPv6 do roteador local para obter as informações necessárias.
- ❑ Os roteadores IPv6 enviam periodicamente mensagens do Anúncio de roteador (RA) ICMPv6 a todos os dispositivos de habilitados com IPv6 na rede. Por padrão, os roteadores Cisco têm mensagens de RA enviadas a cada 200 segundos para o endereço do grupo de multicast de todos os nós IPv6. Um dispositivo IPv6 na rede não tem de esperar por essas mensagens periódicas do RA. Um dispositivo pode enviar uma mensagem de Solicitação de roteador (RS) para o roteador, usando o endereço de grupo de multicast de todos os roteadores IPv6. Quando um roteador IPv6 receber uma mensagem de RS, ele imediatamente responderá com um anúncio de roteador.
- ❑ Mesmo que uma interface em um roteador Cisco possa ser configurada com um endereço IPv6, isso não os torna “roteador IPv6”. Um roteador IPv6 é um roteador que:
 - Encaminha pacotes IPv6 entre redes
 - Pode ser configurado com rotas estáticas IPv6 ou um protocolo de roteamento dinâmico IPv6
 - Envia mensagens de RA ICMPv6
- ❑ O roteamento IPv6 não é ativado por padrão. Para permitir que um roteador como o roteador IPv6, o comando da configuração global **ipv6 unicast-routing** deve ser usado.

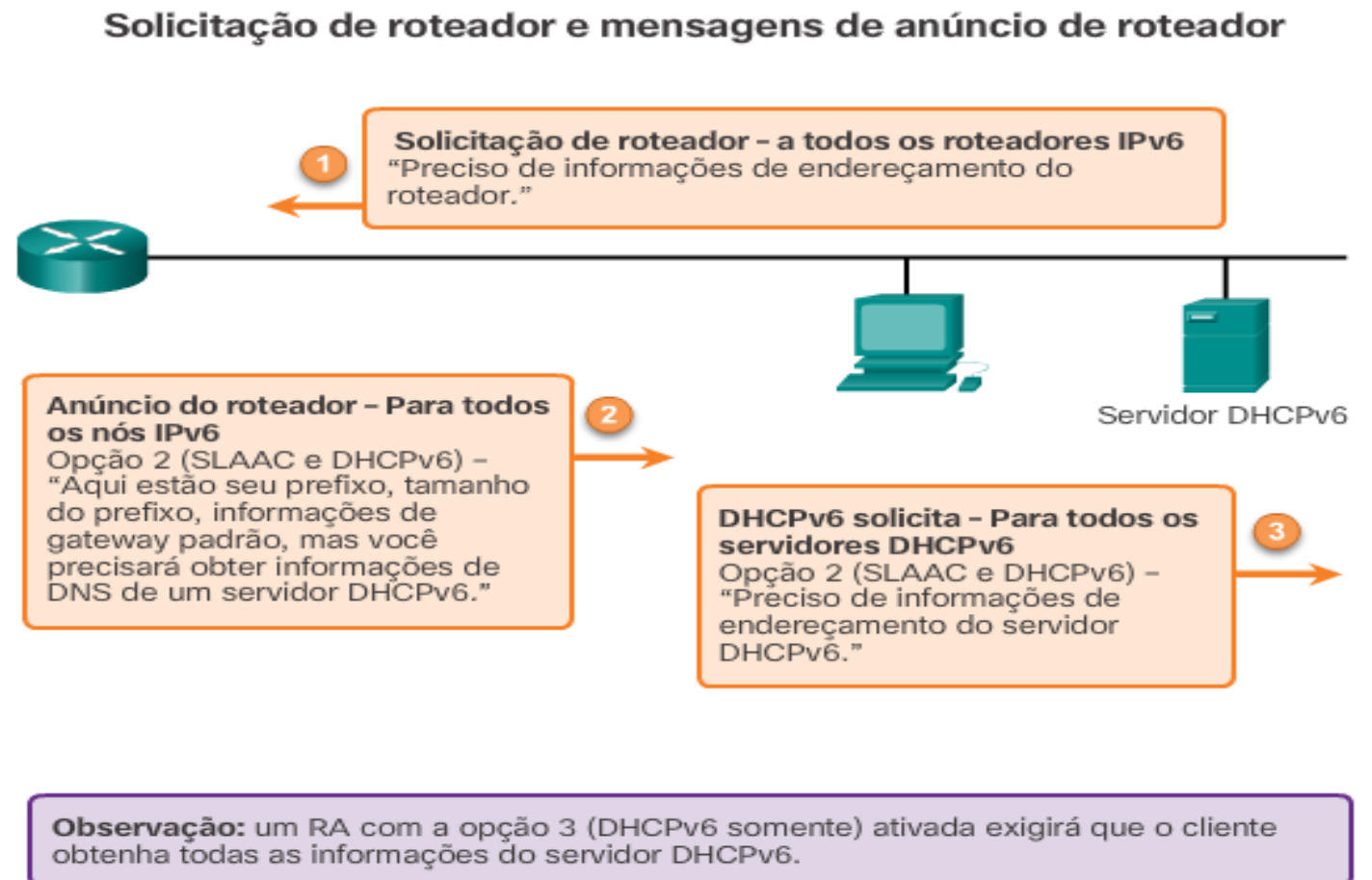
CONFIGURAÇÃO DINÂMICA DE UM ENDEREÇO UNICAST GLOBAL USANDO SLAAC

- ❑ **Opção 1 – SLAAC apenas** – O dispositivo deve usar o prefixo, o tamanho do prefixo e as informações de endereço de gateway padrão contidas na mensagem do RA. Nenhuma outra informação está disponível em um servidor DHCPv6.
- ❑ **Opção 2 – SLAAC e DHCPv6** – O dispositivo deve usar o prefixo, o tamanho do prefixo e as informações de endereço de gateway padrão contidas na mensagem do RA. Há outras informações disponíveis de um servidor DHCPv6 como o endereço de servidor DNS. O dispositivo, com o processo normal de descobrir e de consultar um servidor DHCPv6 obtém essas informações adicionais. Isso é conhecido como DHCPv6 sem estado porque o servidor DHCPv6 não precisa atribuir ou acompanhar qualquer atribuições de endereço IPv6, mas só fornece informações adicionais como endereço de servidor DNS.
- ❑ **Opção 3 – DHCPv6 apenas** – O dispositivo não deve usar informações nessa mensagem do RA para suas informações de endereçamento. Em vez de isso, o dispositivo usará o processo normal de descobrir e de fazer um servidor DHCPv6 para obter todas as suas informações de endereçamento. Isso inclui um endereço global unicast IPv6, o tamanho do prefixo, um endereço de gateway padrão e os endereços dos servidores DNS. Nesse caso, o servidor DHCPv6 está atuando como um servidor DHCP dinâmico semelhante ao DHCP para IPv4. O servidor DHCPv6 atribui e rastreia endereços de IPv6 para que não atribuam o mesmo endereço IPv6 a vários dispositivos.



CONFIGURAÇÃO DINÂMICA DE UM ENDEREÇO UNICAST GLOBAL USANDO DHCPV6

- ❑ O Protocolo de Configuração de Host Dinâmico para IPv6 (DHCPv6) é semelhante ao DHCP para IPv4. Um dispositivo pode receber automaticamente as informações de endereçamento que inclui um endereço global unicast, o tamanho do prefixo, o endereço de gateway padrão e os endereços dos servidores DNS que usam os serviços de um servidor DHCPv6.
- ❑ Um dispositivo pode receber todas ou algumas de suas informações de endereçamento IPv6 de um servidor DHCPv6 dependendo se a opção 2 (SLAAC e DHCPv6) ou a opção 3 (DHCPv6 apenas) for especificada na mensagem do RA ICMPv6



PROCESSO EUI-64 OU GERADO ALEATORIAMENTE

O IEEE definiu o identificador exclusivo estendido (EUI) ou modificou o processo EUI-64. Esse processo usa o endereço MAC Ethernet de 48 bits de um cliente e insere outros 16 bits no meio do endereço MAC de 48 bits para criar um ID de interface de 64 bits.

Os endereços MAC Ethernet geralmente são representados em hexadecimal e compõe-se de duas partes:

- **Organizationally unique identifier (OUI)** – O OUI é um código de fornecedor de 24 bits (6 dígitos hexadecimais) designado pelo IEEE.
- **Identificador de dispositivo** – O identificador do dispositivo é um valor exclusivo de 24 bits (6 dígitos hexadecimais) com um OUI em comum.

Um ID de interface EUI-64 é representado em binário e composto por três partes:

- OUI de 24 bits do endereço MAC do cliente, mas o sétimo bit (o bit universal/local (U/L) bits) é revertido. Isso significa que se o sétimo bit for um 0, ele se torna 1, e vice-versa.
- O valor de 16 bits inserido FFFE (em hexadecimal)
- Identificador do dispositivo de 24 bits do endereço MAC do cliente

CONFIGURAÇÃO DINÂMICA DE UM ENDEREÇO UNICAST GLOBAL USANDO DHCPV6

O processo EUI-64 é ilustrado na figura do próximo slide, usando o endereço MAC de RI GigabitEthernet de FC99:4775:CEE0.

Etapa 1: Divida o endereço MAC entre o OUI e o identificador do dispositivo.

Etapa 2: Insira o valor hexadecimal FFFE, o qual em binário: 1111 1111 1111 1110.

Etapa 3: Converta os primeiros 2 valores hexadecimais do OUI em binário e inicie o bit de U/L (7 bits). Neste exemplo o 0 em 7 bits é alterado para 1. O resultado é um ID de interface gerado do EUI-64 de FE99:47FF:FE75:CEE0.

IDs de interface geradas aleatoriamente

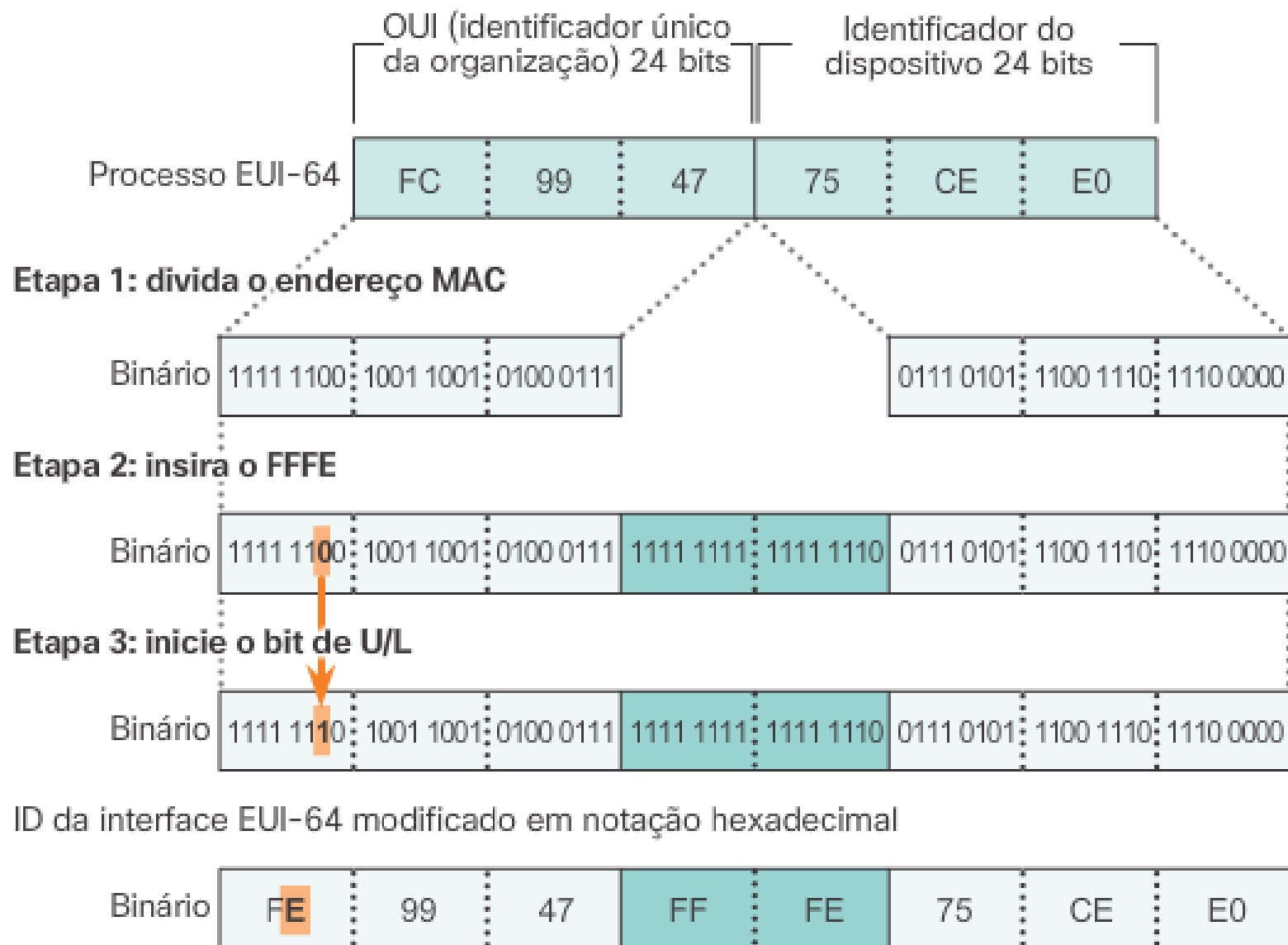
Dependendo do sistema operacional, um dispositivo pode usar um ID de interface gerado de forma aleatória em vez de usar o endereço MAC e o processo EUI-64. Por exemplo, começando com o Windows Vista, o Windows usa um ID de interface gerado de forma aleatória em vez de um criado com o EUI-64. Windows XP e sistemas operacionais com Windows anteriores usaram EUI-64.

Uma maneira fácil de identificar que um endereço foi criado usando EUI-64 é o FFFE localizado no meio do ID de interface, como mostrado na figura 2. Depois que a ID da interface for estabelecida, com o processo EUI-64 ou através da criação aleatória, ela poderá ser combinada com um prefixo IPv6 para criar um endereço global unicast ou um endereço local de conexão:

- **Endereço global unicast** – Ao usar SLAAC, o dispositivo recebe o prefixo do RA ICMPv6 e o combina com o ID da interface
- **Endereço local de conexão** – Um prefixo local de conexão começa com o FE80::/10. Um dispositivo usa normalmente FE80::/64 como o prefixo/comprimento, seguido pelo ID da interface.

PROCESSO EIU-64

Processo EUI-64



IPv6

Necessidade de IPv6

1. A redução do espaço do endereço IPv4 era o fator de motivação para migrar para IPv6.
2. Na segunda-feira, 31 de janeiro de 2011, a IANA atribuiu os últimos dois blocos de /8 um endereço IPv4 para os registros regionais (RIRs) da Internet.
3. Os endereços privados RFC 1918 em combinação com a Network Address Translation (NAT) foi imprescindível para retardar a redução do espaço de endereços IPv4. A NAT tem limitações que impedem a comunicação ponto-a-ponto.

ABREVIANDO O IPV6

- Otimizar os zeros a esquerda quando estamos escrevemos endereços.
 - Um endereço abreviado:
 - 2001:BAA:0:0:0:24D2:12AB:98BC
 - é igual a
 - 2001:0BAA:0000:0000:0000:24D2:12AB:98BC
- Se tivermos uma sequência de blocos com valor zero, podemos abreviar com dois pontos (::)
 - Um endereço abreviado:
 - 2001:BAA::24D2:12AB:98BC
 - e igual a
 - 2001:0BAA:0000:0000:0000:24D2:12AB:98BC



ATIVIDADE!

ATIVIDADE 1 - CORREÇÃO

1 – Como podem ser divididos os endereços IPs por classes?

2– Qual o valor decimal dos seguintes binários:

a) 11100110

b) 11100000

3- Por que existem IPs públicos e IPs privados? Qual a faixa de IPs privados da classe C?

ATIVIDADE I - CORREÇÃO

4- Considerando os intervalos de endereços *classful*, qual seria a classe, máscara, endereço de rede, primeiro e último endereço de host e endereço de broadcast para as redes dos IPs abaixo?

A) 10.26.40.12

B) 200.100.10.2

C) 130.44.55.6

D) 180.254.255.254

E) 222.22.2.2

ATIVIDADE 2 - CORREÇÃO

5 - Qual dos Ips não é válido para identificar host?

A) 10.26.40.1 b) 130.5.255.254 d) 192.168.10.2 E) 127.0.0.1

ATIVIDADE 3 - CORREÇÃO

- 6 - Considerando que você precise configurar uma rede com 5 máquinas classe B. Apresente um endereço de rede, os endereços das máquinas (fixo) e o broadcast.

ATIVIDADE 4 - CORREÇÃO

7- Desafio, monte a rede da atividade 5 no Packet Tracer!

REFERÊNCIAS

- COMER, Douglas E. Redes de Computadores e Internet. Porto Alegre: Bookman, 2016. <https://integrada.minhabiblioteca.com.br/reader/books/9788582603734/>
- TANENBAUM, Andrew. Redes de Computadores. 5.ed. São Paulo: Campus, 2011. <https://plataforma.bvirtual.com.br/Acervo/Publicacao/2610>
- MORAES, Alexandre Fernandes de; Redes de computadores. -- 1. ed. -- São Paulo : Érica, 2014. <https://integrada.minhabiblioteca.com.br/reader/books/9788536532981/>

OBRIGADA!