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.

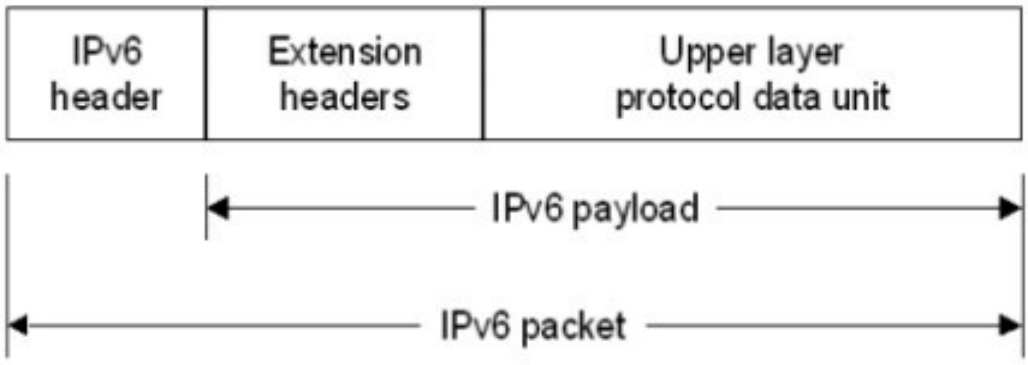
O IPv4 não tem capacidade para atender a demanda por acesso e serviços gerada pelos computadores e dispositivos móveis que temos hoje. O número de usuários vem crescendo de forma rápida, e o resultado disso é não somente o esgotamento de endereços, mas também a falta ou inadequação de recursos necessários 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
Source Address	Um endereço IP de 128 bits que identifica a origem do pacote.
Destination Address	Um endereço IP de 128 bits que identifica o destino do pacote.
Next Header	Um identificador para o próximo extension header (ou cabeçalho de extensão
Hop Limit	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 Listner 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 x 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.

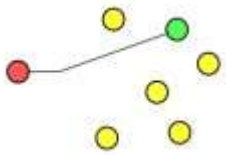
- Header aprimorado

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 fora retiradas e alocadas no extension header (cabeçalho de extensão).

Unicast, Multicast e Anycast

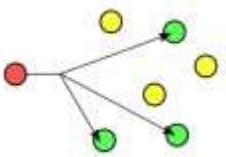
O IPv6 pode utilizar várias formas de transmissão de dados para comunicação entre hosts. A grande diferença aqui é a ausência do broadcast que tínhamos no IPv4 e deu lugar ao Anycast. Abaixo segue a descrição das funcionalidades de cada tipo de transmissão.

Unicast



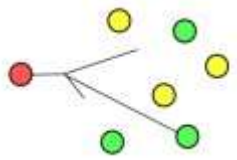
A transmissão utilizando unicast da mesma forma que no IPv4 é utilizada quando um host envia um pacote direto para outro host, uma comunicação do tipo ponto-a-ponto. É a forma padrão e mais comum de transmissão em uma rede.

Multicast



O multicast no IPv6, assim como no IPv4 é utilizando 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 trafego 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 é 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.

Alocação	Formato do Prefixo	Fração do espaço de endereço
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

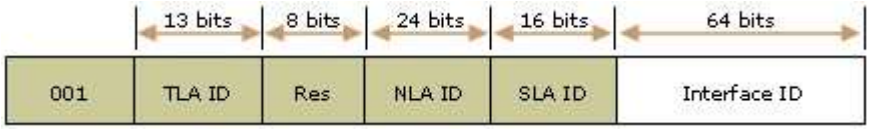
Global Unicast Address

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

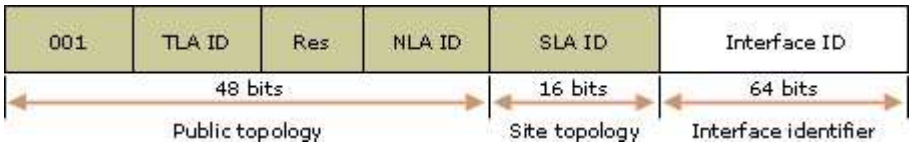
O campo SLA ID indica o identificador de agregação do nível do site (SLA ID) do endereço. Ele é usado por uma organização individual para identificar sub-redes em seu site. O tamanho deste campo é 16 bit s. A organização pode usar esses 16 bits em seu site para criar 65.536 sub-redes ou vários níveis 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

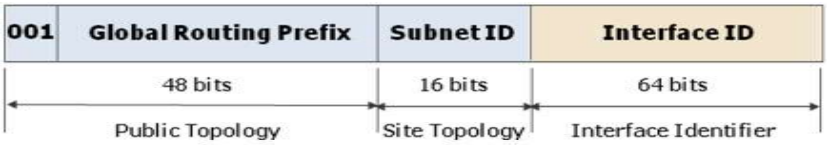
O campo Interface ID indica a interface de um nó em uma sub-rede específica. O tamanho deste campo é 64 bits.

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.

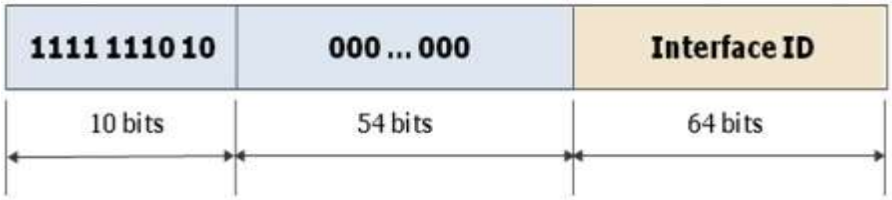
Um roteador IPv6 nunca encaminha o tráfego de conexão local para fora dos limites da sub-rede local.

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).

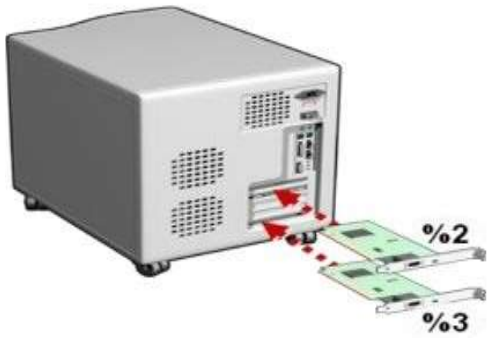
Por exemplo, as intranets privadas que não têm uma conexão roteada direta com a Internet IPv6 podem usar endereços de sites locais sem entrar em conflito com endereços globais de difusão ponto a ponto agregáveis. Os endereços de sites locais não podem ser acessados em outros sites e os roteadores não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

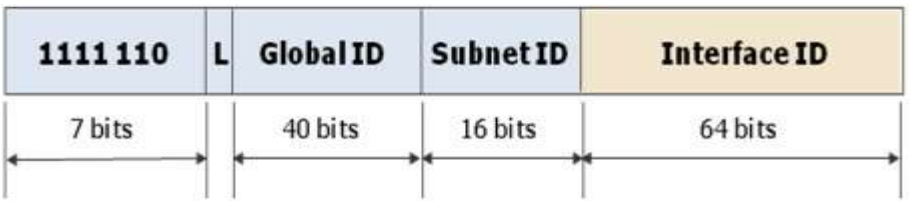
No caso de um computador possuir 2 interfaces de rede, cada uma dessas interfaces terá o seu Zone ID.

Sempre que você for utilizar endereços Link-Local para comunicação é importante lembrar que você deve utilizar o Zone ID da maquina 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 especifico 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

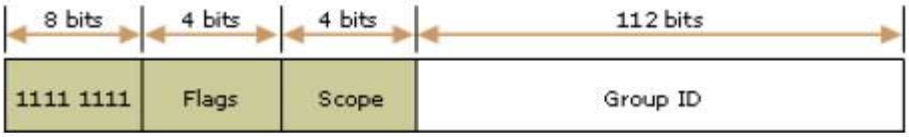
  O endereço de auto-retorno (0:0:0:0:0:0:0:1 ou ::1) é usado para identificar uma interface de auto -retorno, permitindo que um nó envie pacotes para si próprio. Ele equivale ao endereço de auto-retorno IPv4 127.0.0.1. Os pacotes transmitidos ao endereço de autoretorno nunca são enviados em uma conexão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

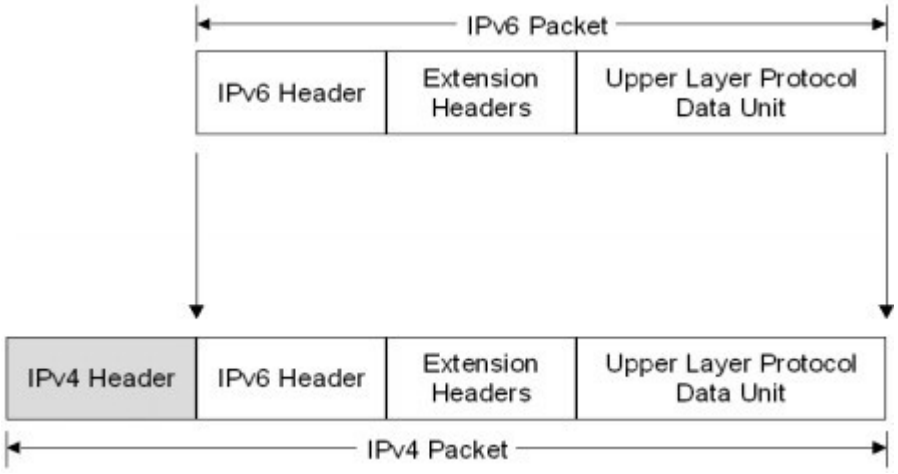
2.5.TEREDO, ISATAP E 6TO4

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-torouter 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.

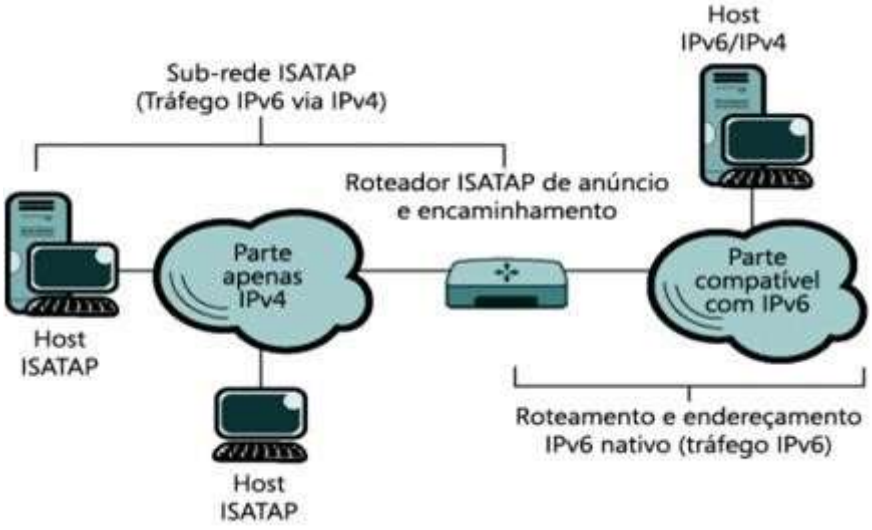
Os hosts ISATAP usam uma interface de encapsulamento lógico para a qual são atribuídos endereços ISATAP, que têm a forma UnicastPrefix:0:5EFE:w.x.y.z (quando w.x.y.z for um endereço IPv4 privado atribuído ao host ISATAP) ou UnicastPrefix:200:5EFE:w.x.y.z (quando w.x. y.z for um endereço IPv4 público 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 subrede ISATAP lógica. Para atingir destinos que estão em outras sub-redes ISATAP ou em subredes 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 do 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 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 Server2008 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 diferent e. 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 quer 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 trafego 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.

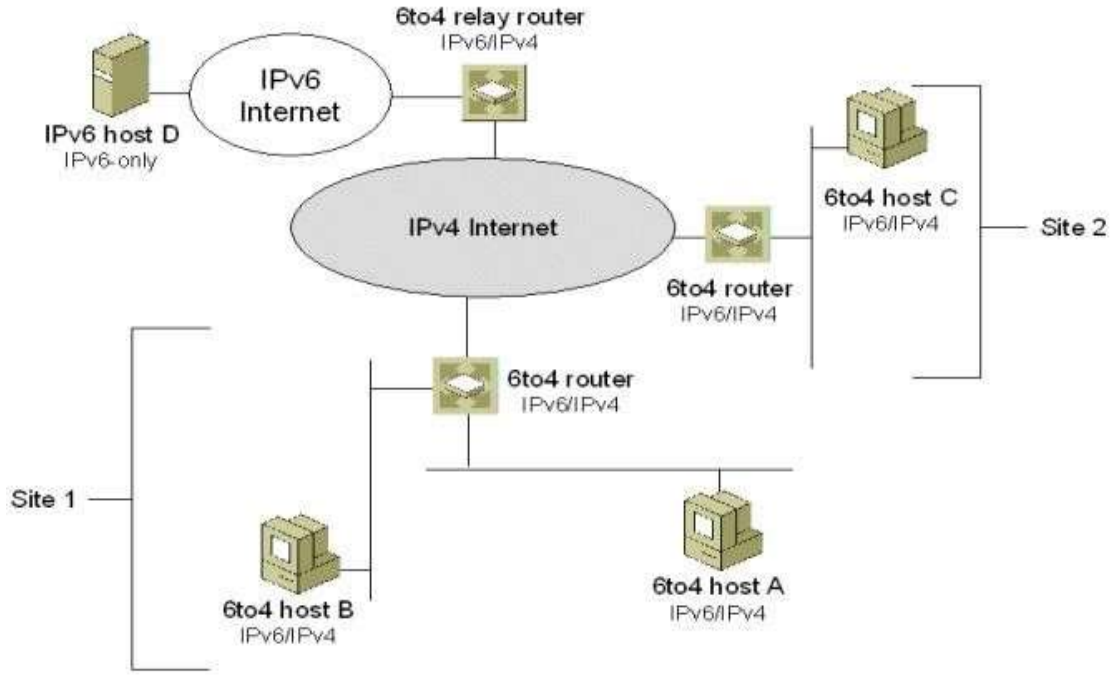
- Um host 6to4 pode se comunicar com outros hosts 6to4 em outros sites da Internet IPv4 (Host A > Host C).

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 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 anuncio na rede interna.
- Habilita o anuncio (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.

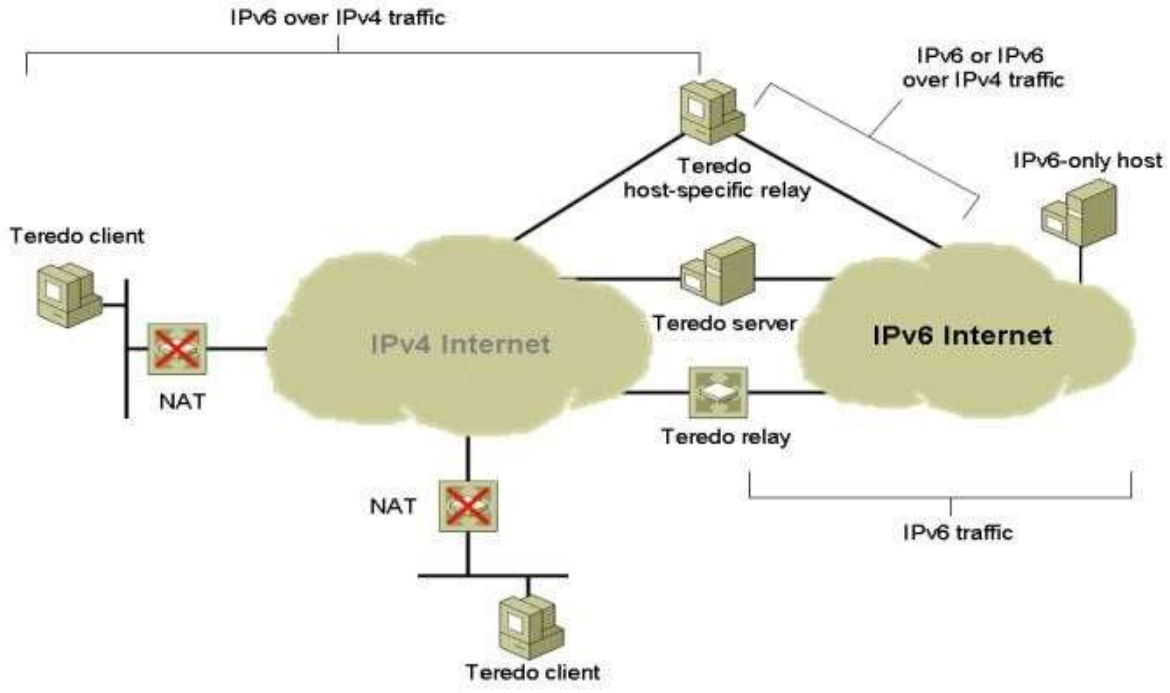
O tunelamento a partir dos hosts apresenta um outro cenário para o NAT: os pacotes IPv6 encapsulados em IPv4 apresentam no campo protocolo o valor 41. A maioria dos NATs somente faz o encaminhamento dos protocolos TCP e UDP. Para que um NAT faça o encaminhamento de outros tipos de protocolos, eles devem 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.

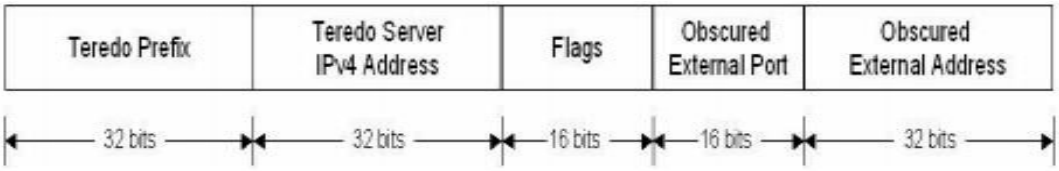
- Retransmissor Teredo (relay):

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 AAAAAAAA. 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.

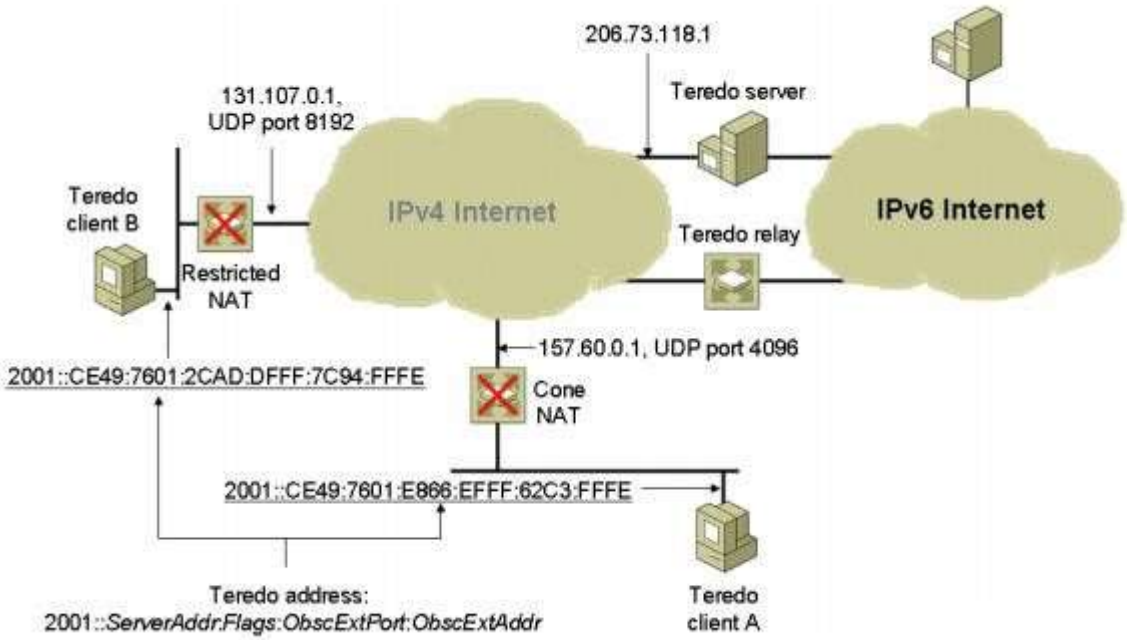
- Porta externa (obscura):

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 inicio de conexão para um servidor Teredo, a porta de origem do pacote é mapeada pelo NAT para uma porta externa diferente. Todo trafego 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 foram que a porta obscura (oculta), quando o Teredo cliente envia um pacote de inicio 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.

2.6. EXERCÍCIOS

1. Quantas camadas encontramos no modelo OSI?

2. Defina a relação das camadas no modelo OSI e no modelo TCP/IP?

3. Qual a utilidade das portas de serviço?

4. Quais as classes de endereço existem?

5. Quais são as classes para os endereços IP: 168.10.1.45, 200.132.73.80 e 130.25.56.2?

6. Quanto bits possui um endereço IPv6 e quantos bits possui um endereço Ipv4?

7. Qual a principal função dos tunelamentos Teredo, ISATAP e 6to4?

Exercício: Calculando uma máscara de sub-rede

1. Determine a potência de 2 que seja dois números acima de 14.

2. Determine o expoente dessa potência de 2, que é o número de bits necessários para a criação da sub-rede.

3. Converta o número necessário de bits no formato decimal da esquerda para direita.

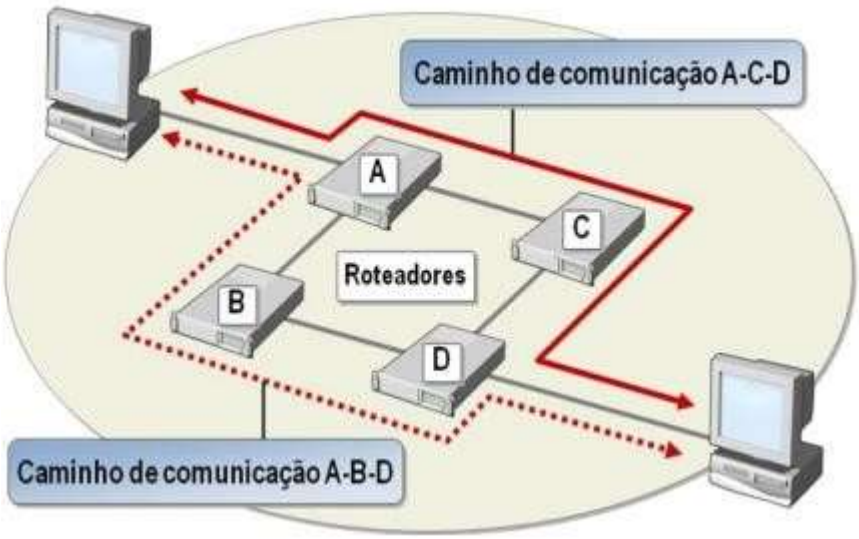
4. Acrescente o número convertido à máscara de sub-rede existente. Qual é a máscara de sub-rede necessária?

5. Liste as primeiras 4 sub-redes criadas a partir da rede 131.107.0.0 utilizando a máscara obtida.

3. MÓDULO 3 - ROTEAMENTO IP

3.1.PRINCÍPIOS DO ROTEAMENTO

Em uma rede com várias sub-redes, os roteadores passam pacotes IP de uma subrede para outra. Esse processo é conhecido como roteamento e é uma função importante do IP. Para tomar decisões relativas a roteamento, o IP consulta uma tabela de roteamento. Para modificar e fazer a manutenção dessas tabelas, você precisa entender como os roteadores usam as tabelas de roteamento em uma conexão entre redes.



A função do roteamento na infraestrutura de rede é fornecer os meios principais de unir duas ou mais sub-redes IP fisicamente separadas em uma rede. A interconexão entre sub-redes IP, permite que os hosts nessas sub-redes se comuniquem, possibilitando aos usuários acesso aos recursos que estão em sub-redes remotas.

Quando um usuário tenta acessar um recurso, o computador cliente deve determinar se o endereço IP que ele está tentado acessar está na sub-rede deste cliente, conhecida como sub-rede local, ou se está em uma sub-rede remota. Se o endereço IP que o usuário está tentando acessar encontra-se na sub-rede local, o cliente pode acessar diretamente o recurso.

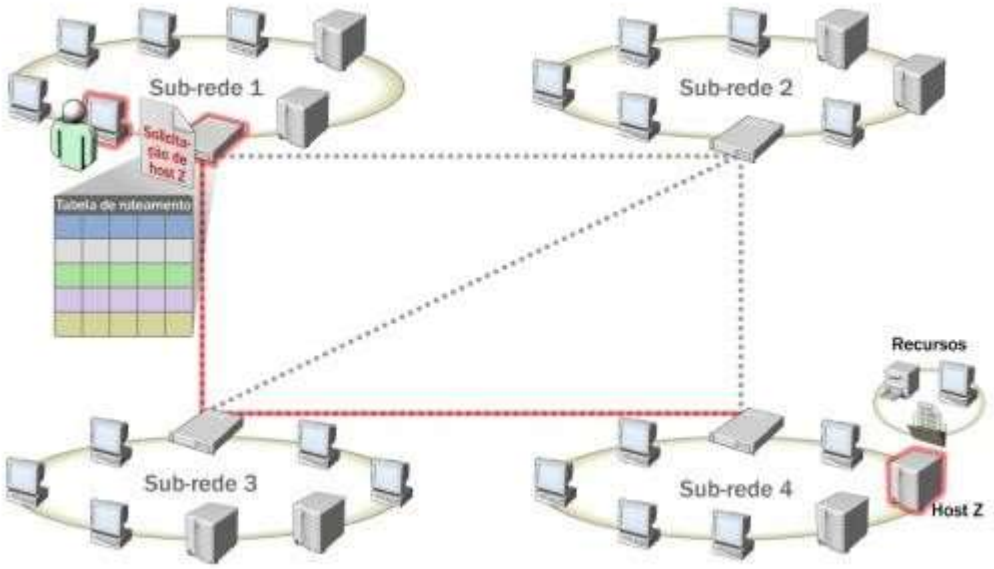
Se o endereço IP que o usuário está tentando acessar não estiver na sub-rede local, a solicitação de conexão deverá ser redirecionada ao roteador (ou gateway padrão). O gateway padrão determina a sub-rede para qual a solicitação deve ser encaminhada.

Se a sub-rede do host remoto estiver diretamente conectada ao roteador, a solicitação será encaminhada ao host remoto, e o usuário poderá acessar o recurso.

No ambiente roteado de uma organização, talvez existam muitas sub-redes conectadas por roteadores.

Se a sub-rede do host remoto não estiver diretamente conectada ao roteador, ele utilizará sua tabela de roteamento para determinar o melhor caminho para o encaminhamento da solicitação.

As tabelas de roteamento armazenam caminhos para as diferente sub-redes e calculam o roteamento mais eficiente para encaminhar a solicitação para a sub-rede apropriada. As informações de tabela de roteamento são compartilhadas entre os roteadores utilizando protocolos de roteamento.



O que é um roteador?

Em uma conexão entre redes, o roteador conecta as sub-redes entre si e também faz a conexão com outras redes. O conhecimento de como o roteador encaminha pacotes de dados a seus endereços IP de destino permite que você verifique se os computadores host de sua rede estão corretamente configurados para transmitir e receber dados.

Os roteadores operam na camada Rede (Layer 3) do modelo de referência OSI (Open Systems Interconnection), de modo que podem conectar redes que executam protocolos com camadas de Enlace (Layer 2) de dados diferentes e diferentes mídias de rede.

Em uma conexão entre redes pequenas, o trabalho de um roteador pode ser bastante simples. Quando duas redes locais são conectadas por um roteador, esse roteador simplesmente recebe pacotes de uma rede e encaminha apenas aqueles que se destinam à outra rede.

Em uma conexão entre redes grandes, os roteadores conectam várias redes diferentes entre si e, em muitos casos, as redes estão conectadas a mais de um roteador. Isso permite que os pacotes escolham caminhos diferentes para chegar a determinado destino. Se um roteador da rede falhar, os pacotes poderão ignorá-lo e, mesmo assim, chegar a seus destinos.

Em uma conexão entre redes complexas, um roteador deve selecionar a rota mais eficiente para levar um pacote a seu destino. Em geral, é o caminho que permite que o pacote alcance o destino com o menor número de saltos (ou seja, passando pelo menor número de roteadores). Os roteadores compartilham com outros roteadores próximos informações sobre as redes às quais estão conectados. Assim, forma-se um desenho composto da conexão entre redes. Em uma conexão entre redes grandes, como a Internet, nenhum roteador possui, sozinho, a imagem completa. Em vez disso, os roteadores trabalham em conjunto, passando cada pacote de um roteador para outro, um salto de cada vez.

Os roteadores usam os endereços IP de destino em pacotes e tabelas de roteamento para encaminhar pacotes entre redes. A tabela de roteamento pode conter todos os endereços da rede e todas as possibilidades de caminhos através da rede, além do custo para alcançar cada rede. Os roteadores roteiam pacotes tomando por base os caminhos disponíveis e seus custos.

3.2.TABELA DE ROTEAMENTO

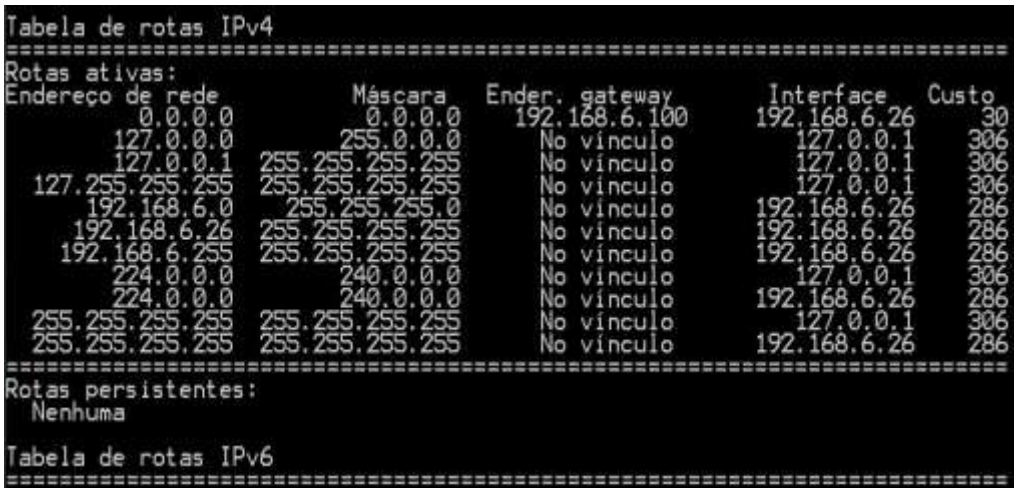
Para tomar decisões de roteamento, o IP consulta uma tabela de roteamento armazenada na memória de um computador host ou roteador.

Como todos os hosts IP realizam alguma forma de roteamento, as tabelas de roteamento não são exclusivas dos roteadores IP.

A tabela de roteamento armazena informações sobre redes IP e como elas podem ser alcançadas, direta ou indiretamente. Existe uma série de entradas padrão, de acordo com a configuração do host, e de entradas adicionais, que podem ser registradas manualmente, com o auxílio dos utilitários TCP/IP, ou de forma dinâmica, por meio de interação com os roteadores. Quando um pacote IP está para ser encaminhado, o roteador usa a tabela de roteamento para determinar:

- O endereço IP de próximo salto. Para uma entrega direta, o endereço IP de encaminhamento é o endereço IP de destino do pacote IP. Para uma entrega indireta, o endereço IP de encaminhamento é o endereço IP de um roteador.

- A interface a ser usada para o encaminhamento. A interface identifica a interface física ou lógica, como um adaptador de rede, que é usada para encaminhar o pacote para seu destino ou para o próximo roteador.



A tabela a seguir lista os campos de uma entrada de rota e descreve as informações que eles contêm.

Campo de Rota	Informações
Identificação de Rede	A identificação de rede ou destino que corresponde à rota. A identificação pode basear-se em classe, uma sub-rede, combinação de redes ou um endereço IP para uma rota de host. Essa é a coluna Endereço de rede.
Máscara	A máscara usada para estabelecer a correspondência entre o endereço IP de destino e a identificação da rede. Essa é a coluna Máscara.
Próximo salto	O endereço IP do próximo roteador para o qual o pacote deve ser encaminhado. Essa é a coluna Gateway.
Interface	Uma indicação de interface que é utilizada para fazer o encaminhamento do pacote. Essa é a coluna Interface.
Métrica	Um número usado para o custo da rota para que se possa escolher a melhor rota. Geralmente utilizado para indicar o número de saltos. Essa é a coluna Custo.

A tabela a seguir descreve os tipos de rotas.

Tipo de Rota	Descrição
Identificação de rede diretamente conectada	Uma rota para identificações de rede que são anexadas diretamente. O campo do próximo pode estar vazio ou conter o endereço IP da interface daquela rede.
Identificação de rede remota	Uma rota para identificações de rede que não estão diretamente conectadas, mas estão disponíveis por intermédio de outros roteadores. O campo Próximo salto é o endereço IP de um roteador local.
Rota de host	Uma rota para um endereço IP específico. As rotas de host permitem que ocorra roteamento em cada endereço IP. A identificação da rede é o endereço IP do host especificado e a máscara de rede é 255.255.255.255.
Rota padrão	A rota que é usada quando uma identificação de rede ou rota de host mais específica não é encontrada. A identificação de rede é 0.0.0.0 com másc ara de rede 0.0.0.0.
Rotas persistentes	Uma rota a que foi adicionada a opção “–p”. Quando usada com o comando Adicionar, essa opção adiciona a rota à tabela de roteamento e a rota é automaticamente adicionada à tabela de roteamento todas as vezes que o protocolo TCP/IP é inicializado.

Para criar ou alterar a tabela de roteamento em um computador ou roteador podemos utilizar algumas ferramentas de configuração. No Windows utilizamos o utilitário route com as seguintes sintaxes para realizar as configurações:

Exibindo uma tabela de roteamento:

Linux: # ***route -n***

Microsot: C:\> ***route print***

Adicionando uma rota: Linux

route add –net <destino> netmask <máscara> gw <gateway>

Exemplo: ***route add -net 10.41.41.0 netmask 255.255.255.0 gw 10.41.42.8***

Microsoft

route add <destino> mask <máscara> <gateway>

Exemplo: ***C:\> route add 192.168.10.0 mask 255.255.255.0 192.168.1.100***

Removendo uma rota:

Microsoft ou Linux route

delete <destino>

Exemplo: ***route delete 192.168.10.0***

3.3.ROTEAMENTO ESTÁTICO E DINÂMICO

Os processos que os roteadores usam para obter informações sobre roteamento variam dependendo caso o roteador realize roteamento IP estático ou dinâmico. O entendimento de cada um desses métodos de roteamento proporciona as informações de que você precisa para fazer a manutenção das tabelas de roteamento de modo que o IP use a rota mais eficiente para transmitir dados a seu destino.

Roteamento estático

O roteamento estático usa tabelas de roteamento fixas. Os roteadores estáticos requerem que você crie e atualize as tabelas manualmente. Os roteadores estáticos:

- Não descobrem as identificações de redes remotas. É preciso configurar essas identificações de rede manualmente.
- Não trocam informações sobre alterações de rota.
- Não compartilham rotas com roteadores dinâmicos.
- Não são tolerantes a falhas. Isso significa que, quando o roteador sai de operação, os roteadores próximos a ele não percebem o defeito e não o informam a outros roteadores.

Roteamento dinâmico

O roteamento dinâmico atualiza automaticamente as tabelas de roteamento. O roteamento dinâmico é uma função dos protocolos de roteamento TCP/IP, como o protocolo RIP (Routing Information Protocol) e OSPF (Open Shortest Path First).

Os roteadores dinâmicos:

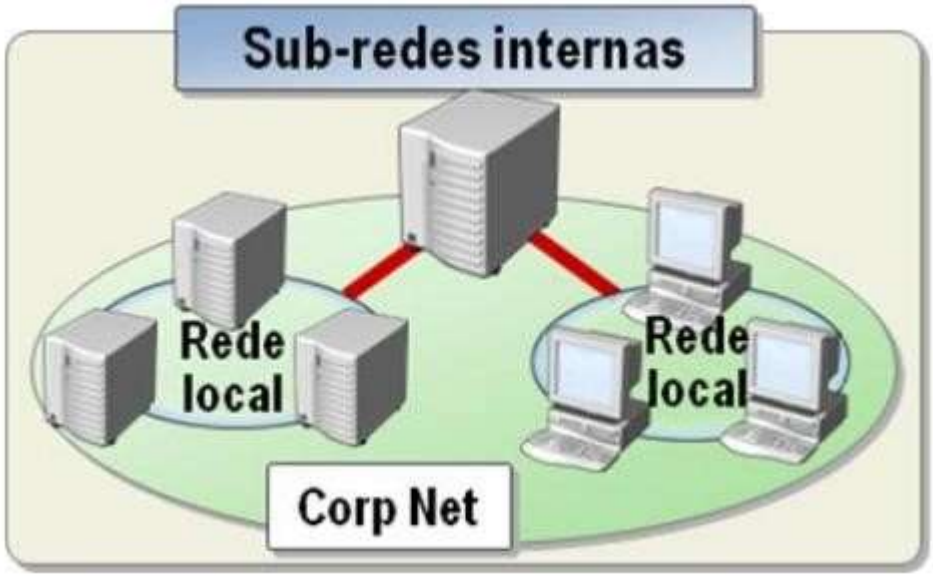
- São capazes de descobrir as identificações de redes remotas.
- Informam automaticamente outros roteadores sobre alterações de rotas.
- Usam protocolos de roteamento para transmitir periodicamente, ou por demanda, os conteúdos de suas tabelas de roteamento para os outros roteadores da rede.
- São tolerantes a falhas (em uma topologia de roteamento com vários caminhos). Quando o roteador sai de operação, o defeito é detectado pelos roteadores próximos a ele que enviam a informação de roteamento alterada para os outros roteadores da conexão entre redes.

3.4.RIP, OSPF E EIGRP

RIP (Routing Information Protocol)

Com o crescimento da rede e consequentemente das tabelas de roteamento, foi necessário a implantação de protocolos de roteamento hierárquicos. Assim os roteadores foram divididos em regiões chamadas Autonomous System - AS, onde cada roteador conhecia todos os detalhes de sua própria região e não conhecia a estrutura interna de outras regiões.

O protocolo RIP (Routing Information Protocol) utiliza o algoritmo vetor-distância. Este algoritmo é responsável pela construção de uma tabela que informa as rotas possíveis dentro do AS.



Algoritmo Vetor-Distância

Os protocolos baseados no algoritmo vetor-distância partem do princípio de que cada roteador do AS deve conter uma tabela informando todas as possíveis rotas dentro deste AS. A partir desta tabela o algoritmo escolhe a melhor rota e o enlace que deve ser utilizado. Estas rotas formam uma tabela.

Cada uma destas rotas contém as seguintes informações

- Endereço -> IP da rede;
- Roteador -> Próximo roteador da rota de destino;
- Interface -> O enlace utilizado para alcançar o próximo roteador da rota de destino;
- Métrica -> Número indicando a distância da rota (0 a 15), sendo uma rota com métrica 16 considerada uma rota infinita;
- Tempo -> Quando a rota foi atualizada pela última vez;

O protocolo RIP utiliza o conceito de broadcast, desta forma um roteador envia sua tabela para todos os seus vizinhos em intervalos predefinidos de tempo (geralmente 30 segundos). Estas mensagens fazem com que os roteadores vizinhos atualizem suas tabelas e que por sua vez serão enviadas aos seus respectivos vizinhos.

Os pacotes RIP são transmitidos através de UDP e IP, usando a porta 520 do UDP tanto para transmissão quanto para recepção. Se uma rota não é atualizada dentro de 180 segundos, sua distância é colocada em infinito e a entrada será mais tarde removida das tabelas de roteamento.

O tempo de convergência é importante para que a rede não fique desatualizada. Para isso existem algumas implementações a respeito de rotas muito grandes. Algumas delas são o método Split Horizon, Split Horizon With Poisonous Reverse e Triggered Update.

Split horizon (horizonte dividido)

Com esta técnica o roteador registra a interface através da qual recebeu informações sobre uma rota e não difunde informações sobre esta rota, através desta mesma interface. No nosso exemplo, o Roteador B receberia informações sobre a rota para a rede 1, a partir do Roteador B, logo o Roteador A não iria enviar informações sobre Rotas para a rede 1, de volta para o Roteador B. Com isso já seria evitado o problema do count-to-infinity. Em outras palavras, esta característica pode ser resumida assim: Eu aprendi sobre uma rota para a rede X através de você, logo você não pode aprender sobre uma rota para a rede X, através de minhas informações.

Split horizon with poison reverse (Inversão danificada)

Nesta técnica, quando um roteador aprende o caminho para uma determinada rede, ele anuncia o seu caminho, de volta para esta rede, com um hope de 16. No exemplo da Figura anterior, o Roteador B, recebe a informação do Roteador A, que a rede 1 está a 1 hope de distância. O Roteador B anuncia para o roteador A, que a rede 1 está a 16 hope de distância. Com isso, jamais o Roteador A vai tentar achar um caminha para a rede 1, através do Roteador B, o que faz sentido, já que o Roteador A está diretamente conectado à rede 1.

Triggered updates (Atualizações instantâneas)

Com esta técnica os roteadores podem anunciar mudanças na métrica de uma rota imediatamente, sem esperar o próximo período de anuncio. Neste caso, redes que se tornem indisponíveis, podem ser anunciadas imediatamente com um hope de 16, ou seja, indisponível.

Esta técnica é utilizada em combinação com a técnica de inversão danificada, para tentar diminuir o tempo de convergência da rede, em situações onde houve indisponibilidade de um roteador ou de um link. Esta técnica diminui o tempo necessário para convergência da rede, porém gera mais tráfego na rede.

Apesar do protocolo RIP apresentar uma série de benefícios e auxiliar na configuração do roteamento de redes que começam a crescer, ele apresenta alguns problemas devido a suas características de funcionamento.

Problemas do Protocolo RIPv1

O protocolo RIP v1 usa broadcast para fazer anúncios na rede:

Com isto, todos os hosts da rede receberão os pacotes RIP e não somente os hosts habilitados ao RIP. Uma contrapartida do uso do Broadcast pelo protocolo RIP v1, é que isso torna possível o uso dos chamados hosts de RIP Silencioso (Silent RIP). Um computador configurado para ser um Silent RIP, processa os anúncios do protocolo RIP (ou seja, reconhece os pacotes enviados pelo RIP e é capaz de processá-los), mas não anuncia suas próprias rotas. Esta funcionalidade pode ser habilitada em um computador que não esteja configurado como roteador, para produzir uma tabela de roteamento detalhada da rede, a partir das informações obtidas pelo processamento dos pacotes do RIP.

A máscara de sub-rede não é anunciada juntamente com as rotas

Isso porque o protocolo RIP v1 foi projetado em 1988, para trabalhar com redes baseadas nas classes padrão A, B e C, ou seja, pelo número IP da rota, deduzia-as a respectiva classe. Com o uso da Internet e o uso de um número variável de bits para a máscara de sub-rede (número diferente do número de bits padrão para cada classe), esta fato tornou-se um problema sério do protocolo RIP v1.

Sem proteção contra roteadores não autorizados

O protocolo RIP v1 não apresenta nenhum mecanismo de autenticação e proteção, para evitar que roteadores não autorizados possam ser inseridos na rede e passar a anunciar várias rotas falsas. Ou seja, qualquer usuário poderá instalar um roteador com RIP v1 e adicionar várias rotas falsas, que o RIP v1 se encarregará de repassar estas rotas para os demais roteadores da rede.

Devido a essas fragilidades na implementação do RIP v1, foi desenvolvido o protocolo RIPv2 que traz algumas melhorias em relação ao seu antecessor.

Melhorias implementadas no RIP v2

Os anúncios do protocolo RIP v2 são baseados em tráfego multicast

O protocolo RIP v2 utiliza o endereço de multicast 224.0.0.9. Com isso os roteadores habilitados ao RIP atuam como se fossem (na verdade é) um grupo multicast, registrado para "escutar" os anúncios do protocolo RIP v2. Outros hosts da rede, não habilitados ao RIP v2, não serão "importunados" pelos pacotes do RIP v2. Por questões de compatibilidade (em casos onde parte da rede ainda usa o RIP v1), é possível utilizar broadcast com roteadores baseados em RIP v2.

Informações sobre máscara são enviadas nos anúncios do protocolo RIP v2

Com isso o RIP v2 pode ser utilizado, sem problemas, em redes que utilizam subnetting, supernetting e assim por diante, uma vez que cada rede fica perfeitamente definida pelo número da rede e pela respectiva máscara de sub-rede.

Segurança, autenticação e proteção roteadores não autorizados

Com o RIP v2 é possível implementar um mecanismo de autenticação, de tal maneira que os roteadores somente aceitem os anúncios de roteadores autenticados, isto é,

identificados. A autenticação pode ser configurada através da definição de uma senha ou de mecanismos mais sofisticados como o MD5 (Message Digest 5). Por exemplo, com a autenticação por senha, quando um roteador envia um anúncio, ele envia juntamente a senha de autenticação. Outros roteadores da rede, que recebem o anúncio, verificam se a senha está OK e somente depois da verificação, alimentam suas tabelas de roteamento com as informações recebidas.

É importante salientar que tanto redes baseadas no RIP v1 quanto no RIP v2 são redes chamadas planas (flat). Ou seja, não é possível formar uma hierarquia de roteamento, baseada no protocolo RIP. Por isso que o RIP não é utilizado em grandes redes. A tendência natural do RIP, é que todos os roteadores sejam alimentados com todas as rotas possíveis (isto é um espaço plano, sem hierarquia de roteadores).

Imagine como seria utilizar o RIP em uma rede como a Internet, com milhões e milhões de rotas possíveis, com links caindo e voltando a todo momento? Impossível. Por isso que o uso do RIP (v1 ou v2) somente é indicado para pequenas redes.

Enquanto a funcionalidade básica do RIP versão 1 é fácil de configurar e implantar, a capacidade do RIP versão 2 e a capacidade avançada do RIP, como segurança de mesmo nível e filtragem de rotas, requerem configuração e testes adicionais.

Para facilitar a identificação e a solução de problemas, recomenda-se implantar seu conjunto de redes baseado no RIP nos seguintes estágios:

1. Configurar o RIP básico e certificar-se de que ele está funcionando.

2. Adicionar um recurso avançado de cada vez, testando após a adição de cada recurso.

Implantando o RIP

Para implantar o RIP no Windows Server, você pode seguir estas etapas:

1. Desenhe um mapa da topologia do conjunto de redes IP que mostre as redes distintas e a localização de roteadores e hosts (computadores não roteadores que executam o TCP/IP).

2. Para cada rede IP (um sistema de cabeamento limitado por um ou mais roteadores), atribua uma identificação de rede IP exclusiva (também conhecida como endereço de rede
IP).

3. Atribua endereços IP a cada interface de roteador. É uma prática comum na indústria atribuir os primeiros endereços IP de uma rede IP a interfaces de roteadores. Por exemplo, para uma identificação de rede IP 192.168.100.0 com uma máscara de sub-rede 255.255.255.0, o endereço IP 192.168.100.1 é atribuído à interface do roteador.

4. Para cada interface de roteador, defina se essa interface será configurada para RIP v1 ou RIP v2. Se uma interface estiver configurada para RIP v2, defina se os anúncios RIP v2 serão feitos por difusão ou por multicast.

5. Usando o Roteamento de acesso remoto, adicione o protocolo de roteamento RIP e configure as interfaces apropriadas para RIP v1 ou RIP v2 de cada servidor que execute o Roteamento e acesso remoto.

6. Quando a configuração estiver concluída, conceda alguns minutos para que os roteadores atualizem as tabelas de roteamento uns dos outros e, em seguida, teste o conjunto de redes.

Para obter mais informações, consulte a documentação do RIP online em: http://technet.microsoft.com/pt-br/library/cc778135.aspx

Testando um conjunto de redes RIP

Para testar seu conjunto de redes RIP, você pode seguir estas etapas:

1. Para verificar se servidor que executa o Roteamento e acesso remoto está recebendo anúncios RIP de todos os roteadores RIP vizinhos, exiba os vizinhos RIP do roteador.

2. Para cada roteador RIP, exiba a tabela de roteamento e verifique se todas as rotas que deveriam ser conhecida s a partir do RIP estão presentes.

3. Use os comandos ping e tracert para testar a conectividade entre os computadores hosts a fim de verificar todos os caminhos de roteamento.

OSPF (Open Shortest Path First)

O protocolo OSPF (Open Shortest Path First) é a alternativa para redes de grande porte, onde o protocolo RIP não pode ser utilizado, devido a suas características e limitações.

O OSPF permite a divisão de uma rede em áreas e torna possível o roteamento dentro de cada área e entre as diferentes áreas, usando os chamados roteadores de borda. Com isso, usando o OSPF, é possível criar redes hierárquicas de grande porte, sem que seja necessário que cada roteador tenha uma tabela de roteamento gigantesca, com rotas para todas as redes, como seria necessário no caso do RIP.

O OSPF é projetado para intercambiar informações de roteamento em uma interconexão de rede de tamanho grande ou muito grande, como por exemplo, a Internet.

A maior vantagem do OSPF é que ele é eficiente em vários pontos: requer pouquíssima sobrecarga de rede mesmo em interconexões de redes muito grandes, pois os roteadores que usam OSPF trocam informações somente sobre as rotas que sofreram alterações e não toda a tabela de roteamento, como é feito com o uso do RIP.

Sua maior desvantagem é a complexidade: requer planejamento adequado e é mais difícil de configurar e administrar do que o protocolo RIP.

O OSPF usa um algoritmo conhecido como Shortest Path First (SPF, primeiro caminho mais curto) para calcular as rotas na tabela de roteamento.

O algoritmo SPF calcula o caminho mais curto (menor custo) entre o roteador e todas as redes da interconexão de redes. As rotas calculadas pelo SPF são sempre livres de loops (laços). O OSPF usa um algoritmo de roteamento conhecido como link-state (estado de ligação). Lembre que o RIP usava um algoritmo baseado em distância vetorial. O OSPF aprende as rotas dinamicamente, através de interação com os roteadores denominados como seus vizinhos.

Em vez de intercambiar as entradas de tabela de roteamento como os roteadores RIP (Router Information Protocol, protocolo de informações do roteador), os roteadores OSPF mantêm um mapa da interconexão de redes que é atualizado após qualquer alteração feita na topologia da rede. Esse mapa, denominado banco de dados do estado de vínculo ou estado de ligação, é sincronizado entre todos os roteadores OSPF e é usado para calcular as rotas na tabela de roteamento. Os roteadores OSPF vizinhos (neghboring) formam uma adjacência, que é um relacionamento lógico entre roteadores para sincronizar o banco de dados com os estados de vínculo.

As alterações feitas na topologia de interconexão de redes são eficientemente distribuídas por toda a rede para garantir que o banco de dados do estado de vínculo em cada roteador esteja sincronizado e preciso o tempo todo.

Ao receber as alterações feitas no banco de dados do estado de vínculo, a tabela de roteamento é recalculada. À medida que o tamanho do banco de dados do estado de vínculo aumenta os requisitos de memória e o tempo de cálculo do roteamento também aumentam. Para resolver esse problema, principalmente para grandes redes, o OSPF divide a rede em áreas (conjuntos de redes contíguas) que são conectadas umas às outras através de uma área de backbone.

Cada roteador mantém um banco de dados do estado de vínculo apenas para aquelas áreas que a ele estão conectadas. Os ABRs (Area Border Routers, roteadores de borda de área) conectam a área de backbone a outras áreas.

Implementando o OSPF

A implantação do OSPF (Open Shortest Path First) requer planejamento cuidadoso e configuração em três níveis:

- O sistema autônomo
- A área
- A rede

Planejando o sistema autônomo

Para o sistema autônomo do OSPF, você precisa:

1. Subdividir o sistema autônomo do OSPF em áreas que possam ser facilmente resumidas usando rotas de resumo.
2. Designar a área de backbone.
3. Atribuir identificações de área.
4. Identificar links virtuais.
5. Identificar roteadores de borda de área (ABRs).
6. Identificar áreas do stub.
7. Identificar roteadores de limite de sistema autônomo (ASBRs).

Planejando cada área

Para cada roteador, você precisa:

1. Adicionar as áreas às quais o roteador está conectado.

2. Se a área for uma área do stub, habilitá-la como uma área do stub.

3. Se o roteador for um ABR, configurar opcionalmente os intervalos que resumem as redes IP dentro da área.

4. Se o roteador for um ABR que usa um link virtual, adicionar a interface virtual.

5. Se o roteador for um ASBR, habilitar o ASBR e configurar filtros de rotas externas opcionais.

Planejando cada rede

Para cada endereço IP de cada interface de roteador que usa o OSPF, você precisa:

1. Adicionar a interface ao protocolo de roteamento OSPF.

2. Habilitar o OSPF na interface.

3. Configurar a interface para a identificação de área apropriada.

4. Configurar a interface para a prioridade de roteador apropriada.

5. Configurar a interface para o custo de link apropriado.

6. Configurar a interface para a senha apropriada.

7. Configurar a interface para o tipo de rede apropriado.

8. Se a interface for uma interface de retransmissão de quadros de adaptador único (ou X.25 ou ATM), configurar os vizinhos de vários acessos sem difusão (NBMA).

Para obter mais informações, consulte a documentação online do OSPF em: http://technet.microsoft.com/pt-br/library/cc778406.aspx.

Testando o OSPF

Para testar seu conjunto de redes OSPF, você pode executar estas etapas:

1. Para verificar se servidor que executa o Roteamento e acesso remoto está recebendo anúncios OSPF de todos os roteadores OSPF adjacentes, exiba os vizinhos OSPF do roteador.

2. Para cada roteador, exiba a tabela de roteamento IP e verifique se todas as rotas que deveriam ser conhecidas do OSPF estão presentes.

3. Use os comandos ping e tracert para testar a conectividade entre os computadores hosts a fim de verificar todos os caminhos de roteamento.

EIGRP (Enhanced Interior Gateway Routing Protocol)

O EIGRP é um protocolo avançado de roteamento por vetor da distância proprietário da Cisco. As principais características do EIGRP são:

- É um protocolo avançado de roteamento por vetor da distância.
- Usa balanceamento de carga com custos desiguais.
- Usa características combinadas de vetor da distância e estado dos links.
- Usa o DUAL (Diffused Update Algorithm – Algoritmo de Atualização Difusa) para calcular o caminho mais curto.
- As atualizações de roteamento são enviadas por multicast usando 224.0.0.10 e são disparadas por alterações da topologia.

3.5. EXERCÍCIOS

1. Quando ocorre um roteamento?

2. Ao visualizar uma tabela de roteamento, como identificar qual é o gateway padrão?

3. Qual a diferença entre o roteamento estático e dinâmico?

Exercício: Alterando a tabela de roteamento

1. Verifique a sua tabela de roteamento e anote aqui quais são as rotas existentes para o seu computador.

2. Crie uma rota para a rede 172.16.0.0/16 apontando para o roteador 192.168.x.100 (onde x é o número da sala).

3. Na rota criada verifique o custo desta rota.

4. Remova a rota criada. Após a remoção verifique se ainda consta na tabela de roteamento.