UNIVERSIDADE
EDUARDO
MONDLANE

FACULDADE DE ENGENHARIA
DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
LICENCIATURA EM ENGENHARIA INFORMÁTICA
REDES DE COMPUTADORES I

TEMA: Endereçamento IPv6

Grupo Docente:

- Engº. Felizardo Munguambe (MsC)
- Engº. Délcio Chadreca (MsC)

Tópicos da Aula

- Introdução ao IPv6;
- Endereçamento IPv6;
- Estrutura do pacote IPv6;
- Interoperabilidade entre IPv4 e IPv6;

Introdução ao IPv6

Limitantes do protocolo IPv4

O protocolo IPv4 revelou-se um protocolo robusto e de fácil manuseamento, não tendo sofrido grandes alterações desde a sua introdução em 1981. No entanto, não levou em consideração alguns aspectos que mais tarde ou mais cedo irão limitar, senão inviabilizar a sua utilização. De entre estes aspectos, destacam-se os seguintes:

- Espaço de endereçamento esgotado
- Simplificação de configuração
- Segurança
- Qualidade de serviço
- Formato do Cabeçalho

Espaço de endereçamento esgotado – O IPv4 considera 32 *bits* de endereço, o que permite gerar até 2^{32} endereços distintos. Pouco mais do que $4x10^9$ endereços. Tendo em conta o rápido crescimento da Internet e o consequente esgotamento causado pelo desperdício de endereços IP decorrente do esquema de endereçamento hierárquico adoptado no IPv4. A solução adoptada para viabilizar o uso do protocolo IPv4 foi a utilização de NAT, que permite usar um único endereço público para vários endereços privados. Entretanto o serviço NAT possui constrangimentos.

Segurança – A segurança na comunicação de dados privados através de uma rede pública é garantida em grande parte através da encriptação de dados..

- **Simplificação de configuração** – A configuração de um endereço IPv4 numa máquina pode ser feita manualmente ou através de um servidor DHCP existente na rede da máquina. Em ambos casos torna-se necessária a intervenção de uma administrador de sistemas, cuja tarefa torna-se mais complexa e trabalhosa com o aumento do números de dispositivos.

- **Qualidade de serviço** – O IPv4 inclui um mecanismo de qualidade de serviço que se baseia no uso do campo ToS *(Type of Service)* e na identificação do tipo de dados através de uma porta UDP ou TCP. O problema é que esse mecanismo não é ideal e tem sido usado e interpretado de diversas formas, dificultando a garantia de **QoS** durante a transmissão de um dado pacote;

- **Formato do Cabeçalho –** O IPv4 considera um cabeçalho que pode ir de 20 a 60 *bytes*. Os 40 *bytes* de campos opcionais não são usados em múltiplas situações, mas estão sempre presentes no cabeçalho. Esta estrutura exige processamento extra dos vários campos, mesmo quando não são usados, aumentado a ocupação de largura de banda e a latência na transmissão do pacote.

Introdução ao protocolo IPv6

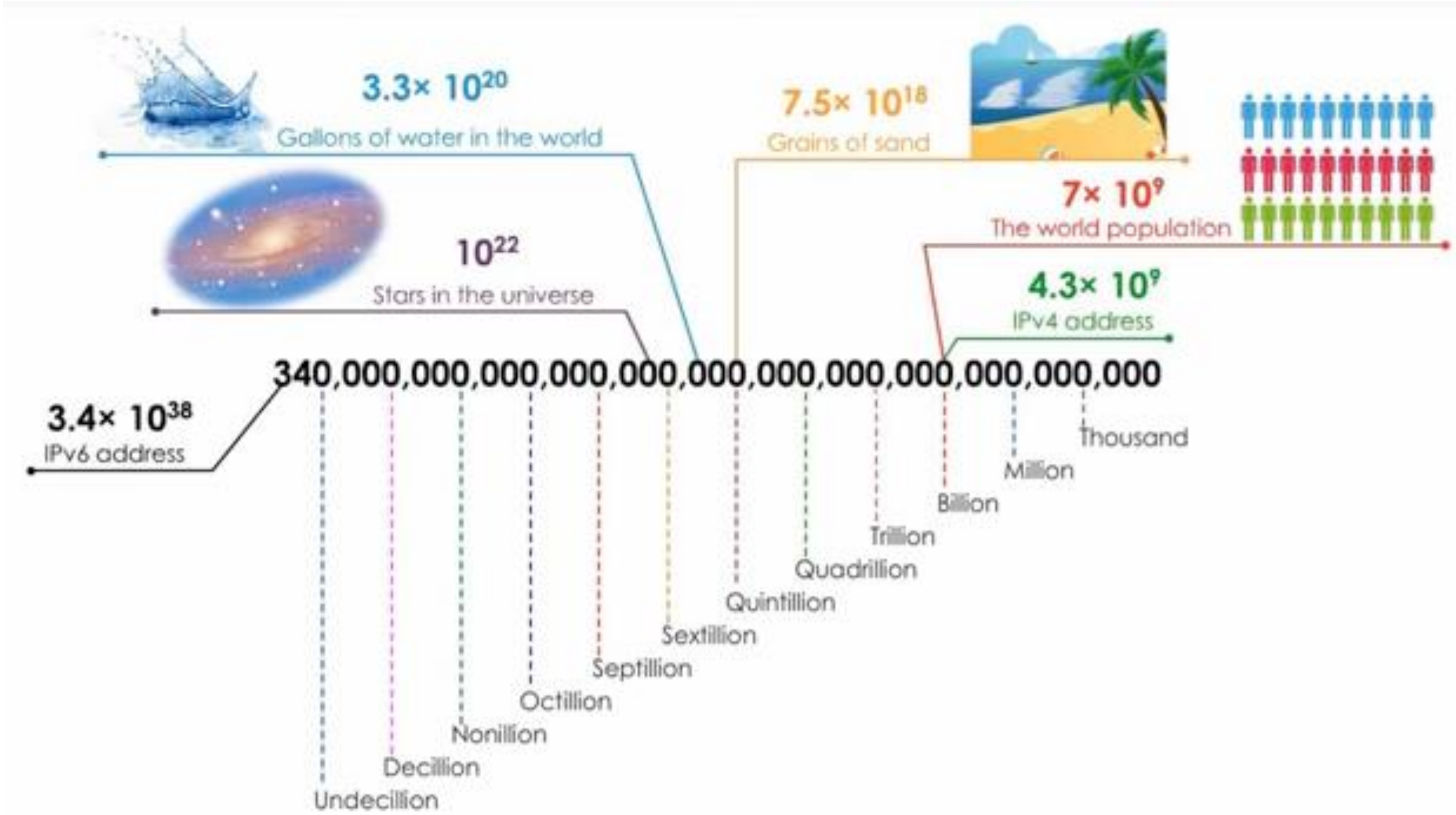
Para superar as limitações do IPv4, no inico da década de 90 começaram os trabalhos de criação do novo protocolo IP. Surgiu desta forma, o IP da próxima geração (IPng – *IP next generation*), hoje conhecido por IPv6. Principais características do IPv6:

- Maior espaço de endereçamento
- Configuração Simplificada
- Segurança
- Melhores Mecanismos de QoS
- Cabeçalho novo

Maior espaço de endereçamento

Os endereços IPv6 têm 128 *bits*, que permitem gerar 2^{128} endereços, aproximadamente $3{,}4x10^{38}$, o que corresponde a um espaço de endereçamento que é 2^{96} vezes do IPv4. Considerando a população total do planeta que é aproximadamente $6{,}5x10^{9}$, podemos dizer que cada um de nós tem ao seu dispor cerca de $5x10^{28}$ endereços (com IPv4 temos um endereço para cada 2 habitantes)! Por causa de questões de estruturação de endereços, não teremos tantos endereços assim disponíveis, mas o número continua a ser tão elevado que não iremos pensar em limitações de endereçamento nos próximos séculos.

Adicionalmente, com a introdução do IPv6, haverá uma distribuição global de endereços pelos usuários da Internet, uma resução das tabelas de encaminhamento, como também vai facilitar a distribuição de endereços pelos fornecedores de serviços. E com o IPv6 o NAT deixa de ser necessário.


3.3× 10^20
Gallons of water in the world
7.5× 10^18
Grains of sand
7× 10^9
The world population
10^22
Stars in the universe
4.3× 10^9
IPv4 address
340,000,000,000,000,000,000,000,000,000,000,000
3.4× 10^38
IPv6 address
Thousand
Million
Billion
Trillion
Quadrillion
Quintillion
Sextillion
Septillion
Octillion
Nonillion
Decillion
Undecillion

Configuração Simplificada

No IPv6 é possível haver autoconfiguração automática e dinâmica dos dispositivos ligados a rede. Com a ploriferação do tipo de equipamentos com necessidades de comunicação, quer fixos, quer móveis, a autoconfiguração assume um papel fundamental. No caso do IPv6, a autoconfiguração pode ser feita de duas formas:

- Sem registo de estado ***(statelesss configuration)*** – possibilita que um equipamento IPv6 “construa” um conjunto de endereços válidos e únicos para acesso a internet, sem necessidade de conectar qualquer servidor.
- Com registo de estado ***(stateful configuration)*** – recorre ao serviço DHCPv6, que é semelhante ao serviço equivalente em IPv4

Segurança

As questões de segurança assumem um papel crucial na concepção da nova versão do protovolo IP. Assim, o recurso ao IPSec passou a ser *standard* integrado no IPv6, integrado como extensão, com os cabeçalhos *Authentication Haeder* e *Encapsulation Security Payload*, o que permite soluções de comunicação mais seguras, logo a partir das camadas mãos baixas do TCP/IP. A segurança com o IPSec não é obrigatória nos pacotes IPv6, daí surgir como cabeçalho de extensão;

Melhores Mecanismos de QoS

O IPv6 inclui um campo que identifica o tipo de tráfego e um campo de identificação de fluxo, que permite aos equipamentos de encaminhamento identificar o fluxo a que pertence um pacote e, desta forma processar os pacotes de um determinado fluxo da mesma maneira. Uma vez que esta informação surge toda no cabeçalho, é possível realizar qualidade de serviço *(Quality of Service, QoS)* mesmo em pacotes encriptados.

Cabeçalho novo

O IPv6 procura minimizar o tamanho do cabeçalho, para tal, todos os ampos opcionais são retirados do cabeçalho principal e passam para o cabeçalho de extensão, que surge após o principal quando escolhidos. O número de cabeçalhos adicionais é apenas limitado pelo tamanho máximo de um pacote IPv6. Devemos ter em conta que o cabeçalho do IPv6 não é uma extensão do IPv4, pelo que os equipamentos deverão ter alguma forma de lidar com ambos simultaneamente, como veremos mais a seguir.

Endereçamento IPv6

Representação de Endereços

Existem 3 (três) convecções para a representação textual de endereços IPv6, para compactar a representação dos 128 *bits*, o endereço é escrito em Hexadecimal. A conversão entre binário e hexadecimal é imediata, bastando agrupar 4 dígitos binários para obter um dígito hexadecimal correspondente. Para representação dos endereços, existem as seguintes conveções:

- Forma predefinida (ou padrão):
- Forma comprimida (ou reduzida);
- Forma Mista;

Forma predefinida

Nesta forma, o endereço IPv6 é representado por 32 números hexadecimais, em grupos de 4 dígitos separados por dois pontos “**:**”.

X:X:X:X:X:X:X:X

Representa 16 *bits*, ou seja, 4 dígitos hexadecimais
Cada X designa-se campo, ou bloco, ou grupo

Exemplo 01: **AF0A:2A5F:2B55:AEAB:FFAA:02AD:3D12:1030**

Exemplo 02: A30C:9C:**0:0**:500:200C:34D:AC

Forma predefinida

Nota: No Exemplo 02, houve uma simplificação na escrita, usou-se a 1º Regra de simplificação (consiste em ocultar os zeros a esquerda de cada campo).

Exemplo-02 A30C:9C:**0:0**:500:200C:34D:AC

Exemplo-02 A30C:**00**9C:**0000:0000**:500:200C:34D:00AC

Forma comprimida ou reduzida

Escrever um endereço de 32 dígitos é sempre trabalhoso e mais difícil de ler. Como tal, sempre que possível, podemos optar pela forma reduzida, aplicando as regras de simplificação.

Regras de simplificação

Regra 01: Podem omitir-se os zeros iniciais de um determinado grupo. A omissão consiste em eliminar os zeros a esquerda de cada campo.

Regra 02: Podem representar-se grupos de zeros consecutivos por duplo dois pontos “::”.

Forma comprimida - Regra 01

Regra 01: Podem omitir-se os zeros iniciais de um determinado grupo. A omissão consiste em eliminar os zeros a esquerda de cada campo.

Exemplo: Considere o seguinte endereço IPv6:

4300:00AE:092B:38BB:0000:0000:BCD1:1221**.**

Aplicando a 1ª Regra, teríamos:

4300:AE:92B:38BB:0:0:BCD1:1221

Forma comprimida - Regra 02

Regra 02: Podem representar-se grupos de zeros consecutivos por duplo dois pontos "::".

Exemplo: Considere o seguinte endereço IPv6:

4300:00AE:092B:38BB:0000:0000:BCD1:1221.

Aplicando a 2ª Regra, ficamos com:

4300:AE:92B:38BB::BCD1:1221

Forma comprimida

A forma comprimida pode ser usada para a escrita de endereços com longas cadeias de zeros. Por exemplo:

FF08:0:0:0:0:0:209A:61 <> FF08::209A:61

0:0:0:0:0:0:0:1 <> **::1** (endereço de *loopback*)

0:0:0:0:0:0:0:0 <> **::** (endereço *unspecified*)

Forma mista

Em ambientes mistos, isto é, ambientes com nós IPv4 e IPv6, pode ser conveniente a utilização da forma mista de representação. Nesta forma os endereços são expressos como **X:X:X:X:X:X.D.D.D.D**, na qual os ‘X’ são valores hexadecimais dos 6 blocos de 16 *bits* mas significativos que compõem um endereço IPv6 e os ‘D’ são valores decimais dos 4 grupos de de 8 *bits* menos significtivos do endereço, representados usando o *dotted decimal notation* do IPv4.

Existem duas formas de referir aos endereços IPv6 com endereços IPv4 embutidos, que são:

- Endereço IPv6 compatíel com IPv4 (utilizados em hosts e *routers* com ligação de redes IPv4 e IPv6 simultaneamente, normalmente para efeitos de *tunnelling*)

Forma mista

- Endereço IPv4 mapeado em IPv6 (endereços de nós que apenas entendem IPv4, escritos na forma de IPv6). São exemplos deste tipos de endereços:

→ 0:0:0:0:0:0.193.169.239.163 (**endereço IPv6 compatível com IPv4**)

→ 0:0:0:0.0:FFFF:129.145.34.10 (**endereço IPv4 mapeado em IPv6**)

Ou, na forma comprimida,

→ ::193.169.239.163 (**endereço IPv6 compatível com IPv4**)

→ ::FFFF:129.145.34.10 (**endereço IPv4 mapeado em IPv6**)

Conversão de Binário para Hexadecimal

- Verificação da direita para esquerda
- Separar os valores binários em grupo de 4 dígitos ou bits
- Se necessário adicionar zeros a esquerda se algum grupo de bits não completar 4 dígitos
- Converter o valor de grupo de bits para decimal
- Converter o valor decimal para hexadecimal

Exemplo

(1101000111100)

0001.1010.0011.1100

1 10 3 12

1 A 3 C

(1101000111100) = (1A3C)

Endereço IPv6

Um endereço IPv6 subdivide-se em duas partes:

Prefixo	**Utilizador**

O endereço é formado pelo prefixo, que pode incluir ou não sub-redes, pelo utilizador *(host)*. Quando escrevemos um endereço IPv6, devemos indicar a parte do endereço que está associada ao prefixo, usando uma barra seguida de um número de *bits* do prefixo. Por exemplo:

Cont.

Exemplo: 2100:00AE:091B:38CC:0000:0000:BCD1:1001**/64**

Neste exemplo, o prefixo é formado pela primeira metade do endereço, ou seja:

2100:00AE:091B:38CC	0000:0000:BCD1:1001
Prefixo	**Utilizador**

Sempre que se pretende apenas indicar o prefixo, os dígitos do utilizador assumem valor zero. Assim o prefixo do endereço será:

2100:00AE:091B:38CC::/64

Cont.

O exemplo usado até agora considera um prefixo com tamanho múltiplo de 16. Caso isso não se verifique, a representação do prefixo deve completar o grupo com zeros. Por exemplo:

2100:00AE:091B:3000::/52

No exemplo, os últimos três zeros a direita (12 bits) já não fazem parte do prefixo, existindo apenas para completar o grupo de quatro.

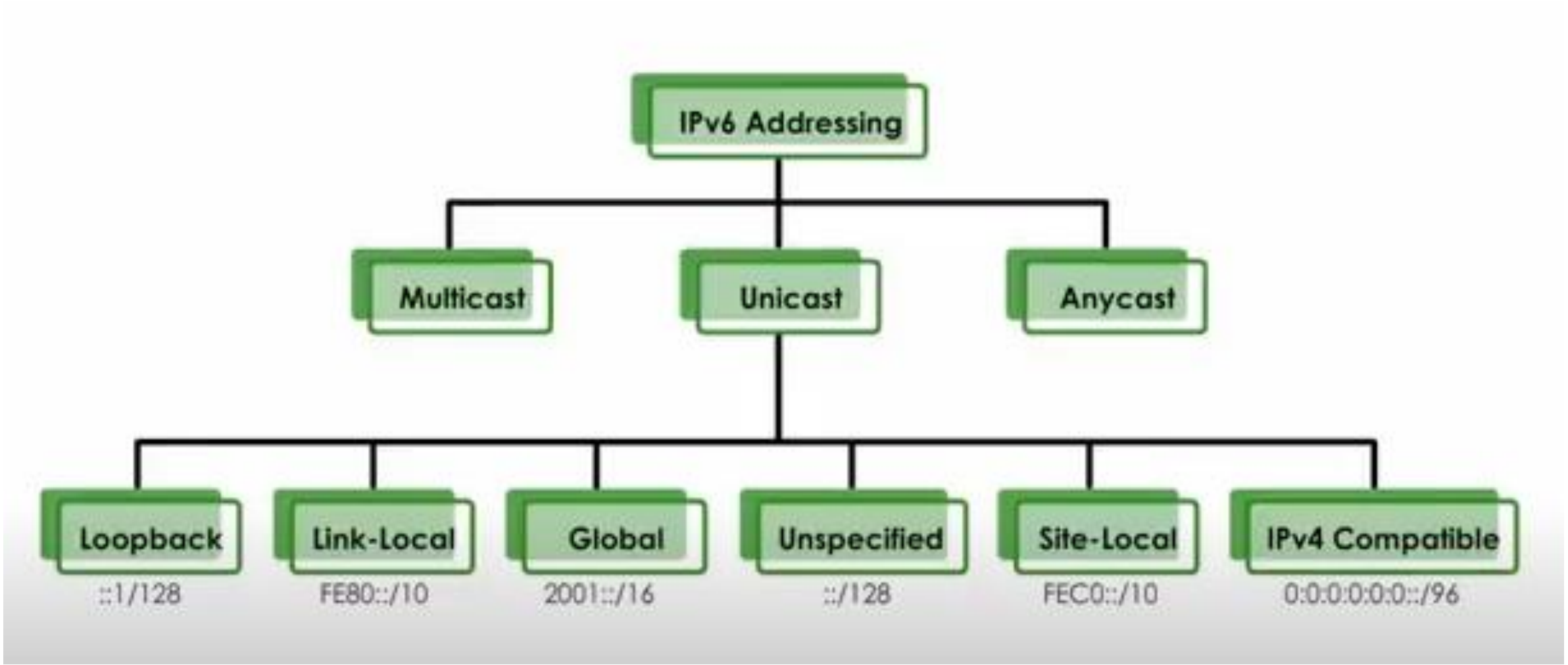
Tipos de Endereço IPv6

Existem 3 tipos de endereço IPv6: ***unicast, multicast e anycast***. Lidar com endereços IPv6 obriga a identificar o tipo de endereço através do próprio endereço, pois não existe qualquer informação adicional ao endereço que identifique o seu tipo.

Em IPv6 não existem endereços de *Broadcast*, dado que esta função pode ser desempenhada pelos endereços *multicast*.

Endereços ***Unicast*** – identificam uma única interface de uma máquina. Um pacote enviado para um endereço *unicast* será entregue à interface identificada pelo endereço. Existem várias formas de endereços *unicast*:

Endereços globais, Endereços locais únicos *(unique local)*, Endereços de ligação local *(link-local)*, Endereços de zona local *(site-local)*, Endereços especiais, Endereços de transição.

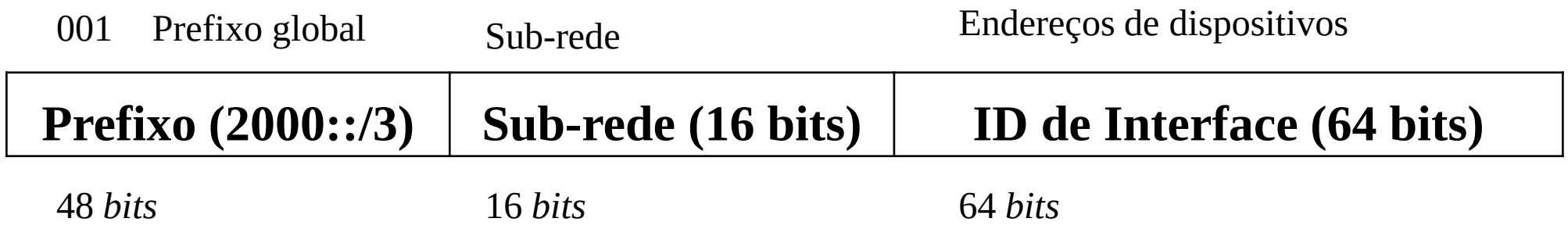

IPv6 Addressing
Multicast
Unicast
Anycast
Loopback
::1/128
Link-Local
FE80::/10
Global
2001::/16
Unspecified
::/128
Site-Local
FEC0::/10
IPv4 Compatible
0:0:0:0:0:0::/96

Endereços *Unicast*

☺ **Endereços Globais**

Um endereço é equivalente a um endereço público usado no IPv4. Os endereços globais são atribuídos por entidades próprias por forma a garantir a unicidade dos endereços IP de todos os utilizadores e para garantir uma hierarquia de endereços que possam ser sumarizados.

Eles são identificados pelo prefixo 2000::/3, ou seja, todos os endereços começados por 2 ou 3 em hexadecimal



Endereços *Unicast*

☺ **Endereços locais únicos *(unique local)***

Um endereço local único permite um tipo de endereçamento privado. É um endereço que é único em todas as sub-redes de uma organização. Esta classe de endereços é identificada com o prefixo FD00::/8, ou seja, os dígitos iniciais são **FD.**

Prefixo		ID de Interface (64 bits)	
FD (8 bits)	**ID Global** (40 bits)	**Sub-rede** (16 bits)	**Endereço de dispositivos** (64 bits)

Endereços *Unicast*

- ☺ **Endereços de ligação local *(link-local)***

Um endereço de ligação local é usado em comunicações que não necessitam sair da sua sub-rede e são configurados automaticamente, descoberta de nós vizinhos ou quando não há *routers* presentes; nunca serão encaminhados para outros *'links'* pelos *routers;* Semelhante ao que acontece com as classes anteriores, um endereço local de ligação é identificado por um prefixo constante – FE80::/10, que identifica todos os endereços começado por FE80, FE90, FEA0 e FEB0, seguido de 54 *bits* a zero.

Prefixo		ID de Interface (64 bits)
FE80::/10	**00000000…000000 (**54 bits**)**	**Endereço de dispositivos**
10 *bits*		64 *bits*

Endereços *Unicast*

☺ **Endereços de zona locais *(site-local)***

Um endereço de zona local também é uma forma de endereço privado que pode ser atribuído a sub-redes locais. Ao contrário de um endereço local único que é exclusivo dento de uma organização, um endereço de zona local pode ser duplicado dentro de uma organização em locais diferentes**.**

Os endereços de zona local tem como prefixo FEC0::/10

Prefixo		ID de Interface (64 bits)
FEC0::/10	**00000000…000000 (**54 bits**)**	**Endereço de dispositivos**
10 *bits*		64 *bits*

Endereços *Unicast*

- **Endereços Especiais**

Existem dois endereços especias, que também são encontrados na versão IPv4.

O endereço não especificado é representado com todos os dígitos a 0 - **0:0:0:0:0:0:0:0** ou '**::**', equivalente a 0.0.0.0 no IPv4. Um endereço não especificado é apenas usado como endereço de origem, caso em que indica que ainda não foi atribuído um endereço.

O endereço de retorno (de *loopback*) é representado com todos os *bits* a zero, excepto o último – **0:0:0:0:0:0:0:1**, que no IPv4 é representado por 127.0.0.1.

- **Endereços de Transição**

Este endereço é usado apelas no processo de transição entre as duas versões de IP.

Endereços *Multicast*

Os endereços *multicast* (prefixo ‘1111 1111’) identificam um conjunto de interfaces tipicamente pertencentes a diferentes nós. Um pacote enviado para um endereço *multicast* é entregue a todas as intefaces identificadas pelo endereço.

A RFC 4291 define endereços *multicast* permanentes (atribuídos pela autoridade global de numeração da Internet) e transitórios, cada um com um espaço de endereçamento próprio.

Endereços *Multicast*

Seguem-se três campos específicos deste tipo de endereços:*Flags*, *Scope e Group ID*.

FF (8 *bits*)	**Flags** (4 *bits*)	**Scope** (4 *bits*)	**Group ID** (112 *bits*)

- ***Flags* –** campo formado por três *flags:* T, P e R. A flag T *(Transient)* a 0 indica que se trata de um endereço *multicast* predefinido, e o contrário trata-se de um endereço transitório. A *flag* P *(Prefix)* indica se o endereço se baseia ou não num endereço *unicast*. A *flag* R *(Rendevouz Point Address)* indica se o endereço contem um *Rendevouz Point Address*.

Cont.

- ***Scope*** – indica até onde o pacote *multicat* pode ser encaminhado. Exemplos de valores de *scope* são: 2 – *link-local;* 4 – *admin-local*; 5 *site-local;* E – *global*;
- *Group ID* – identifica grupos *multicast* dentro de um determinado *scope.* Os endereços *multicast* reservados para fins bem determinados.

Todos as formas de *Broadcast* do IPv4 são substituídos pelo endereço *multicast* FF02::1 com *scope* igual a *link-local* e determinado a todos os nós.

Endereços *Anycast*

Um endereço *anycast* corresponde a um endereço atribuído a múltiplas interfaces. Pacotes que tenham como destino um endereço *anycast* são entregues a interface mais “próxima”, de acordo com a métrica usada pelos protocolos de encaminhamento em vigor.

Os endereços *anycast utilizam* o mesmo espaço de endereçamento que os endereços *unicast*, sendo sintacticamente indistiguíveis destes. O que torna um endereço *unicast* num endereço *anycast* é o facto de ser atribuído a mais de uma interface. Por sua vez, os nós que têm interfaces com endereços *anycast* têm que ser explicitamente configuradas para saber se esses endereços são endereços *anycast* e não *unicast*.

Endereços *Anycast*

Os endereços *any*cast podem ser utilizados, por exemplo, para identificar um conjunto de *routers* pertencentes a uma dada organização ou ligados a uma dada sub-rede. Esta configuração também permite o balanceamento de carga controlado pelos *routers*. Não devem ser usados como endereço de origem de qualquer pacote.

Existe um endereço *anycast* predefinido, designado *subnet-router anycast addderess*.

Resumo da atribuição de prefixos

USO	PREFIXO BINÁRIO	PREFIXO HEXADECIMAL
Reservado	00000000	::0/128
Reservado para NSAP	0000001	
Reservado para IPX	0000010	
Unicast global	001	
Unicast de ligação local	1111111010	FE80::/10
Unicast de zona local	1111111011	FEC0::/10
Multicast	11111111	FF00::/8

Endereços presentes em todas as máquinas

Qualquer máquina tem, obrigatoriamente, que reconhecer os seguintes endereços:

→ Endereço de ligação local;

→ Endereços *unicast* e *anycast* que foram configurados para cada uma das suas interfaces.

→ Endereços de *loopback*;

→ Endereços *multicast* do tipo *all-nodes*. Que designam todos os nós, nomeadamente: FF01::1 e FF02::1;

→ Endereços de nós *solicited;*

→ Endereços de *multicast* a que o dispositivo pertença.

Cont.

No caso específico de um *router*, deve ainda incluir:

→ Os endereços *subner-router anycast;*

→ Todos os endereços *anycast* configurados;

→ Todos os endereços *multicast* do tipo *all-routers*;

→ O endereço *multicast* do tipo *all-routers*;

→ Endereços de *multicast* a que o dispositivo pertença.

Criação de Sub-redes com IPv6

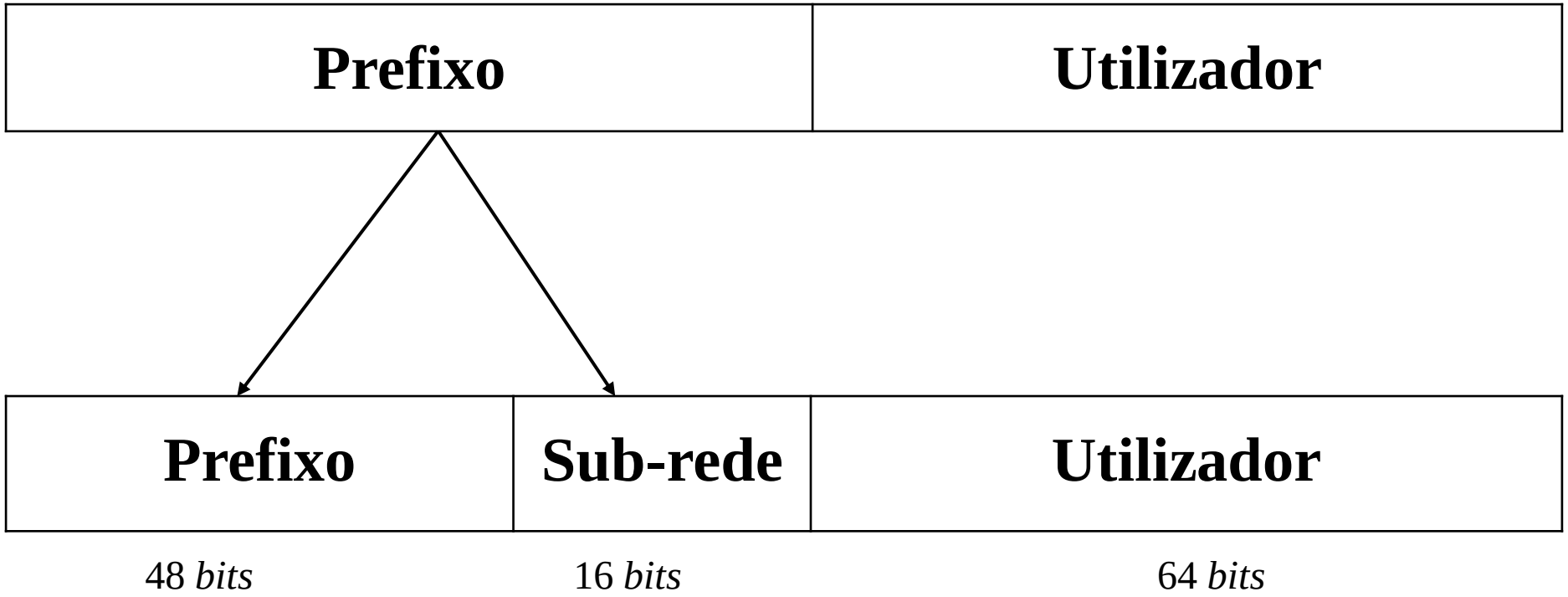
Conforme foi explicado anteriormente, um endereço IPv6 subdivide-se em duas partes, conforme ilustra da figura abaixo:

Prefixo	**Utilizador**

Diferentemente do IPv4 onde são usados *bits* inicialmente destinados a identificação do dispositivo para a criação de sub-redes, no caso dos endereços IPv6 *(unucast)*o tamanho do IP da interface é sempre de 64 *bits*, ou seja, os *bits* usados na identificação da sub-rede são os que fazem parte do prefixo.

Confira a ilustração na figura a seguir:

Subendereçamento

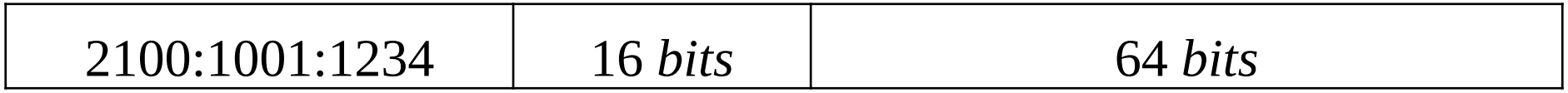


Cont.

A geração de endereços de sub-rede é feita a partir de 16 bits disponíveis. O número de *bits* usados para identificação das sub-redes depende do número de sub-redes necessárias.

Com 16 *bits* de sub-rede conseguem criar-se 65536 sub-redes, cada uma com a possibilidade de ter 2^{64} utilizadores. Com este número, é pouco provável que tenhamos de nos preocupar com o projecto de sub-redes de tamanho variável.

No seguinte exemplo, os endereços de sub-rede seriam:

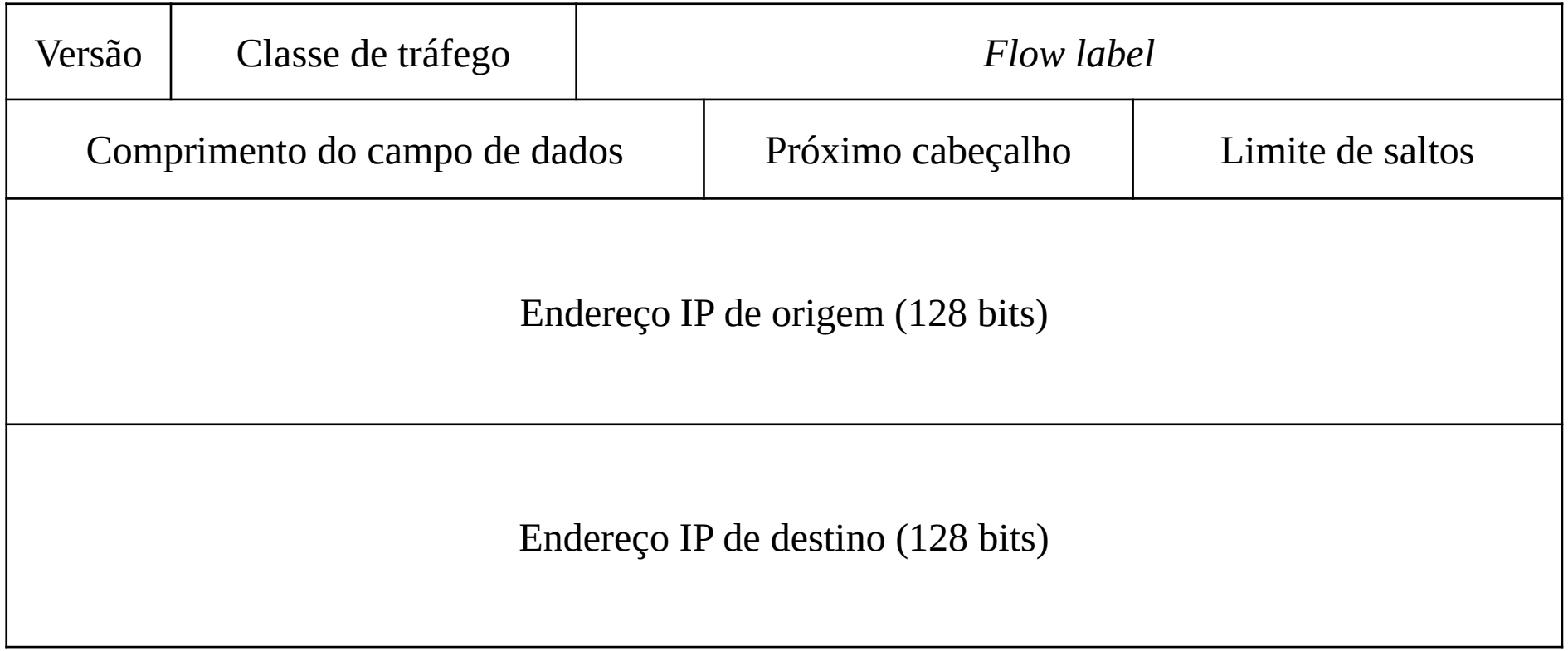


Prefixo **Sub-rede** **Utilizador**

2100:1001:1234:0001:/64
2100:1001:1234:0002:/64
….
2100:1001:1234:F000:/64
….

Estrutura do Pacote IPv6

Formato do cabeçalho IPv6



O cabeçalho Ipv6 é mais simplificado, pois possui somente sete campos, ao contrário do IPv4 que contem treze. Com isso, os *routers* conseguem processar pacotes de um modo mãos rápido, reduzindo assim o atraso de processamento.

Campos do cabeçalho:

- **Versão** – 4 *bits*. Esse campo é sempre seis para IPv6 e quatro para o IPv4. Serve para a identificação do protocolo do pacote.
- **Classe de tráfego** – 8 *bits*. Serve para identificar o tipo de dado no pacote, ou seja, se é mídia contínua como vídeo, som, ou de outros tipos.
- **Identificação do fluxo (*Flow label*)** – 20 *bits*. Permite a criação de um "pseudo canal de comunicação" entre a fonte e o destino, que possui requerimentos e propriedades particulares.
- **Comprimento do campo de dados** – 16 *bits*. Tamanho total do pacote excluindo o cabeçalho principal. O campo tem 16 *bits*, pelo que é possível ter tamanhos até 2^{16} *bytes*. Para tamenhos maiores é necessário usar o cabeçalho de extensão.
- **Proximo cabeçalho** – 8 *bits*. O campo identifica o tipo do primeiro cabeçalho de extensão ou o protocolo de nível seguinte.
- **Limite de saltos** – 8 *bits*. Indica o número máximo de ligações que podem ser percorridas pelo pacote antes de ser descartado.

Cabeçalho de extensão IPv6

A especificação actual do IPv6 define seis cabeçalhos de extensão que devem ser suportados por todos os dispositivos que interferem na comunicação. São eles:

- Cabeçalho de opções de salto-a-Salto *(hop-bu-hop)*;
- Cabeçalho de opções de destino;
- Cabeçalho de encaminhamento;
- Cabeçalho de fragmentação;
- Cabeçalho de autenticação;
- Cabeçalho de encapsulamento de segurança.

Interoperabilidade entre IPv4 e IPv6

Interoperabilidade entre IPv4 e IPv6

A migração de IPv4 para IPv6, se bem que necessária, não pode ser realizada de um dia para o outro, não só pelo grande número de dispositivos configurados com IPv4, mas também por questões ligadas a compatibilidade de software.

Tendo em consciência de que é um processo lento que implica a coexistência de ambos os protocolos durante um longo período, a especificação RFC 1752 determinou um conjunto de critérios de transição:

- Qualquer dispositivo já existente pode passar a IPv6 independentemente do protocolo usado pelos outros dispositivos;
- Qualquer dispositivo novo com IPv6 pode ser adicionado a rede à qualquer momento;
- Os dispositivos a funcionar com IPv4 e que tenham IPV6 instalado podem optar por continuar a usar IPV4;
- A passagem a IPv6 pode ser um processo relativamente simples.

Classificação dos Dispositivos

De acordo com a(s) versão(ões) de IP suportada(s) (RFC 2893). Os dispositivos podem ser:

- ☺ **Unicamente IPv4**: Apenas funcionam com IPv4 e, consequentemente, não percebem IPv6. Este tipo de dispositivos irá diminuir gradualmente ao longo do período de transição;
- ☺ **Unicamente IPv6:** Apenas funcionam com IPv6 e, consequentemente, não percebem IPv4. Este tipo de dispositivos irá aumentar gradualmente ao longo do período de transição;
- ☺ **IPv6/IPv4:** As suas interfaces estão configuradas com endereços IPv4 e IPv6, pelo que funcionam simultaneamente com ambos os protocolos;
- ☺ **IPv4:** Inclui todos os dispositivos que conseguem pacotes com IPv4. Podem ser do tipo unicamente IPv4 ou IPv6/IPv4;
- ☺ **IPv6:** Inclui todos os dispositivos que conseguem pacotes com IPv6. Podem ser do tipo unicamente IPv4 ou IPv6/IPv4;

Métodos de Interoperabilidade

Tendo várias técnicas de interoperabilidade entre IPv4 e o IPv6, o administrador da rede terá de optar por uma das técnicas.

- ***Dual-Stack***
- ***Tunneling***
- **Tradução entre IPv6 e IPv4 com NAT-PT**

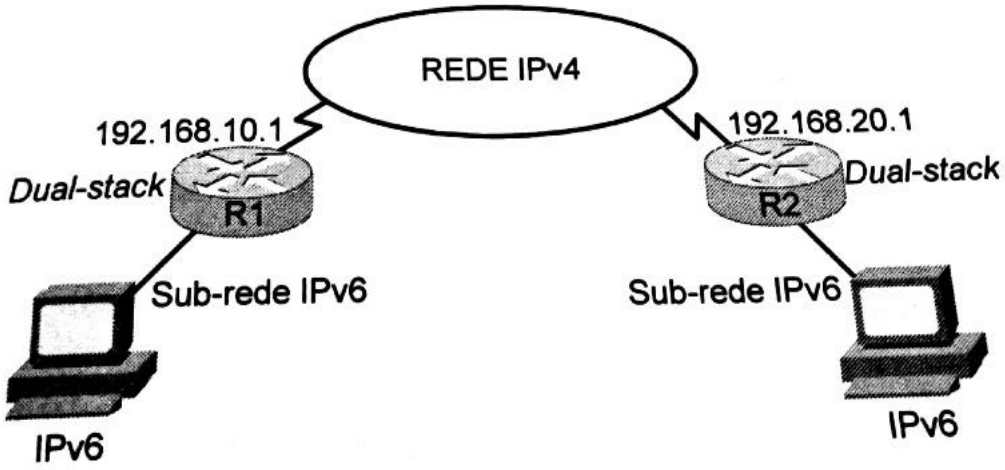
Dual-Stack

É uma forma de coexistir ambas versões e configurar em todos os dispositivos endereços IPv4 e IPv6. Assim, um dispositivo consegue enviar ou receber pacotes IPv4 e IPv6. Este método é designado *dual-stack* devido a existência de informação de encaminhamento duplicada. Os *routers* também suportam este tipo de solução através da configuração simultânea dos protocolos e endereços IPv4 e IPv6.

É bastante simples de utilizar e permite que após a migração completa da rede para IPv6 se retire facilmente o IPv4. A grande desvantagem é que temos dois protocolos a funcionar em simultâneo, com a consequente utilização aumentada do processador e de memória. Por exemplo: o servidor DNS tem de ser capaz de lidar com ambos tipos de endereço.

Tunneling

O *tunneling* consiste em encapsular um pacote IPv6 num pacote IPv4 para atravessar numa rede configurada com IPv4.



Não necessitam de duplicação existente no *dual-stack*, mas necessitam de tempo de processador para o encapsulamento e desencapsulamento. Por vezes é difícil corrigir erros de comunicação devido a problemas de fragmentação ou limite de MTU.

Network Address Translation – Protocol Translation

Neste método, o *router* é configurado de modo a fazer a tradução, estática ou dinamicamente, entre as duas versões de IP, similar ao método NAT de tradução de endereços e portos.

A utilização de NAT permite comunicação directa entre dispositivos IPv4 e IPv6. No entanto, é a técnica menos aconselhada, pois não suporta algumas das características do IPv6, como a de segurança. Além disso, o ponto de entrada e saída de pacotes tem de ser o mesmo, criando um ponto único de falha.

Exercícios

1. Um endereço *unicast* pode ser atribuído a mais de uma interface? Justifique.
2. Os endereços de rede local podem ser encaminhados?
3. Os endereços *multicast* podem ter como destino apenas um dispositivo?
4. Qual é a menor abreviatura para o endereço IPv6: 2001:0001:0000:0000:ABC1:0000:0000:0013?
5. Qualquer endereço pode ser usado para *ulticast*, desde que as interfaces sejam configuradas para identificar os endereços como *multicast*?
6. Se pretende ligar um dispositivo unicamente IPv4 com um outro IPv6 qual método de interoperabilidade usaria?

Bibliografia consultada

→Barrett, D., & King, T. (2010). *Redes de Computadores*. Rio de Janeiro: LTC Livros Técnicos e Científicos Editora.

→Boavida, F., Bernardes, M., & Vapi, P. (2011). *Administração de Redes de Informáticas*. Lisboa: FCA - Editora de Informática, LDA.

→Leon-Garcia, A., & Widjaja, I. (2001). *Communication Networkd - Fundamental Concepts and Key Architectures*. The McGraw-Hill Campanies.

→Véstias, M. (2009). *Redes Cisco - Para profissionais*. Lisboa: FCA - Editora de Informática, LDA.

OBRIGADO !!!