

IPv6 - Características do IP Next Generation

1 - Introdução

As três das principais motivações que conduziram à necessidade de superar as limitações de crescimento da versão atual do protocolo IP (Internet Protocol Version 4) são: o crescimento da Internet, serviços IP Enabled durante os últimos anos e a necessidade de endereços IP globalmente únicos, de forma a responder à futura implementação de redes de telefonia móveis com acesso a esses serviços.

2 - Novo Formato

Uma das novas características deste novo protocolo é, o novo formato do endereço. O IPv6 amplia o atual endereço de 32 para 128 bits possibilitando assim um método mais simples de autoconfiguração através do uso da identificação EUI-64 da maior parte das interfaces de rede.

Existem três formas de representação de um endereço IPv6. A forma mais utilizada é `x:x:x:x:x:x:x`, onde, os "x" são números hexadecimais. Assim o endereço Ipv6 é dividido em oito partes de 16 bits, como apresentado no seguinte exemplo:

`3ffe:3102:0:0:8:800:200C:417A`

Apenas 15% de todo espaço de endereçamento IPv6 estão previamente alocado, ficando os restantes reservados para uso futuro. Devido a essa pré-alocação, serão comuns endereços com seqüências de bits com o valor zero.

De forma a simplificar a representação de tais endereços as seqüências de zeros podem ser substituídas pela agregação `::`. No entanto, esta apenas poderá ser efetuada uma única vez em cada endereço.

A tabela abaixo apresenta alguns exemplos de endereçamento IPv6 tanto na sua representação extensa como na forma abreviada:

Endereço	Representação Extensa	Forma Abreviada
Unicast	<code>3ffe:3102:0:0:8:800:200C:417A</code>	<code>3ffe:3102::8:800:200C:417A</code>
Multicast	<code>FF01:0:0:0:0:0:0:43</code>	<code>FF01::43</code>
Loopback	<code>0:0:0:0:0:0:0:1</code>	<code>::1</code>
Unspecified	<code>0:0:0:0:0:0:0:0</code>	<code>::</code>

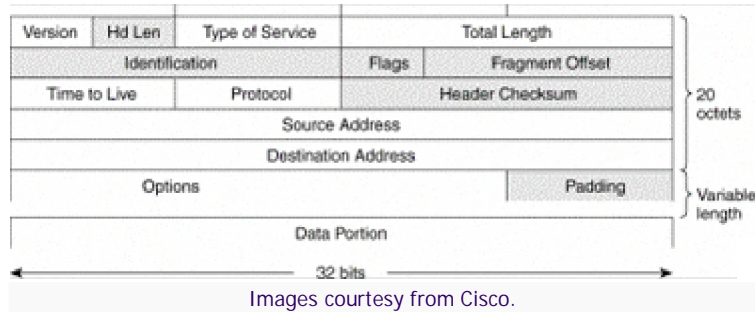
A terceira opção é utilizada na representação de endereçamento compatível Ipv6-Ipv4, sendo útil no período de migração e coexistência de ambos os protocolos. Assim utilizamos a representação `x:x:x:x:x:z.z.z.z`, onde, os "x" indicam números hexadecimais (16 bits) e os "z" são valores que representam os 8 bits referentes ao endereço IPv6 - `0:0:0:0:0:0:192.168.1.1` ou, na forma abreviada - `::192.168.1.1`

3 - Novo Cabeçalho

Outra característica importante do IPv6 é o seu novo e simplificado formato de cabeçalho.

O cabeçalho IPv4 possui 12 campos, num total de 160 bits. O último campo poderá ser seguido de um outro opcional, sendo finalizado por uma porção de dados que normalmente diz respeito ao pacote da camada de transporte.

3.1 - Formato de um cabeçalho IPv4



Os campos sombreados não aparecem no cabeçalho IPv6.

3.2 - Formato de um cabeçalho IPv6

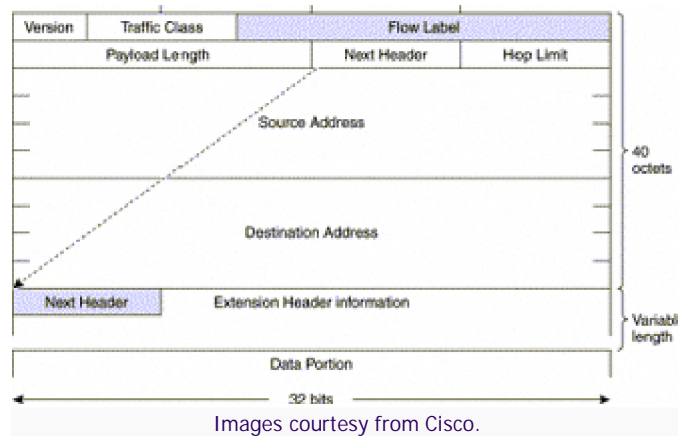
O cabeçalho IPv6 é constituído por 8 campos, num total de 320 bits.

Alguns campos, foram removidos do cabeçalho IPv6 devido à ausência da necessidade de fragmentação nos roteadores e da verificação ao nível de camada de rede. Assim, a fragmentação é assegurada pela origem do pacote IPv6 e as verificações são efetuadas ao nível das camadas de link e de transporte.

Adicionalmente, o pacote referente ao cabeçalho IPv6 e o campo de opções estão alinhados para 64 bits facilitando o processamento dos pacotes IPv6.

A remoção do "checksum" do cabeçalho poderia originar problemas no roteamento de pacotes, mas, o IPv6 baseia-se no pressuposto de que as camadas inferiores são confiáveis, com o seu respectivo controle de erros. Por exemplo, o IEEE 802.2 LLC (Logical Link Control) para redes Ethernet e o controle do PPP (Point to Point Protocol) para links "Serial".

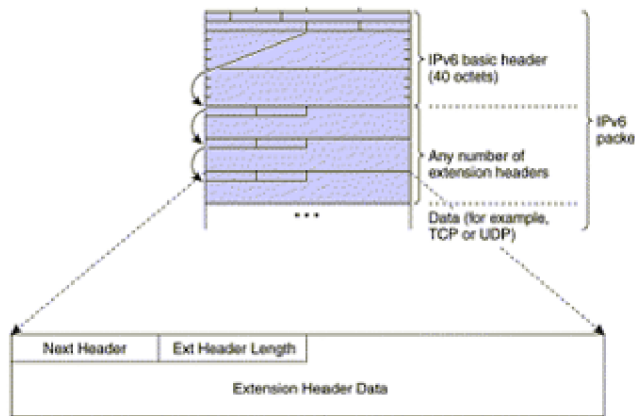
Todas estas modificações irão aumentar substancialmente o desempenho dos equipamentos de roteamentos.



Os campos genéricos do cabeçalho IPv6 são:

Version	Indica a versão do protocolo (v6)
Traffic Class	Utilizado para diferenciar classes de serviço
Flow Label	Utilizado para diferenciar pacotes na camada de rede
Payload Length	Indica o tamanho total dos dados no pacote
Next Header	Determina o tipo de informação que se segue ao header IPv6. Poderá ser um pacote no nível da camada de transporte (TCP/UDP) ou cabeçalhos denominados de (extension headers)
Hop Limit	Especifica o número máximo de "saltos" entre equipamentos
Source Address	Especifica o endereço de origem (128 bits)
Destination Address	Especifica o endereço de destino (128 bits)

3.2.1 - Formato do "Extension Header"



Images courtesy from Cisco.

3.2.2 Tipo de "Extension Headers"

Tipo Cabeçalho	Valor	Cabeçalho Descrição
Hop-by-hop options header	0	Este cabeçalho é processado por todos os "saltos" no path do pacote.
Destination options header	60	Este cabeçalho segue o anterior sendo processado pelo destino final e por cada endereço visitado especificado pelo cabeçalho de roteamento. Alternativamente pode seguir o cabeçalho ESP (Encapsulating Security Payload) sendo apenas processado no destino final.
Routing header	43	Utilizado para "source routing".
Fragment header	44	Este cabeçalho é utilizado quando uma origem tem de fragmentar um pacote cujo tamanho é superior ao MTU (Maximum Transmission Unit) para o caminho entre ela e o seu destino.
Authentication header and ESP header	51 e 50	O cabeçalho de autenticação e o ESP são utilizados dentro do IPSec (IP Security Protocol) de modo a possibilitar autenticação, integridade e confidencialidade de um pacote.
Upper-layer header	6 (TCP) - 17 (UDP)	Cabeçalho típico dentro de um pacote para transporte.

Assim concluindo e comparando o formato do cabeçalho IPv6 com o IPv4.

Seis campos foram suprimidos no IPv6: header length, type of service, identification, flags, fragment offset e header checksum.

Três foram renomeados e, em alguns casos, modificados - length, protocol type e time to live.

Dois foram criados - traffic class e flow label.

4 - Tipos de Endereçamento

No IPv6, existem apenas três tipos de endereços - unicast, anycast e multicast.

Os endereços de broadcast (IPv4) foram substituídos no IPv6 pelos endereços multicast.

4.1 - Endereços Unicast

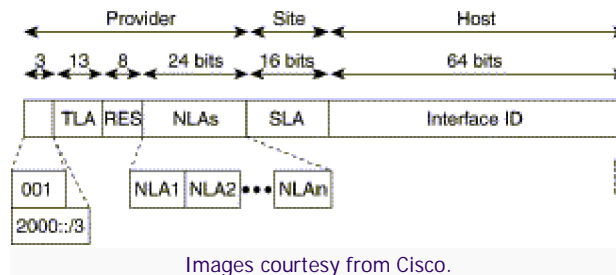
Identificam apenas uma interface. Um pacote destinado a um endereço unicast é enviado diretamente para o interface associado a esse endereço.

No IPv6 foram definidos vários tipos de endereços unicast:

4.1.1 - Agregable Global Address

Agregable Global Address representa um endereço que será globalmente usado. Baseia-se no mesmo princípio do CDIR (Classless InterDomain Routing) possibilitando uma estreita agregação de prefixos de roteamento e contribuindo para a diminuição do número de entradas nas tabelas globais de roteamento.

Este tipo de endereços quando utilizados em links, são agregados hierarquicamente, começando pelos clientes, em seguida por ISP's intermédios e, eventualmente por um ISP de topo.



Images courtesy from Cisco.

O prefixo 2000::/3 (001) indica um endereço do tipo "Agregable Global"

TLA Top Level Aggregator é utilizado para identificar ISP's de topo. Todos os TLA's são ligados por defeito numa zona livre e todos os roteadores existentes nessa zona devem possuir uma tabela de roteamento livre contemplando todas as identificações desses mesmos TLA's.

Um campo de 8 bits encontra-se reservado para suportar o crescimento de TLA's e NLA's (Next Level Aggregator). Este campo deverá ser sempre igual a "0".

NLA's (Next Level Aggregator) é utilizado para identificar ISP's intermédios e de modo a estes criarem a sua hierarquia de endereçamento identificando a sua rede e a comunidade que desejam servir.

Usualmente à parte de topo deste endereçamento é utilizado na rede do ISP e os bits restantes na identificação dos seus clientes.

SLA (Site Level Aggregator) é utilizado por empresas de modo a possibilitar uma utilização semelhante ao que as subnets constituíam no IPv4.

A grande diferença encontra-se no número de endereços disponíveis para essas entidades, 65.535 (16 bits) o equivalente a 256 classes de 256 endereços no IPv4.

O campo Interface Identifier é utilizado para identificar interfaces num link e deverá pertencer unicamente a esse. Em muitos casos o identificador da interface poderá ser o mesmo ou baseado no endereço da interface da camada de link (parte física).

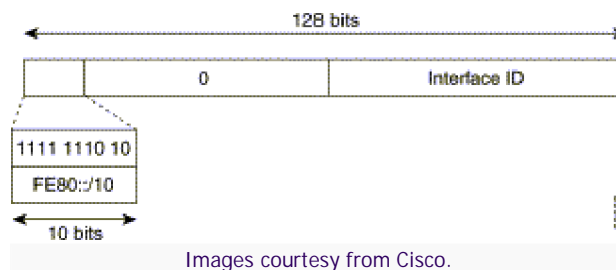
Identificadores de Interface utilizados em endereços do tipo "Global Aggregable" e outro tipo de endereços IPv6 deverão ter o tamanho de 64bits e construídos utilizando o formato EUI 64.

4.1.2 - Link-Local Address

Este tipo de endereço pode ser automaticamente configurado em qualquer interface pela conjugação do seu prefixo FE80::/10 (1111111010), e a identificação da interface no formato EUI-64.

Estes endereços são utilizados nos processos de configuração dinâmica automática e no processo de descoberta de elementos na hierarquia de roteamento (Neighbour Discovery). Este endereçamento permite também a comunicação entre nós pertencentes ao mesmo link local.

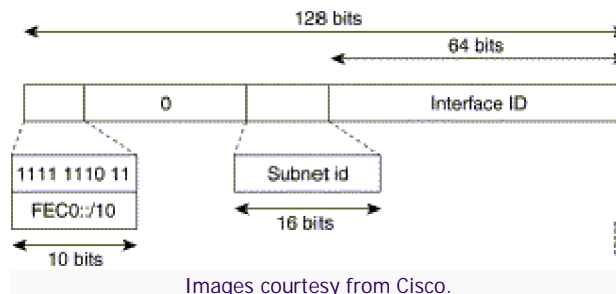
Equipamentos de roteamentos não devem enviar pacotes que contenham este tipo de endereçamento como origem ou destino.



4.1.3 - Site-Local Address

Este tipo de endereço é identificado pelo prefixo FEC0::/10 (1111111011) e pode ser definido para uso interno numa organização através da concatenação do campo de SLA (16 bits) com a identificação da interface (64 bits). Este tipo de endereçamento pode ser considerado como privado; visto estar restrito a um domínio sem ligação à Internet.

Este tipo de endereçamento não pode ser anunciado externamente por roteadores.



4.1.4 - Unspecified Address

Representado por 0:0:0:0:0:0:0:0 ou "::", indica a ausência de um endereço e nunca deverá ser utilizado em nenhum nó.

Este endereço apenas poderá ser utilizado como "source address" de máquinas/nós que não tenham obtido os seu próprio endereçamento.

4.1.5 - Loopback Address

Representado por 0:0:0:0:0:0:0:1 ou "::1".

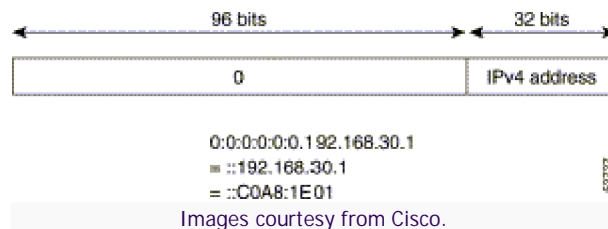
Apenas pode ser utilizado quando um nó envia um datagrama a si próprio e não pode ser associado a nenhuma interface.

4.1.6 - IPv4 Compatible IPv6 Address

Representa um endereço IPv6 cujos últimos 32 bits representam um endereço IPv4. Assim anexando-se um prefixo nulo (96 bits de zeros) a um endereço IPv4 obtém-se o seguinte formato:

0:0:0:0:0:0:194.65.3.20 ou no seu formato abreviado ::194.65.3.20

Este tipo de endereço foi projetado como mecanismo de transição entre IPv6 e IPv4.



Para hosts sem suporte IPv6, quando da transição, foi definido um outro tipo de endereço (IPv4-mapped IPv6):

::FFFF:172.16.25.32.

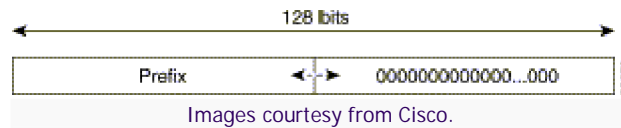
4.2 - Endereços Anycast

Utilizado para identificar um grupo de interfaces pertencentes a nós diferentes. Um pacote destinado a um endereço anycast é enviado para um das interfaces identificados pelo endereço. Especificamente, o pacote é enviado para a interface mais próximo de acordo com o protocolo de roteamento.

Um endereço anycast não pode ser utilizado como endereço de origem (source address) de um pacote IPv6.

Este tipo de endereçamento será útil na detecção rápida de um determinado servidor ou serviço. Por exemplo, poderá ser definido um grupo de servidores de DNS configurados com endereçamento anycast; assim um host irá aceder ao servidor mais próximo utilizando este endereço.

Para cada endereço anycast atribuído, existe um prefixo mais longo desse mesmo endereço que identifica a região ao qual todas as interfaces pertencem.



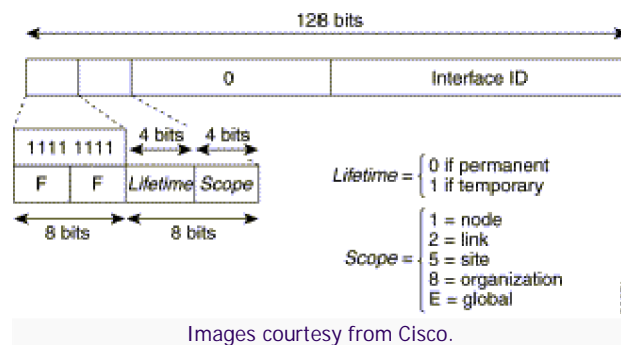
4.3 - Endereços Multicast

Identicamente ao endereço anycast, este endereço identifica um grupo de interfaces pertencente a diferentes nós, mas um pacote destinado a um endereço multicast é enviado para todas as interfaces do grupo.

O segundo octeto que se segue ao prefixo define o tempo de vida (lifetime) e o contexto do endereço multicast.

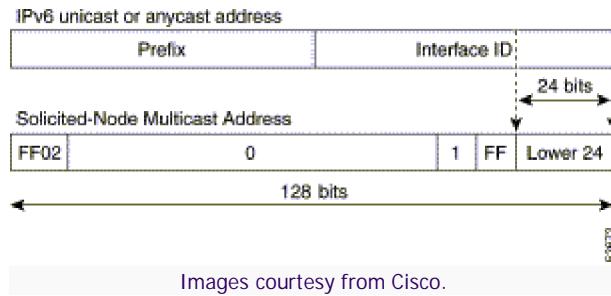
Um endereço multicast permanente tem um parâmetro de tempo de vida igual a "0" enquanto um endereço temporário tem o mesmo parâmetro igual a "1".

O contexto para este tipo de endereço apresenta os valores de 1,2,5,8 ou "E" para identificar um nó, link, site, organização ou um contexto global, respectivamente.



Nós Ipv6 necessariamente tem de receber pacotes destinados aos grupos seguintes:

All Nodes FF02:0:0:0:0:0:0:1 (Perspectiva Link-Local) All Routers FF02:0:0:0:0:0:0:2 (Perspectiva Link-Local) Solicited-Node FF02:0:0:0:0:1:FF00:0000/104 para cada um dos endereços unicast e anycast atribuídos. Um endereço solicited-node é um grupo multicast que corresponde a um endereço IPv6 unicast ou anycast. Nós em IPv6 devem juntar-se ao grupo solicited-node associado a cada endereço unicast e anycast a que está atribuído. O endereço do tipo solicited-node possui o prefixo FF02:0:0:0:0:1:FF00:0000/104 concatenado com os últimos 24 bits do endereço unicast ou anycast. Por exemplo, o endereço solicited-node correspondente ao endereço IPv6 2001::01:800:200E:8C6C é FF02::1:FF0E:8C6C. Este tipo de endereçamento é utilizado nas mensagens de solicitação de vizinhança de rede.

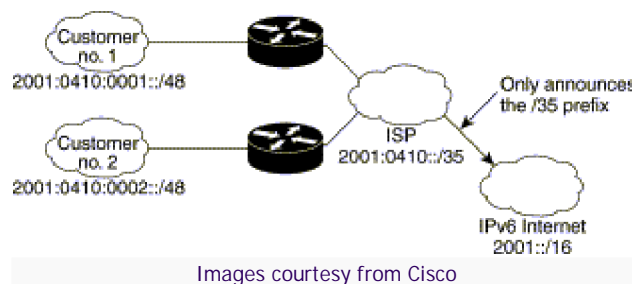


5 - Novas Funcionalidades

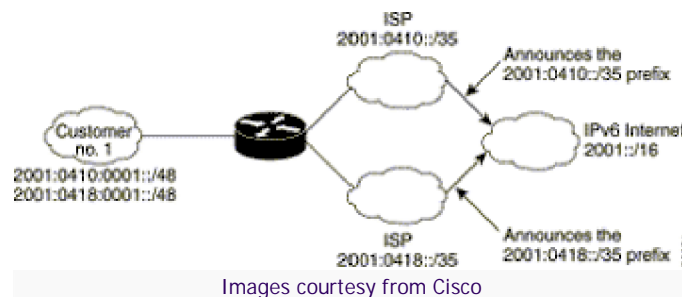
Além de representar um maior espaço de endereçamentos e das modificações apresentadas anteriormente, o IPv6 possui várias outras características importantes como:

5.1 - Agregação de Prefixo

Este tipo de agregação permite estabelecer um tipo de endereçamento hierárquico. Por exemplo, um ISP pode dividir o seu prefixo pelos seus clientes agregando-os de seguida quando o anuncia na Internet



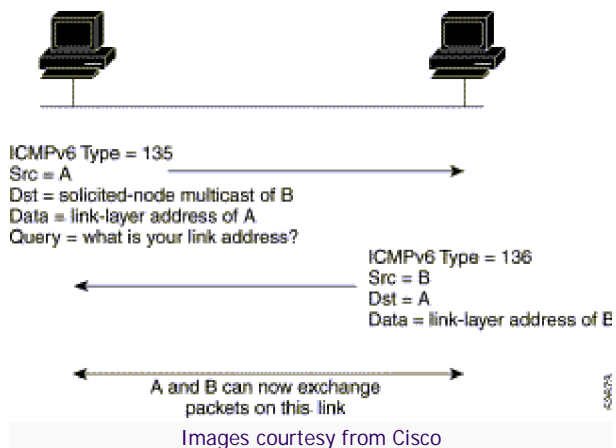
Também facilita as tarefas de endereçamento e roteamento quando um cliente tem mais de uma saída para a Internet (multihomed) visto os prefixos serem atribuídos a redes e hosts automaticamente aprendidos por estes sem quebra da tabela de roteamento global.



No entanto, o processo de seleção do endereço de origem em rede multihomed ainda se encontra em estudo pelo IETF.

5.2 - Descoberta de vizinhança (Neighbour Discovery)

Este processo de descoberta utiliza ICMPv6 e endereços Solicited Node Multicast para determinar o endereço da camada de rede de um elemento vizinho nessa mesma rede e verificar a sua acessibilidade.

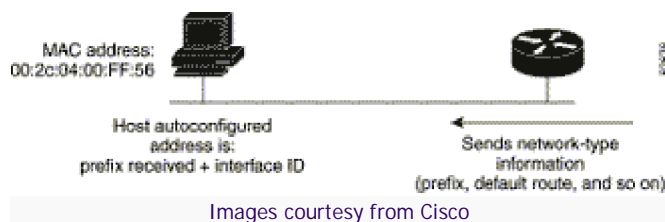


Quando da determinação da identificação do endereço da camada de rede de outro nó, a origem de uma solicitação de descoberta de vizinhança de rede é o endereço IPv6 do nó solicitador.

O endereço de destino de uma solicitação de descoberta de vizinhança de rede é o endereço solicited-node multicast que corresponde ao endereço IPv6 do nó de destino. Esta mensagem de solicitação também inclui o endereço da camada de rede do nó de origem.

5.3 - Autoconfiguração

Quando se instala um host (servidor/cliente) numa rede, automaticamente será atribuído um endereço composto pelas componentes AG:TLA:NLA:SLA:EUI64. Esta característica de autoconfiguração, denominada "stateless autoconfiguration", estará presente no IPv6 eliminando a necessidade de se configurar manualmente este tipo de equipamentos.

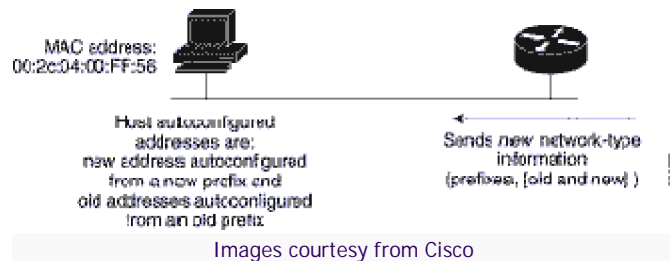


Para maior controlo de redes de grande dimensão, os seus administradores poderão optar por uma outra forma de autoconfiguração, conhecida como "statefull autoconfiguration".

Esta opção será disponibilizada por uma nova versão de DHCP (DHCPv6).

5.4 - Renumeração de rede facilitada.

De modo a possibilitar a renumeração bastará que um novo prefixo com tempo de vida distinto seja anunciado a todos os hosts. Durante o período de renumeração o prefixo antigo será removido das mensagens de propagação dos roteadores.



5.5 - Segurança

As especificações do IPv6 definiram dois mecanismos de segurança inclusos no IPSec: autenticação de cabeçalho (authentication header) e segurança do encapsulamento IP (encrypted security payload).

O IPSec no IPv6 encripta os dados em todo o seu percurso enquanto no IPv4 os dados apenas podiam se encriptados entre roteadores da camada de distribuição.

A autenticação de cabeçalho assegura ao destinatário que os dados IP são realmente do remetente indicado no endereço de origem, e que o conteúdo foi entregue sem modificações. A autenticação utiliza o algoritmo de assinatura normalmente o MD5 (Message Digest 5).

A segurança do encapsulamento IP permite confidencialidade, autenticação da origem e integridade dos dados encapsulados no pacote IP. E tudo é feito através de um algoritmo de criptografia DES/3DES (Data Encryption Standard).

Os algoritmos de autenticação e criptografia citados acima utilizam o conceito de associação de segurança entre o transmissor e o receptor.

Assim, o transmissor e o receptor devem concordar com uma chave secreta e com outros parâmetros relacionados à segurança, conhecidos apenas pelos membros da associação. Para gerar as chaves provavelmente será utilizado o IKMP (Internet Key Management Protocol), desenvolvido pelo grupo de trabalho do IETF em Segurança IP.

5.6 - Suporte a Serviços em Tempo Real

Na especificação do IPv6, o termo "flow" ou fluxo pode ser definido como uma seqüência de pacotes de uma determinada origem para um determinado destino (unicast ou multicast), na qual a origem requer um tratamento especial pelo equipamento de roteamento.

Os campos "Traffic Class" e "Flow Label" foram criados especialmente para facilitar o desenvolvimento de protocolos para controle de tráfego em tempo real, como o RSVP (Resource Reservation Protocol), de forma a permitir a implementação na Internet de aplicações multimídia e com a integração de serviços de dados, voz e vídeo em tempo real.

5.7 - Suporte a Multiprotocolos e Mobilidade

Uma grande parte do espaço de endereçamento IPv6 foi reservada para uso futuro. Essa parte poderá ser alocada para outros protocolos.

O suporte para comunicações móveis também é um dos direcionamentos do IPv6, constituindo este, um fator determinante nas funcionalidades e crescimento na telefonia móvel de 3ª geração.

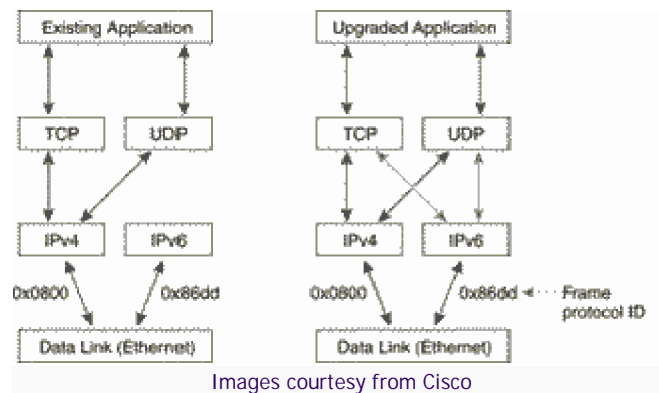
6 - Transição

A coexistência do IPv4 e IPv6 é um dos fatores determinantes de modo a possibilitar uma transição suave de serviços para IPv6.

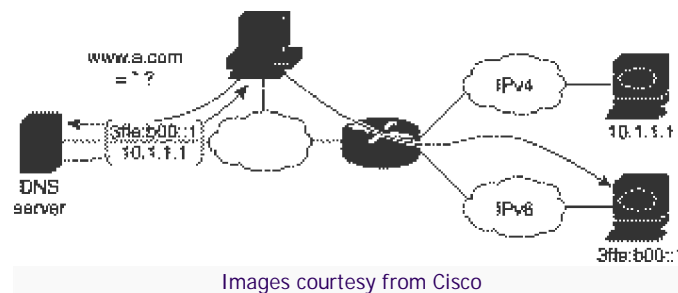
Eis algumas perspectivas de modo a possibilitar esta transição:

6.1 - Perspectiva Dual Stack

Os nós e aplicações funcionam fazendo uso do transporte IPv4 e IPv6 assegurando assim a funcionalidade e acessibilidades de serviços.



A acessibilidade a esses serviços pode ser efetuada usando mapeamento ao nível de DNS, identificando o nó onde se encontra esse serviço com registro A para IPv4 ou AAAA ou A6 para IPv6.

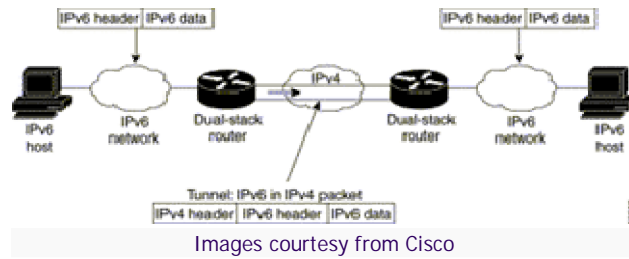


6.2. - Perspectiva de Tunneling

Esta perspectiva permite encapsular pacotes IPv6 em cima do atual transporte IPv4 permitindo a acessibilidade de nós e serviços IPv6.

Esta perspectiva é atualmente utilizada no 6Bone e poderá ser também utilizada por prestadores de serviços de telefonia móvel numa primeira fase de disponibilização de serviços de 3ª geração.

Contudo esta solução não deve ser encarada como final devido às dificuldades de despiste de anomalias que o tunelamento apresenta.



6.2.1 - Túneis Configurados manualmente

Neste caso o endereço IPv6 é configurado manualmente numa interface de tunelamento e endereços IPv4 são também configurados manualmente nas extremidades desse túnel. As extremidades devem suportar transporte IPv4 e IPv6 e podem ser roteadores ou hosts.

6.2.2 - Túneis Automáticos

O endereço IPv6 de origem e destino do túnel são determinados automaticamente usando os 32 bits do endereço IPv4, formando um endereço do tipo IPv5 - IPv4 Compatible. Ex: `::194.65.3.21` - As extremidades devem suportar transporte IPv4 e IPv6 e podem ser roteadores ou hosts.

6.2.3 - Túneis 6 to 4

Este tipo de túneis são estabelecidos entre roteadores IPv6 sobre uma infra-estrutura IPv4.

O endereço IPv6 de origem e destino são determinado pela concatenação do endereço IPv4 com o prefixo `2002::/16` formando um endereço do tipo `2002:194.65.3.20::/48`. As extremidades devem suportar transporte IPv4 e IPv6 e podem ser apenas roteadores