Protocolo IPV6

O protocolo de internet versão 6 (IPv6), o formato do datagrama, o formato do endereço e os mecanismos de transição e coexistência.

Prof. Isaac Newton Ferreira Santa Rita

Propósito

Compreender os conceitos básicos de endereçamento IPv6 por se tratar do protocolo que irá substituir o IPv4 nas conexões de redes. Além disso, facilitará o desenvolvimento de projetos, a configuração e a manutenção de redes de computadores.

Preparação

Antes de iniciar, é recomendado acesso à internet, por meio de um computador com os softwares Packet Tracer (versão 7.3.0.0838), da Cisco, e Wireshark instalados para realizar as simulações propostas. Além disso, você deve possuir em mãos lápis e caderno para confeccionar cálculos de rede.

Objetivos

- Descrever as características do payload e endereçamento IPv6.
- Esquematizar o endereçamento de redes e sub-redes IPv6.
- Descrever as soluções de integração entre o IPv4 e o IPv6.
- Identificar as funcionalidades do protocolo ICMPv6.

Introdução

Aprenderemos sobre os conceitos fundamentais do protocolo de internet IPv6. Para isso, faremos inicialmente a análise dos elementos componentes da estrutura do IPv6 e como deve ser representado.

Visto isso, apresentaremos como devemos realizar o planejamento de redes IPv6 observando as peculiaridades desse protocolo e realizaremos, de forma prática, a configuração de redes IPv6.

Além disso, identificaremos as principais técnicas de transição e coexistência entre redes IPv4 e redes IPv6, necessárias à manutenção do funcionamento da internet durante o processo de migração entre esses protocolos.

Por fim, mostraremos algumas funcionalidades introduzidas no IPv6, facilitadores da administração de redes que utilizam esse protocolo.

O PROTOCOLO IPv6

Neste vídeo, você entenderá um pouco da importância da criação do protocolo IPv6 em substituição ao protocolo IPv4, garantindo o crescimento da internet e a criação de novas aplicações de rede.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Surgimento do IPv6

Neste vídeo, abordamos o esgotamento dos endereços IPv4 e a transição para o IPv6. Entenda os desafios, benefícios e os passos práticos rumo a uma era de endereçamento IP mais amplo e sustentável.

> **Conteúdo interativo**
>
> Acesse a versão digital para assistir ao vídeo.

Definido na RFC 791 em 1981, o protocolo de internet versão 4 (IPv4) mostrou-se muito robusto, e de fácil implantação e interoperabilidade. Entretanto, seu projeto original não previu o grande crescimento das redes de computadores e um possível esgotamento das faixas de endereçamento IPv4.

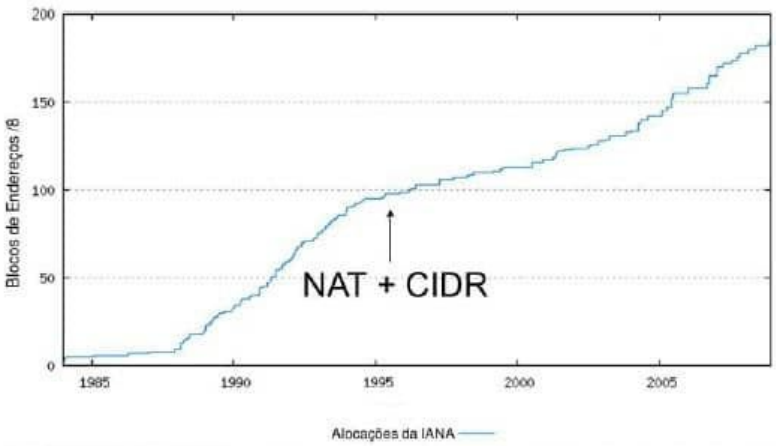
Composto por 32 bits, o IPv4 possui a capacidade de endereçar aproximadamente 4,3 bilhões de dispositivos, que era dado como inalcançável no momento de sua concepção. Porém, o ritmo de crescimento foi assustador: já em 1992, 38% das faixas de endereços classe A, 43% da classe B e 2% da classe C estavam alocados.

Diante desse cenário, técnicas para retardar a exaustão do IPv4 foram implantadas. Entre elas, destacam-se:

- Classless Inter-Domain Routing (CIDR)
- Variable Length Subnet Mask (VLSM)
- Dynamic Host Configuration Protocol (DHCP)
- Networking Address Translation (NAT)

Todas essas técnicas conceberam uma boa sobrevida ao IPv4.

A imagem a seguir apresenta a evolução de entrega de endereços IPv4 classe A ao longo dos anos, e o efeito retardante provocado pelas técnicas citadas anteriormente, principalmente o CIDR e o VLSM.



Esgotamento do IPv4

Em dezembro de 1993, a IETF formalizou, por meio da RFC 1550, as pesquisas a respeito da nova versão do protocolo IP, cujo objetivo consistia na criação de um novo protocolo IP de próxima geração com as seguintes funcionalidades:

- Escalabilidade
- Segurança
- Configuração e administração de rede
- Suporte a QoS
- Mobilidade
- Políticas de roteamento
- Transição

Em dezembro de 1998, foi concebida a RFC 2460, versando sobre o IPv6, evidenciando-se:

Maior capacidade para endereçamento

No IPv6 o espaço para endereçamento aumentou de 32 bits para 128 bits, elevando a capacidade de endereçamento de aproximadamente 4,3 bilhões para $3{,}4*10^{38}$ dispositivos.

Simplificação do formato do cabeçalho

Alguns campos do cabeçalho IPv4 foram suprimidos, ou tornaram-se opcionais, reduzindo, assim, o custo de processamento de dados dos roteadores.

Suporte a cabeçalhos de extensão

O campo **Opções** foi suprimido do cabeçalho base, permitindo um roteamento mais eficaz.

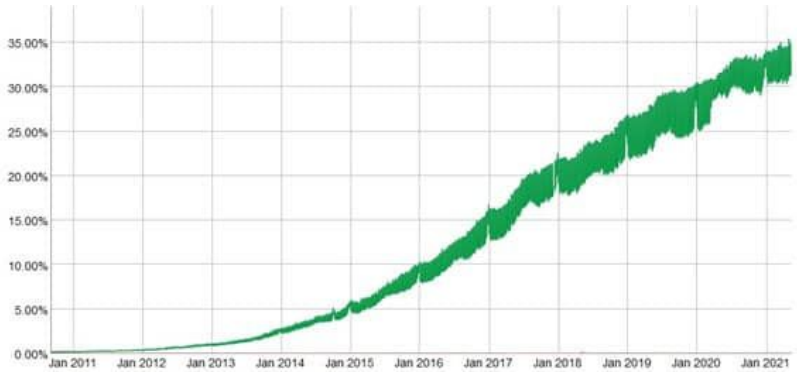
Capacidade de identificar fluxos de dados

Foi adicionado um novo campo que permite identificar pacotes pertencentes a determinados tipos de tráfego, para facilitar priorização etc.

Suporte à autenticação e privacidade

Foram especificados cabeçalhos de extensão capazes de fornecer mecanismos de autenticação, integridade e confidencialidade dos dados transmitidos.

A imagem a seguir mostra a evolução percentual de máquinas com endereço IPv6 que acessam a plataforma do Google disponível na internet. Por meio dela, podemos observar que cerca de 35% dos pacotes roteados na internet já operam sob endereçamento IPv6.



Percentual de máquinas com IPv6 no acesso à plataforma do Google.

Cabeçalho IPv6

Neste vídeo, examinamos detalhadamente o cabeçalho do datagrama IPv6. Descubra as informações essenciais contidas nessa estrutura, compreendendo como o IPv6 aprimora a eficiência na transmissão de dados.

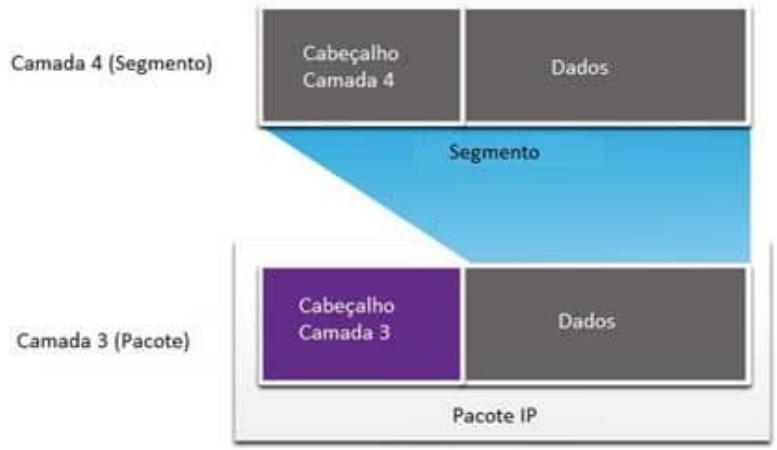
> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

O quadro a seguir evidencia que o protocolo IP está situado na camada de rede do modelo OSI (Interconexão de Sistemas Abertos), sendo o IPv6 e o IPv4 os protocolos mais utilizados no processo de roteamento global.

Camadas de redes: modelo OSI		
Nº	Nome	Principais protocolos
1	Física	
2	Enlace	
3	**Rede**	**IPv4**
		IPv6
4	Transporte	
5	Sessão	
6	Apresentação	

Modelo OSI de camadas de rede.
Elaborado por Isaac Newton Ferreira Santa Rita.

O Protocol Data Unit (PDU) da camada de rede é composto por um cabeçalho IP, e as informações contidas na camada superior, normalmente a PDU da camada de transporte, aqui chamada de **Dados**. Esse conjunto **Cabeçalho IP** e **Dados** recebe o nome de **Pacote IP**, ou **Datagrama IP**, como podemos observar na imagem a seguir.



Pacote IPv6.

O cabeçalho IPv6 será examinado por todos os dispositivos de camada 3 durante a execução do processo de roteamento. É nele que essas máquinas buscarão o endereço de origem e de destino do pacote em análise.

Nesse sentido, vamos observar a próxima imagem, que ilustra os diversos campos existentes no cabeçalho do protocolo IPv6.

Cabeçalho IPv6.

A seguir, apresentaremos as funções dos campos que compõem o cabeçalho IPv6 ilustrados na imagem.

Versão

Possui 04 bits que indicam a versão do protocolo IP (valor 6 para o IPv6). É por meio desse número que os roteadores podem definir, por exemplo, qual a tabela de roteamento mais apropriada a se utilizar.

Classe de tráfego

Possui 08 bits (1 Byte) com a função de identificar e diferenciar os pacotes por classes de serviços ou prioridade. Ele continua provendo as mesmas funcionalidades e definições do campo **Tipo de Serviço** do IPv4.

Identificador de fluxo

Possui 20 bits, com objetivo de identificar e/ou diferenciar pacotes do mesmo fluxo de dados na camada de rede. Esse campo permite ao roteador identificar o tipo de fluxo de cada pacote, sem a necessidade de verificar sua aplicação.

Tamanho dos dados

Possui 16 bits (02 Bytes) e indica o tamanho, em Bytes, apenas dos dados carregados pelo pacote IPv6. Substituiu o campo **Tamanho Total** do IPv4, que indica o tamanho do conjunto cabeçalho IPv4 e dados transportados. Os cabeçalhos de extensão também são incluídos no cálculo do tamanho.

Próximo cabeçalho

Possui 16 bits (02 Bytes) e referencia o protocolo de camada superior que o datagrama IPv6 encapsula, por exemplo, TCP, UDP etc. Além disso, indica os valores dos cabeçalhos de extensão, que veremos mais à frente.

Limite de encaminhamento

Possui 08 bits (1 Byte) e indica o número máximo de roteadores que o pacote IPv6 pode passar antes de ser descartado, função similar ao campo **Time-to-Live** do protocolo IPv4.

Endereço IPv6 de origem

Possui 128 bits (16 bytes) e indica o endereço de origem do pacote IPv6.

Endereço IPv6 de destino

Possui 128 bits (16 bytes) e indica o endereço de destino do pacote.

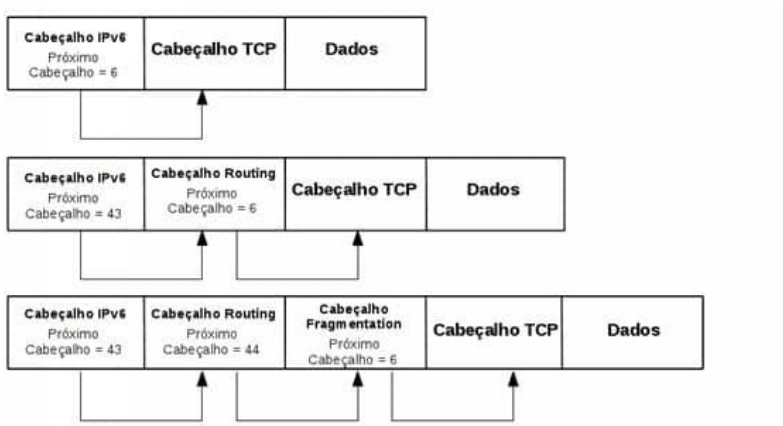
O IPv6 não permite fragmentação, como ocorria no IPv4. Essas operações são extremamente dispendiosas e foram deixadas para ser realizadas entre a fonte e o destino dos dados.

Caso exista um pacote muito grande para ser processado por um roteador, ele simplesmente descartará esse pacote e enviará um ICMP ao remetente informando sobre seu tamanho. O remetente deverá reconstruir o pacote em tamanho menor até que ele possa ser roteado.

Outro campo suprimido pelo IPv6 foi o **Checksum** de cabeçalho. Isso ocorre devido ao fato de essa operação já ser realizada na maioria dos protocolos das camadas de enlace de dados e de transporte, e sua supressão prover celeridade no processo de roteamento.

Diferentemente do IPv4, o campo **Opções** não está colocado dentro do cabeçalho base do IPv6. Essas informações são tratadas nesse protocolo por meio de cabeçalhos de extensão localizados entre o cabeçalho base do IPv6 e o cabeçalho da camada superior.

A inserção dos cabeçalhos de extensão é realizada por meio do campo **Próximo Cabeçalho**, que, por meio de uma série de valores específicos, pode inserir até 06 cabeçalhos desse tipo num mesmo pacote, cuja operação é ilustrada na imagem a seguir.



Cabeçalhos de extensão.

Conforme informado, 06 cabeçalhos de extensão são definidos pelo IPv6, cujas características são apresentadas a seguir.

Hop-by-Hop

Possui valor 00 no campo **Próximo Cabeçalho** do cabeçalho base IPv6, e deve ser colocado imediatamente após esse cabeçalho. Ele deve ser processado por todos os roteadores até o destino do pacote. Possui apenas dois tipos, o Router Alert e Jumbogram.

Destination Options

Possui valor 60 no campo **Próximo Cabeçalho** do cabeçalho base IPv6. Possui campos com a mesma definição do Hop-by-Hop e é utilizado no suporte à mobilidade do IPv6 por meio da opção Home Address, que contém o Endereço de Origem do dispositivo móvel, quando este está em trânsito.

Routing

Possui valor 43 no campo **Próximo Cabeçalho** do cabeçalho base IPv6, e foi definido para ser utilizado como parte do mecanismo de suporte à mobilidade do IPv6, carregando o Endereço de Origem do dispositivo móvel em pacotes enviados pelo roteador.

Fragmentation

Possui valor 44 no campo **Próximo Cabeçalho** do cabeçalho base IPv6, e carrega informações sobre fragmentação do pacote IPv6.

Authentication Heather

Possui valor 51 no campo **Próximo Cabeçalho** do cabeçalho base IPv6, e faz parte da pilha IPSec para prover autenticação e garantia de integridade aos pacotes IPv6.

Encapsulating Security Protocol

Possui valor 52 no campo **Próximo Cabeçalho** do cabeçalho base IPv6, e faz parte da pilha IPSec para garantir integridade e confiabilidade aos pacotes IPv6.

Endereçamento IPv6

Neste vídeo, exploramos a representação única do endereçamento IPv6 e seus diversos tipos. Compreenda as peculiaridades desse protocolo, fundamental para uma comunicação eficiente e sustentável na era digital.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

A motivação da criação do IPv6, como visto, foi a escassez do IPv4, que conta com aproximadamente 4 bilhões de endereços, dado que ele é composto por 32 bits, e essa quantidade não seria suficiente para atender à crescente demanda global por conexão.

Dessa forma, a RFC 2460, que especifica o protocolo IPv6, impõe o mesmo espaço de endereçamento de 128 bits, sendo possível endereçar até 2^{128} (340.282.366.920.938.463.463.374.607.431.768.211.456) dispositivos.

> O espaço especificado pelo protocolo IPv6 é entendido como infinito, uma vez que suporta uma quantidade de dispositivos cerca de 79 octilhões ($7{,}9*10^{28}$) de vezes maior que a quantidade de dispositivos atendidos pelo IPv4.

Como visto, não seria muito fácil trabalhar com um número desse tamanho utilizando a representação decimal, mesmo que para isso utilizássemos a separação em grupos de 8 bits, como feito no IPv4, pois para essa representação precisaríamos de 16 octetos.

Dessa forma, optou-se por representar o endereço IPv6 por meio da base de numeração hexadecimal, que utiliza os símbolos “0”, “1”, “2”, “3”, “4”, “5”, “6”, “7”, “8”, “9”, “A”, “B”, “C”, “D”, “E” e “F”.

Além disso, o IPv6 foi dividido em 8 (oito) grupos de 16 (bits) cada, o que permite até 4 símbolos hexadecimais por grupo de 16 bits, conhecido extraoficialmente como **hexteto**, que adotaremos ao longo do nosso estudo. O símbolo "**:**" é utilizado para separar esses 8 (oito) grupos. Um exemplo de um endereço IPv6 pode ser observado a seguir.

> **IPv6: 2001:0DB8:ACAD:25E2:CADE:CAFE:0021:8456**

Para facilitar a representação do endereço IPv6, foram estabelecidas duas regras de abreviação, que apresentaremos em seguida:

1 Regra 1: Omitir zeros à esquerda

Esta regra permite a omissão dos hexadecimais “0”, quando eles estão à esquerda de cada hexteto.

Exemplo:
IPv6: 2001: 0db8: 0000:1111: 0000: 0000: 0000: 0200
IPv6 (sem zeros à esquerda): 2001:db8:0:1111: 0: 0: 0: 200

2 Regra 2: Dois pontos duplos “::”

Esta regra permite a utilização **única** do “::” para substituir qualquer sequência de hextetos preenchidos unicamente por símbolos zero.

Exemplo:
IPv6: 2001: 0db8: 0000:1111: **0000: 0000: 0000**: 0200
IPv6 (sem zeros à esquerda): 2001:db8:0:1111:**0:0:0**:200
IPv6 (sem zeros à esquerda e “::”): 2001:db8:0:1111**::**200

Tipos de endereços IPv6

Neste vídeo, apresentamos os diversos tipos de endereços IPv6, incluindo endereços unicast, multicast e anycast. Entenda suas funções e aplicações específicas na comunicação de rede, proporcionando uma compreensão abrangente da estrutura de endereçamento IPv6.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

No IPv6 existem 03 (três) tipos de endereços:

Unicast

O pacote é enviado unicamente a uma interface de um único destino.

Anycast

O pacote é endereçado a um grupo de dispositivos. Um pacote encaminhado a esse tipo de endereço é entregue ao dispositivo, pertencente a esse grupo, mais próximo da origem.

Multicast

O pacote IPv6 é encaminhado para um grupo específico de dispositivos.

Diferentemente do IPv4, o IPv6 não possui um endereço broadcast. Entretanto, há um endereço multicast capaz de encaminhar pacotes a todos os dispositivos de uma rede, que fornece, basicamente, o mesmo resultado.

A seguir veremos mais detalhes sobre cada tipo.

Unicast

O IPv6 prevê alguns tipos diferentes de endereços unicast. São eles:

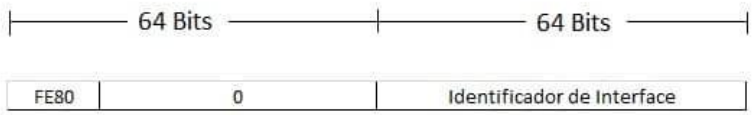
Unicast global

Este tipo de endereço é único, semelhante aos endereços públicos IPv4, e é globalmente roteável e acessível na internet IPv6.

Atualmente, somente os endereços iniciados pelos bits “001” estão sendo atribuídos a esse tipo de endereço, o que implica nos endereços compreendidos entre o endereço 2000:: até o 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

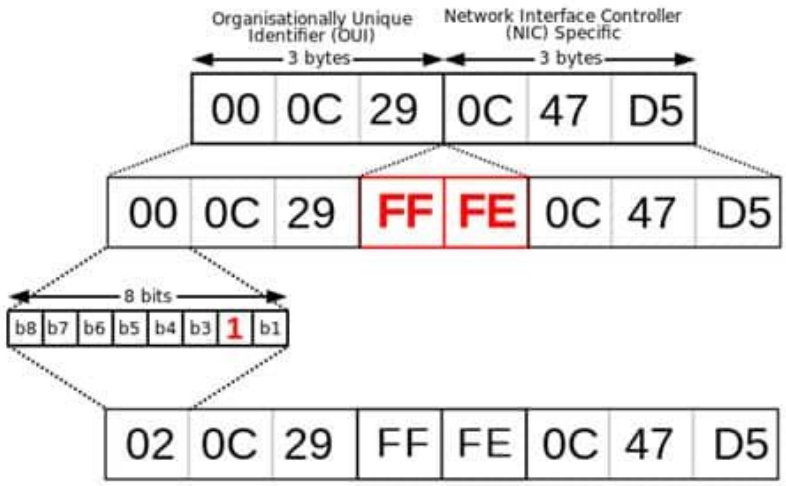
Unicast link local

É utilizado apenas no enlace específico, onde a interface está conectada. É um endereço normalmente atribuído automaticamente no formato IEEE EUI-64 para identificar o dispositivo dentro do prefixo de rede FE80::/64, ilustrado a seguir.



Endereço unicast link local.

A formação do endereço por meio do processo IEEE EUI-64 consiste na inserção dos hexadecimais FFFE no centro do endereço MAC de 48 bits, para criar o identificador de interface de 64 bits. Além disso, o sétimo bit mais significativo do endereço é invertido. A próxima imagem ilustra o processo de formações do IEEE EUI-64 para o identificador de interface do endereço link local.



Processo IEEE EUI-64.

Unicast unique local

Utiliza a o prefixo de rede FC00::/7 e apresenta alguma semelhança com os endereços privados IPv4, pois não é roteado na internet, sendo utilizado somente em um conjunto de redes particulares.

Unicast de loopback

Sua finalidade é semelhante à do endereço IPv4 de loopback, 127.0.0.1, pois também referencia a própria interface de rede por meio do IPv6 0:0:0:0:0:0:0:1, que pode ser representado por ::1.

Unicast não especificado (unspecified)

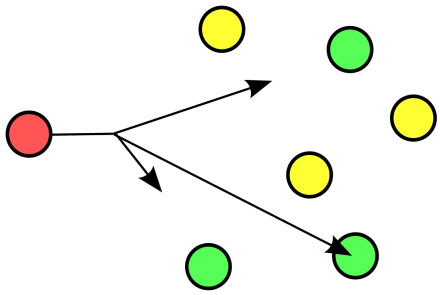
É representado pelo endereço 0:0:0:0:0:0:0:0 ou ::0 (equivalente ao endereço IPv4 0.0.0.0), que nunca deve ser atribuído a nenhum dispositivo, indicando apenas a ausência de um endereço. É bastante utilizado no processo de roteamento, principalmente para especificar a rota default de um roteador.

Unicast IPv4-mapeado

Representa um endereço IPv4 em um endereço IPv6 de 128 bit. Para isso, é utilizado o IPv6 :: 0:0:0:0:FFFF:wxyz ou ::FFFF:wxyz, onde wxyz representa os 32 bits do endereço IPv4 a ser mapeado. Apresenta grande utilidade em técnicas de transição do IPv4 para o IPv6. Para exemplificar, podemos observar o mapeamento do IPv4 192.168.100.1 no endereço IPv6 ::FFFF:192.168.100.1.

Endereços anycast

Identifica um grupo de interfaces pertencentes a diferentes dispositivos. Um pacote IPv6 com destino a um endereço anycast é remetido para uma das interfaces identificadas por esse tipo de endereço. Especificamente, o pacote é enviado para a interface mais próxima, de acordo com o protocolo de roteamento.



Roteamento Anycast.

Ele é especialmente útil na detecção rápida de determinado servidor ou serviço. Como exemplo, podemos citar um grupo de servidores de nomes, Domain Name Server (DNS), acessíveis por meio de um endereçamento Anycast, em que determinado dispositivo passará a ser servido pelo DNS mais próximo.

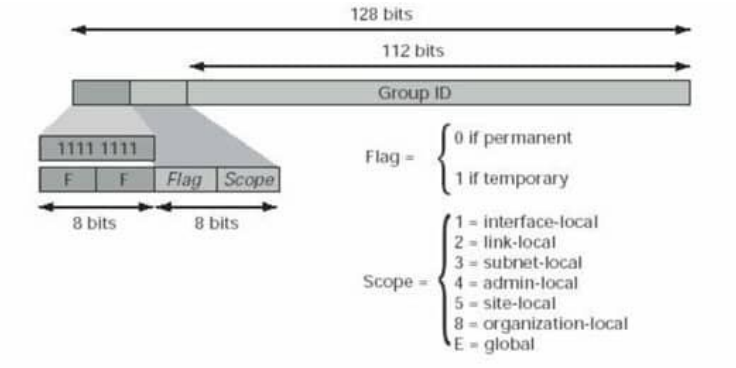
Cabe ressaltar que existem, ainda, outras faixas de endereços com finalidades especiais:

- **2002::/16:** Prefixo utilizado no mecanismo de transição 6to4.
- **2001:0000::/32:** Prefixo utilizado no mecanismo de transição TEREDO.
- **2001:db8::/32:** Prefixo utilizado para representar endereços IPv6 em textos e documentações.

Endereços multicast

Usado para identificar grupos de dispositivos, sendo que cada dispositivo pode pertencer a mais de um grupo. Os pacotes enviados para esse endereço são entregues a todas as interfaces que compõem o grupo.

Os endereços multicast não devem ser utilizados como endereço de origem de um pacote. Esses endereços derivam do bloco FF00::/8, onde o prefixo FF, que identifica um endereço multicast, é sucedido por quatro bits, que representam quatro flags, e um valor de quatro bits que define o escopo do grupo multicast. Os 112 bits restantes são utilizados para identificar o grupo multicast, conforme ilustrado a seguir.



Datagrama multicast IPv6.

Dentro dos endereços multicast já reservados, podemos identificar alguns endereços especiais utilizados para funções específicas:

- **FF01::1:** Indica todas as interfaces de escopo local, isto é, somente as interfaces de um mesmo host.
- **FF02::1:** Indica todas as interfaces de um escopo de enlace local, isto é, todos os dispositivos de um mesmo domínio de colisão.
- **FF01::2:** Indica todos os roteadores dentro de um escopo local, isto é, todas as interfaces de um mesmo roteador.
- **FF02::2:** Indica todos os roteadores dentro de um escopo de enlace local, isto é, todos os roteadores interligados por um mesmo enlace.
- **FF05::2:** Indica todos os roteadores dentro de um escopo de site local, isto é, todos os roteadores que possuem um mesmo site ID.
- **FF02::1:FFxx:xxxx:** Endereço especial chamado de Solicited-Node Multicast Address, onde xx:xxxx representam os últimos 24 bits do endereço IPv6 unicast do dispositivo.

Verificando o aprendizado

Questão 1

Após estudarmos sobre o endereçamento IPv6, assinale a alternativa que representa um IPv6 Link Local.

A

::1

B

::

C

FE80::1

D

2001::1::2

E

2001:acad:23:abdf:aa::

A alternativa C está correta.

O endereço apresentado é o Unicast Link Local. Esse tipo de endereço é utilizado apenas no enlace específico em que a interface está conectada. É um endereço atribuído automaticamente no formato IEEE EUI-64 para identificar o dispositivo dentro do prefixo de rede FE80::/64.

Questão 2

Após estudarmos sobre o endereçamento IPv6, assinale a alternativa que representa um IPv6 válido.

A

FE80::db8::1

B

127.0.0.1::db8::0000

C

FE80:db8:1

D

2001:db8:1::2

E

2001:acad:23:cafe::aa::

A alternativa D está correta.

Pela regra 02, podemos utilizar dois pontos duplos **::** para suprimir uma sequência de zeros no endereço. Essa regra permite a utilização **única** do **::** para substituir qualquer sequência de hextetos preenchidos unicamente por símbolos zero.

Numeração IPv6

Neste vídeo, exploramos a notação do endereço IPv6, esclarecendo a divisão entre prefixo de rede e identidade da interface. Descubra como os órgãos de registro determinam esses prefixos, essenciais para a eficiência na comunicação on-line.

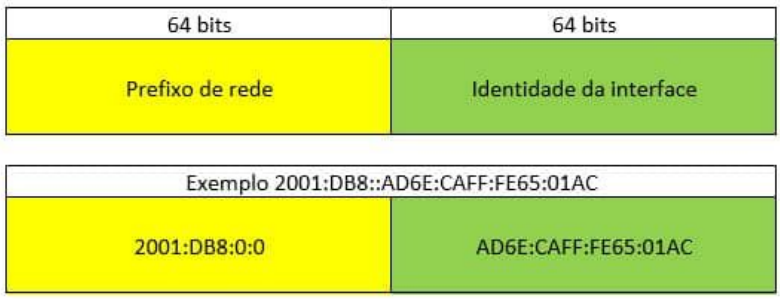
Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

A notação adotada para a representação de redes IPv6 é a mesma adotada no processo CIDR IPv4, ou seja, o comprimento do prefixo é representado na notação de barra e é usado para indicar o prefixo de rede de um endereço IPv6.

Logicamente, por se tratar de um endereço composto por 128 bits, o prefixo de rede pode variar de 0 até 128. Entretanto, o comprimento de prefixo de rede IPv6 mais utilizado para definição de redes locais é o /64, pois normalmente a técnica IEEE EUI-64 é utilizada para compor a identidade de interface do endereço IPv6 de um dispositivo.

A imagem a seguir apresenta a divisão entre o prefixo de rede IPv6 e a parte inerente à identidade da interface.



Prefixo de rede e identidade de interface.

Os endereços unicast global estão distribuídos dentro da rede 2000::/3, ou seja, possuem os bits iniciais “001” que implicam endereços IPv6 compreendidos entre 2000:: e o 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Essa faixa de IPv6, 2000::/3 de endereços é gerenciada pela IANA (Internet Assigned Numbers Authority), que possui a responsabilidade de distribui-la entre os principais RIR (Registros Regionais de Internet), a saber:

American Registry for Internet Numbers (ARIN) América do Norte e partes do Caribe	Réseaux IP Européens Network Coordination Centre (RIPE NCC) Europa, Oriente Médio e Ásia Central

Asia-Pacific Network Information Centre (APNIC)

Parte da Ásia e do Pacífico

Latin American and Caribbean Internet Addresses Registry (LACNIC)

América Latina e partes do Caribe

African Network Information Centre (AfriNIC)

África

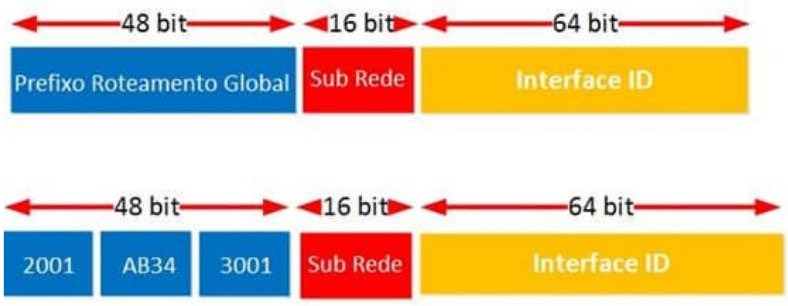
Cada RIR recebe da IANA um bloco de endereços unicast global /12, que, por sua vez, distribuem sub-redes desses blocos aos distribuidores regionais. Como exemplo, podemos citar a LACNIC, que possui a gestão do bloco 2800::/12 e distribui um bloco /16 dessa faixa para o NIC.Br, responsável pela distribuição de endereços no Brasil.

E, por fim, de um modo geral, redes /48 são distribuídas a todos os tipos de usuários, sejam usuários domésticos, sejam pequenas ou grandes empresas.

Essa forma de alocação permite que o endereço IPv6 seja mapeado em três partes diferentes, sendo elas:

- O prefixo de roteamento global, composto pelos 48 bits iniciais.
- A identidade de sub-rede local, composta por 16 bits.
- A identificação de interface, composta pelos 64 bits restantes.

A próxima imagem ilustra essa distribuição.



Distribuição de endereços IPv6.

Por meio dessa forma de distribuição, fica facultado ao cliente a possibilidade de configurar 2^{16} sub-redes diferentes para compor seu parque de máquinas. Da rede apresentada pela imagem anterior (2001:AB34:3001::/48), podemos criar as seguintes sub-redes /64:

1. 2001:AB34:3001:0000::/64

2. 2001:AB34:3001:0001::/64
3. 2001:AB34:3001:0002::/64
4. 2001:AB34:3001:0003::/64
5. ....

65.536 - 2001:AB34:3001:FFFF::/64

Outro ponto a importante sobre o endereçamento IPv6 a ser observado é a descoberta do prefixo de rede a partir do endereço IPv6 e o comprimento do endereço.

A identificação do prefixo de rede é realizada por meio da operação lógica AND bit-a-bit, entre o endereço IPv6 em questão e o comprimento do prefixo de rede. A seguir, veremos o resultado da operação lógica AND bit-a-bit.

Operação lógica AND		
Bit A	Bit B	AND
0	0	0
0	1	0
1	0	0
1	1	1

Operação lógica AND.
Elaborado por Isaac Newton Ferreira Santa Rita.

A seguir, apresentaremos a determinação dos prefixos de rede para o IPv6 2001:DB8:ACAD:1:46:2FF:FE23:24A1 com os tamanhos de bloco /64, /88 e /90. Esses prefixos foram escolhidos para evidenciar o resultado da operação AND bit-a-bit, quando comprimentos do bloco de rede não respeitam os limites dos hextetos, nem as palavras hexadecimais.

				IPv6 2001:DB8:ACAD:1:46:2FF:FE23	
IPv6	2001	DB8	ACAD	1	
	0010.0000.0000.0001	0000.1101.1011.1000	1010.1100.1010.1101	0000.0000.0000.0001	0000.000
Tamanho do bloco	1111.1111.1111.1111	1111.1111.1111.1111	1111.1111.1111.1111	1111.1111.1111.1111	0000.000
				OPERAÇÃO AND BIT-A-BIT	
Prefixo de rede	2001	DB8	ACAD	1	
	0010.0000.0000.0001	0000.1101.1011.1000	1010.1100.1010.1101	0000.0000.0000.0001	0000.000

Determinação do prefixo de rede do IPv6 2001:DB8:ACAD:1:46:2FF:FE23:24A1/64.
Elaborado por Isaac Newton Ferreira Santa Rita.

				IPv6 2001:DB8:ACAD:1:46:2FF:FE23:2	
IPv6	2001	DB8	ACAD	1	46

	0010.0000.0000.0001	0000.1101.1011.1000	1010.1100.1010.1101	0000.0000.0000.0001	0000.0000.
				OPERAÇÃO AND BIT-A-BIT	
Prefixo de rede	2001	DB8	ACAD	1	46
	0010.0000.0000.0001	0000.1101.1011.1000	1010.1100.1010.1101	0000.0000.0000.0001	0000.0000.

Determinação do prefixo de rede do IPv6 2001:DB8:ACAD:1:46:2FF:FE23:24A1/88.
Elaborado por Isaac Newton Ferreira Santa Rita.

				IPv6 2001:DB8:ACAD:1:46:2FF:FE23:	
IPv6	2001	DB8	ACAD	1	
	0010.0000.0000.0001	0000.1101.1011.1000	1010.1100.1010.1101	0000.0000.0000.0001	0000.000
Tamanho do bloco	1111.1111.1111.1111	1111.1111.1111.1111	1111.1111.1111.1111	1111.1111.1111.1111	1111.111
				OPERAÇÃO AND BIT-A-BIT	
Prefixo de rede	2001	DB8	ACAD	1	
	0010.0000.0000.0001	0000.1101.1011.1000	1010.1100.1010.1101	0000.0000.0000.0001	0000.000

Determinação do prefixo de rede do IPv6 2001:DB8:ACAD:1:46:2FF:FE23:24A1/90.
Elaborado por Isaac Newton Ferreira Santa Rita.

Como resultado dessa operação, observamos os seguintes prefixos de rede:

```plain-text
2001:DB8:ACAD:1:46:2FF: FE23:24A1/64 -> 2001:DB8:ACAD:1::
2001:DB8:ACAD:1:46:2FF: FE23:24A1/88 -> 2001:DB8:ACAD:1:46:200::
2001:DB8:ACAD:1:46:2FF: FE23:24A1/90 -> 2001:DB8:ACAD:1:46:2C0::
```

Projeto de redes IPv6

Neste vídeo, discutimos abordagens tangíveis para o projeto de redes IPv6. Explore práticas eficazes para implementar essa nova geração de endereçamento IP.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Logicamente, a padronização não é mandatória e podemos projetar redes com prefixos de rede variados, respeitando o prefixo de roteamento global recebido de seu provedor de internet.

Para exemplificar, vamos utilizar um exemplo básico de configuração, onde há necessidade de se interconectar 02 roteadores por meio de uma rede de ligação IPv6.

Projeto de rede IPv6.

Para projetos de rede IPv6, cabe observar que, diferentemente do IPv4, o IPv6 não possui IP de rede nem de broadcast, não havendo, então, a necessidade de deixar vago o primeiro IP nem o último IP em uma rede. Esses IPv6 podem ser normalmente atribuídos a qualquer dispositivo.

Para a determinação da menor rede capaz de atender à demanda desse projeto, é necessário entender qual será o prefixo de rede capaz de comportar determinado número de dispositivos.

Nesse sentido, para determinar a quantidade máxima de máquinas (Mmax) que uma rede IPv6 pode comportar, devemos realizar o seguinte cálculo:

> **$Mmax = 2^{(128-N)}$, onde N é o prefixo da rede IPv6.**

Observe que no endereçamento IPv6 não existe limitação do uso do identificador de rede e do broadcast como acontece no endereçamento IPv4. Inclusive, não existe endereço de broadcast no IPv6.

Exemplo

Vamos determinar a capacidade máxima da rede 2001::/120.Mmax = 2(128-N) = Mmax = 2(128-120) = Mmax = 2(8) = Mmax = 256 dispositivos.

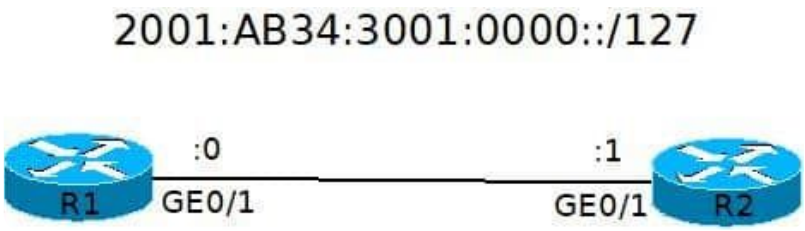
Assim, para determinar o comprimento do prefixo de rede necessária para suportar determinada quantidade de máquinas, basta encontrar o menor **N** que satisfaz a inequação exponencial apresentada a seguir:

> **$2^{(128-N)} \geq$ (nº máquinas desejado)**

No projeto de rede IPv6 apresentado na imagem anterior, onde há necessidade de comportar 02 endereços IPv6, podemos determinar o menor prefixo possível da seguinte forma:

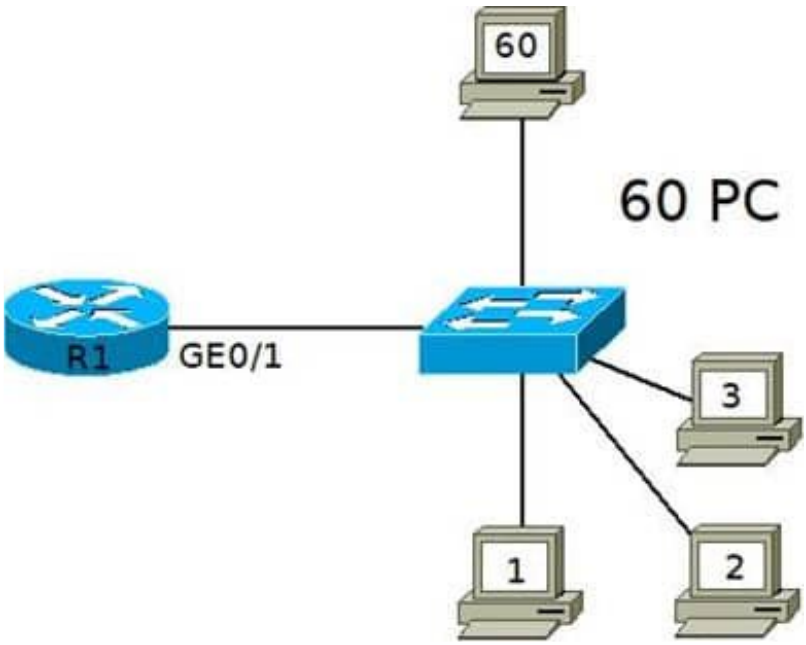
> $2^{(128-N)} \geq$ (nº máquinas desejado)
>
> $2^{(128-N)} \geq 2$
>
> $2^{(128-N)} \geq 2 = 2^1$
>
> $128 - N \geq 1$
>
> $N \leq 128 - 1$
>
> $N \leq 127$
>
> $N = 127$

Para endereçar esse projeto, vamos utilizar a faixa de rede 2001:AB34:3001:0000::/127, onde uma das interfaces receberá o primeiro IPv6 dessa rede, o IPv6 2001:AB34:3001:0000::, e a segunda interface receberá o IPv6 2001:AB34:3001:0000::1. A próxima imagem ilustra o projeto dessa rede de ligação IPv6 concluído.



Projeto de rede IPv6 2001:AB34:3001:0000::/127 concluído.

Outro projeto interessante para realizarmos é o projeto de uma rede local com capacidade de comportar até 60 dispositivos mais o Default Gateway, apresentado a seguir.



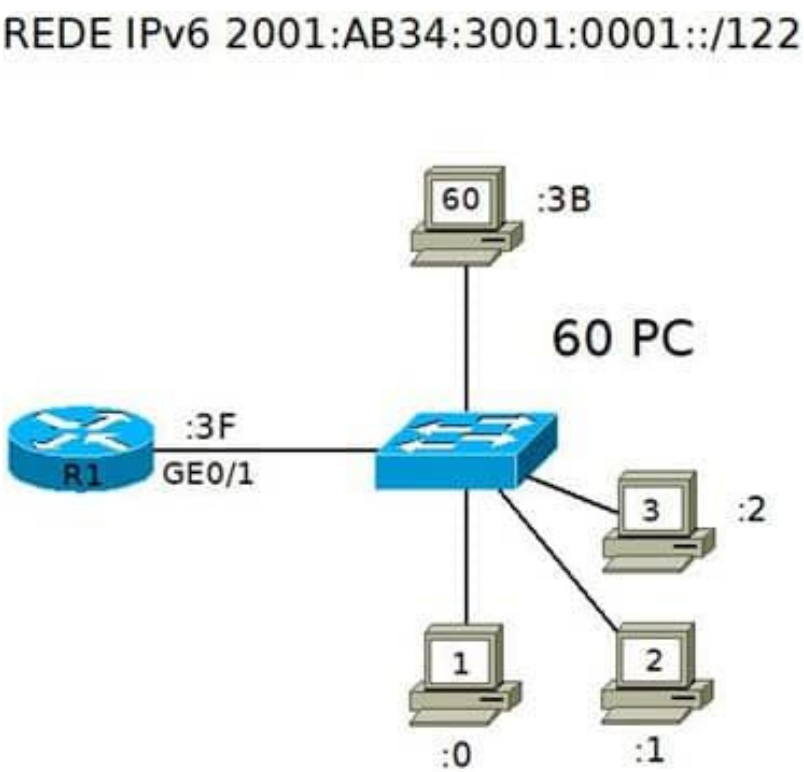
Projeto de rede IPv6 concluído.

Nesse projeto, vamos inicialmente realizar o cálculo para o menor prefixo possível.

> $2^{(128-N)} \geq$ (nº máquinas desejado)
>
> $2^{(128-N)} \geq 61$
>
> $2^{(128-N)} \geq 64 = (2^6)$
>
> $N \leq 128 - 6$
>
> $N \leq 122$
>
> $N = 122$ (menor prefixo possível é a /122)

Uma vez determinado o prefixo de rede a ser utilizado, vamos escolher a faixa de rede 2001:AB34:3001:0001::/122, considerando que ainda não temos a obrigação de utilizar uma faixa de rede predeterminada. Dessa forma, poderemos associar os endereços IPv6 compreendidos entre 2001:AB34:3001:0001:: e 2001:AB34:3001:0001::3F aos dispositivos componentes dessa rede IPv6.

Utilizando para o default gateway o último IPv6 dessa rede, e os endereços em sequência para os PCs, com o primeiro PC recebendo o IPv6 2001:AB34:3001:0001:: e o sexagésimo PC recebendo o IPv6 o IP 2001:AB34:3001:0001::3B, teremos o projeto dessa rede conforme ilustrado a seguir



Projeto de Rede IPv6 2001:AB34:3001:0001::/122 concluído.

Quando há necessidade de inserir um projeto dentro de uma faixa de rede predefinida, podemos proceder de forma semelhante àquela realizada em projetos VLSM em IPv4.

Como exemplo, vamos projetar uma rede com necessidade de 10 (dez) sub-redes, utilizando a faixa predefinida de rede 2001:AB34:3001:0002::/112. As primeiras 05 sub-redes possuem necessidade de até 100 dispositivos, e as sub-redes restantes, necessidade de até 50 dispositivos.

A primeira ação a ser realizada é a determinação do prefixo de rede de cada tipo de sub-rede.

Para redes de até 100 dispositivos:

> $2^{(128-N)} \geq$ (nº máquinas desejado)
>
> $2^{(128-N)} \geq 100$
>
> $2^{(128-N)} \geq 128 = (2^7)$
>
> $N \leq 128 - 7$
>
> $N \leq 121$
>
> N = 121 (menor prefixo possível é a /121)

Para redes de até 50 dispositivos:

> $2^{(128-N)} \geq$ (nº máquinas desejado)

$2^{(128-N)} \geq 50$

$2^{(128-N)} \geq 64 = (2^6)$

$N \leq 128 - 6$

$N \leq 122$

$N = 122$ (menor prefixo possível é o /122)

Como resultado, verificamos que para as redes com necessidade de até 100 dispositivos devemos trabalhar, minimamente, com redes /121. E para as redes com necessidade de até 50 dispositivos, com sub-redes /122. A seguir veremos a capacidade de segmentação da rede original 2001:AB34:3001:0002::/112 nesses dois tipos de sub-redes.

Rede original	Tipo de sub-rede	Quantidade de sub-redes
/112	/121	512
	/122	1024

Decomposição da rede /112.
Elaborado por Isaac Newton Ferreira Santa Rita.

Dessa forma, vamos inicialmente decompor a rede 2001:AB34:3001:0002::/112 em redes /121, para atendermos à necessidade de sub-redes com capacidade de até 100 dispositivos. A seguir, veremos essa decomposição, evidenciando como ficam os bits do último hexteto e o endereço de rede de cada sub-rede /121.

Rede original	Nº sub-rede	Último hexteto (binário)	Decomposição em sub-redes /121	Rede atendida
2001:AB34:3001:0002::/112	1	000.0000.0000.0000	2001:AB34:3001:0002::0000/121	Rede 1 (Até 100 Disp)
	2	000.0000.1000.0000	2001:AB34:3001:0002::0080/121	Rede 2 (Até 100 Disp)
	3	0000.0001.0000.0000	2001:AB34:3001:0002::0100/121	Rede 3 (Até 100 Disp)
	4	000.0001.1000.0000	2001:AB34:3001:0002::0180/121	Rede 4 (Até 100 Disp)
	5	000.0010.0000.0000	2001:AB34:3001:0002::0200/121	Rede 5 (Até 100 Disp)
	6	000.0010.1000.0000	2001:AB34:3001:0002::0280/121	Disponível
	7	0000.0011.0000.0000	2001:AB34:3001:0002::0300/121	Disponível
	8	000.0011.1000.0000	2001:AB34:3001:0002::0380/121	Disponível
	9	000.0100.0000.0000	2001:AB34:3001:0002::0400/121	Disponível

10	000.0100.1000.0000	2001:AB34:3001:0002::0480/121	Disponível
11	0000.0101.0000.0000	2001:AB34:3001:0002::0500/121	Disponível
12	000.0101.1000.0000	2001:AB34:3001:0002::0580/121	Disponível
13	000.0110.0000.0000	2001:AB34:3001:0002::0600/121	Disponível
14	000.0110.1000.0000	2001:AB34:3001:0002::0680/121	Disponível
15	0000.0111.0000.0000	2001:AB34:3001:0002::0700/121	Disponível
16	0000.0111.1000.0000	2001:AB34:3001:0002::0780/121	Disponível
...		...	...
512	1111.1111.1000.0000	2001:AB34:3001:0002::FF80/121	Disponível

Sub-redes /121.
Elaborado por Isaac Newton Ferreira Santa Rita.

Como cada rede /121 é capaz de se decompor em 02 sub-redes /122, vamos utilizar as sub-redes 6, 7 e 8 apresentadas anteriormente para encontrar as 05 sub-redes com necessidades de até 50 dispositivos. A seguir veremos o projeto solicitado consolidado, evidenciando cada uma das 10 sub-redes demandadas nessa divisão.

Rede regional	Nº sub-rede	Último hexteto (binário)	Decomposição /121 & /122	Rede atendida
2001:AB34:3001:0002::/112	1	000.0000.0000.0000	2001:AB34:3001:0002::0000/121	Rede 1 (Até 100 Disp)
	2	000.0000.1000.0000	2001:AB34:3001:0002::0080/121	Rede 2 (Até 100 Disp)
	3	0000.0001.0000.0000	2001:AB34:3001:0002::0100/121	Rede 3 (Até 100 Disp)
	4	000.0001.1000.0000	2001:AB34:3001:0002::0180/121	Rede 4 (Até 100 Disp)
	5	000.0010.0000.0000	2001:AB34:3001:0002::0200/121	Rede 5 (Até 100 Disp)
	6	000.0010.1000.0000	2001:AB34:3001:0002::0280/122	Rede 1 (Até 50 Disp)
	6	000.0010.1100.0000	2001:AB34:3001:0002::02C0/122	Rede 2 (Até 50 Disp)
	7	0000.0011.0000.0000	2001:AB34:3001:0002::0300/122	Rede 3 (Até 50 Disp)

7	0000.0011.0100.0000	2001:AB34:3001:0002::0340/122	Rede 4 (Até 50 Disp)
8	000.0011.1000.0000	2001:AB34:3001:0002::0380/122	Rede 5 (Até 50 Disp)
8	000.0011.1100.0000	2001:AB34:3001:0002::03C0/122	Disponível
9	000.0100.0000.0000	2001:AB34:3001:0002::0400/121	Disponível
10	000.0100.1000.0000	2001:AB34:3001:0002::0480/121	Disponível
11	0000.0101.0000.0000	2001:AB34:3001:0002::0500/121	Disponível
12	000.0101.1000.0000	2001:AB34:3001:0002::0580/121	Disponível
13	000.0110.0000.0000	2001:AB34:3001:0002::0600/121	Disponível
14	000.0110.1000.0000	2001:AB34:3001:0002::0680/121	Disponível
15	0000.0111.0000.0000	2001:AB34:3001:0002::0700/121	Disponível
16	0000.0111.1000.0000	2001:AB34:3001:0002::0780/121	Disponível
...		...	...
512	1111.1111.1000.0000	2001:AB34:3001:0002::FF80/121	Disponível

Sub-redes /122.
Elaborado por Isaac Newton Ferreira Santa Rita.

Projeto de redes IPv6 com prefixo de rede /64

O prefixo de rede /64 é o mais utilizado para projetos de rede IPv6, pois pode comportar os endereços IEEE EUI-64, que possuem a capacidade de identificar o endereço MAC dos dispositivos. Por esse motivo, é importante estudar projetos de rede com esse tamanho de prefixo de sub-rede.

Vamos efetuar o projeto de rede apresentado anteriormente, mas utilizando somente redes /64 em sua composição.

Atenção

Redes /64 têm a capacidade de suportar até 264 endereços, cujo limite não será alcançado por nenhuma rede local conhecida.

Vamos supor que o provedor de internet entregou ao administrador de rede a faixa 2001:AB34:3001::/48 para que ele possa compor o projeto para as 10 redes já mencionadas anteriormente, ou seja: 05 redes com capacidade de até 100 dispositivos e 05 redes com capacidade de até 50 dispositivos. A seguir, veremos a composição do projeto de rede em questão, utilizando prefixos de sub-rede /64.

Rede	Nº sub-rede	Rede /64	Rede atendida
2001:AB34:3001::/48	1	2001:AB34:3001:0000::/64	Rede 1 (Até 100 Disp)
	2	2001:AB34:3001:0001::/64	Rede 2 (Até 100 Disp)
	3	2001:AB34:3001:0002::/64	Rede 3 (Até 100 Disp)
	4	2001:AB34:3001:0003::/64	Rede 4 (Até 100 Disp)
	5	2001:AB34:3001:0004::/64	Rede 5 (Até 100 Disp)
	6	2001:AB34:3001:0005::/64	Rede 1 (Até 50 Disp)
	7	2001:AB34:3001:0006::/64	Rede 2 (Até 50 Disp)
	8	2001:AB34:3001:0007::/64	Rede 3 (Até 50 Disp)
	9	2001:AB34:3001:0008::/64	Rede 4 (Até 50 Disp)
	10	2001:AB34:3001:0009::/64	Rede 5 (Até 50 Disp)

Projeto com redes /64.
Elaborado por Isaac Newton Ferreira Santa Rita.

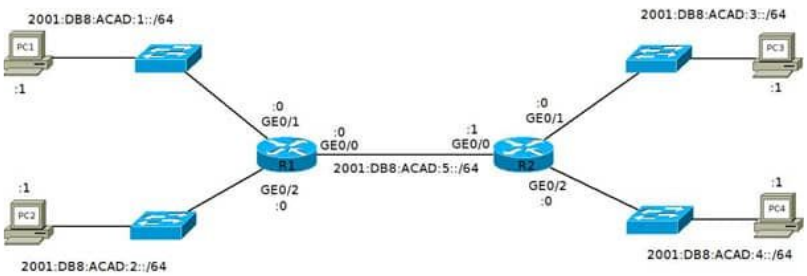
Configuração de redes IPv6

Neste vídeo, guiaremos você passo a passo na configuração de redes IPv6 utilizando o **Packet Tracer**. Desvende as práticas essenciais para garantir uma implementação eficiente e funcional de redes IPv6.

> **Conteúdo interativo**
>
> Acesse a versão digital para assistir ao vídeo.

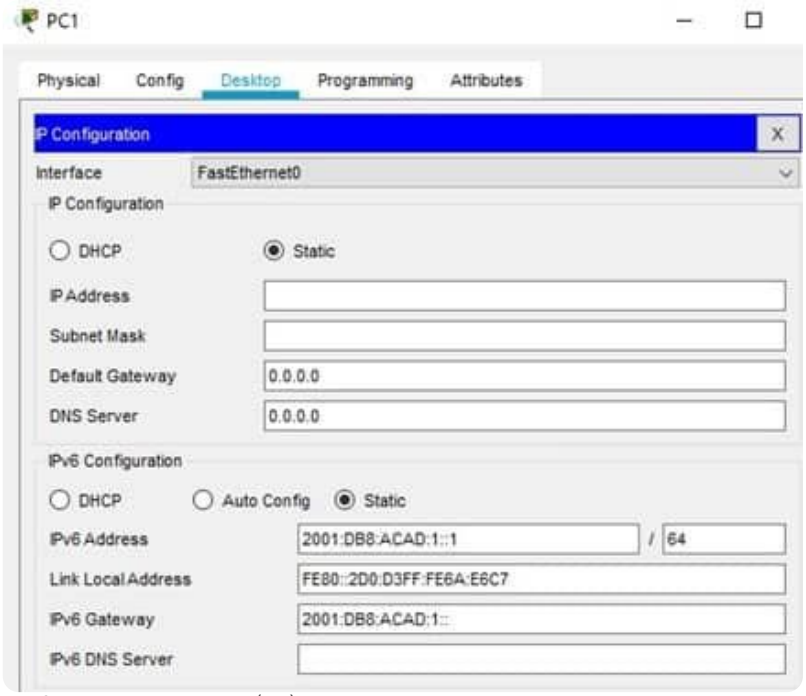
Para compreendermos a configuração de redes IPv6, vamos realizar a configuração da rede apresentada por meio do diagrama a seguir.

Para poder realizar o exercício, você pode montar a topologia no Packet Tracer ou baixar o arquivo pré-configurado.



Configuração de rede IPv6 (diagrama).

Inicialmente, devemos configurar cada um dos PCs, observando o IPv6 do respectivo Default Gateway, o prefixo /64, e o IPv6 do PC. A próxima imagem ilustra a configuração do PC1.



Configuração de rede IPv6(PC)

Cabe observar que o PC1 já possui um IPv6 link local configurado que permite a comunicação desse PC com outros dispositivos em sua rede local, antes mesmo de receber o IPv6 unique global.

O IPv6 link local utiliza o prefixo de rede FE80::/64 e compõe seu endereço pelo processo IEEE EUI-64, o que nos permite, observando o IPv6 apresentado, concluir que o endereço MAC do PC1 é o 00D0.D36A.E6C7.

Atenção

O processo IPv6 não é habilitado por padrão no roteador Cisco, modelo 2911, escolhido para esse laboratório. Dessa forma, é necessário habilitar o processo IPv6 no roteador.

A configuração do roteador R1 é apresentada a seguir.

```
plain-text

R1#
R1# conf t (Entrar no modo de configuração)
R1(config)#
R1(config)# ipv6 unicast-routing (Habilitar o processo IPv6 no roteador)
R1(config)# interface gigabitEthernet 0/0 (Entrar na interface Gigabitethernet 0/0)
R1(config-if)# ipv6 address 2001:db8:acad:5::/64 (Configuração do IPv6 na interface 0/0)
R1(config-if)# no shutdown (Ligar a interface)
R1(config-if)#
R1(config-if)# interface gigabitEthernet 0/1 (Entrar na interface Gigabitethernet 0/0)
R1(config-if)# no shutdown (Ligar a interface)
R1(config-if)# ipv6 address 2001:db8:acad:1::/64 (Configuração do IPv6 na interface 0/0)
R1(config-if)# no shutdown (Ligar a interface)
R1(config-if)#
R1(config-if)# interface gigabitEthernet 0/2 (Entrar na interface Gigabitethernet 0/0)
R1(config-if)# ipv6 address 2001:db8:acad:2::/64 (Configuração do IPv6 na interface 0/0)
R1(config-if)# no shutdown (Ligar a interface)
R1(config-if)#
R1(config-if)# exit
R1(config)#
R1(config)# end
R1#
```

Agora, configure os PC2, PC3, PC4 e o roteador R2 do projeto de rede apresentado no diagrama anterior. Após essa configuração, teste a conexão entre os PCs do laboratório, por meio da ferramenta de teste de rede ping.

Atenção

Não se esqueça de verificar as rotas e criar as que forem necessárias. Para criar rotas IPv6 no Packet Tracer, você deve utilizar o comando ipv6 route acompanhado do prefixo de rede a ser alcançado.

Verificando o aprendizado

Questão 1

Estudamos sobre o planejamento de endereços IPv6, muito importante para o desenvolvimento de projetos de rede IPv6. Para o endereço/prefixo IPv6 2001:DB8:ACAD:1:FCD:1:4E66:1/96, assinale a alternativa que representa o prefixo de rede desse IPv6.

A

2001:DB8:ACAD:1:FCD:1:4E66::

B

2001:DB8:ACAD:1::

C

2001:DB8:ACAD:1:FCD:1::

D

2001:DB8:ACAD:1:FCD::

E

2001:DB8:ACAD::

A alternativa C está correta.

Cada hexteto possui 16 bits.

16 × 6 = 96 (Até o fim do sexto hexteto)

2001:DB8:ACAD:1:FCD:1:4E66:1

Questão 2

Após estudarmos sobre projetos de rede IPv6, considere que um provedor recebeu o bloco de endereços 2001:CAFE:ABA::/32 e que precisa distribuir blocos de endereços para os seus clientes com tamanho /64. Assinale a alternativa que apresenta corretamente uma sub-rede /64.

A

2001:CAFE:ABA:ACAD:1::/64

B

2001:CAFE:ABA:CAFE:1::/64

C

2001:CAFE:ABA::1::/64

D

2001:CAFE:ABA:1:1::/64

E

2001:CAFE:ABA:CAFE::/64

A alternativa E está correta.

O prefixo /64 inclui os 64 bits mais à esquerda do endereço IPv6. Como os endereços IPv6 são representados em hextetos, ou seja, separados a cada 16 bits, teremos um bloco /64 quando tivermos quatro hextetos preenchidos, como o apresentado em 2001:CAFE:ABA:CAFE::/64. Lembre-se de que, na notação do IPv6, os zeros à esquerda não são representados.

Visão geral

Integração IPv4 e IPv6 e a pilha dupla

Neste vídeo, abordaremos os mecanismos práticos de integração entre os protocolos IPv4 e IPv6, destacando as técnicas de pilha dupla. Compreenda como essas estratégias possibilitam uma transição fluida e eficiente na evolução das redes.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

A introdução do IPv6 na rede mundial de computadores não poderia ser realizada simplesmente apertando um botão e informando aos usuários que a partir de uma data todos deveriam migrar seus dispositivos e sistemas do IPv4 para o IPv6.

Essa transição deveria ser gradual e com o mínimo de impactos aos usuários da rede IPv4. Por isso, surgiu a necessidade da coexistência entre as duas versões do protocolo de internet para viabilizar a interoperabilidade entre as redes IPv4 já implantadas e aquelas com a nova versão do protocolo de internet.

Dessa necessidade, surgiram diversas técnicas de transição entre o IPv4 e o IPv6, baseadas principalmente em:

Pilha dupla

Provê o suporte a ambos os protocolos no mesmo dispositivo.

Tunelamento

Permite o tráfego de pacotes IPv6 sobre estruturas de rede IPv4.

Tradução

Permite a comunicação entre dispositivos com suporte apenas ao IPv6 com dispositivos que suportam apenas IPv4.

Veremos mais detalhes sobre pilha dupla, tunelamento e tradução a seguir.

Pilha dupla

Na fase inicial de implantação do IPv6, não é aconselhado que os dispositivos trabalhem somente com o novo protocolo, mas que exista a capacidade de operar sob as duas plataformas, tanto a IPv4 quanto a IPv6, pois existirá a necessidade de esse equipamento se comunicar tanto com equipamentos IPv4 como com equipamentos IPv6.

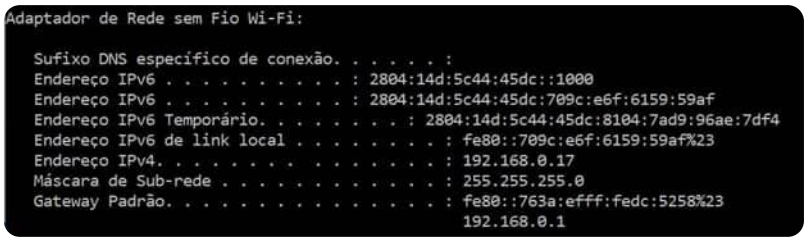
> A essa possibilidade de trabalhar sobre os dois protocolos damos o nome de **pilha dupla**, o que permite aos dispositivos processar tanto pacotes IPv4, numa comunicação dessa natureza, quanto IPv6, quando existir a possibilidade de trocar informação sob o novo protocolo.

Esse processo está ilustrado a seguir.

Pilha dupla.

Para que exista a possibilidade de operar sobre esses dois protocolos, cada dispositivo deve ser configurado tanto com endereço IPv4 quanto com endereço IPv6. Logicamente, isso deve estar atrelado a uma série de aspectos que possibilitem esse funcionamento, tais como o ajuste do Domain Name Server (DNS), configuração do Firewall de borda da rede e a possibilidade de encaminhamento dos pacotes ao seu destino.

A próxima imagem ilustra um PC com a configuração de pilha dupla, cabendo observar a coexistência de endereço IPv4 e IPv6.



PC com endereçamento pilha dupla. Captura de tela do terminal.

Agora você vai verificar em seu PC a existência de pilha dupla e realizar teste de conexão com os endereços de gateway IPv4 e IPv6. Abra um prompt de comando se for uma máquina Windows ou um terminal Linux e veja se aparece tanto um endereço IPv4 quanto IPv6. Caso exista, você já estará habilitado a trabalhar com a pilha dupla.

Técnicas de tunelamento

Técnicas de tunelamento para integração IPv4 e IPv6

Descubra os detalhes práticos dos mecanismos de integração entre os protocolos IPv4 e IPv6, focando especialmente nas técnicas baseadas em tunelamento. Aprenda como essa abordagem eficaz viabiliza a coexistência e a transição harmoniosa entre os protocolos IPv4 e IPv6.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

As técnicas de tunelamento, também conhecidas como encapsulamento, permitem o trânsito de pacotes IPv6 sob redes IPv4 já existentes, sem a necessidade de realizar qualquer alteração nos processos de roteamento já implantados, efetuando simplesmente o encapsulamento de pacotes IPv6 em pacotes IPv4.

> Essas técnicas estão documentadas na RFC 4213 e são as mais utilizadas no processo de transição do IPv4 para o IPv6.

Existem diversas técnicas que utilizam esse modelo de transição. Entre elas, podemos destacar:

Técnicas de encapsulamento de pacotes IPv6 em pacotes IPv4:

- Tunnel Broker
- 6to4
- ISATAP

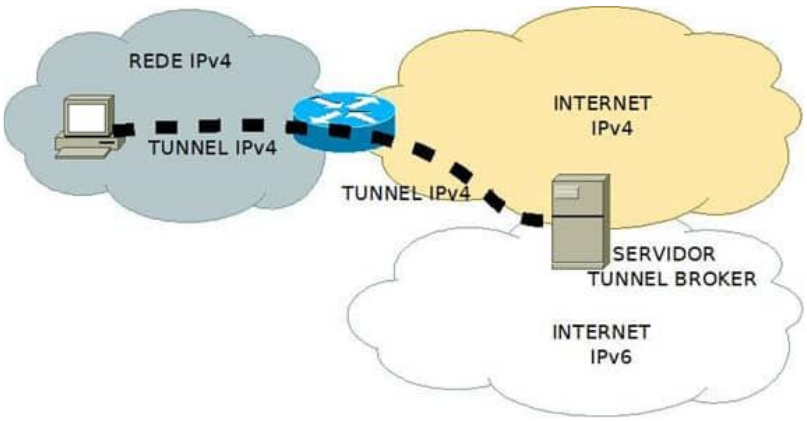
Pacotes IPv6 encapsulados em túneis GRE

- Protocolo GRE

Tunnel Broker

A técnica Tunnel Broker está documentada na RFC 3053. Permite que dispositivos numa rede IPv4 acessem redes IPv6. Isso é possível por meio de um provedor de acesso IPv6 Tunnel Broker: um equipamento IPv4 pode iniciar o download de um software, e por meio dele, realizar uma conexão túnel IPv4 com esse provedor, que, após autenticação, atribui um endereço IPv6 ao solicitante. A partir desse momento, o dispositivo na rede IPv4 pode acessar qualquer dispositivo sob o protocolo IPv6.

Observe, a seguir, a ilustração da conexão tunelada entre um PC e o servidor Tunnel Broker, que permite o acesso do PC à rede IPv6.



Tunnel Broker.

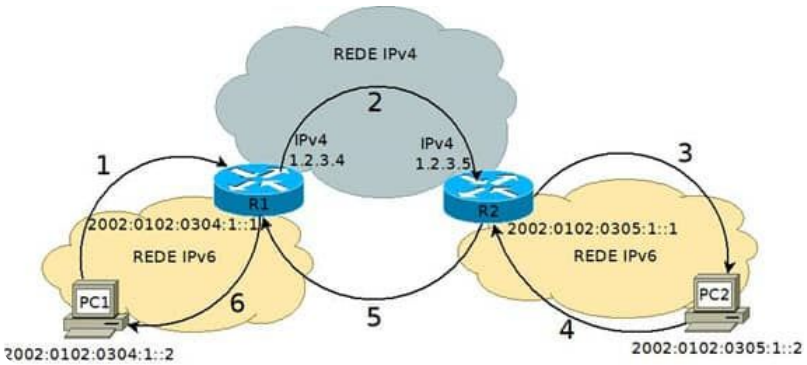
6to4

A técnica de tunelamento 6to4 está documentada na RFC 3056. Permite a conexão entre roteadores e sub-redes IPv6 por meio de redes IPv4. Essa técnica está baseada na configuração de endereços IPv6 únicos a partir de endereços IPv4 públicos.

Para isso, a técnica 6to4 utiliza o prefixo de endereçamento global 2002:wwxx:yyzz/48, onde wwxx:yyzz são os 32 bits do endereço IPv4 público a ser utilizado para atravessar redes IPv4, convertido em seu correspondente hexadecimal. O processo dentro do endereçamento 6to4 acontece como ilustrado a seguir.

Endereçamento 6to4.

Os passos de 1 até 6 apresentados na imagem seguinte exemplificam o processo ocorrido no tunelamento 6to4, no acesso de um dispositivo em uma rede IPv6 até outro dispositivo em outra rede IPv6, utilizando para isso uma rede de passagem IPv4.



Processo tunelamento 6to4.

O processo ilustrado na imagem está descrito a seguir.

PC1

PC1 envia um pacote com destino ao PC2 (IPv6 de destino 2002:0102:0305:1::2), que é encaminhado inicialmente até o seu default gateway, roteador R1.

IPv6

O pacote IPv6 é recebido por R1, que o processa e observa que deve enviá-lo por meio de sua interface virtual 6to4 (rota para rede2002::/16). Nessa interface, o pacote IPv6 é encapsulado em um pacote IPv4 (protocolo 41), que é endereçado ao roteador IPv4 de R2 (endereço extraído do endereço IPv6 do destinatário do pacote original).

IPv4

O pacote IPv6 encapsulado em IPv4 é recebido por R2. Como o pacote é do protocolo 41, ele é encaminhado à interface virtual 6to4. Assim, o roteador R2 pode encaminhar o pacote IPv6 ao seu destino, o IPv6 2002:0102:0305:1::2.

Atenção

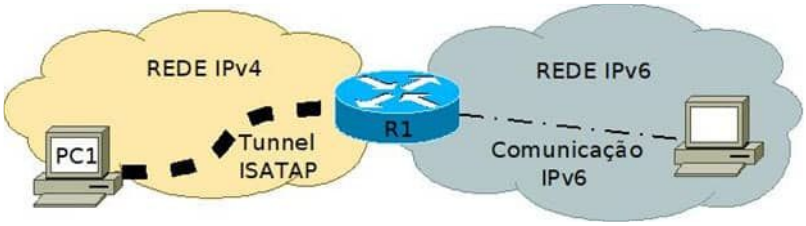
Os passos 4, 5 e 6 discriminam o processo de retorno do pacote ao PC1, sob a mesma lógica descrita nos passos 1, 2 e 3.

ISATAP

A técnica de Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) está documentada na RFC 5214 e é utilizada para conectar infraestruturas de rede IPv4 já implantadas em redes IPv6 como a internet.

Utiliza túneis IPv6 criados automaticamente dentro de redes IPv4 para conectar dispositivos em redes IPv4 aos seus gateways, que possuem contato com a rede IPv6, para encaminhar pacotes IPv6. A troca de informação entre o dispositivo e seu gateway é semelhante ao processo 6to4 visto anteriormente e está definida na RFC 4213, em sua seção 3, que trata do protocolo 41.

O processo ISATAP de encaminhamento de pacotes IPv6 pela rede IPv4 está ilustrado a seguir.



Processo tunelamento ISATAP.

Nessa técnica, o endereço dos dispositivos IPv4 estão inseridos como parte do endereço ISATAP IPv6. Isso permite que os dispositivos ISATAP identifiquem os equipamentos IPv4 sem a necessidade de protocolos adicionais.

A composição do endereço ISATAP é ilustrada na próxima figura.

Endereço ISATAP.

Agora, vamos entender cada elemento ilustrado na imagem.

Prefixo unicast

É qualquer prefixo unicast válido em IPv6, que pode ser link local ou global.

ID IPv4 público ou privado

Se o endereço IPv4 for público, recebe valor 200; se for privado, recebe o valor 0.

ID ISATAP

Valor hexadecimal 5EFE.

Endereço IPv4

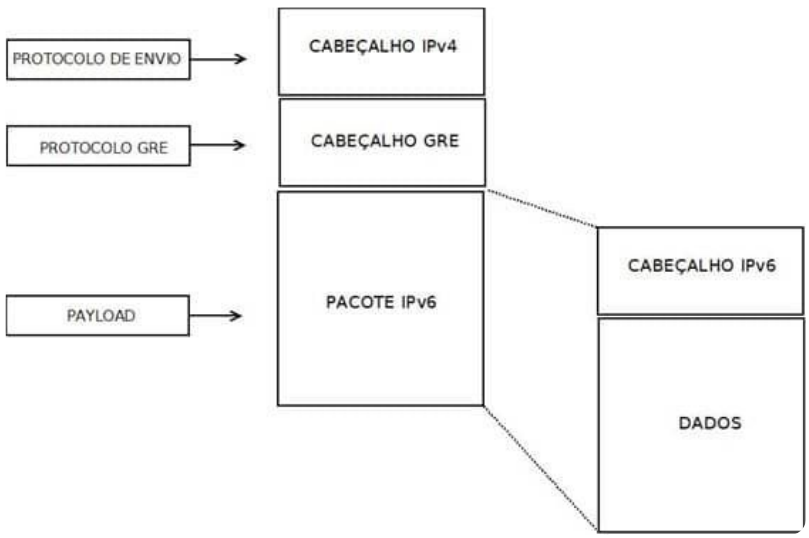
É o IPv4 associado representado em hexadecimal.

Protocolo GRE

O GRE (Generic Routing Encapsulation) é um protocolo de tunelamento com a finalidade de encapsular vários tipos diferentes de protocolos, como IPv6 sobre o protocolo IPv4. Devido à sua simplicidade, ele é suportado pela maioria dos dispositivos. Sua principal desvantagem consiste na necessidade de configuração manual, que demanda grande esforço de manutenção e gerenciamento com o crescimento no número de túneis.

A forma de operação do GRE é bem simples: ele simplesmente mantém o formato original do pacote a ser transportado, adiciona o cabeçalho GRE e encaminha até a outra ponta do túnel, utilizando o protocolo de transporte viável.

A imagem a seguir ilustra um pacote IPv6 sendo transportado por um túnel GRE numa rede IPv4.



Tunelamento GRE.

Tradução

Técnicas de tradução para integração IPv4 e IPv6

Explore os detalhes dos mecanismos de integração entre os protocolos IPv4 e IPv6, concentrando-se nas técnicas baseadas em tradução. Descubra como essa abordagem simplifica a coexistência e promove uma transição suave nas redes modernas.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

A técnica de tradução, como o próprio nome sugere, consiste em realizar traduções de endereços IPv6 em endereços IPv4 e vice-versa. Dessa forma, possibilitam o simples roteamento entre dispositivos com suporte ao cabeçalho IP, seja ele IPv4, IPv6 ou pilha dupla.

Veremos, a seguir, as técnicas mais conhecidas.

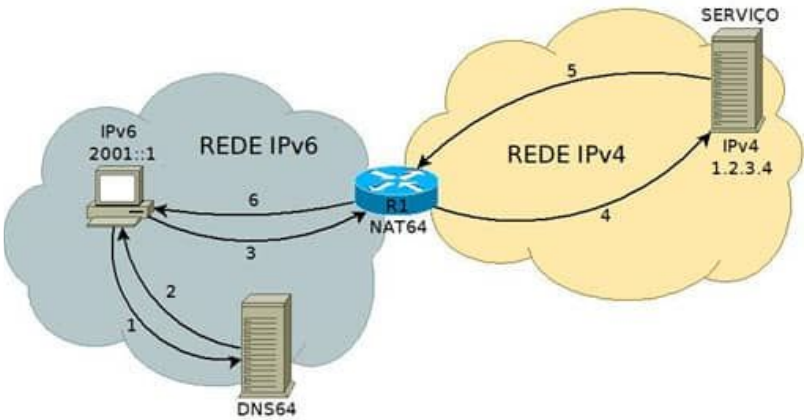
NAT64

Está definida na RFC 6146 e possibilita o acesso de dispositivos configurados unicamente com IPv6 a dispositivos em redes IPv4. Para que isso ocorra, há necessidade de um DNS com capacidade de realizar o mapeamento de endereços IPv4 e endereços IPv6. A esse tipo damos o nome de **DNS64**.

O prefixo de rede utilizado para realizar esse tipo de tradução é o 64:ff9::/32, ao qual um endereço IPv4 pode ser transportado nos últimos 32 bits desse prefixo.

Dessa forma, quando uma máquina IPv6 deseja acessar um serviço hospedado em um servidor IPv4 sob o IPv4 1.2.3.4, o dispositivo IPv6 deve realizar encaminhamento dos pacotes ao destino 64:ff9::102:304, que nada mais é que o prefixo de rede reservado ao NAT64 com os últimos 32 bits compostos pelos 32 bits do IPv4 a ser acessado.

O funcionamento do NAT64, por meio de 6 passos, está ilustrado a seguir.



NAT64.

Agora, vamos entender cada passo ilustrado na imagem:

- Inicialmente, o PC realiza uma consulta ao DNS64 para receber o mapeamento realizado por esse servidor de nomes, que converte endereços de rede IPv4 em endereços IPv6 mapeados.
- O servidor DNS64 informa ao PC o endereço do serviço já mapeado pela técnica NAT64, 64:ff9::102:304.
- O PC encaminha a solicitação de acesso ao destino IPv6 informado. O pacote é encaminhado ao default gateway da rede IPv6, que opera a tradução do tipo NAT64.

- O roteador identifica, por meio do prefixo de rede 64:ff9::/32, que o destino do pacote é um endereço reservado ao NAT64, realiza a tradução do IPv6 de destino para o IPv4 1.2.3.4 do servidor e encaminha o pacote.
- O servidor sob o IPv4 1.2.3.4 responde a solicitação ao roteador R1 que, além da tradução NAT64, também realizou a tradução do IPv6 de origem do PC, para um IPv4 válido na internet.
- O roteador R1 realiza a operação de tradução inversa e encaminha o pacote de resposta ao PC.

SIIT (Stateless IP/ICMP Translation Algorithm)

Está definida pela RFC 2765 e permite comunicação entre redes com suporte apenas ao protocolo IPv6 e redes com suporte apenas ao protocolo IPv4. Consiste na tradução de campos específicos dos cabeçalhos de pacotes IPv6 em cabeçalhos de pacotes IPv4 e vice-versa.

Esse processo ocorre por meio de um mapeamento de um endereço IPv4 em um endereço IPv6 por meio do endereço 0::FFFF:a.b.c.d, onde a.b.c.d identifica o destino IPv4, e outro endereço traduzido no formato 0::FFFF:0:a.b.c.d identifica o endereço de origem.

Quando esse pacote chega à máquina que opera o SIIT, ela é capaz de identificar os endereços IPv4 transportados de origem e de destino.

BIS (BIS Bump in the Stack)

Está definida pela RFC 2767 e possibilita a comunicação entre aplicações IPv4 com redes IPv6. O BIS tem seu funcionamento entre as camadas de aplicação e de rede, por meio da adição de três módulos:

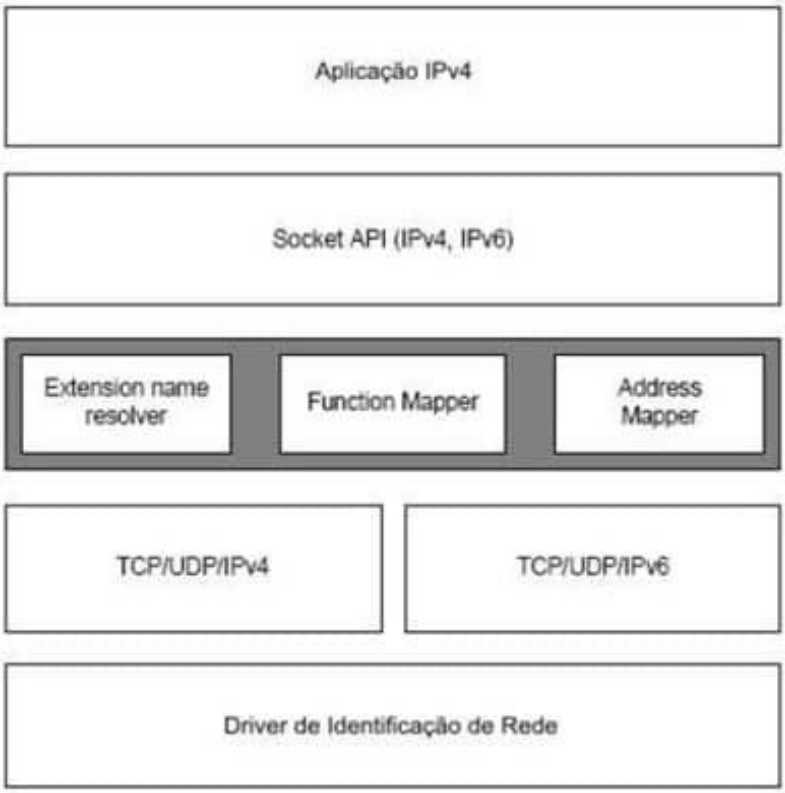
- **Módulo tradutor:** Traduz os cabeçalhos IPv4 enviados em cabeçalhos IPv6, e os cabeçalhos IPv6 recebidos em cabeçalhos IPv4.
- **Extension Name Resolver:** Atua nos questionamentos IPv4 do Domain Name Server (DNS) de forma que, quando o servidor de nomes retorna uma resposta IPv6, o Extension Name Resolver realiza uma tradução para o IPv4 correspondente.
- **Address Mapper:** Consiste na associação de endereços IPv4 mapeados a endereços IPv6 recebidos.

A técnica permite somente a comunicação de aplicações IPv4 com dispositivos IPv6, mas não permite que o caminho inverso seja realizado, além de não funcionar em comunicações multicast.

BIA (BIA Bump in the API)

Similar à BIS, utiliza o Extension Name Resolver e o Address Mapper. Entretanto, opera um Function Mapper, que traduz as funções do socket IPv4 em funções do socket IPv6 e vice-versa.

A imagem a seguir ilustra a pilha de funcionamento do processo BIA, que, assim como o BIS, não possui a capacidade de processar pacotes multicast.



Pilha de funcionamento BIA.

Configurando túneis GRE para integração IPv4 e IPv6

Configurando túneis GRE para integração IPv4 e IPv6 no Packet Tracer

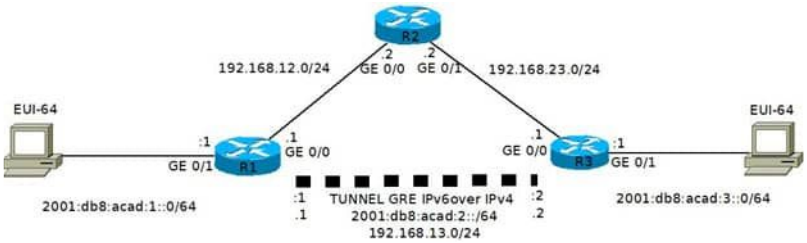
Aprenda de forma prática a configurar túneis GRE para integrar os protocolos IPv4 e IPv6 no Packet Tracer. Explore passo a passo essa técnica eficaz de tunelamento, promovendo a comunicação harmoniosa entre as versões.

> **Conteúdo interativo**
>
> Acesse a versão digital para assistir ao vídeo.

Para sintetizar o conhecimento das técnicas de convivência entre o IPv6 e o IPv4, vamos realizar a configuração de um túnel GRE, que realizará o transporte de informação IPv6 por meio de uma rede IPv4.

Para esse trabalho, vamos configurar a rede apresentada por meio da imagem a seguir, onde devemos evidenciar que o roteador R2 não possui qualquer configuração nem roteamento IPv6. Você pode montar a topologia no Packet Tracer ou baixar o arquivo pré-configurado.

A configuração dos IPv4 e IPv6 é realizada da seguinte forma:



Configuração túnel GRE.

Agora, vamos realizar as configurações necessárias em cada um dos equipamentos. Em R1, você deve configurar as interfaces de rede IPv4, a rota padrão IPv4 e ativar o roteamento IPv6.

```
plain-text

R1#
R1# conf t
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip address 192.168.12.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface gigabitEthernet 0/1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config)# ipv6 unicast-routing
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.12.2
R1(config)# exit
R1#
```

Em R2, vamos configurar as interfaces de rede com os endereços IPv4.

```
plain-text

R2#
R2# conf t
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface gigabitEthernet 0/1
R2(config-if)# ip address 192.168.23.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2#
```

De forma semelhante à R1, você deve configurar as interfaces de rede IPv4, a rota padrão IPv4 e ativar o roteamento IPv6 em R3.

```
plain-text

R3#
R3# conf t
R3(config)# interface gigabitEthernet 0/0
R3(config-if)# ip address 192.168.23.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# interface gigabitEthernet 0/1
R3(config-if)# ipv6 address 2001:db8:acad:3::1/64
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)# ipv6 unicast-routing
R3(config)# ip route 0.0.0.0 0.0.0.0 192.168.23.2
R3(config)# end
R3#
```

Agora, vamos configurar os túneis e a habilitação do processo de roteamento dinâmico **RIPng** nos roteadores R1 e R3.

RIPng

Versão do protocolo RIP para funcionar com o protocolo IPv6.

```
plain-text

R1# conf t
R1(config)# interface tunnel 0
R1(config-if)# ip address 192.168.23.1 255.255.255.0
R1(config-if)# ipv6 2001:db8:acad:2::1/64
R1(config-if)# ipv6 add 2001:db8:acad:2::1/64
R1(config-if)# tunnel source gigabitEthernet 0/0
R1(config-if)# tunnel destination 192.168.23.1
R1(config-if)# tunnel mode ipv6ip
R1(config-if)# ipv6 rip RIPNG enable
R1(config-if)# ipv6 enable
R1(config-if)# exit
R1(config)# ipv6 router rip RIPNG
R1(config-rtr)# exit
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ipv6 rip RIPNG enable
R1(config-if)# end
R1#
```

Vamos agora configurar R3.

```
plain-text

R3# conf t
R3(config)# interface tunnel 0
R3(config-if)# ip address 192.168.13.2 255.255.255.0
R3(config-if)# ipv6 address 2001:db8:acad:2::2/64
R3(config-if)# tunnel source gigabitEthernet 0/0
R3(config-if)# tunnel destination 192.168.12.1
R3(config-if)# tunnel mode ipv6ip
R3(config-if)# ipv6 rip RIPNG enable
R3(config-if)# ipv6 enable
R3(config-if)# exit
R3(config)# ipv6 router rip RIPNG
R3(config-rtr)# exit
R3(config)# interface gigabitEthernet 0/1
R3(config-if)# ipv6 rip RIPNG enable
R3(config-if)# end
R3#
```

Após essas configurações, é possível verificar que o PC1 é capaz de estabelecer contato com a rede 2001:db8:acad:3::/64, sem que haja qualquer configuração IPv6 no roteador R2.

Para testar, vamos realizar o ping no PC1 para ping 2001:db8:acad:3::1. O resultado deve ser semelhante ao que veremos a seguir.

```
plain-text

C:\>ping 2001:db8:acad:3::1

Pinging 2001:db8:acad:3::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:3::1: bytes=32 time=1ms TTL=254

Reply from 2001:DB8:ACAD:3::1: bytes=32 time=13ms TTL=254

Reply from 2001:DB8:ACAD:3::1: bytes=32 time=16ms TTL=254

Reply from 2001:DB8:ACAD:3::1: bytes=32 time=12ms TTL=254

Ping statistics for 2001:DB8:ACAD:3::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 16ms, Average = 10ms

C:\>
```

Configurando NAT64 para integração IPv4 e IPv6

Configurando NAT64 para Integração IPv4 e IPv6 no Packet Tracer

Vamos recapitular o desenvolvimento da configuração do NAT64 no vídeo a seguir. Você pode montar a topologia apresentada no vídeo no Packet Tracer ou baixar o arquivo pré-configurado.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Após estudarmos sobre as técnicas de coexistência entre o IPv4 e o IPv6, apresente o prefixo de endereçamento da técnica de tunelamento 6to4, definido na RFC 3056, para o IPv4 192.168.1.1.

A

2002:c8:c1::/48

B

2002:a101::/48

C

2002:c0a8:101::/48

D

FE80::/16

E

2002:192:168::/48

A alternativa C está correta.

Prefixo: 2002:xxww:aabb::/48, onde xxww:aabb representa o IPv4 em hexadecimal.

192.168.1.1 = c0a8:0101

2002:c0a8:101::/48

Questão 2

Após estudarmos sobre as técnicas de coexistência entre o IPv4 e o IPv6, identifique a faixa de IPv6 reservada ao processo de tradução NAT64.

A

2002::/48

B

64:ff9::/32

C

2002::/32

D

FE80::/16

E

2001::/32

A alternativa B está correta.

O prefixo de rede utilizado para realizar esse tipo de tradução é o 64:ff9::/32, onde um endereço IPv4 pode ser transportado nos últimos 32 bits desse prefixo.

64:ff9::/32

ICMPv6: mensagens e suporte a funcionalidades

Explorando as funcionalidades do protocolo ICMPv6

Neste vídeo, analisaremos detalhadamente as funcionalidades do protocolo ICMPv6. Descubra como esse componente essencial na arquitetura IPv6 contribui para o diagnóstico, monitoramento e correto funcionamento das redes, promovendo uma comunicação eficiente e confiável.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

O protocolo IPv6 insere uma série de funcionalidades e moderniza outras já existentes no protocolo IPv4.

A base dessas funcionalidades está nas mudanças ocorridas no protocolo ICMP para IPv6, Internet Control Message Protocol version 6 — ICMPv6 —, que permite a execução de ferramentas de descoberta de vizinhança e a configuração parcial das informações de IPv6 nos dispositivos.

O protocolo DHCPv6 também fornece uma série de funcionalidades que modernizam o funcionamento de redes IPv6 em relação às redes IPv4.

ICMPv6

O Internet Control Message Protocol version 6 (ICMPv6) está definido pela RFC 4443 como protocolo 58, que além de efetuar as funções já executadas pelo seu antecessor (o ICMP para o IPv4, tais como reportar erros no processamento de pacotes, enviar mensagens sobre o status e características da rede), insere as seguintes novas funcionalidades:

MLD (Multicast Listener Discovery)

Opera com o gerenciamento dos grupos multicast.

NDP (Neighbor Discovery Protocol)

É responsável por identificar e conhecer características da vizinhança.

Path MTU Discovery

Trabalha no processo de descoberta do menor MTU em comunicação entre dispositivos.

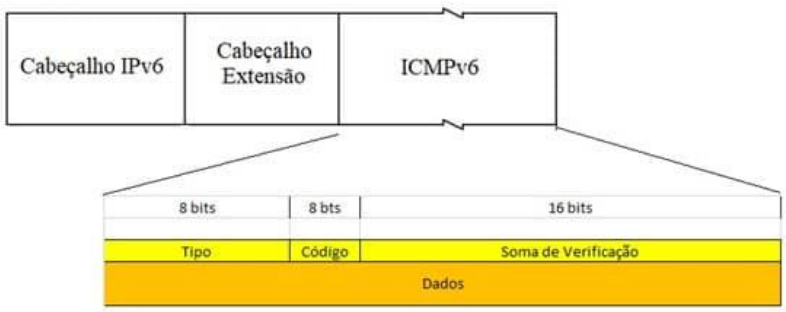
Mobility Support

Cuida do gerenciamento de endereços de origem dos dispositivos dinamicamente.

Autoconfiguração Stateless

Permite a aquisição de endereços globais sem o uso de DHCP.

A estrutura base do ICMPv6 é apresentada pela imagem a seguir, onde podemos observar o cabeçalho base do IPv6, o campo Cabeçalho de Extensão, quando existe, e a parte inerente às informações do ICMPv6, evidenciando os campos que o compõem.



Estrutura básica do ICMPv6.

Como observado, o ICMPv6 possui um cabeçalho de estrutura simples, baseado em quatro campos básicos descritos a seguir.

Type (8 bits)

Especifica o tipo da mensagem e, assim, determina o formato do corpo da mensagem (Campo dados).

Code (8 bits)

Apresenta algumas informações adicionais sobre o motivo da mensagem.

Soma de verificação (16 bits)

É utilizado para verificar a integridade do cabeçalho ICMPv6, também conhecido como Checksum de cabeçalho ou file checksum.

Data

Mostra as informações relativas ao tipo da mensagem, podendo ser desde diagnósticos de rede até erros. Seu tamanho é variável de acordo com a mensagem, desde que não exceda o tamanho de MTU mínimo do IPv6 (1.280 bits).

Devido ao amplo conjunto de informações que podem ser transmitidas por meio dos pacotes ICMPv6, foram designadas duas classes para categorizar as mensagens, as mensagens de Erro e as mensagens de Informação.

Veremos, a seguir, as principais mensagens de erro, onde podemos evidenciar as mensagens de Destino Inalcançável, Pacotes Grandes, Tempo Excedido e Problemas.

Tipo	Nome	Descrição
1	Destination Unreachable	Indica falhas na entrega do pacote como endereço ou porta desconhecida ou problemas na comunicação.
2	Packet Too Big	Indica que o tamanho do pacote é maior que a Unidade Máxima de Trânsito (MTU) de um enlace.
3	Time Exceeded	Indica que o Limite de Encaminhamento ou o tempo de remontagem do pacote for excedido.
4	Parameter Problem	Indica erro em algum campo do cabeçalho IPv6 ou que o tipo indicado no campo Próximo Cabeçalho não foi reconhecido.
100-101		Uso experimental.
102-126		Não utilizado.
127		Reservado para expansão das mensagens de erro ICMPv6.

Mensagens ICMPv6 de erro.
Elaborado por Isaac Newton Ferreira Santa Rita.

A seguir, temos as principais mensagens de informação, onde podemos evidenciar as mensagens utilizadas na Descoberta de Vizinhança, no gerenciamento de grupos Multicast e no teste de conexão ping.

Tipo	Nome	Descrição
128	Echo Request	Utilizadas pelo comando ping.
129	Echo Reply	
130	Multicast Listener Query	Utilizadas no gerenciamento de grupos multicast.
131	Multicast Listener Report	
132	Multicast Listener Done	

133 134 135 136 137	Router Solicitation Router Advertisement Neighbor Solicitation Neighbor Advertisement Redirect Message	Utilizadas com o protocolo Descoberta de Vizinhança.
138	Router Renumbering	Utilizadas no mecanismo de reendereçamento (Renumbering) de roteadores.
139 140	ICMP Node Information Query ICMP Node Information Response	Utilizadas para descobrir informações sobre nomes e endereços, atualmente limitadas a ferramentas de diagnóstico, depuração e gestão de redes.
141 142	Inverse ND Solicitation Message Inverse ND Advertisement Message	Utilizadas em uma extensão do protocolo de Descoberta de Vizinhanca.
143	Version 2 Multicast Listener Report	Utilizada no gerenciamento de grupos multicast.
144 145 146 147	HA Address Discovery Req. Message HA Address Discovery Reply Message Mobile Prefix Solicitation Mobile Prefix Advertisement	Utilizadas no mecanismo de mobilidade IPV6.

148 149	Certification Path Solicitation Message Cert. Path Advertisement Message	Utilizadas pelo protocolo SEND.
150		Utilizada experimentalmente com protocolos de mobilidade como o Seamoby.
151 152 153	Multicast Router Advertisement Multicast Router Solicitation Multicast Router Termination	Utilizadas pelo mecanismo Multicast Router Discovery.
164	FMIPv6 Messages	Utilizada pelo protocolo de mobilidade Fast Handovers.
200-201		Uso experimental.
255		Reservado para expansão do mensagens de erro ICMPv6.

Mensagens ICMPv6 de informação.
Elaborado por Isaac Newton Ferreira Santa Rita.

Descoberta de vizinhança

Protocolo de descoberta de vizinhança para o IPv6

Descubra como o protocolo de descoberta de vizinhança para o IPv6 simplifica e otimiza a identificação de dispositivos na rede. O vídeo a seguir abrange a funcionalidade dessa ferramenta essencial para uma comunicação eficiente em ambientes IPv6.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

A descoberta de vizinhança está discriminada na RFC 4861, e é utilizada por dispositivos IPv6 para:

- Determinar o endereço MAC dos dispositivos de rede.
- Encontrar roteadores vizinhos.
- Determinar prefixos e outras informações de configuração da rede.
- Detectar endereços duplicados.
- Determinar a acessibilidade dos roteadores.
- Redirecionar pacotes.
- Autoconfiguração de endereços.

Para efetuar essas atividades, o processo de descoberta de vizinhança utiliza cinco mensagens descritas no protocolo ICMPv6, a saber:

Router Solicitation (RS)

Definida no ICMPv6 por meio do tipo 133, é utilizada pelos dispositivos para requisitar aos roteadores mensagens Router Advertisements. Normalmente é enviada para o endereço multicast FF02::2 (all-routers on link).

Router Advertisement (RA)

Definida no ICMPv6 por meio do tipo 134, é enviada periodicamente, ou em resposta a uma Router Solicitation, e tem por finalidade anunciar a presença de roteadores em uma rede. As mensagens periódicas são enviadas para o endereço multicast FF02::1 (all-nodes on link), e as solicitadas são enviadas diretamente para o endereço unicast do solicitante.

Neighbor Solicitation (NS)

Definida no ICMPv6 por meio do tipo 135, é uma mensagem multicast enviada por um dispositivo para determinar o endereço MAC e a acessibilidade de um vizinho, além de detectar a existência de endereços duplicados.

Neighbor Advertisement (NA)

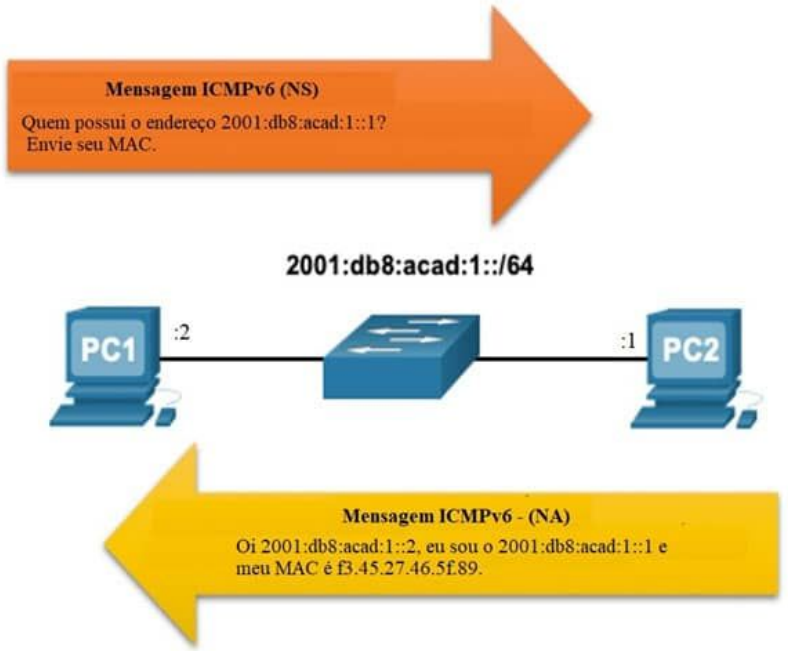
Definida no ICMPv6 por meio do tipo 136, é enviada como resposta a uma Neighbor Solicitation e pode também ser enviada para anunciar a mudança de algum endereço dentro do enlace.

Redirect

Definida no ICMPv6 por meio do tipo 137, é utilizada por roteadores para informar aos dispositivos o melhor roteador para encaminhar o pacote ao destino.

A **descoberta de um dispositivo vizinho** é um processo semelhante ao efetuado pelo protocolo ARP em redes IPv4, realizada por meio do envio de uma mensagem multicast NS (Neighbor Solicitation) com a solicitação do MAC de um vizinho que, por sua vez, responde à solicitação com uma mensagem NA (Neighbor Advertisement), informando seu MAC.

O processo de descoberta de vizinhança está ilustrado a seguir.



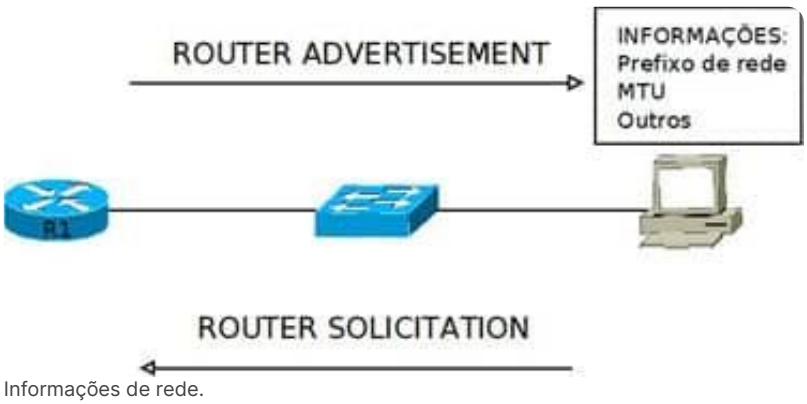
Descoberta de vizinhança.

Anúncio de roteadores

Realizado por equipamentos com capacidade de roteamento, normalmente o default gateway da rede, muito útil em processos de autoconfiguração de endereços IPv6.

Isso é possível por meio da mensagem RA (Router Advertisement), enviada periodicamente pelos roteadores, ou em resposta a uma mensagem RS (Router Solicitation), enviada por um dispositivo da rede. Além de anunciar a existência do roteador como alternativa de saída da rede, essas mensagens também podem transmitir dados, como prefixos de rede, MTU, DNS e outros, para que os dispositivos realizem autoconfiguração.

A imagem a seguir ilustra esse processo.

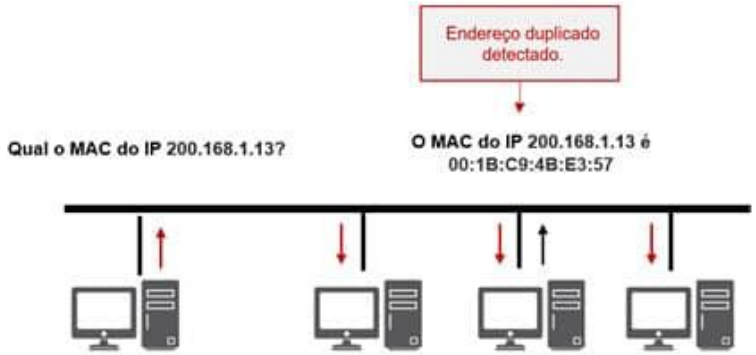


Informações de rede.

Detecção de endereços duplicados

Nada mais é que um procedimento utilizado pelos dispositivos IPv6 para verificar a unicidade dos endereços, devendo ser realizado antes de se atribuir qualquer endereço unicast a uma interface.

Consiste no envio de uma mensagem NS pelo dispositivo, solicitando o MAC do próprio endereço. Caso alguma mensagem NA seja recebida como resposta, isso indicará que o endereço já está em uso, e o processo de configuração deve ser interrompido. Caso contrário, o IPv6 em questão está livre para ser utilizado.



Detecção de endereços duplicados

Autoconfiguração de endereços (statelless)

Está definida pela RFC 4862, e permite que endereços IPv6 sejam atribuídos automaticamente a dispositivos, a partir do recebimento do prefixo de rede de roteadores IPv6 presentes em suas redes.

Para isso, os dispositivos componentes de uma rede IPv6 realizam uma solicitação por meio da mensagem Router Solicitation (RS), para obter o prefixo de rede de um roteador IPv6 presente nessa rede. Essa mensagem é remetida em multicast aos roteadores da rede, que por sua vez respondem por meio de mensagens Router Advertisement (RA), informando o prefixo de rede e seu endereço. Após isso, a composição completa do IPv6 desses dispositivos é concluída com a utilização do processo IEEE EUI-64.

Atenção

Além das informações de prefixo de rede e de default gateway, essa troca de mensagens pode informar ao dispositivo solicitante um valor predefinido para o campo Limite de Encaminhamento e o MTU da rede. Caso não haja equipamento roteador presente na rede IPv6, o dispositivo ficará somente com seu endereço link local para comunicação local.

Outras funcionalidades do IPv6

Explorando funcionalidades IPv6

Neste vídeo, abordamos as funcionalidades do IPv6, incluindo o protocolo DHCPv6, renumeração de redes, descoberta de tamanho de MTU e mobilidade IPv6. Compreenda como essas ferramentas fundamentais contribuem para a eficiência e adaptabilidade na comunicação em redes IPv6.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

DHCPv6

O Dynamic Host Configuration Protocol (DHCPv6) está definido na RFC 3315 e permite a autoconfiguração de endereços statefull para dispositivos e IPV6, realizando a configuração de informações necessárias ao funcionamento de redes, como o endereço de:

- Servidores de nomes (Domain Name Server — DNS)
- Servidores de tempo (Networking Time Protocol — NTP)
- Servidores de arquivos (File Transfer Protocol – FTP)

No DHCPv6, a troca de mensagens entre cliente e servidor é realizada utilizando-se o protocolo UDP. Os clientes utilizam um endereço link local para transmitir ou receber mensagens DHCPv6, enquanto os servidores utilizam um endereço multicast reservado (FF02::1:2 ou FF05::1:3) para receber mensagens dos clientes.

Renumeração de redes

O endereçamento de redes IPv6 está, normalmente, baseado nos prefixos atribuídos por provedores de internet, que em uma eventual alteração demandam a renumeração de todos os endereços de dispositivos naquela rede.

> O mecanismo **router renumbering**, definido na RFC 2894, utiliza mensagens ICMPv6 do tipo 138, enviadas aos roteadores, por meio do endereço multicast all-routers, contendo as instruções de como atualizar seus prefixos automaticamente, desonerando os administradores de rede dessa tarefa.

As mensagens router renumbering são formadas por sequências de operações dos tipos:

Match-prefix

Indica qual prefixo deve ser modificado.

Use-prefix

Indica o novo prefixo, o que permite aos roteadores alterar a numeração dos dispositivos de rede.

Descoberta de tamanho de MTU

O Maximum Transmission Unit (MTU) é uma limitação de tamanho máximo de pacote que cada rede pode processar. Isso implica que pacotes com tamanho maior que o definido pelo MTU devem sofrer fragmentação, em um processo dispendioso aos roteadores.

A fragmentação ocorre de formas diferentes em cada tipo de rede:

Redes IPv4	Redes IPv6
Cada roteador pode fragmentar os pacotes, caso sejam maiores do que o MTU permitido.	A fragmentação dos pacotes é realizada apenas na origem, não sendo permitida durante o trânsito de dados.

Em redes IPv6, faz-se necessária a descoberta do MTU vigente para que os dispositivos possam montar os pacotes de acordo com a limitação imposta.

Para isso, é utilizado, no início do processo de fragmentação, o protocolo PMTUD (Path MTU Discovery), descrito na RFC 1981, que descobre, de forma dinâmica, qual o tamanho máximo permitido ao pacote, identificando previamente os MTU da referida rede.

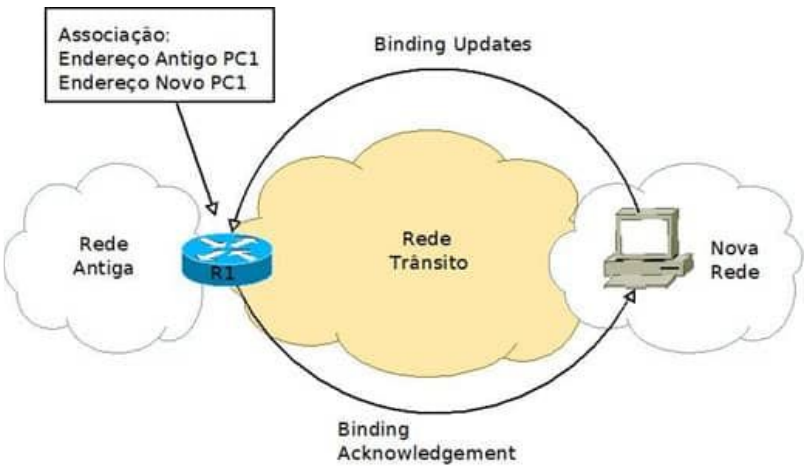
Mobilidade IPv6

O suporte à mobilidade foi mais uma funcionalidade incorporada ao IPv6. Permite que o dispositivo em trânsito entre redes IPv6, muito comum em redes celulares, desloque-se sem a necessidade de alterar seu endereço IPv6 de origem, tornando a movimentação entre redes invisível ao destino de suas comunicações.

> A mobilidade IPv6 permite que todos os pacotes enviados para esse dispositivo móvel continuem sendo encaminhados a ele, sem necessidade de alteração de endereço.

Para que isso ocorra, quando um dispositivo está em trânsito, ou seja, saindo de uma rede para uma nova rede, deve enviar uma mensagem Binding Updates para o roteador de sua rede antiga, informando sobre as novas configurações de IPv6 na rede nova. O roteador confirma a atualização de dados por meio do envio de um Binding Acknowledgement ao dispositivo móvel.

A imagem a seguir ilustra esse processo de associação dos endereços IPv6 de um dispositivo em trânsito.



Mobilidade IPv6.

Configuração de endereços IPv6

Vamos então configurar as formas de endereçamento IPv6 que vimos até agora. Você pode montar a topologia apresentada no vídeo no Packet Tracer ou baixar o arquivo pré-configurado.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Roteadores Cisco possuem duas importantes flags com essa finalidade, a Flag O e a Flag M, capazes de ajustar a configuração de entrega de endereços IPv6. A combinação entre elas permite que roteadores entreguem informações de endereçamento aos dispositivos de formas diferentes, conforme apresentado a seguir.

Flag O	Flag M	Estado	OBS
0	0	Stateless	Valor padrão.
1	0	Stateless + DHCPv6	Definição de endereços pelo roteador e emissão de outras informações pelo servidor DHCPv6.
X	1	DHCPv6	Todo endereçamento será entregue pelo servidor DHCPv6.

Flags de endereçamento Cisco.
Elaborado por Isaac Newton Ferreira Santa Rita.

⚠

Atenção

A Flag O pode ser alterada pelo comando ipv6 nd other-config-flag e a Flag M pelo comando ipv6 nd managed-config-flag.

Para facilitar a compreensão, faremos juntos uma atividade na qual será necessário atribuir endereços IPv6 em três cenários diferentes:

Cenário 1

Utilizaremos o processo padrão, com a entrega de endereçamento pelo processo stateless.

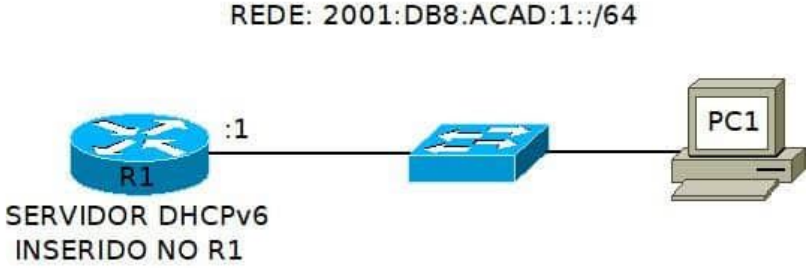
Cenário 2

Utilizaremos a entrega de endereçamento pelo processo stateless e a informação de DNS pelo servidor DHCPv6.

Cenário 3

Faremos a entrega de todas as informações por um servidor DHCPv6.

O cenário geral de nossa atividade está ilustrado a seguir.



Cenário geral de configuração de endereço IPv6 automático.

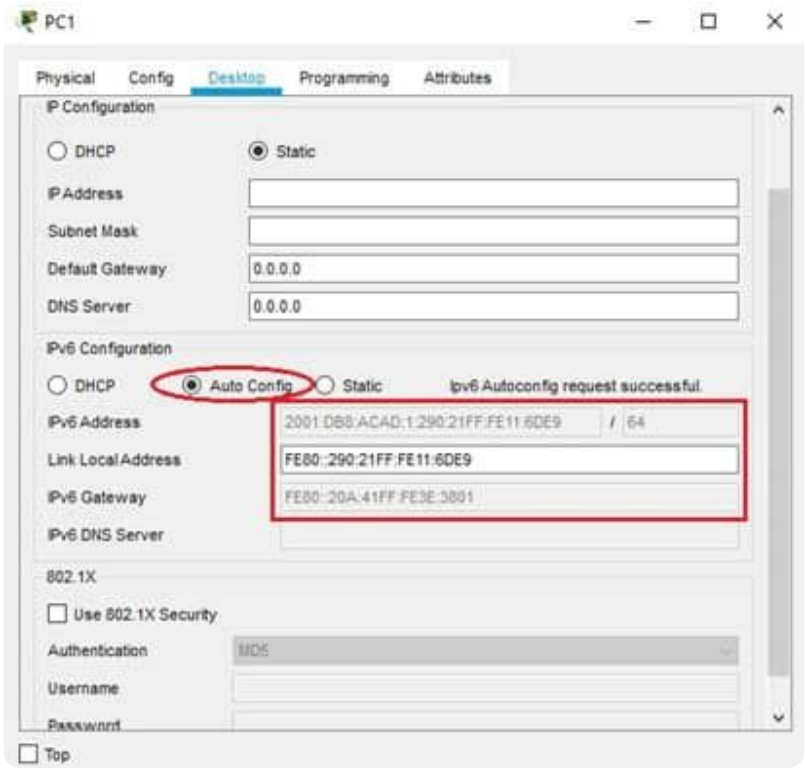
Cenário 1: Endereçamento stateless

Crie a topologia de nosso cenário geral e faça as configurações no roteador R1 conforme a seguir:

```
plain-text

R1# conf t
R1(config)# ipv6 unicast-routing (habilita processo IPv6)
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64 (configure IPv6 na interface)
R1(config-if)# no shutdown
R1#
```

Uma vez realizadas as configurações básicas no roteador, o processo stateless já é estabelecido e o PC1 já recebe endereço IPv6, composto pelo prefixo de rede do roteador e o processo EUI-64. A imagem a seguir apresenta as configurações de IPv6 do PC1.



Endereçamento do PC1 pelo processo stateless.

Cenário 2: Endereçamento stateless + DHCPv6

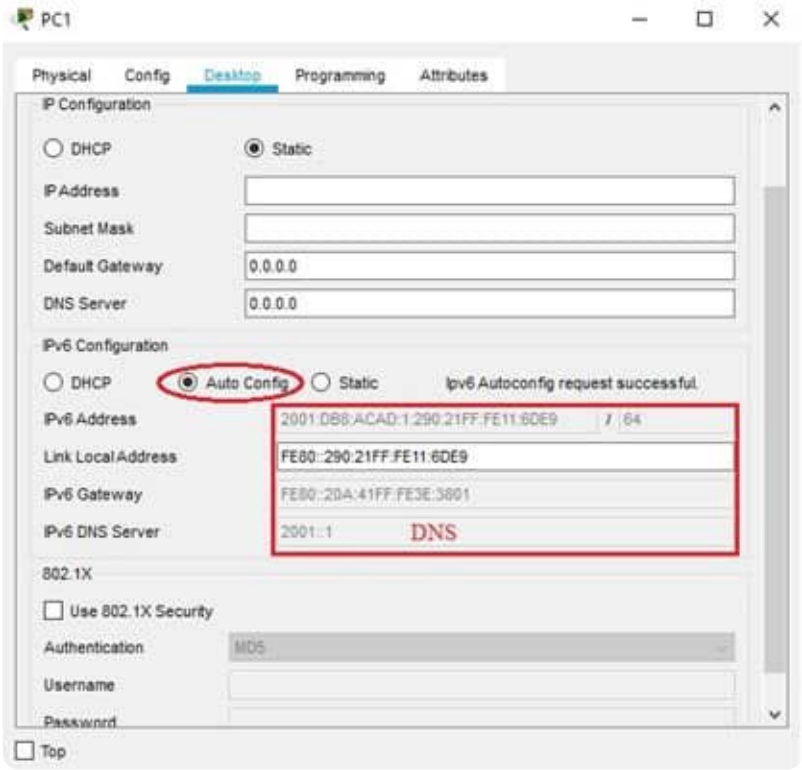
O endereçamento básico, composto por IPv6, prefixo de rede e gateway será entregue por meio do processo stateless, e o endereço de DNS será entregue pelo servidor DHCPv6 configurado no próprio roteador R1.

Utilizando a mesma topologia inicial do cenário 1, realize a configuração no roteador R1 conforme demonstrado a seguir.

```
plain-text

R1# conf t
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 dhcp server DHCPv6(Informa quem é o servidor DHCPv6)
R1(config-if)# ipv6 nd other-config-flag (Define que informações adicionais serão obtidas
pelo servidor DHCPv6)
R1(config-if)#
R1(config-if)# exit
R1(config)# ipv6 dhcp pool DHCPv6 (Define o servidor local DHCPv6)
R1(config-dhcpv6)# dns-server 2001::1 (Define o servidor DNS)
R1(config-dhcpv6)# end
R1#
```

A próxima imagem mostra que o PC1 recebeu, além das informações do cenário 1, pelo processo stateless, o endereço do servidor DNS por meio do servidor DHCPv6 definido no roteador R1.



Endereçamento do PC1 pelo processo stateless + DHCPv6.

Cenário 3: Endereçamento statefull (DHCPv6)

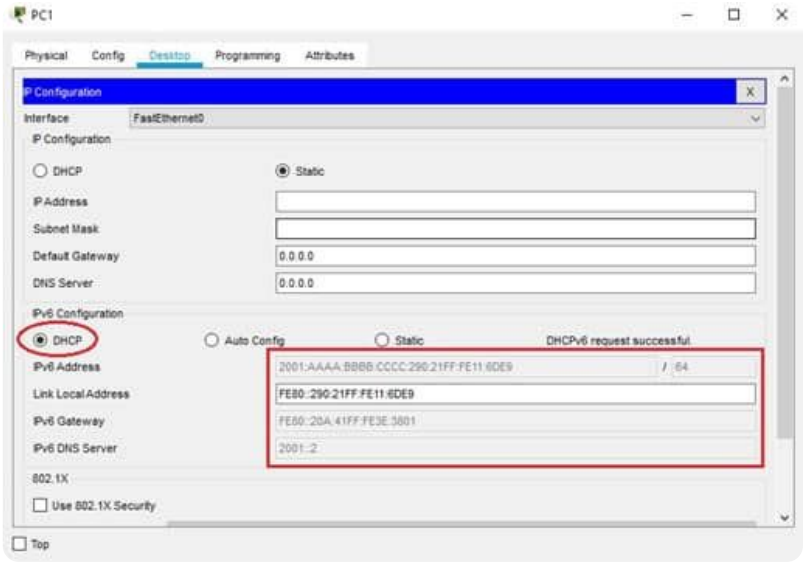
Toda configuração do PC será realizada pelo servidor DHCPv6 definido no roteador R1.

Novamente utilizando a mesma topologia, configure o roteador R1 conforme abaixo.

```
plain-text

R1# conf t
R1(config)# ipv6 dhcp pool DHCPv6 (configura o servidor DHCPv6)
R1(config-dhcpv6)# dns-server 2001::2 (DNS)
R1(config-dhcpv6)# domain-name cisco.com(Dominio)
R1(config-dhcpv6)# address prefix 2001:aaaa:bbbb:cccc::/64 (indica o conjunto de
endereços a serem alocados pelo servidor)
R1(config-dhcpv6)# exit
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 dhcp server DHCPv6(Define o servidor local DHCPv6)
R1(config-if)# ipv6 nd managed-config-flag(Define que informações serão obtidas
exclusivamente pelo servidor DHCPv6)
```

A imagem seguinte mostra que o PC recebeu todas as configurações do servidor DHCPv6 definido no roteador R1.



Endereçamento do PC1 pelo servidor DHCPv6.

Verificando o aprendizado

Questão 1

O protocolo ICMPv6 apresenta uma importância maior do que o seu correlato ICMPv4, assumindo funções que antes eram executadas por outros protocolos, por exemplo, o ARP. Entre as funcionalidades que foram implementadas no ICMPv6, podemos dizer que

A

o NDP (Neighbor Discovery Protocol) é responsável por realizar a descoberta do menor MTU na comunicação entre dispositivos.

B

a autoconfiguração statefull permite a aquisição de endereços globais sem o emprego de servidores DHCP.

C

o MLD (Multicast Listener Discovery) permite realizar o gerenciamento de grupos multicast.

D

o Mobility Support é responsável pelo suporte à utilização do IPv6 nas redes celulares.

E

o Path MTU Discovery é responsável pela definição, na origem, do caminho a ser seguido pelos datagramas IPv6.

A alternativa C está correta.

O protocolo ICMPv6 é responsável por diversas funcionalidades em uma rede IPv6 e, inclusive, o bloqueio do tráfego ICMPv6 nos firewalls pode impedir o correto funcionamento da rede. Entre suas funções, o MLD permite que os grupos multicast possam ser gerenciados em redes IPv6.

Questão 2

A descoberta de vizinhança é utilizada pelos dispositivos que funcionam com o protocolo IPv6 para realizar diversas atividades, como determinar o endereço MAC dos dispositivos de rede. Para que essas funcionalidades sejam atendidas, são utilizadas 5 mensagens ICMPv6. Assinale a alternativa que apresenta corretamente a funcionalidade da mensagem ICMPv6.

A

A mensagem Neighbor Solicitation (NS) é utilizada para anunciar a mudança de algum endereço utilizado dentro do enlace.

B

A mensagem Router Advertisement (RA) pode ser enviada periodicamente e tem como objetivo anunciar a existência de roteadores na rede.

C

A mensagem Router Solicitation (RS) é utilizada para que a estação de origem obtenha um caminho prévio até o destino.

D

A mensagem Redirect tem por objetivo redirecionar as mensagens ICMPv6 entre os roteadores quando for necessária a fragmentação.

E

A mensagem Neighbor Advertisement (NA) é enviada para as estações clientes IPv6 informando a lista de servidores DHCPv6.

A alternativa B está correta.

O protocolo IPv6 apresentou novas funcionalidades para facilitar a operação da rede por meio das mensagens ICMPv6 Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA) e Redirect. Entre essas novas funcionalidades, as mensagens RS são utilizadas para que sejam solicitadas aos roteadores mensagens RA com o objetivo de anunciar a presença dos roteadores dentro de determinada rede.

Considerações finais

Vimos os conceitos básicos do protocolo de rede IPv6 e como agrega funcionalidades em relação ao IPv4.

Mostramos que possui uma capacidade gigantesca de endereçamento e como esses endereços são organizados globalmente. Além disso, vimos as principais técnicas de transição que viabilizam a coexistência entre as versões 4 e 6 do protocolo de internet.

É necessário aprofundar os conhecimentos na camada de transporte do modelo OSI, para melhorar o entendimento sobre os processos de comunicação entre máquinas na internet.

Podcast

A seguir, ouça sobre o protocolo IPv6.

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore+

- Para saber mais sobre os assuntos tratados neste conteúdo, pesquise na internet as RFC do protocolo IPv6 comentadas neste curso.

Referências

KUROSE, J. F.; ROSS, K. **Redes de computadores e a internet**. 6. ed. São Paulo: Pearson, 2014.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. 5. ed. São Paulo: Pearson Universidades, 2011.