Endereçamento de Rede

Nessa unidade veremos como funciona o endereçamento na camada de rede da Internet. O protocolo dessa camada utilizado ainda hoje na maioria das empresas é o IPV4, entretanto estamos presenciando uma migração para o IPV6 e dentro de alguns anos esse será o protocolo predominante nas redes de computadores e na Internet.

IPV4.

Conforme o cabeçalho do pacote da camada de rede da Internet na Figura 1, pode-se ver que são reservados dois campos para endereço IP de origem e destino (Source address e Destination address), estes endereços são formados por sequências de 32 bits e a partir de agora serão apresentadas algumas características e formas de cálculos para um melhor entendimento de onde vêm às informações do IP que está configurado nos computadores.

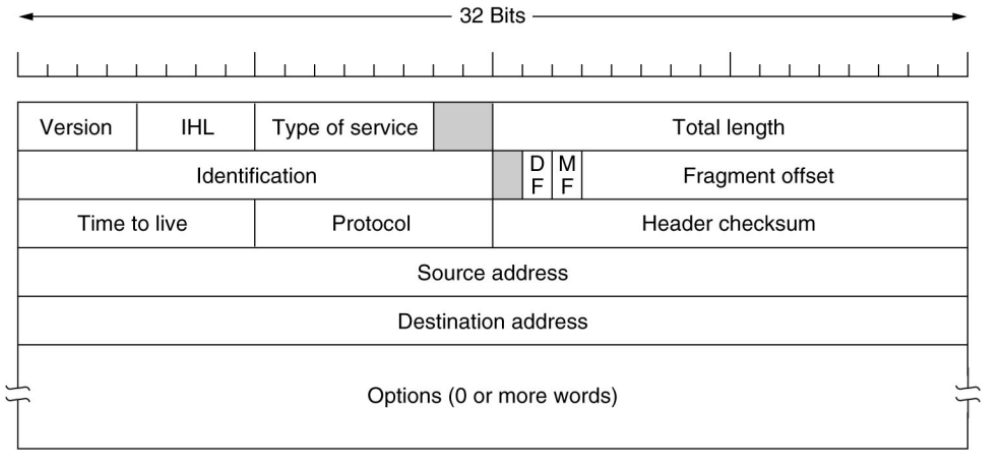

Figura 1 – Cabeçalho do Pacote IP.

Fonte: Tanenbaum, 2012.

Os endereços IPs estão associados às interfaces dos equipamentos. As interfaces podem ser seriais, Ethernet RJ45, Ethernet Fibra Optica, WiFi, etc.

Um hospedeiro, ou host, normalmente tem apenas uma interface. Um roteador normalmente tem várias interfaces, figura 2.

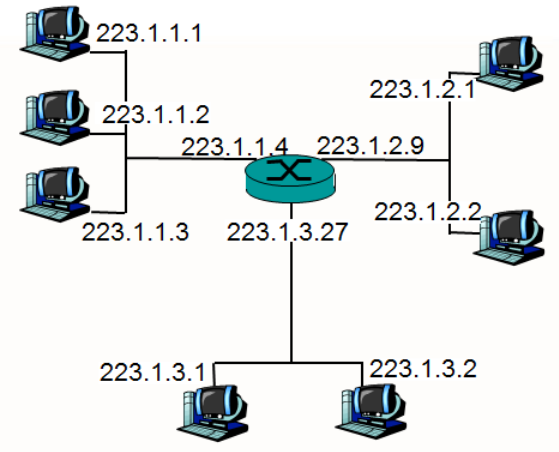

Figura 2 – Endereçamento IP de Host e de roteador

Devido à dificuldade de gravarmos e configurarmos os endereços das máquinas como uma sequência de 32 bits, esse endereço é dividido em 4 (quatro) grupos de 8 (oito) bits e cada grupo é convertido para decimal, sendo que cada decimal deve ficar entre 0 e 255.

Ex 1.

223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Figura 3 – Endereço IPv4

Ex 2.

10101100000100000000010000010101 é representado por: 172.16.4.21.

Cada separação é formada por um conjunto de 8 bits (1 byte), chamada de octeto.

Rede e Host

Os 32 bits do endereço IPV4 são separados em dois grupos, sendo que parte dos bits representa o endereço de rede a qual um computador pertence e os bits restantes representam a máquina dentro daquela rede, figura 4.

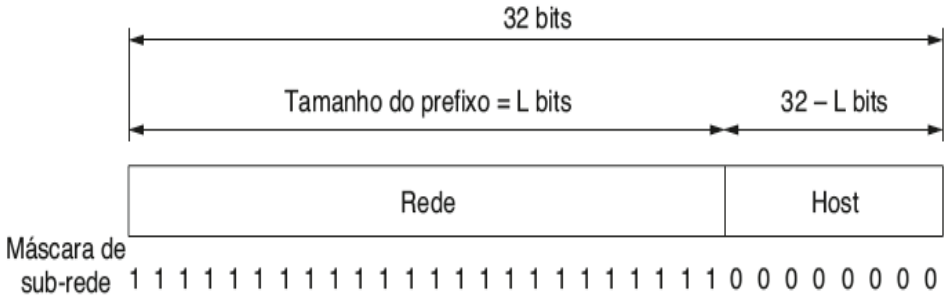

Figura 4 – Endereço de Rede e de Host

Fonte: Tanenbaum, 2012.

Podemos fazer uma analogia aos endereços residenciais onde parte representa nossa rua (endereço de rede) e o resto representa nossa casa dentro da rua (a máquina dentro da rede).

Tipos de Endereços.

- **Rede:** O endereço pelo qual nos referimos à rede (os bits de host ficam com 0)
- **Broadcast:** Endereço especial usado para enviar dados a todos os hosts da rede.
- **Host:** Os endereços designados aos dispositivos finais da rede.

Ex.
Host: 200.243.217.1 até 200.243.217.254.
Rede: 200.243.217.0.
Broadcast: 200.243.217.255.

Classes de Endereços.

Inicialmente para distinguir quais eram os bits para rede e quais eram para máquina dentro da rede foram criadas 5 classes que eram identificadas a partir dos primeiros bits do endereço. Sendo assim, endereços da Classe A possui o primeiro bit 0. Classe B 10, classe C 110 e classe D 1110.

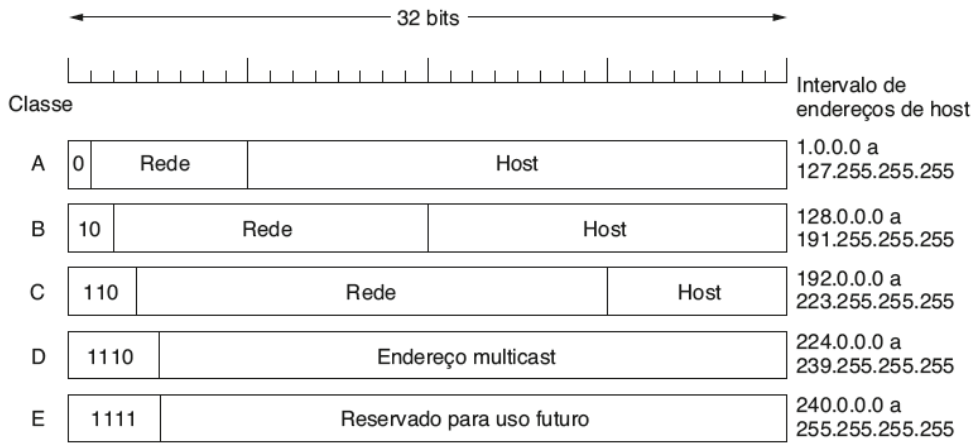

Figura 5 – Classes de Endereços IPV4
Fonte: Tanenbaum, 2012.

Class	First Octet Range	Valid Network Numbers*	Total Number for This Class of Network	Number of Hosts Per Network
A	1 to 126	1.0.0.0 to 126.0.0.0	$2^7 - 2$ (126)	$2^{24} - 2$ (16,777,214)
B	128 to 191	128.0.0.0 to 191.255.0.0	2^{14} (16,384)	$2^{16} - 2$ (65,534)
C	192 to 223	192.0.0.0 to 223.255.255.0	2^{21} (2,097,152)	$2^8 - 2$ (254)

Figura 6 – Quantidade de redes e hosts por classes de IPV4.

Com apenas estas três classes, existe um desperdício muito grande de endereços, pois a menor unidade de alocação é de 254 endereços e se a empresa precisar de um pouco mais a próxima alocação seria de 65.534, que não representa a realidade de nenhuma rede.

Máscara de rede.

Quando configuramos uma rede local com endereços IPv4, precisamos configurar também a máscara. Ela indica quais bits estão sendo usados para rede e sub-rede e quais identificam a máquina dentro da rede. A máscara funciona apenas na rede local e é utilizada para verificar se duas máquinas estão na mesma rede. O sistema operacional do hospedeiro faz uma operação lógica *and* bit a bit entre a mascara e o endereço IP, se o resultado for igual,

significa que as máquinas estão na mesma rede, caso contrário em redes diferentes.

Ex.

A)192.168.0.1	B)192.168.0.2	C)192.168.1.1
255.255.255.0	255.255.255.0	255.255.255.0

A e B estão na mesma rede, pois a operação lógica *and* bit a bit do endereço com a máscara é **192.168.0**.**0**. C está em uma rede diferente pois o *and* bit a bit é **192.168.1.0**.

Existem três formas de representar a máscara:

- /x, onde 8 < x <= 30;
- Como uma sequência de 32 bits onde os bits de rede e sub-rede ficam em 1 (um) e o restante em 0 (zero);
- Convertendo a sequência anterior em decimal.

Por exemplo, a máscara /24 = 11111111.11111111.11111111.00000000 = 255.255.255.0, sendo esta última a mais conhecida por ser aquela usada para configurar a maioria dos equipamentos e sistemas operacionais.

Para resolver a escassez de endereços ip´s foram sugeridas três técnicas: IPv6, NAT[1] e CIDR[2]. O IPv6 é uma solução definitiva que altera o cabeçalho da camada de rede e aumenta os campos reservados para endereços ip´s para 128 bits. Alguns sites na Internet já estão com este tipo de pacote e aos poucos o restante da Internet vem migrando para esta solução. O NAT tem a característica de trabalhar com endereços inválidos dentro da rede local e converter os endereços inválidos para válidos quando as máquinas internas precisam navegar na Internet. Os órgãos internacionais que regulamentam a distribuição de endereços reservaram algumas redes para uso restrito às redes locais, são eles:

[1] NAT – Tradução de endereço de rede.
[2] Roteamento interdomínios sem classe.

- 10.0.0.0/8;
- 172.16.0.0 a 172.31.0.0 /16;
- 192.168.0.0 /16;

Uma máquina configurada com um endereço dentro dos intervalos listados anteriormente, só navega na Internet se algum computador ou roteador fizer a conversão para um endereço válido.

O NAT apresenta outros benefícios além de economizar IP: a rede interna fica protegida, tendo em vista que outros computadores na Internet não têm conhecimento da existência de uma rede por trás do NAT; é possível implementar regras de filtros, tanto de entrada como de saída; e em caso de alteração de provedor só é necessário trocar o endereço do NAT o resto da rede não precisa ser alterada. O NAT quase sempre é implementado em conjunto com o CIDR, vale recordar que a menor unidade de alocação de endereços válidos é de 254 IPs válidos e com o NAT, um ou dois endereços serão suficientes de acordo com a estrutura montada.

O CIDR procurar desvincular o conceito de classe e agora podemos ter qualquer quebra em relação à quais bits são para rede e sub-rede e quais são para as máquinas. Antes só poderíamos ter as máscaras /8, /16 e /24, ou ainda, 255.0.0.0, 255.255.0.0 ou 255.255.255.0. Agora podemos ter outras combinações 255.255.255.224 = 11111111.11111111.11111111.11100000 = /27.

A ideia básica é dividir os endereços de classe A, B e C em mais redes, porém com menos máquinas em cada rede. Verifiquemos um exemplo. O endereço 200.30.40.0, ele originalmente é um endereço de classe C, pois 200 = **110**01000, ou seja, eu tenho uma rede de classe C com 254 máquinas, mas com o CIDR eu posso dividir este classe C em 2, 4, 8, 16, 32, 64 sub-redes, mas é claro que cada uma delas com menos máquinas.

Vamos analisar este exemplo melhor. Quando eu tinha o Classe C, os oito últimos bits estavam reservados para endereço da máquina dentro da rede. Com 8 (oito) bits temos 256 combinações diferentes ($2^8 = 256$), a primeira combinação é 00000000 (tudo em zero), esta não pode ser usado por uma máquina pois é reservada para identificar o endereço da própria rede, a

combinação 11111111 (tudo em 1) também é reservada para quando queremos mandar um pacote para todas as máquinas de uma rede. Logo das 256 combinações possíveis às máquinas só podem usar de 1 a 254. Então temos duas novas regras, quando queremos os endereço da rede temos que, obrigatoriamente , colocar os bits para host em 0, e quando queremos fazer um broadcast colocamos os bits para host em 1.

Em suma:

- 200.30.40.0 /24 é o endereço da rede
- 200.30.40.1 a 254 são endereços possíveis para as máquinas com a máscara /24, ou seja, 255.255.255.0.
- 200.30.40.255 é o endereço para o qual mando um pacote destinado a todos da rede 200.30.40.0.

Desmembramos o classe C 200.30.40.0, mas digamos que o provedor que tem este endereço para distribuir para as empresas, tem 6 empresas distintas e não vale a penas repassar 254 endereços para cada uma. Vamos então dividir o classe C. Para tanto, vamos analisar os bits para host, já que os de rede não podem mais ser alterados.

Dos oito bits que restam, se eu usar apenas 1 (um) para identificar para qual cliente eu vou, eu só terei 2 opções. Se eu usar 2 (dois) bits eu terei 4 opções, e se eu usar 3 (três) bits tem-se 8 combinações. Então verificamos que dos 8 bits reservados para host, nós vamos usar 3 para identificar qual é a empresa. Os outros 5 bits ficam a cargo da empresa distribuir entre as máquinas de sua rede.

Para simplificar os cálculos, apenas o ultimo endereço decimal está sendo desmembrado para binário.

Empresa 1 fica com a rede 200.30.40.**000**00000 = 200.30.40.0 /27 (perceba que os bits em negrito indicam qual é o cliente, os bits restante que são destinados ao host ficam em 0 para identificar a rede, o /27 indica que os primeiros 27 bits identificam a rede e a sub-rede). Assim, 200.30.40.**000**00001 = 200.30.40.1/27 é o primeiro endereço que pode ser usado na rede da Empresa 1 200.30.40.**000**11110 = 200.30.40.30/27 é o último endereço que

pode ser usado na rede dessa empresa. Lembre-se que /27 = 11111111.11111111.11111111.11100000 = 255.255.255.224

Empresa 2 fica com a rede 200.30.40.**001**00000 = 200.30.40.32 /27 (perceba que os bits em negrito indicam qual é a empresa, os bits restante que são destinados ao host ficam em 0 para identificar a rede, o /27 indica que os primeiros 27 bits identificam a rede e a sub-rede). Assim, 200.30.40.**001**00001 = 200.30.40.33 /27 é o primeiro endereço que pode ser usado na rede da Empresa 2 200.30.40.**001**11110 = 200.30.40.62/27 é o último endereço que pode ser usado na rede dessa empresa.

(...)

Empresa 8 fica com a rede 200.30.40.**111**00000 = 200.30.40.224 /27 (perceba que os bits em negrito indicam qual é a empresa, os bits restante que são destinados ao host ficam em 0 para identificar a rede, o /27 indica que os primeiros 27 bits identificam a rede e a sub-rede). Assim, 200.30.40.**111**00001 = 200.30.40.225/27 é o primeiro endereço que pode ser usado na rede da empresa 8 e 200.30.40.**111**11110 = 200.30.40.254/27 é o último endereço que pode ser usado na rede dessa empresa.

Cada uma das oito redes pode endereçar até um total de 30 máquinas, que poderia ter sido calculado com a conta 2^5-2 = 30, a potência de dois é determinada pela quantidade de bits que restaram para host. O exemplo foi dado com um classe C, mas poderia ser um de classe A ou B. nada impede que um dos clientes resolva quebrar novamente a rede em mais sub-redes, no entanto os primeiros 27 bits não podem ser mais alterados, sobrando a ele apenas trabalhar com os últimos 5 bits.

Uma outra opção, caso queiramos dividir na maior quantidade possível de empresas, seria alocar os dois bits finais para os hosts e o restante para a rede.

Ex.

Empresa 1.

200.30.40.**000000**00 = 0 /30 – Endereço da rede da Empresa 1.

200.30.40.**000000**01 = 1 /30 – Primeiro Endereço válido da Empresa 1.

200.30.40.**000000**10 = 2 /30 – Último Endereço válido da Empresa 1.

200.30.40.**000000**11 = 3 /30 – Endereço de broadcast da Empresa 1.

Empresa 2.
200.30.40.**00000**100 = 4 /30 – Endereço da rede da Empresa 2.
200.30.40.**00000**101 = 5 /30 – Primeiro Endereço válido da Empresa 2.
200.30.40.**00000**110 = 6 /30 – Último Endereço válido da Empresa 2.
200.30.40.**00000**111 = 7 /30 – Endereço de broadcast da Empresa 2.
...
Empresa 64
200.30.40.**111111**00 = 252 /30 – Endereço da rede da Empresa 64.
200.30.40.**111111**01 = 253 /30 – Primeiro Endereço válido da Empresa 64.
200.30.40.**111111**10 = 254 /30 – Último Endereço válido da Empresa 64.
200.30.40.**111111**11 = 255 /30 – Endereço de broadcast da Empresa 64

Redes vizinhas não precisam ficar com a mesma máscara, só devemos tomar o cuidado para não repetir endereços em duas redes vizinhas.

Assim como as redes locais, os *links* que interligam duas LANs também devem ser endereçadas, quando o *link* é ponto a ponto, cada ponta deve receber um endereço IP, normalmente inválido, dentro da mesma rede, por exemplo 192.168.0.1/24 e 192.168.0.2/24. Cada *link* ponto a ponto deve usar uma nova rede, mesmo que esteja ligada ao mesmo roteador.

Quando temos um *link frame-relay*, todas as pontas são consideradas como fazendo parte de uma mesma rede, assim podemos colocar uma ponta com 192.168.0.1/24, outra como 192.168.0.2/24 e uma terceira como 192.168.0.3/24

Os endereços IPs são administrados pelas seguintes instituições:

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

Figura 7 – Instituições[3] responsáveis pela distribuição de Endereços IPs.

No Brasil, quem faz a distribuição de endereços IPs é o NIC[4].br que surgiu muito antes do LACNIC.

Também temos os seguintes endereços IPs reservados:

- 0.0.0.0 - utilizado para roteamento padrão
- 127.0.0.0/8 – reservado para loopback, quando queremos testar se a pilha TCP/IP do host está funcionando.
- 169.254.0.0/16 – Utilizado para Link Local.
- 192.0.2.0/24 – Utilizado para Testes e documentação

IPV6.

O IPV6, *Internetworking Protocol* Versão 6 ou IPng, *Internetworking Protocol*, próxima geração, é a nova versão do IP. Ele foi projetado para se adaptar ao crescimento Imprevisto da Internet, além de oferecer qualidade de serviço e mais segurança. Ele resolverá os problemas de alocação de IPs no mundo, uma vez que o espaço de endereço de 32 bits logo estará completamente alocado.

[3] IANA - *Internet Assigned Numbers Authorit*.
[4] NIC.br - *Network Information Centre* do Brasil.

O cabeçalho do datagrama IPv6 possui 40 bytes e tem o seguinte formato:

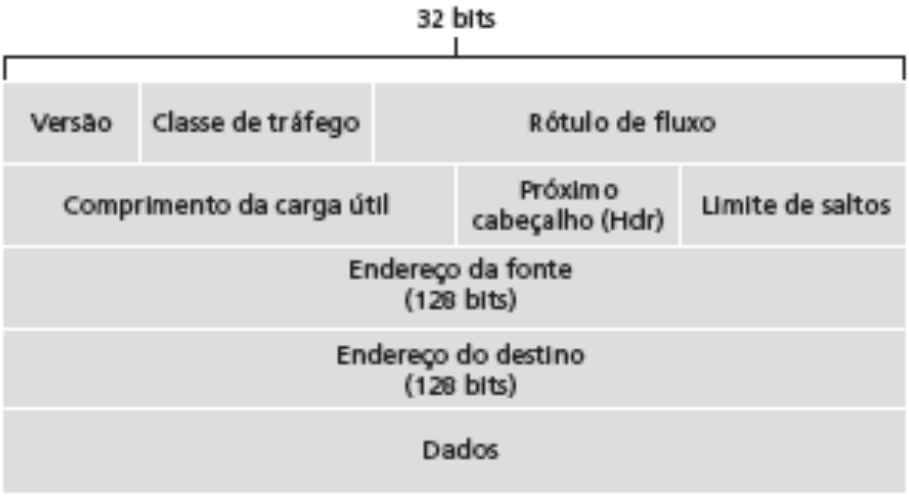

Figura 8 – Cabeçalho IPV6

Fonte: Tanenbaum, 2012.

O IPV6 possui um endereçamento hierárquico de 128 bits, totalizando 340.282.366.920.938.463.463.374.607.431.768.211.456 de host. Ele é organizado em 8 grupos de 4 dígitos hexadecimais, separados por (:). Assim, temos 8 grupos x 4 dígitos hexadecimais x 4 dígitos binários (cada digito hexadecimal corresponde a 4 dígitos binários), o que da um total de 128 bits.

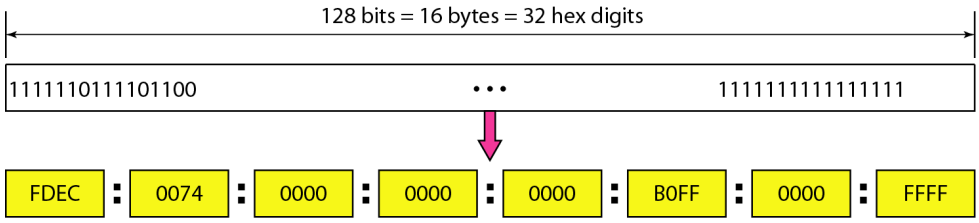

Figura 9 – Formato do Endereço IPV6

Fonte: Forouzan, 2008.

Escrever ou digitar 32 números Hexa, é mais simples do que 128 Binários. Mesmo assim é uma tarefa árdua. Para facilitar a representação do IPv6 duas convenções são possíveis:

- Omita os 0s na frente em qualquer quarteto

- Represente um ou mais quartetos consecutivos, todos com 0s hexa, com dois pontos duplos (::), mas somente para uma destas ocorrências em um dado endereço

Ex1.

FE00:**0000**:**0000**:**000**1:**0000**:**0000**:**0000**:**00**56

Possíveis abreviações:

- FE00**::**1:0:0:0:56
- FE00:0:0:1**::**56

Abreviação com ambiguidade (inválida)

- FE00**::**1**::**56

No caso acima com ambiguidade, não sabemos se o endereço é: FE00:0:1:0:0:0:0:0056 ou FE00:0:0:0:0:1:0:0056 ou FE00:0:0:1:0:0:0:0056

Ex2.

2000:1234:5678:9ABC:**0000:0000:0000:0000**/64

Após a abreviação:

- 2000:1234:5678:9ABC::/64

Prefixos IPV6

Segundo o IPV6.br, o IPV6 possui as representações dos prefixos de rede. Os prefixos são representados na forma “endereco-IPv6/tamanho do prefixo”, onde “tamanho do prefixo” e um valor decimal que especifica a quantidade de bits contíguos à esquerda do endereço que compreendem o prefixo. O exemplo de prefixo de sub-rede apresentado a seguir indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a sub-rede.

Ex.

- Prefixo **2001:db8:3003:2::/64**

- Prefixo global **2001:db8::/32**
- ID da sub-rede **3003:2**

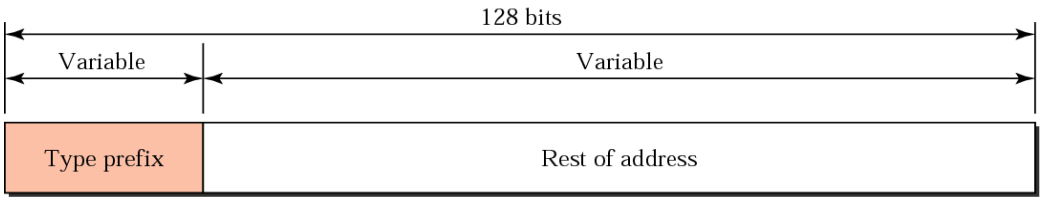

Figura 10 – Prefixo IPv6.
Fonte: Forouzan, 2008.

Com a representação dos prefixos, é possui agregar os endereços de forma hierárquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da sub-rede, etc. Com isso, e possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

Categorias de endereços IPv6.

Existem no IPv6 três tipos de categorias de endereços definidas:

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

Diferente do IPv4, no IPv6 não existe endereço broadcast, responsável por direcionar um pacote para todos os nos de um mesmo domínio. No IPv6, essa função foi atribuída a tipos específicos de endereços multicast.

Endereços Unicast.

Os endereços unicast são utilizados para comunicação entre dois nós, por exemplo, telefones VoIPv6, computadores em uma rede privada, etc., e sua estrutura foi definida para permitir agregações com prefixos de tamanho flexível, similar ao CIDR do IPv4.

Existem alguns tipos de endereços unicast IPv6: Global Unicast; Unique-Local; e Link-Local por exemplo. Existem também alguns tipos para usos especiais, como endereços IPv4 mapeados em IPv6, endereço de loopback e o endereço não especificado, entre outros.

O endereço global unicast é roteável e acessível na Internet IPv6. Equivalente aos endereços públicos IPv4, ele é constituído por três partes: o prefixo de roteamento global, utilizado para identificar o tamanho do bloco atribuído a uma rede; a identificação da sub-rede, utilizada para identificar um enlace em uma rede; e a identificação da interface, que deve identificar de forma única uma interface dentro de um enlace. Sua estrutura foi projetada para utilizar os 64 bits mais a esquerda para identificação da rede e os 64 bits mais a direita para identificação da interface. Portanto, exceto casos específicos, todas as sub-redes em IPv6 tem o mesmo tamanho de prefixo, 64 bits (/64), o que possibilita 2^{64} =18.446.744.073.709.551.616 dispositivos por sub-rede.

Atualmente, está reservada para atribuição de endereços faixa 2000::/3 (001), que corresponde aos endereços de **2000::** a **3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff**. Isto representa 13% do total de endereços possíveis com IPv6, o que nos permite criar $2^{(64-3)}$ = 2.305.843.009.213.693.952 ($2{,}3\times10^{18}$) sub-redes (/64) diferentes ou $2^{(48-3)}$ = 35.184.372.088.832 ($3{,}5\times10^{13}$) redes /48.

Na hierarquia das politicas de atribuição, alocação e designação de endereços, cada RIR, Regional Internet Registry, recebe da IANA um bloco /12 IPv6. O bloco **2800::/12** corresponde ao espaço reservado para o LACNIC alocar na América Latina. O **NIC.br** por sua vez, trabalha com um /16 que faz parte deste /12. O Bloco **2001:1200::/23** também está alocado para o LACNIC.

Endereços IPV6 especiais.

Endereço não especificado.

É representado pelo endereço **0:0:0:0:0:0:0:0** ou **::0** (equivalente ao endereço IPv4 unspecified **0.0.0.0**). Ele nunca deve ser atribuído a nenhum no, indicando apenas a ausência de um endereço. Ele pode, por exemplo, ser utilizado no campo Endereço de Origem de um pacote IPv6 enviado por um host durante o processo de inicialização, antes que este tenha seu endereço exclusivo determinado. O endereço unspecified não deve ser utilizado como endereço de destino de pacotes IPv6.

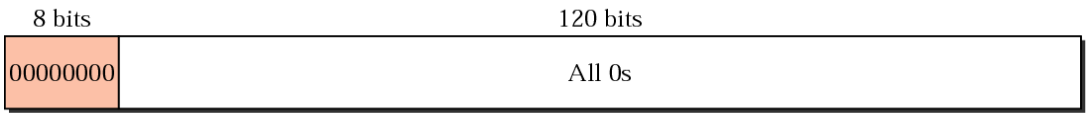

Figura 11 – Endereço não especificado.

Fonte: Forouzan, 2008.

Endereço de retorno (loopback).

O endereço de retorno representado pelo endereço unicast **0:0:0:0:0:0:0:1** ou **::1** (equivalente ao endereço IPv4 loopback **127.0.0.1**). Este endereço e utilizado para referenciar a própria maquina, sendo muito utilizado para teste internos. Este tipo de endereço não deve ser atribuído a nenhuma interface física, nem usado como endereço de origem em pacotes IPv6 enviados para outros nos. Além disso, um pacote IPv6 com um endereço loopback como destino não pode ser enviado por um roteador IPv6, e caso um pacote recebido em uma interface possua um endereço loopback como destino, este deve ser descartado;

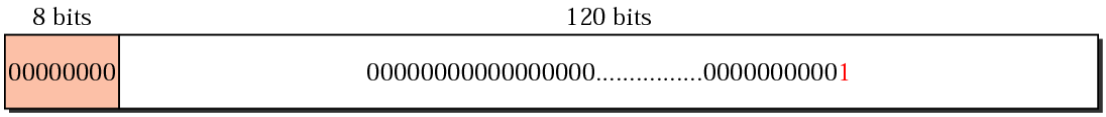

Figura 12 – Endereço Loopback IPv6

Fonte: Forouzan, 2008.

Endereço Mapeado.

O endereço mapeado é representado por **0:0:0:0:0:FFFF:wxyz** ou **::FFFF:wxyz.** Ele é usado para mapear um endereço IPv4 em um endereço IPv6 de 128 bita, onde **wxyz** representa os 32 bits do endereço IPv4, utilizando

dígitos decimais. E aplicado em técnicas de transição para que IPv6 e IPv4 se comuniquem. Ex. **::FFFF:192.168.100.1.**

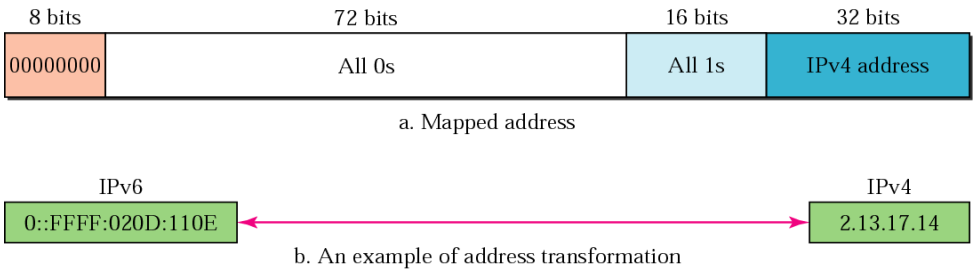

Figura 13 – Endereço IPv6 mapeado.

Fonte: Forouzan, 2008.

Endereço Compatível.

O endereço compatível é utilizado para representar o endereço IPv4-compativel. Sua função e a mesma do endereço IPv4-mapeado, tornando-se obsoleto por desuso.

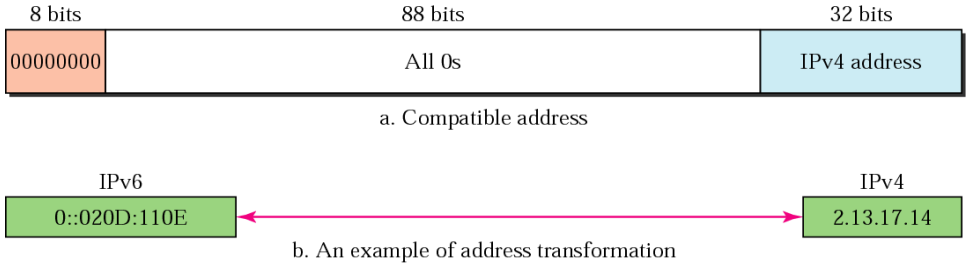

Figura 14 – Endereço IPv6 compatível com IPv4.

Fonte: Forouzan, 2008.

Endereços Multicast

Os endereços multicast são utilizados para identificar grupos de interfaces, sendo que cada interface pode pertencer a mais de um grupo. Os pacotes enviados para esses endereço são entregues a todos as interfaces que compõe o grupo. Seu funcionamento e similar ao do broadcast, dado que um único pacote e enviado a vários hosts, diferenciando-se apenas pelo fato de que no broadcast o pacote e enviado a todos os hosts da rede, sem exceção, enquanto que no multicast apenas um grupo de hosts recebera esse pacote.
Deste modo, a possibilidade de transportar apenas uma copia dos dados a todos os elementos do grupo, a partir de uma arvore de distribuição, pode reduzir a utilização de recurso de uma rede, bem como otimizar a entrega de

dados aos hosts receptores. Aplicações como videoconferência, distribuição de vídeo sob demanda, atualizações de softwares e jogos on-line, são exemplos de serviços que vem ganhando notoriedade e podem utilizar as vantagens apresentadas pelo 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, e 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.

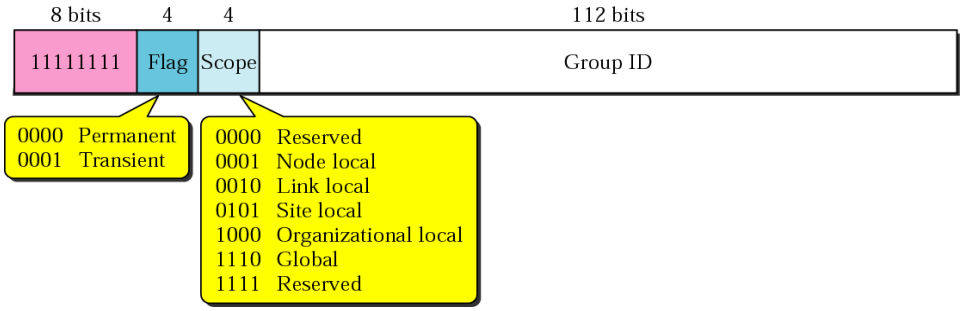

Figura 15 – Flags multicast IPv6

Fonte: Forouzan, 2008.

Sub-redes.

Como no IPv4 o IPv6 também permite a divisão em sub-redes. Elas podem ser criadas a partir do prefixo unicast global atribuído.

Tomemos como exemplo a Companhia 1 que recebeu o prefixo de um ISP e precisa criar 4 sub-redes:

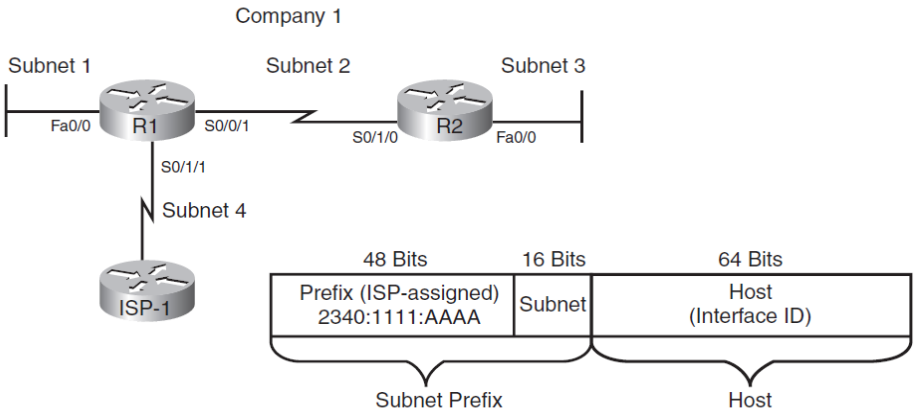

Figura 16 – Empresa com 04 sub-redes.

Solução:

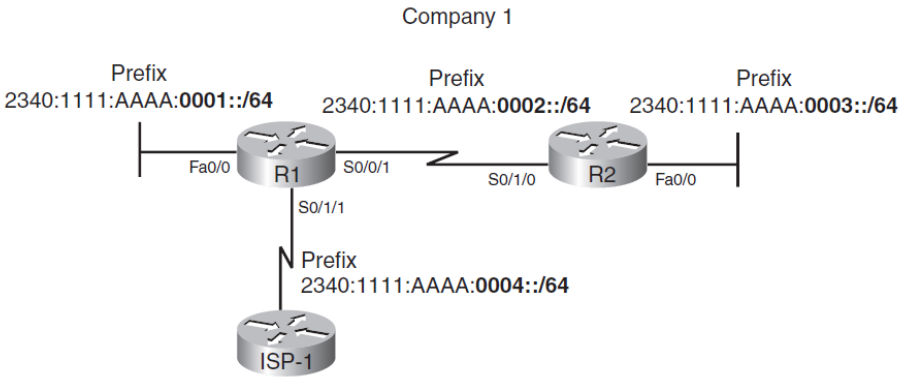

Figura 17 – Alocação de IPV6 em 4 sub-redes.

Recomendação do NIC.br para alocação de IPV6.

O NIC.br recomenda utilizar:

/64 a /56 para usuários domésticos: Para usuários moveis pode-se utilizar /64, pois normalmente apenas uma rede e suficiente. Para usuários residenciais recomenda-se redes maiores. Se o provedor optar por, num primeiro momento, oferecer apenas /64 para usuários residenciais, ainda assim recomenda-se que no plano de numeração se reserve um /56.

/48 para usuários corporativos. Empresas muito grandes podem receber mais de um bloco /48. Para planejar a rede é preciso considerar que para cada rede física ou VLAN com IPv6 e preciso reservar um /64. Esse e o tamanho

padrão e algumas funcionalidades, como a autoconfiguração dependem dele. É preciso considerar também a necessidade de expansão futura, assim como a necessidade de agregação nos protocolos de roteamento.

Técnicas de Migração do IPV4 para o IPV6

Devido ao enorme número de redes instaladas com IPV4 na Internet, a transição do IPV6 deve ser feita de maneira gradual. Abaixo são relatadas algumas técnicas para migração.

Pilha Dupla.

Na atual fase de implantação do IPv6, não e aconselhável a instalação apenas desta versão do protocolo IP, visto que muitos serviços e dispositivos na Internet ainda trabalham somente com IPv4. Deve-se manter o IPv4 já existente funcionando de forma estável e implantar o IPv6 nativamente, para que coexistam nos mesmos equipamentos, e a forma básica escolhida para a transição na Internet. Esta técnica e conhecida como pilha dupla (Dual Stack ou DS) e deve ser usada sempre que possível.

A utilização deste método permite que dispositivos e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois tipos de pacotes, IPv4 e IPv6. Com isso, um nó Pilha Dupla, ou nó IPv6/IPv4, se comportara como um nó IPv6 na comunicação com outro nó IPv6 e se comportará como um no IPv4 na comunicação com outro nó IPv4.
Cada nó IPv6/IPv4 é configurado com ambos endereços, utilizando mecanismos IPv4 (ex. DHCP) para adquirir seu endereço IPv4 e mecanismos IPv6 (ex. configuração manual ou DHCPv6) para adquirir seu endereço IPv6.
Este método de transição permite uma implantação gradual, com a configuração de pequenas seções do ambiente de rede uma de cada vez. Além disso, caso no futuro o IPv4 não seja mais usado, basta simplesmente desabilitar a pilha IPv4 em cada nó.

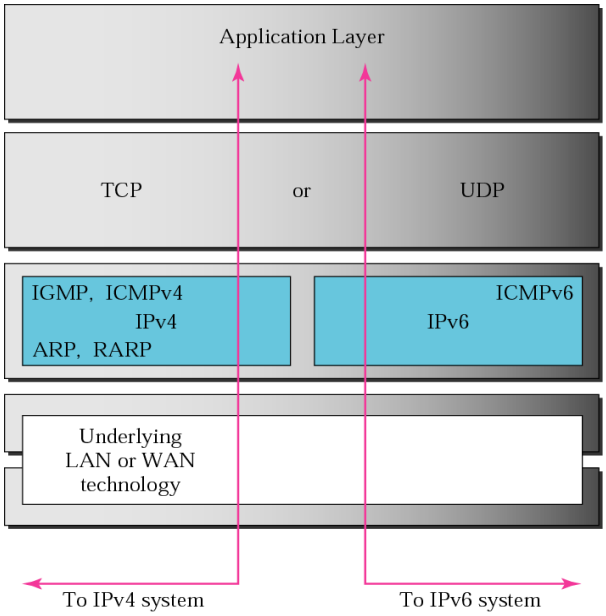

Figura 18 – Pilha dupla IPv4 e IPv6.

Fonte: Forouzan, 2008.

Túneis 6over4

Quando a utilização de pilha dupla não é possível, uma das alternativas a ser considerada e a utilização de tuneis. As técnicas de tunelamento fazem o encapsulamento de pacotes IPv6 em pacotes IPv4. Este encapsulamento e conhecido como 6in4 ou IPv6-in-IPv4 (**RFC 4213**). Ele consiste em colocar o pacote IPv6 dentro de um pacote IPv4, adequar os endereços de origem e destino para o IPv4 e colocar no cabeçalho o tipo 41 (29 em hexadecimal). Esse tipo de encapsulamento e conhecido por 6in4, ou como “protocolo 41”. Quando o destino receber o pacote com tipo 41 ele ira remover o cabeçalho IPv4 e tratar o pacote como IPv6.

Também e possível, de forma análoga, encapsular pacotes IPv4 em pacotes IPv6, técnica conhecida como 4in6.

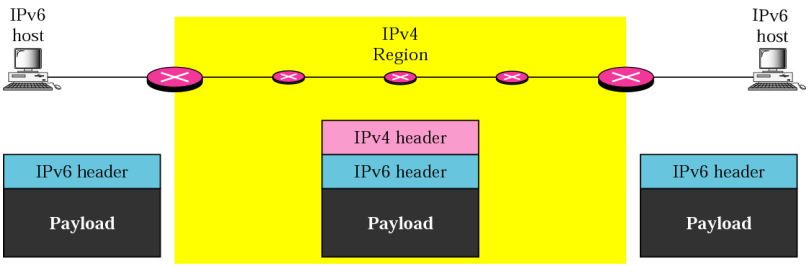

Figura 19 – Tunelamento IPv6 em rede IPv4.

Fonte: Forouzan, 2008.