

## 2.4.PROTOCOLO IPV6

### Introdução

O IPv6 surgiu baseado nas limitações de funcionalidades do IPv4. As novas funcionalidades do IPv6 foram desenvolvidas para com a finalidade de fornecer uma forma mais simples de configuração para redes baseadas em IP, uma maior segurança na comunicação entre hosts na rede interna e internet, e também um melhor aproveitamento e disponibilidade de recursos.

O IPv4 como conhecemos hoje foi publicado em 1981 através da RFC 791 e não sofreu nenhuma mudança significativa desde então. Ele funcionou muito bem até agora, mas muito em breve as redes e os serviços de internet terão necessidades que as limitações impostas por este protocolo exigirão uma atualização para o IPv6.

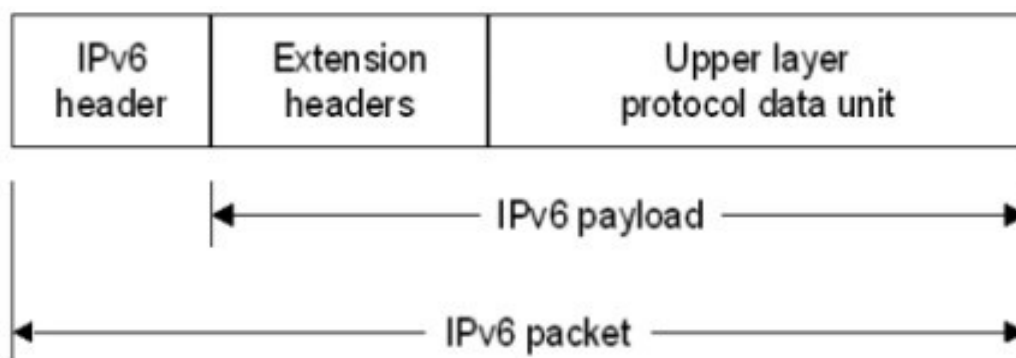
O IPv4 não tem capacidade para atender a demanda por acesso e serviços gerada pelos computadores e dispositivos móveis que temos hoje. O número de usuários vem crescendo de forma rápida, e o resultado disso é não somente o esgotamento de endereços, mas também a falta ou inadequação de recursos necessários para o fornecimento dos serviços.

**001:0DB8:0000:0000:02AA:00FF:FE28:9C5A/ 64**

### Visão geral do IPv6

O IPv6 vai gradualmente substituir o IPv4 em redes que são baseadas em TCP/IP. Os desenvolvedores de software não precisam modificar os seus aplicativos na camada de Transporte (Layer 4) ou Aplicação (Layer 7) para operar em uma rede IPv6.

Da mesma forma que o IPv4, o IPv6 é um protocolo responsável pelo endereçamento de hosts e roteamento de pacotes entre redes baseadas em TCP/IP. A RFC 2460 define a estrutura de um pacote IPv6, que consiste de um header (ou cabeçalho) e payload (ou dados). O payload pode conter ou não extension headers (ou cabeçalhos de extensão).



Na tabela abaixo segue uma descrição das principais informações do cabeçalho IPv6.

Cabeçalho IPv6	Descrição
<b>Source Address</b>	Um endereço IP de 128 bits que identifica a origem do pacote.
<b>Destination Address</b>	Um endereço IP de 128 bits que identifica o destino do pacote.
<b>Next Header</b>	Um identificador para o próximo extension header (ou cabeçalho de extensão)
<b>Hop Limit</b>	O número de redes pela qual o pacote pode passar antes de ser descartado pelo roteador

- IPv4 por IPv6  
O sistema de endereçamento agora tem 128bits, ao invés dos 32bits do IPv4.
- ICMP por ICMPv6  
O ICMPv6 fornece funcionalidades de diagnóstico e relatórios de erros quando um pacote ICMPv6 não pode ser enviado.
- IGMP por MLD (Multicast Listener Discovery)  
O protocolo MLD gerencia os grupos de multicast para redes baseadas em IPv6 e suas mensagens são baseadas no ICMPv6.
- ARP por ND (Neighbor Discovery)  
O protocolo ND gerencia a comunicação entre hosts vizinhos em um mesmo segmento de rede, incluindo a configuração automática de endereçamento IP e descoberta MAC Address.

O IPv6 também é conhecido como The Next Generation IP (IPng). Em resumo algumas das melhorias que ele fornece são as seguintes:

- Roteamento mais eficiente  
Os endereços Globais que são fornecidos para internet são provisionados de forma a permitir um roteamento totalmente baseado em hierarquia. Isso reduz o número de rotas que um roteador terá que armazenar em sua tabela de roteamento.
- Mais espaço para endereçamento  
Os cabeçalhos de endereço de origem e de destino do IPv6 tem 128 bits de comprimento, possibilitando a disponibilização de um número bem maior de IPs que o IPv4. Um cálculo aproximado nos diz que será possível alocar  $6.67 \times 10^{27}$  por metro quadrado da Terra.

- Configuração de host simplificada

O IPv6 continua tendo suporte a configuração dinâmica utilizando o DHCPv6. No entanto, o IPv6 permite que o host se configure automaticamente com informações enviadas pelo roteador.

Também é possível que os hosts em uma rede IPv6 se configurem automaticamente sem o auxílio de um roteador. Essa configuração é similar ao sistema de endereçamento APIPA do IPv4, e permite a comunicação em uma rede local.

- Segurança integrada

O IPv6 possui suporte nativo ao protocolo IPSEC, o que permite o uso de criptografia por parte dos hosts para o envio de dados pela rede de forma mais simples e segura.

- Suporte a QoS

O protocolo IPv6 possui um Flow Label (etiqueta de controle de fluxo) para priorizar a entrega de pacotes. Isso permite que os hosts se comuniquem utilizando o conceito de QoS para entrega dos pacotes, tornando alguns serviços mais funcionais.

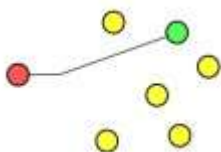
- Header aprimorado

Todo o cabeçalho do IPv6 foi redesenhado para uma melhor flexibilidade na disponibilização de novos protocolos ou serviços, e um melhor processamento das informações por parte dos roteadores. Todas as informações não essenciais foram retiradas e alocadas no extension header (cabeçalho de extensão).

### Unicast, Multicast e Anycast

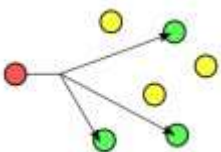
O IPv6 pode utilizar várias formas de transmissão de dados para comunicação entre hosts. A grande diferença aqui é a ausência do broadcast que tínhamos no IPv4 e deu lugar ao Anycast. Abaixo segue a descrição das funcionalidades de cada tipo de transmissão.

#### Unicast



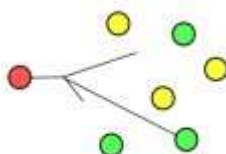
A transmissão utilizando unicast da mesma forma que no IPv4 é utilizada quando um host envia um pacote direto para outro host, uma comunicação do tipo ponto-a-ponto. É a forma padrão e mais comum de transmissão em uma rede.

#### Multicast



O multicast no IPv6, assim como no IPv4 é utilizado quando a transmissão deve sair de uma origem e atingir mais de um destinos. Esse tipo de transmissão cria grupos de multicast e normalmente é utilizado para tráfego de streaming de vídeo e áudio.

### Anycast



O Anycast é uma forma de transmissão intermediária entre o Multicast e o Broadcast, que não existe mais. Nessa transmissão o pacote de dados tem uma origem e um destino mais próximo ou o melhor, que podem ser vários, onde caso um destino não responda, o próximo pode responder.

### Endereçamento IPv6

Semelhante ao modo de divisão do espaço de endereço IPv4, a divisão do espaço de endereço IPv6 baseia-se no valor dos bits superiores do endereço.

Os bits superiores e seus valores fixos são conhecidos como prefixo de formato (FP).

A tabela a seguir mostra a alocação do espaço de endereço IPv6 com base nos FPs.

<b>Alocação</b>	<b>Formato do Prefixo</b>	<b>Fração do espaço de endereço</b>
Reservado	0000 0000	1/256
Reservado para alocação NSAP	0000 001	1/128
Global Unique Address	001	1/8
Link-Local Address	1111 1110 10	1/1024
Unique Local Address	1111 1100	1/256
Site-Local Address	1111 1110 11	1/1024
Multicast Address	1111 1111	1/256

### Global Unicast Address

Os endereços globais de difusão ponto a ponto agregáveis (ou Global Unicast Address), identificados pelo prefixo de formato (FP) 001 (ou 2000::), são equivalentes aos endereços IPv4 públicos.

Eles podem ser roteados e encontrados globalmente na Internet IPv6. Os endereços globais de difusão ponto a ponto agregáveis também são conhecidos como endereços globais (ou Global Address).

Como já está implícito no nome, os endereços globais de difusão ponto a ponto agregáveis foram projetados para serem agregados ou resumidos, a fim de oferecer uma infraestrutura de roteamento eficiente. Diferente da Internet atual baseada em IPv4, que apresenta uma mistura de roteamento simples e hierárquico, a Internet baseada em IPv6 foi projetada desde o princípio para oferecer suporte a um endereçamento e roteamento hierárquicos eficientes.

O escopo, ou seja, a região da rede IPv6 em que o endereço é exclusivo, de um endereço global de difusão ponto a ponto agregável é toda a Internet IPv6.



### TLA ID

O campo TLA ID indica o identificador de agregação do nível superior (TLA ID) do endereço. O tamanho deste campo é 13 bits. O TLA identifica o nível superior da hierarquia de roteamento. Os TLAs são administrados pela IANA e alocados em registros locais da Internet que, por sua vez, alocam identificações de TLA individuais em provedores de serviços de Internet grandes e globais.

Um campo de 13 bits permite, no máximo, 8.192 identificações de TLA diferentes. Os roteadores no nível superior da hierarquia de roteamento da Internet IPv6 (denominados roteadores padrão livres) não têm uma rota padrão somente rotas com prefixos de 16 bits que correspondem a TLAs alocados.

### Res

O campo Res é reservado para uso futuro, quando for necessário expandir o tamanho da identificação de TLA ou de NLA. O tamanho deste campo é 8 bits.

### NLA ID

O campo NLA ID indica o identificador de agregação do próximo nível (NLA) do endereço. Ele é usado para identificar um site de cliente específico. O tamanho deste campo é 24 bits. A identificação de NLA permite que um ISP crie vários níveis de hierarquia de endereçamento para organizar o endereçamento e roteamento e para identificar sites. A estrutura da rede do ISP não pode ser vista pelos roteadores padrão livres.

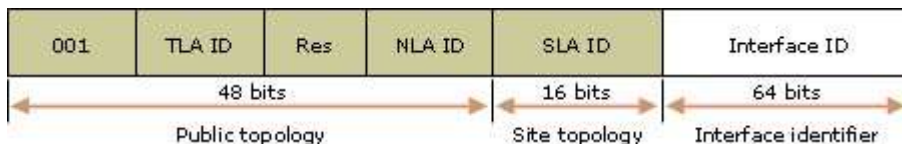
### SLA ID

O campo SLA ID indica o identificador de agregação do nível do site (SLA ID) do endereço. Ele é usado por uma organização individual para identificar sub-redes em seu site. O tamanho deste campo é 16 bits. A organização pode usar esses 16 bits em seu site para criar 65.536 sub-redes ou vários níveis de hierarquia de endereçamento e uma infraestrutura de roteamento eficiente. Com 16 bits de flexibilidade de sub-rede, um prefixo global de difusão ponto a ponto agregável atribuído a uma organização significa que essa organização está

recebendo uma identificação de rede de classe A IPv4 (partindo do pressuposto de que o último octeto é usado para identificar nós em sub-redes).

A estrutura da rede do cliente não pode ser vista pelo ISP.

### Interface ID

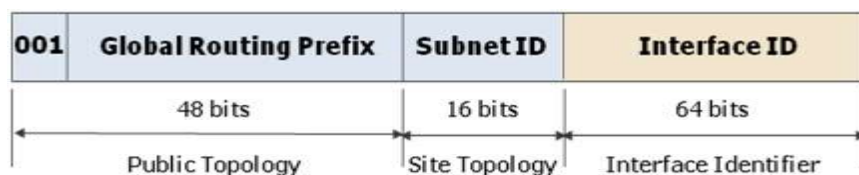


O campo Interface ID indica a interface de um nó em uma sub-rede específica. O tamanho deste campo é 64 bits.

A ilustração a seguir mostra como os campos de um endereço global de difusão ponto a ponto agregável criam uma estrutura topológica de três níveis.

A topologia pública é a coleção de ISPs maiores e menores que fornecem acesso à Internet IPv6. A topologia de site é a coleção de sub-redes no site de uma organização. O identificador de interface identifica a interface específica de uma sub-rede no site de uma organização.

De forma mais simplificada, omitindo o TLA e o NLA os campos de um IPv6 podem ser resumidos de acordo com a seguinte figura:



Para obter mais informações sobre os endereços globais de difusão ponto a ponto agregáveis, consulte a RFC 2374, "An IPv6 Aggregatable Global Unicast Address Format".

### Link-Local Address

Os endereços de conexões locais (ou Link-Local), identificados pelo FP 1111 1110 10 (ou FE80::), são usados pelos nós quando se comunicam com nós vizinhos na mesma conexão.

Por exemplo, em uma rede IPv6 de conexão única que não tenha roteador, os endereços de conexões locais são usados para estabelecer a comunicação entres os hosts na conexão.

Os endereços de conexões locais equivalem a endereços IPv4 com endereçamento IP particular automático (APIPA) (usando o prefixo 169.254.0.0/16). O escopo de um endereço de conexão local é a conexão local. Um endereço de conexão local é necessário aos processos do Neighbor Discovery e sempre é configurado automaticamente, mesmo que todos os outros endereços de difusão ponto a ponto não estejam presentes.



Os endereços de conexões locais sempre começam com FE80. Com o identificador de interface de 64 bits, o prefixo dos endereços de conexões locais sempre é FE80::/64.

Um roteador IPv6 nunca encaminha o tráfego de conexão local para fora dos limites da sub-rede local.

### Site-Local Address

Os endereços de sites locais (ou Site-Local), identificados pelo FP 1111 1110 11 (ou FEC0::), equivalem ao espaço de endereço privado IPv4 (10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16).

Por exemplo, as intranets privadas que não têm uma conexão roteada direta com a Internet IPv6 podem usar endereços de sites locais sem entrar em conflito com endereços globais de difusão ponto a ponto agregáveis. Os endereços de sites locais não podem ser acessados em outros sites e os roteadores não devem encaminhar o tráfego de site local para fora do site.

Os endereços de sites locais podem ser usados, assim como podem ser usados os endereços globais de difusão ponto a ponto agregáveis. O escopo de um endereço de site local é o site (a rede da organização). Diferente dos endereços de conexões locais, os endereços de sites locais não são configurados automaticamente e devem ser atribuídos através de processos de configuração de endereço stateful ou stateless. A figura abaixo mostra a estrutura de um endereço Site-Local



Os primeiros 48 bits são sempre fixos nos endereços de sites locais, começando com FEC0::/48. Depois dos 48 bits fixos, está um identificador de sub-rede de 16 bits (campo Subnet ID) que fornece os 16 bits com os quais você poderá criar sub-redes em sua organização. Com 16 bits, você pode ter até 65.536 sub-redes em uma estrutura de sub-rede simples ou pode subdividir os bits superiores do campo Subnet ID para criar uma infraestrutura de roteamento hierárquica e agregável. Depois do campo Subnet ID, está o campo Interface ID de 64 bits que identifica uma interface específica em uma sub-rede.

## Zone IDs para endereços Locais



Endereços de uso local não são únicos em uma rede interna. Endereços de link-local podem ser duplicados por link (sub-rede). Endereços de Site-Local podem ser duplicados por site. Devido a essa possibilidade, ao especificar um endereço Link-Local é necessário especificar em qual link (sub-rede) ele se localiza.

Para fazer a identificação do link (sub-rede) onde um endereço Link-Local está localizado, utilizamos o Zone ID.

Quando for utilizar um ping, por exemplo, em um endereço de Link-Local, a sintaxe para especificar o endereço IPv6 será IPv6Address%ID.

Para endereço Link-Local o Zone ID normalmente representa a identificação do índice da interface de rede ao qual o endereço está atribuído. Este índice da interface de rede é uma numeração interna sequencial que o Windows usa para identificar as interfaces de rede e pode ser verificado através da saída comando netsh interface ipv6 show interface.

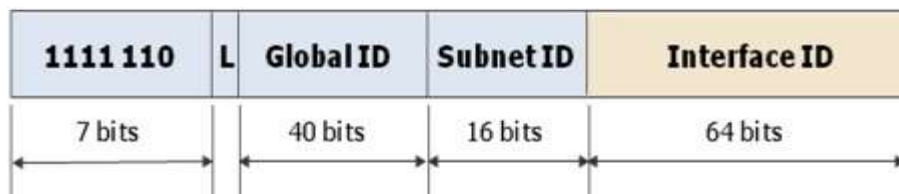
No caso de um computador possuir 2 interfaces de rede, cada uma dessas interfaces terá o seu Zone ID.

Sempre que você for utilizar endereços Link-Local para comunicação é importante lembrar que você deve utilizar o Zone ID da máquina local para identificar qual interface você estará utilizando.

No caso de utilizar um ping para testar a comunicação com um host remoto, o comando deve ter a seguinte sintaxe: IPv6AddressRemoto%ID (o ID aqui representado é do computador local).

## Unique Local Address

Para substituir o endereços de Site-Local que foram descontinuados devido a possibilidade de reutilização do prefixo e consequente transtorno a sua administração, foi definido o endereço único local (ou Unique Local) que são equivalentes aos IPs privados da implementação do IPv4. A figura a seguir mostra a estrutura de um endereço Unique Local





Os primeiros 7 bits tem o valor binário fixo 1111 110. Todos os endereços únicos locais utilizam o prefixo FC00::/7. A flag Local (L) é configurada como 1 para representar um endereço local. O valor da flag Local (L) configurado como 0 ainda não foi implementado e está reservado para uso futuro.

Isso significa que o nosso prefixo padrão para trabalhar com redes internas privadas então é definido pelo FP 1111 1101, ou seja, em hexadecimal representado por FD00::/8.

O Global ID identifica um site específico dentro da organização, e é definido por um valor aleatório de 40 bits. Devido a atribuição desse Global ID ser aleatória, isso possibilita a organização a ter sites configurados com prefixos únicos estáticos de 48 bits. E, no caso de duas organizações unirem suas redes, a probabilidade de terem um mesmo Global ID duplicado é muito baixa.

O Global Unicast Address e o Unique Local Address compartilham a mesma estrutura a partir dos 48 bits iniciais. No Global Unicast Address, o Subnet ID representa os sites dentro de uma organização. Para o Unique Local Address ele pode ter a mesma finalidade

## Endereços Especiais

Estes são endereços IPv6 especiais:

- Endereço não especificado

O endereço não especificado (0:0:0:0:0:0:0:0 ou ::) é usado somente para indicar a ausência de um endereço. Ele equivale ao endereço IPv4 não especificado 0.0.0.0. O endereço não especificado costuma ser usado como endereço de origem dos pacotes que estão tentando verificar a exclusividade de um endereço de tentativa. O endereço não especificado nunca é atribuído a uma interface ou usado como endereço de destino.

- Endereço de auto-retorno

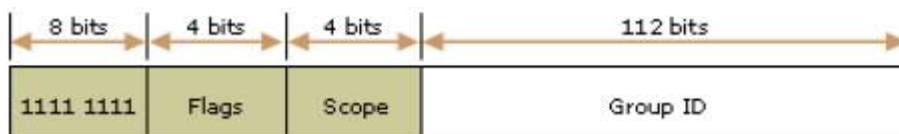
O endereço de auto-retorno (0:0:0:0:0:0:0:1 ou ::1) é usado para identificar uma interface de auto-retorno, permitindo que um nó envie pacotes para si próprio. Ele equivale ao endereço de auto-retorno IPv4 127.0.0.1. Os pacotes transmitidos ao endereço de autoretorno nunca são enviados em uma conexão ou encaminhados por um roteador IPv6.

## Multicast Address

Um endereço de difusão seletiva identifica várias interfaces. Com a topologia de roteamento de difusão seletiva apropriada, os pacotes envia dos a um endereço de difusão seletiva são entregues a todas as interfaces identificadas pelo endereço.

Os endereços IPv6 de difusão seletiva têm o prefixo de formato (FP) 1111 1111 (ou FF00::). É simples classificar um endereço IPv6 como endereço de difusão seletiva porque ele sempre começa com FF. Os endereços de difusão seletiva não podem ser usados como endereços de origem.

Além do FP, os endereços de difusão seletiva incluem uma estrutura adicional para identificar seus sinalizadores, escopo e grupo de difusão seletiva, conforme mostrado na ilustração a seguir.



Os campos do endereço de difusão seletiva são os seguintes

### Flags

O campo Flags indica os sinalizadores que estão definidos no endereço de difusão seletiva. O tamanho deste campo é 4 bits. De acordo com a RFC 2373, o único sinalizador definido é o Transient (T). O sinalizador T usa o bit inferior do campo Flags.

Quando definido para 0, o sinalizador T indica que o endereço de difusão seletiva é um endereço permanentemente atribuído (conhecido) alocado pela IANA. Quando definido para 1, o sinalizador T indica que o endereço de difusão seletiva é temporário (não é permanentemente atribuído).

### Escopo

O campo Scope indica o escopo da rede IPv6 desejado para o tráfego de difusão seletiva. O tamanho deste campo é 4 bits. Além das informações fornecidas pelos protocolos de roteamento de difusão seletiva, os roteadores usam o escopo de difusão seletiva para determinar se o tráfego de difusão seletiva pode ser encaminhado.

Os escopos a seguir são definidos na RFC 2373:

Valor do campo Scope	Escopo
1	Node-local
2	Link-local
5	Site-local
8	Organizational-local
E	Global-local

Por exemplo, o tráfego com o endereço de difusão seletiva FF02::2 possui o escopo de conexão local. Um roteador IPv6 nunca encaminha esse tráfego para fora dos limites da conexão local.

### Group ID

O campo Group ID identifica o grupo de difusão seletiva e é exclusivo no escopo. O tamanho deste campo é 112 bits. As identificações de grupo permanentemente atribuídas são independentes do escopo. As identificações de grupo temporárias são relevantes somente para um escopo específico. Os endereços de difusão seletiva de FF01:: a FF0F:: são endereços conhecidos reservados.

Para identificar todos os nós dos escopos de nó local e de conexão local, os endereços de difusão seletiva a seguir são definidos:

FF01::1 (endereço de todos os nós do escopo de nó local)

FF02::1 (endereço de todos os nós do escopo de conexão local)

Para identificar todos os roteadores dos escopos de nó local, de conexão local e de site local, os endereços de difusão seletiva a seguir são definidos:

FF01::2 (endereço de todos os roteadores do escopo de nó local)

FF02::2 (endereço de todos os roteadores do escopo de conexão local) FF05::2

(endereço de todos os roteadores do escopo de site local)

Com 112 bits no campo Group ID, é possível ter 2112 identificações de grupo. No entanto, devido à maneira como os endereços IPv6 de difusão seletiva são mapeados para os endereços Ethernet MAC de difusão seletiva, a RFC 2373 recomenda que a identificação de grupo seja atribuída a partir dos 32 bits inferiores do endereço IPv6 de difusão seletiva e que os bits originais restantes dessa identificação sejam definidos para 0. Usando somente os 32 bits inferiores da identificação de grupo, cada identificação é mapeada para um endereço Ethernet MAC de difusão seletiva exclusivo.

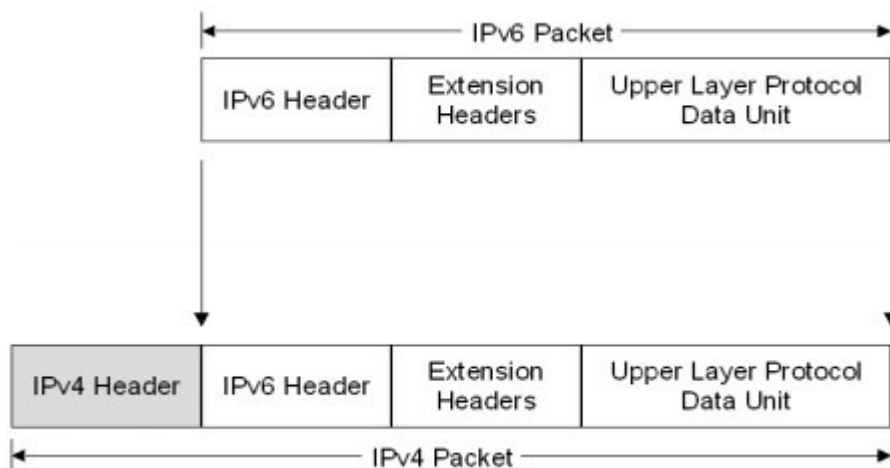
## 2.5.TEREDO, ISATAP E 6TO4

### IPv6 over IPv4 tunneling

O tunelamento de IPv6 dentro do IPv4 é o encapsulamento de pacotes IPv6 com cabeçalhos IPv4 para que ele possa trafegar em uma infraestrutura de rede baseada em IPv4. No cabeçalho IPv4:

- O campo protocolo do cabeçalho IPv4 é definido como 41, que indica um pacote IPv6 encapsulado.
- Os campos de origem e destino são definidos com endereços IPv4 de um túnel, que pode ser criado manualmente ou de forma automática.

Nota: O tunelamento de IPv6 sobre IPv4, descreve um encapsulamento de pacotes IPv6 com cabeçalhos IPv4 para que nós IPv6 possam se comunicar dentro de uma infraestrutura de rede IPv4. Diferente do tunelamento PPTP e L2TP de VPN, não existem troca de mensagens para criação, manutenção ou fechamento do túnel. O tunelamento de IPv6 sobre IPv4 também não fornece nenhum tipo de segurança ou criptografia dos dados.



### Considerações sobre tunelamento

- **Router-to-Router:**  
No tunelamento de router-to-router, temos dois roteadores IPv4/IPv6 interligando duas redes IPv6 através de uma infraestrutura de rede IPv4.
- **Host-to-Router ou Router-to-Host:**  
No tunelamento host-to-router, um nó IPv4/IPv6 que está em uma infraestrutura IPv4 cria um túnel de IPv6 sobre IPv4 para se comunicar com um roteador IPv4/IPv6
- **Host-to-Host:**  
No tunelamento host-to-host, um nó IPv4/IPv6 que está em uma infraestrutura IPv4 cria um túnel de IPv6 sobre IPv4 para se comunicar com outro host IPv6/IPv4 que está na mesma estrutura IPv4.

Em cada nó IPv6/IPv4, uma interface representando o túnel é criada. Rotas IPv6 para utilização do túnel são criadas. Baseado na interface de túnel, na rota e no destino do pacote de rede, o cliente encapsula o pacote IPv4 com cabeçalho IPv4 e envia pelo túnel para o próximo nó.

Esses túneis podem ser configurados de forma manual ou automática

### Tipos de túneis

A RFC 2893 define os seguintes tipos de túneis:

- **Configurados:**

Um túnel configurado requer uma configuração manual. Em um túnel configurado, os endereços IPv4 dos endpoints não são derivados do próximo salto do endereço correspondente ao destino. Normalmente, túneis router-to-router são configurados manualmente. A configuração da interface de tunelamento consiste dos endereços IPv4 dos endpoints, e devem ser definidos junto com as rotas para estes túneis.

- Automáticos:

Um túnel automático é aquele que não precisa de configuração manual, os seus endpoints são determinados pelas interfaces lógicas, rotas e endereços IPv6 de destino.

Atualmente existem 3 tecnologias de tunelamento disponíveis e utilizadas em ambientes de migração:

### Tipos de tunelamento

- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
- 6to4
- Teredo

### ISATAP

ISATAP é uma tecnologia de endereçamento e tunelamento host-to-host, host-to-router e router-to-host automático, que fornece conectividade entre hosts IPv6 em redes de infraestrutura IPv4. A RFC 4214 descreve o ISATAP.

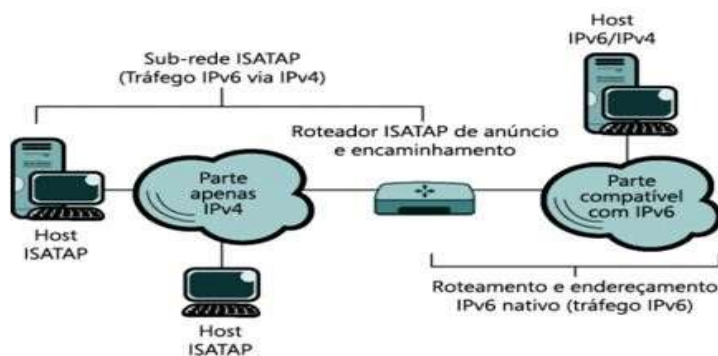
Os hosts ISATAP não requerem nenhuma configuração manual e criam endereços ISATAP utilizando mecanismos de autoconfiguração.

Os hosts ISATAP usam uma interface de encapsulamento lógico para a qual são atribuídos endereços ISATAP, que têm a forma UnicastPrefix:0:5EFE:w.x.y.z (quando w.x.y.z for um endereço IPv4 privado atribuído ao host ISATAP) ou UnicastPrefix:200:5EFE:w.x.y.z (quando w.x.y.z for um endereço IPv4 público atribuído ao host ISATAP). O UnicastPrefix é um prefixo de endereço unicast de 64 bits, incluindo prefixos de link local, global e local exclusivo. Exemplos de endereços ISATAP são 2001:DB8::98CA:200:131.107.28.9 e 2001:DB8::98CA:0:10.91.211.17.

Uma implantação ISATAP consiste em uma ou mais sub-redes ISATAP lógicas, que são redes IPv4 com prefixo de sub-rede IPv6 de 64 bits. Em uma sub-rede ISATAP lógica, há hosts ISATAP e roteadores ISATAP. Um host

ISATAP utiliza uma interface de encapsulamento ISATAP para encapsular tráfego IPv6. Esse tráfego pode ser enviado diretamente para outros hosts ISATAP na mesma sub-rede ISATAP lógica. Para atingir destinos que estão em outras sub-redes ISATAP ou em sub-redes IPv6 nativas, o tráfego é enviado para um roteador ISATAP. Um roteador ISATAP é um roteador IPv6 que anuncia prefixos de sub-rede para hosts ISATAP e encaminha tráfego IPv6 entre hosts ISATAP e hosts em outras sub-redes IPv6.

A figura abaixo mostra os componentes de ISATAP em uma intranet simplificada.



Por exemplo, se um host A tem a interface de rede configurada com o endereço IPv4 10.40.1.29 e um host B, tem a interface de rede configurada com o endereço IPv4 192.168.41.30 e ambos também são clientes ISATAP, automaticamente eles obteriam um endereço ISATAP parecido com o seguinte: FE80::5EFE:10.40.1.29 para o host A e FE80::5EFE:192.168.41.30 para o host B.

O ISATAP permite que você implante recursos de endereçamento e roteamento IPv6 nativos na sua intranet em três fases.

### **Fase 1: Intranet Somente IPv4**

Nessa fase, a sua intranet inteira pode ser uma única sub-rede ISATAP lógica. Você precisará na sua rede IPv4 de um roteador ISATAP para anunciar somente um prefixo de endereço local único ou global para hosts ISATAP.

### **Fase 2: Partes compatíveis com IPv6 e Somente IPv4 de sua intranet**

Nessa fase intermediária, a sua intranet tem uma parte somente IPv4 (a sub-rede ISATAP lógica) e uma parte compatível com IPv6. A parte com capacidade IPv6 da sua intranet deve ser compatível com IPv4 e também oferece suporte a endereçamento e roteamento IPv6 nativos.

### **Fase 3: Intranet compatível com IPv6**

Nessa fase final, a sua intranet inteira será compatível com endereçamento e roteamento IPv4 e IPv6 nativos. Observe que o ISATAP não é mais necessário.

### **Windows Server 2008 e Windows Vista**

O protocolo IPv6 para Windows Server 2008 e Windows Vista é compatível com ISATAP tanto como host ISATAP quanto roteador ISATAP.

Há uma interface de encapsulamento ISATAP separada para cada interface de rede local instalada no computador com um sufixo DNS diferente. Por exemplo, se um computador executando Windows Vista tiver duas interfaces de rede e ambas forem conectadas à mesma intranet e receberem o mesmo sufixo DNS, haverá somente uma interface de encapsulamento ISATAP. Se essas duas interfaces de rede estiverem conectadas a duas redes diferentes com sufixos DNS distintos, haverá duas interfaces de encapsulamento ISATAP.

Para computadores executando Windows Server 2008 ou Windows Vista SP1, as interfaces de encapsulamento ISATAP serão posicionadas em um estado sem conexão de mídia, a não ser que o nome "ISATAP" possa ser resolvido.

Por padrão, o protocolo IPv6 para Windows Vista sem service packs instalado configura automaticamente endereços ISATAP de link local (FE80::5EFE:w.x.y.z ou FE80::200:5EFE:w.x.y.z) nas interfaces de encapsulamento ISATAP para endereços IPv4 para os quais foram atribuídas as interfaces de rede local correspondentes.

Para receber do roteador ISATAP uma mensagem de anúncio de roteador, o host ISATAP deverá enviar ao roteador ISATAP uma mensagem de solicitação do roteador. Em uma sub-rede local, um host IPv6 nativo enviará uma mensagem multicast de solicitação para o roteador, então, os roteadores na sub-rede responderão a uma mensagem de anúncio de roteador.

Como o ISATAP não usa tráfego multicast IPv4, o host ISATAP deve transmitir em unicast a mensagem de solicitação do para o roteador ISATAP. Para transmitir em unicast a mensagem de solicitação ao roteador ISATAP, o host ISATAP deve primeiro determinar o endereço IPv4 unicast da interface do roteador na sub-rede ISATAP lógica.

Para o protocolo IPv6 do Windows Server 2008 e Windows Vista, um host ISATAP obterá o endereço IPv4 unicast do roteador ISATAP através da resolução bem-sucedida do nome de host "ISATAP" para um endereço IPv4 ou com o comando netsh interface isatap set router.

## 6to4

O 6to4 é uma técnica de encapsulamento descrita na RFC 3056. Quando o 6to4 é usado, o tráfego IPv6 é encapsulado com um cabeçalho IPv4 antes de ser enviado pela Internet IPv4.

O 6to4 usa o prefixo de endereço global 2002:WWXX:YYZZ::/48, onde WWXX:YYZZ é a parte da identificação da agregação do próximo nível (NLA ID) de um endereço global e também a representação hexadecimal com dois -pontos de um endereço IPv4 público (w.x.y.z) atribuído ao site ou host.

O endereço 6to4 completo de um host 6to4 é:

2002:WWXX:YYZZ:[Identificação\_da\_SLA]:[Identificação\_da\_Interface].

A RFC 3056 define os seguintes termos:

- Host 6to4:

Um host IPv6 configurado com, no mínimo, um endereço 6to4 (um global address com o prefixo 2002::/16). Hosts 6to4 não precisam de configuração manual, o endereçamento é obtido utilizando os mecanismos de configuração automática.

- Roteador 6to4:

Um roteador 6to4 que cria túneis 6to4 e é utilizado para encaminhar pacotes 6to4 entre hosts em um site ou para outros roteadores 6to4. Ele também é utilizado para encaminhar pacotes para roteadores de retransmissão (relay) quando o tráfego for destinado a redes IPv6.

- Roteador de retransmissão 6to4 (relay):

Um roteador IPv4/IPv6 que encaminha pacotes 6to4 dos roteadores 6to4 na Internet IPv4 para os hosts na Internet IPv6.

Quando você usa hosts 6to4, uma infraestrutura de roteamento IPv6 em sites 6to4, um roteador 6to4 na borda da rede e um roteador de retransmissão 6to4, os seguintes tipos de comunicação são possíveis:

- Um host 6to4 pode se comunicar com um outro host 6to4 no mesmo site (Host A > Host B).

Esse tipo de comunicação está disponível através da infraestrutura de roteamento IPv6, que fornece acessibilidade a todos os hosts no site.

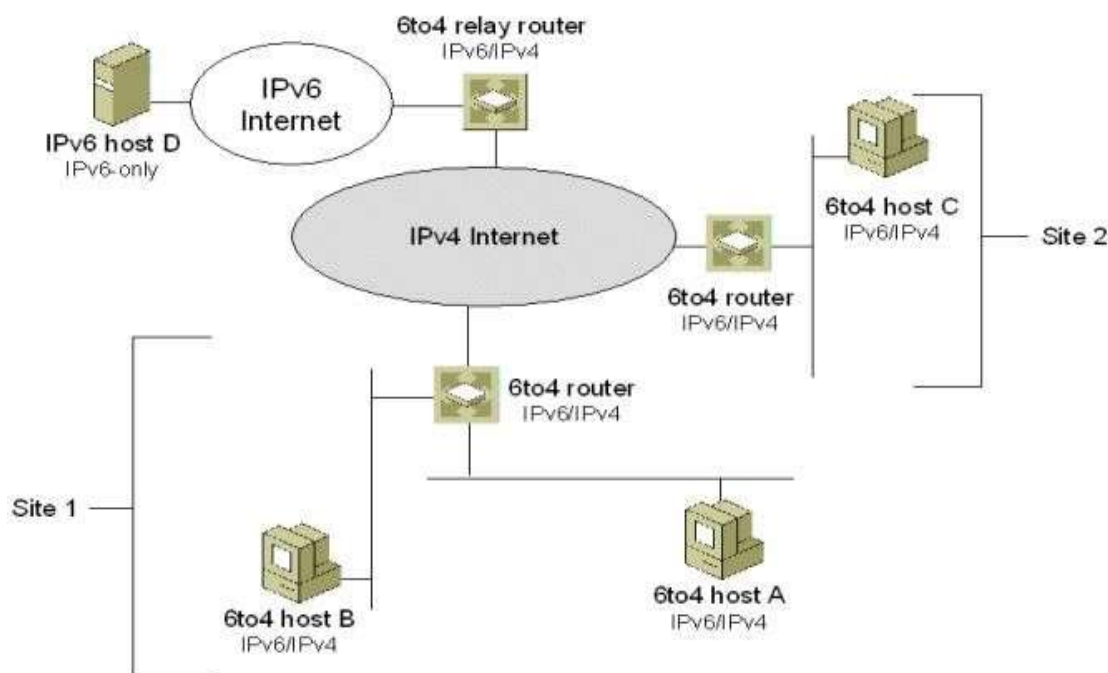
- Um host 6to4 pode se comunicar com outros hosts 6to4 em outros sites da Internet IPv4 (Host A > Host C).

Esse tipo de comunicação ocorre quando um host 6to4 encaminha o tráfego IPv6 destinado a um host 6to4 de outro site para o roteador 6to4 do site local. O roteador 6to4 do site local encapsula o tráfego IPv6 com um cabeçalho IPv4 e o envia ao roteador 6to4 no site de destino na Internet. O roteador 6to4 no site de destino remove o cabeçalho IPv4 e encaminha o pacote IPv6 para o host 6to4 apropriado usando a infraestrutura de roteamento IPv6 do site de destino.

- Um host 6to4 pode se comunicar com hosts na Internet IPv6 (Host A > Host D).

Esse tipo de comunicação ocorre quando um host 6to4 encaminha o tráfego IPv6 destinado a um host Internet IPv6 para o roteador 6to4 do site local. O roteador 6to4 do site local encapsula o tráfego IPv6 com um cabeçalho IPv4 e o envia a um roteador de retransmissão 6to4 conectado à Internet IPv4 e Internet IPv6. O roteador de retransmissão 6to4 remove o cabeçalho IPv4 e encaminha o pacote IPv6 para a Internet IPv6 apropriado usando a infraestrutura de roteamento IPv6.

Os três tipos de comunicação podem ser identificados na figura abaixo:



Todos esses tipos de comunicações usam o tráfego IPv6 sem precisar obter uma conexão direta com a Internet IPv6 ou um prefixo de endereço global IPv6 de um provedor de serviços de Internet (ISP). Suporte ao 6to4 no Vista e Server 2008

Um computador rodando Windows Server 2008 ou Windows Vista podem atuar como um roteador 6to4 simplesmente habilitando o ICS (Internet Connection Sharing). Se o ICS estiver habilitado em uma interface de rede com um endereço IPv4 público, o componente 6to4 automaticamente:



- Habilita o encaminhamento de pacotes IPv6 nas interfaces de rede privada e de tunelamento 6to4
- Determina um prefixo IPv6 de 64 bits para fazer o anúncio na rede interna.
- Habilita o anúncio (Router Advertisement) na interface de rede privada.

## Teredo

Teredo, também conhecido como NAT IPv4 para IPv6, fornece endereçamento e tunelamento host-to-host para tráfego IPv6 através da internet IPv4, mesmo quando os hosts IPv6/IPv4 estiverem atrás de NATs IPv4. Para atravessar o NAT IPv4, os pacotes IPv6 são enviados utilizando UDP.

6to4 fornece funcionalidades similares ao Teredo. No entanto, para habilitar o 6to4 é necessário um roteador conectado à internet com suporte ao serviço, e as funcionalidade dos roteadores 6to4 não são suportadas por todas as implementações NATs IPv4. Mesmo que o NAT tenha suporte ao 6to4, ele não conseguiria passar por mais de um NAT.

O Teredo resolve esse falha funcional do 6to4 onde é necessário trabalhar com várias camadas de NAT criando túneis para o encaminhamento de pacotes IPv6 entre os hosts, em contraste com o 6to4 que criava túneis entre os roteadores.

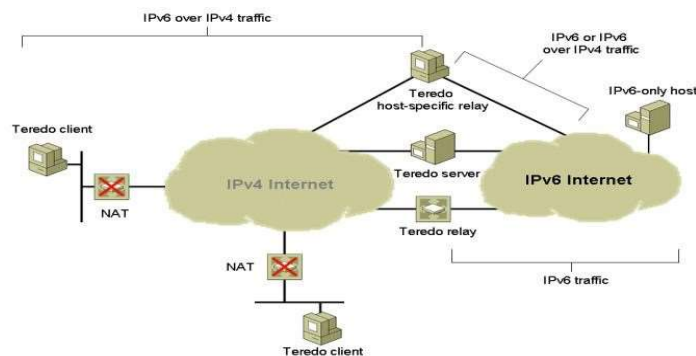
O tunelamento a partir dos hosts apresenta um outro cenário para o NAT: os pacotes IPv6 encapsulados em IPv4 apresentam no campo protocolo o valor 41. A maioria dos NATs somente faz o encaminhamento dos protocolos TCP e UDP. Para que um NAT faça o encaminhamento de outros tipos de protocolos, eles devem ser configurados manualmente ou em alguns casos é necessário instalar algum componente extra.

Devido ao protocolo 41 não ser um protocolo padrão utilizando pelo NAT para o encaminhamento, os pacotes IPv6 encapsulados em IPv4 não seriam ser encaminhados pelo NAT.

No entanto, o pacote IPv6 é encapsulado como um pacote do tipo mensagem UDP IPv4, contendo os cabeçalhos IPv4 e UDP. As mensagens UDP podem são encaminhadas pela maioria dos NATs.

O Teredo é uma tecnologia que foi desenvolvida como último recurso para conectividade IPv6. Caso exista a implementação do IPv6, ISATAP ou 6to4, o Teredo não é utilizado. Quanto mais equipamentos que fazem NAT tiverem suporte a IPv6 ou 6to4, menos uso faremos do Teredo.

## Componentes de uma infraestrutura com Teredo



- **Cliente Teredo:**

Um nó IPv6/IPv4 que tem suporte a interface de tunelamento Teredo que é utilizada para encaminhar pacotes para outros clientes Teredo (host-to-host) ou para clientes IPv6 na internet através de um retransmissor (relay) (host-to-router).

- **Servidor Teredo:**

Um nó IPv6/IPv4 que é conectado em redes IPv4 e IPv6. O servidor Teredo é responsável por auxiliar a configuração inicial dos clientes e facilitar o estabelecimento da conexão entre eles.

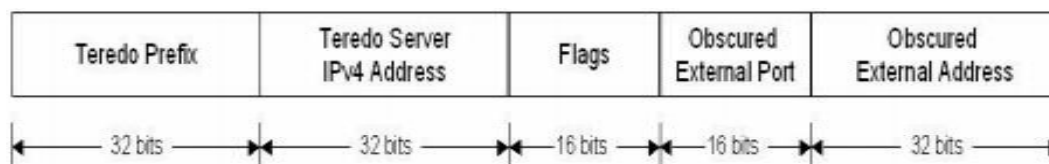
- **Retransmissor Teredo (relay):**

Um roteador IPv6/IPv4 que pode criar túneis host-to-router e router-to-host para encaminhar pacotes entre clientes Teredo em uma rede IPv4 e uma rede IPv6.

- **Host retransmissor específico Teredo (host-specific relay):**

Um nó IPv6/IPv4 que é conectado em redes IPv4 e IPv6 e pode se comunicar diretamente com clientes Teredo sem a necessidade de um retransmissor Teredo. A conexão com uma rede IPv4 pode ser utilizando endereçamento público ou privado, e a conexão com uma rede IPv6 pode ser através do endereçamento IPv6 nativo ou 6to4.

### O formato do endereçamento Teredo



Um endereço Teredo consiste de:

- **Prefixo Teredo:**

Os primeiros 32 bits são para o prefixo Teredo, que é o mesmo para todos os endereços Teredo. O espaço de endereço 2001::/32 foi reservado pelo IANA na RFC 4380.

- **Endereço IPv4 do Servidor Teredo:**

Os próximos 32 bits contém o endereço público IPv4 do servidor Teredo que auxiliou a configuração deste endereço Teredo.

- **Flags:**

Os próximos 16 bits são reservados para flags Teredo. Os 16 bits consistem do seguinte: CRAAAAUG AAAAAAAAAA. O bit C é par AA flag “Cone” é definida quando um cliente está atrás de um NAT Cone. O bit R é reservado para uso futuro. O bit U é para a flag Universal/Local (definida em 0). O bit G é para a flag Individual/Group (definida em 0). Os bits A são uma sequência gerada aleatória.

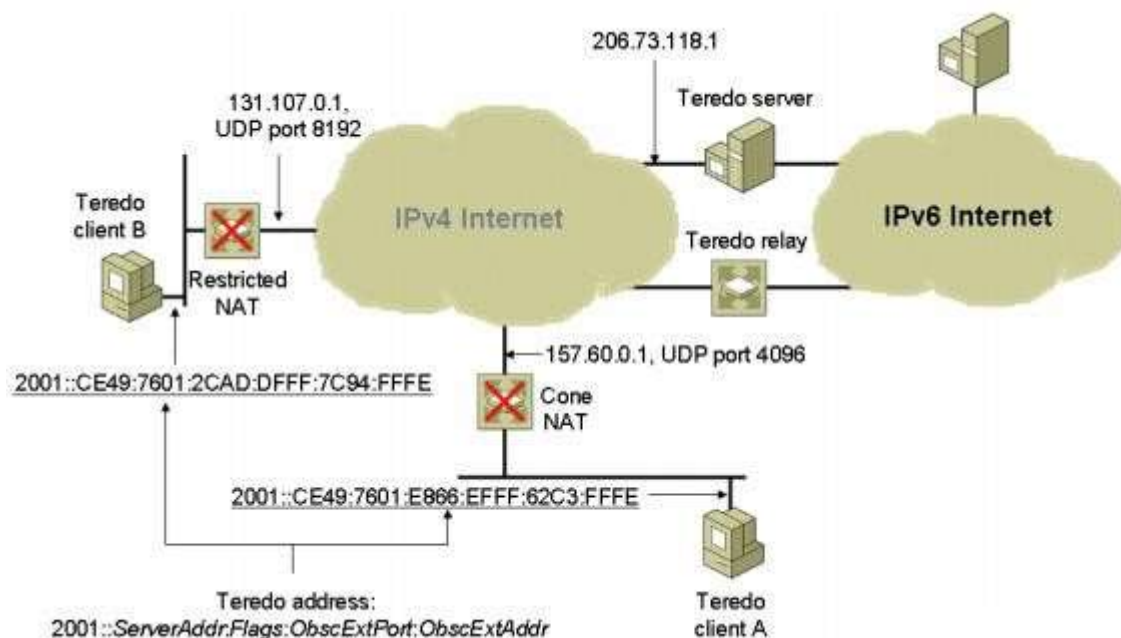
- Porta externa (obscura):

Os próximos 16 bits armazenam uma versão obscura (oculta) das portas externas que corresponde as portas UDP utilizadas para tráfego pelo cliente Teredo. Quando um cliente Teredo envia um pacote de início de conexão para um servidor Teredo, a porta de origem do pacote é mapeada pelo NAT para uma porta externa diferente. Todo tráfego Teredo para os hosts utilizam uma mesma porta UDP externa.

- Endereço externo (obscuro):

Os últimos 32 bits armazenam uma versão obscura (oculta) do endereço IPv4 externo utilizando pelo cliente Teredo. Da mesma forma que a porta obscura (oculta), quando o Teredo cliente envia um pacote de início de conexão para o servidor Teredo, o NAT mapeia o IP do pacote para um endereço externo diferente.

### Exemplo de endereçamento Teredo



Normalmente o Teredo é reconfigurado ou desabilitado em alguns cenários onde outras tecnologias (ISATAP, 6to4 ou IPv6) estão em uso. Existem 3 maneiras de fazer isso:

- Informando o IP do servidor de Teredo manualmente através do comando netsh.
- Desabilitando o Teredo através do comando netsh.
- Desabilitando o Teredo através de chave de registro.