Redes de Computadores I

Aula 11 - IPv6 - Parte I

Apresentação

Em aulas anteriores, estudamos a arquitetura da rede mundial de computadores conhecida como Internet. Vimos que a arquitetura TCP/IP permitiu que todas as redes conseguissem se comunicar independentemente da tecnologia empregada, ou seja, de modo que todas elas formassem uma única rede. O principal protocolo responsável por permitir essa integração é o *Internet Protocol*, chamado simplesmente de IP.

Nesta aula, aprofundaremos nossos estudos sobre a versão mais recente do protocolo IP citada em aulas anteriores, conhecida como IPv6. Destacaremos o problema do esgotamento da faixa de endereçamento IPv4, as relações de compatibilidade entre as diferentes versões do IP e os detalhes da implementação do protocolo, tais como o formato do datagrama.

Objetivos

- Compreender o problema do esgotamento do IPv4;
- Entender aspectos da compatibilidade entre IPv4 e IPv6;
- Explicar estratégias de compatibilidade e transição;
- Descrever detalhes de implementação do protocolo IPv6.

Evolução da Internet e Esgotamento do IPv4

Ao estudarmos sobre a arquitetura da Internet, vimos que o seu crescimento e popularização ocorreram de forma bastante acentuada. Uma das principais consequências desse rápido crescimento foi o consumo e o consequente esgotamento dos endereços IPv4.

A versão de protocolo utilizada, desde aquela época até os dias atuais, é a 4, frequentemente referida com o nome do protocolo de IPv4, como estudamos em aulas anteriores. Apesar de essa versão se mostrar muito robusta (sendo utilizada até hoje) e de fácil implantação, sua concepção original não previu alguns aspectos, como o crescimento das redes e um possível esgotamento dos endereços IP; o aumento da tabela de roteamento; os problemas relacionados à segurança dos dados transmitidos; e a prioridade na entrega de determinados tipos de pacotes.

Relembremos, agora, o esquema de endereçamento do IPv4: sua especificação reserva 32 *bits* para o endereço IP, o que possibilita gerar mais de 4 bilhões de endereços distintos. Inicialmente, esses endereços foram divididos nas seguintes classes de tamanhos fixos:

- Classe A: definia o *bit* mais significativo como 0, utilizava os 7 *bits* restantes do primeiro octeto para identificar a rede, e os 24 *bits* restantes para identificar o host. Esses endereços utilizavam a faixa de 1.0.0.0 até 126.0.0.0;

- Classe B: definia os 2 *bits* mais significativos como 10, utilizava os 14 *bits* seguintes para identificar a rede, e os 16 *bits* restantes para identificar o host. Esses endereços utilizavam a faixa de 128.1.0.0 até 191.254.0.0;

- Classe C: definia os 3 *bits* mais significativos como 110, utilizava os 21 *bits* seguintes para identificar a rede, e os 8 *bits* restantes para identificar o host. Esses endereços utilizavam a faixa de 192.0.1.0 até 223.255.254.0.

Embora essa divisão tenha uma ideia de flexibilizar a distribuição de faixas de endereçamento, ela se mostrou bastante ineficiente, à medida que as redes TCP/IP começaram a crescer em taxas aceleradas. A classe A atendia um número muito pequeno de redes e ocupava metade de todos os endereços disponíveis, enquanto a classe C permitia criar muitas redes, mas com poucos endereços disponíveis. Em outras palavras, ao mesmo tempo em que algumas classes acarretavam desperdícios, as outras não supriam a necessidade de endereços disponíveis. Para exemplificar o problema, imagine que se precise endereçar 300 dispositivos em uma rede. Nessa situação, seria necessário obter um bloco de endereços da classe B, desperdiçando, assim, quase o total dos 65 mil endereços.

Diante desse cenário, a IETF (*Internet Engineering Task Force*) passou a estudar e discutir medidas objetivando solucionar o problema do esgotamento da faixa de endereçamento do IPv4. Tais medidas já foram estudadas intensamente em aulas anteriores: a implantação do CIDR, a utilização do DHCP e a tradução de endereços de rede (NAT).

Endereçamento IPv6

A estratégia de endereçamento do IPv6 é a utilização de 128 *bits*, permitindo, assim, uma quantidade de endereços distintos da ordem de 10^{38}, eliminando o problema de escassez de endereços no futuro previsível. Além de aumentar o número de endereços disponíveis, a implantação do protocolo IPv6 também resolve determinados problemas recorrentes no IPv4. Alguns dos pontos que merecem destaque são a simplificação do protocolo, a incorporação de requisitos de segurança e as questões relacionadas à qualidade de serviço.

A notação normalmente adotada é a hexadecimal dois pontos, agrupando blocos de 16 *bits* (denotado por 4 dígitos hexadecimais) em um total de 8 grupos divididos por dois pontos “:”. Ainda na representação de endereços IPv6, é permitido utilizar caracteres maiúsculos ou minúsculos. Abaixo podemos ver alguns exemplos de endereços IPv6:

2001:cdba:0000:0000:0000:0000:3257:9652

2001:0db8:85a3:0000:0000:8a2e:0370:7334

fec0:0000:0000:0000:bd92:a4b8:d233:b05f

Algumas regras de simplificação podem ser adotadas, como a omissão de zeros presentes nos bits mais significativos, conforme o exemplo abaixo:

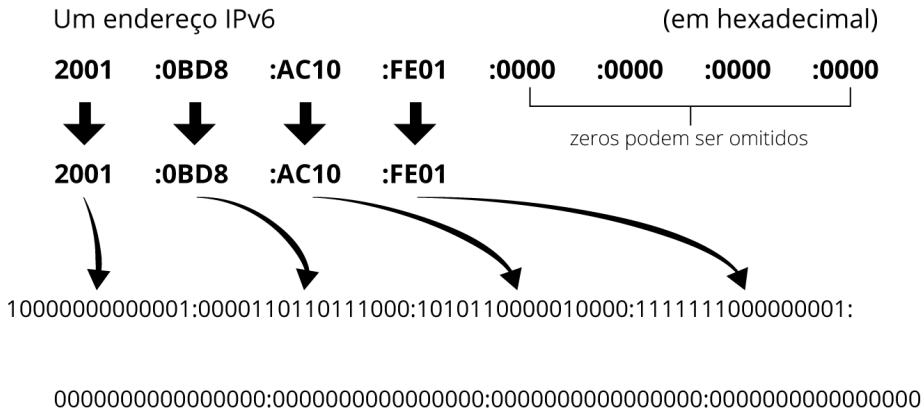
FF05:0000:0000:0000:0000:0000:0000:00B3 → FF05:0:0:0:0:0:0:B3

Outra regra de simplificação é a omissão de zeros consecutivos por "::", regra que só pode ser aplicada uma vez em cada endereço IPv6, como o exemplo abaixo (aplicando as duas regras estudadas):

FF05:0000:0000:0000:0000:0000:0000:00B3 → FF05::B3

A Figura 1 ilustra outro exemplo de aplicação das regras de simplificação em endereços IPv6.

Figura 01 - Formato do endereço IPv6



Outra forma de representação importante a ser destacada é a dos prefixos de rede. Como estudado no IPv4, no IPv6 também temos uma parte do endereço identificador da rede. Essa notação continua sendo escrita do mesmo modo que no IPv4, utilizando a notação CIDR. Ela é representada na forma:

ENDEREÇO IPV6 / TAMANHO DO PREFIXO

Onde "tamanho do prefixo" é um valor decimal que determina a quantidade de bits mais significativos (à esquerda) do endereço IPv6 que representam o prefixo de rede. Veja abaixo exemplos dessa representação:

2001:db8::ca5a:0:2000/64

2002:C0A8::/48

Atividade 01

1. Simplifique ao máximo os seguintes endereços IPv6 usando as técnicas estudadas:
    a. 2001:0db8:0000:1200:0fe0:0000:0000:0003
    b. 2001:0db8::ca5a:0000:2000
    c. 2001:0db8:face:b00c:0000:0000:0100:00ab

Clique aqui para visualizar as respostas

Respostas

a. 2001:db8:0:1200:fe0::3

b. 2001:db8::ca5a:0:2000

c. 2001:db8:face:b00c::100:ab

Datagrama IPv6

O Quadro 1 mostra o formato do datagrama definido na versão 6 do protocolo IP. Assim como o protocolo IPv4, o datagrama IPv6 é composto de duas partes: o cabeçalho e a carga útil (dados).

VERSÃO	CLASSE DE TRÁFEGO	IDENTIFICADOR DE FLUXO	
TAMANHO DOS DADOS		PRÓXIMO CABEÇALHO	LIMITE DE SALTOS
ENDEREÇO DE ORIGEM			
ENDEREÇO DE DESTINO			
DADOS			

Quadro 1 – Formato do datagrama IPv6

O cabeçalho consiste em uma parte fixa com funcionalidade mínima necessária para todos os pacotes, mas que opcionalmente pode ser adaptada por extensões que permitem agregar novas funcionalidades (veremos mais sobre isso ainda nesta aula). O cabeçalho fixo ocupa um total de 40 *bytes* (320 *bits*). Em relação aos campos que compreendem o cabeçalho base no IPv6, temos o seguinte:

- **Versão** (4 *bits*): indica a versão do protocolo. No caso, versão 6 representada em binário 0110.

- **Classe de Tráfego** ou *Traffic Class (8 bits):* indica a classe de serviço à qual o datagrama pertence, permitindo um tratamento diferenciado a pacotes provenientes de determinadas aplicações. É uma das bases para o funcionamento do mecanismo de qualidade de serviço (QoS).

- **Fluxo de Rótulo** ou *Flow Label (20 bits):* inexistente no IPv4, permite marcar pacotes de um fluxo específico, com o objetivo de diferenciar esses pacotes na camada de rede. Portanto, esse campo habilita uma identificação de fluxo e um processo por fluxo em cada roteador no caminho do pacote, facilitando, assim, o mecanismo de qualidade de serviço (QoS).

- **Tamanho dos dados** (*16 bits*): indica o tamanho total da área de dados (carga útil) do pacote.

- **Próximo cabeçalho** (*8 bits*): semelhante ao campo “Protocolo” do IPv4, indicando o tipo de informação que segue o cabeçalho base do IPv6. Essa informação pode ser o protocolo usado na camada de transporte, UDP ou TCP, ou um cabeçalho de extensão (que estudaremos adiante).

- **Limite de Saltos** (*8 bits*): semelhante ao campo TTL do IPv4, limitando o número máximo de roteadores (hops) que um pacote IPv6 pode passar antes de ser descartado.

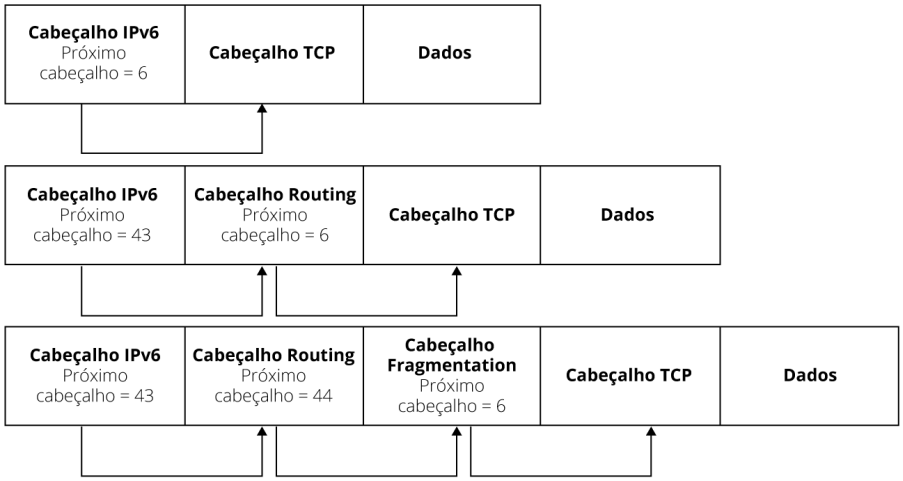
- **Endereço de origem** (*128 bits*): indica o endereço de origem do pacote.

- **Endereço de destino** (*128 bits*): indica o endereço de destino do pacote.

Cabeçalhos de extensão

Diferentemente da versão 4 do IP, que inclui informações opcionais diretamente no cabeçalho base, no IPv6 temos o conceito de cabeçalhos de extensão. Estes localizam-se entre o cabeçalho base e a carga útil, não possuindo quantidade ou tamanho fixo. No caso da existência de múltiplos cabeçalhos de extensão no mesmo pacote, eles serão adicionados em série, formando uma cadeia de cabeçalhos. Assim como no cabeçalho base, cada cabeçalho de extensão contém um campo “Próximo cabeçalho”, indicando o tipo de informação que segue o cabeçalho em questão. Essa informação pode ser o protocolo usado na camada de transporte, ou, então, um outro cabeçalho de extensão. A Figura 2 exemplifica a utilização dos cabeçalhos de extensão.

Figura 02 - Utilização de cabeçalhos de extensão



Existem diversos cabeçalhos de extensão definidos, e novas extensões podem ser definidas no futuro.

Entre eles, é possível citar: *Hop-by-Hop Options, Destination Options, Routing, Fragmentation, Authentication Header e Encapsulating Security Payload*. A seguir, veremos brevemente a função de cada um desses cabeçalhos:

- ***Hop-by-Hop Options:*** único dos cabeçalhos de extensão que é processado também nos nós intermediários (roteadores), além do *host* de origem e de destino.

- ***Destination Options:*** opções que devem ser examinadas somente no destino.

- ***Routing:*** utilizado para direcionar um pacote para um ou mais nós intermediários antes de ser enviado para o seu destino.

- ***Fragmentation:*** para que seja realizado o envio de um pacote maior que o MTU da rede, o nó origem deve dividir o pacote em múltiplos fragmentos. Esse campo carrega informações necessárias para a remontagem do pacote original.

- ***Authentication Header:*** parte do IPSec, que será estudado em Segurança de Redes, provê recursos de segurança que oferecem confidencialidade, autenticidade e integridade.

- ***Encapsulating Security Payload:*** parte do IPSec, que será estudado em Segurança de Redes, provê recursos de segurança que oferecem confidencialidade, autenticidade e integridade.

Compatibilidade: IPv4 e IPv6

Podemos notar, pela especificação do projeto IPv6, que esse protocolo tem diferenças em relação a sua versão anterior, as quais tornam os protocolos IPv6 e IPv4 incompatíveis, a começar pelo comprimento do endereço, o qual deixou de ter 32 *bits* para ter 128 *bits*.

Dessa forma, durante o período de transição entre as duas versões do protocolo IP, faz-se necessária a adoção de técnicas e estratégias para que exista interoperabilidade entre os protocolos. Assim, enquanto o IPv6 não substitui completamente o IPv4, são necessários alguns mecanismos para permitir a comunicação e a coexistência entre eles. Cada mecanismo desse apresenta uma característica específica, podendo ser utilizado individualmente ou em conjunto com outras técnicas, de modo a atender as necessidades de cada situação, seja a migração para o IPv6 feita passo a passo, iniciando por um único *host* ou sub- rede, ou até mesmo de toda uma rede corporativa.

As estratégias de transição podem ser agrupadas em três classes:

- **Pilha Dupla (*dual stack*):** opera suportando ambos os protocolos (v4 e v6) no mesmo dispositivo;

- **Tunelamento (*tunelling*):** opera permitindo o tráfego de pacotes IPv6 sobre infraestrutura de rede IPv4, ou vice-versa;

- **Tradução (*translation*):** opera permitindo a comunicação dos nós que operam exclusivamente IPv6 com os nós que operam exclusivamente IPv4 através da conversão dos pacotes.

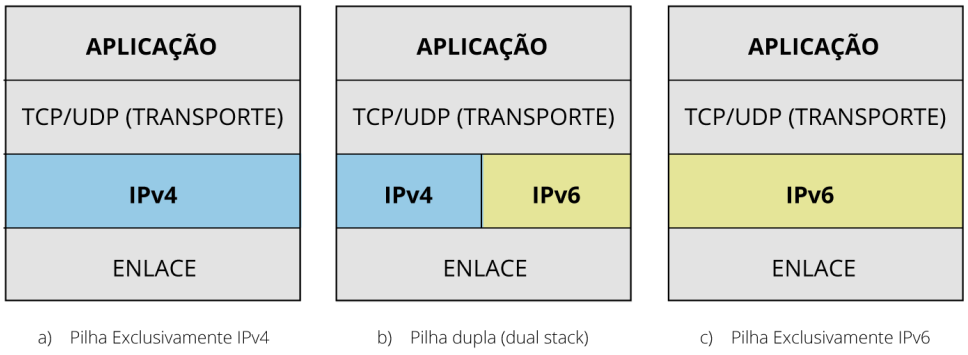
Estratégias de transição

Pilha Dupla (*dual stack*)

Neste mecanismo de transição, os nós se tornam capazes de enviar e receber pacotes tanto para o IPv4 quanto para a nova versão IPv6. Dessa forma, um nó IPv4/IPv6, ao se comunicar com um nó IPv6, comporta-se como um nó IPv6 e, ao se comunicar com um nó IPv4, comporta-se como um nó IPv4. Em outras palavras, são nós que proveem suporte a ambas as versões do *Internet Protocol*.

Esse método permite que *hosts* e roteadores estejam equipados com pilhas para ambos os protocolos (como pode ser visto na Figura 3), tendo a capacidade de receber e enviar os dois formatos de datagrama, IPv4 e IPv6. Sendo assim, cada nó operando em *dual stack* é configurado com ambos os endereços.

Figura 03 - a) Pilha exclusivamente IPv4. b) Pilha dupla (dual stack). c) Pilha exclusivamente IPv6.



Fonte: Elaborado pelo Autor

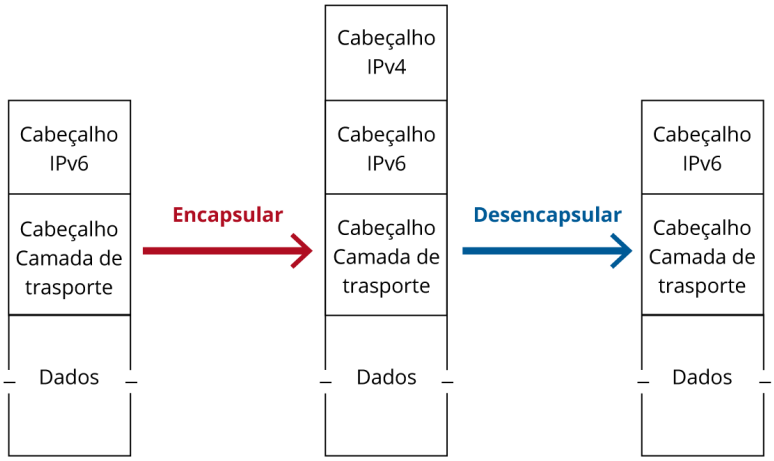
Essa estratégia de transição facilita a implantação do IPv6, pois permite que esta seja feita de forma gradual, configurando apenas pequenas seções do ambiente de rede a cada vez. No momento em que o IPv4 não seja mais utilizado, basta, então, simplesmente desabilitar a pilha IPv4 de cada nó operando em pilha dupla.

Tunelamento

Quando não se é possível implantar pilhas duplas nos nós da rede, uma das alternativas é a utilização de técnicas de tunelamento. As estratégias de tunelamento permitem encapsular pacotes IPv6 dentro de pacotes IPv4. Esse tipo de encapsulamento é conhecido como *6in4* ou *IPv6-in-IPv4*. É uma técnica eficiente quando os *hosts* de origem e destino estão em um mesmo tipo de rede, mas estão separados por um tipo de rede diferente.

Basicamente, a técnica *6in4* encapsula o pacote IPv6 dentro do campo de dados de um pacote IPv4, adequa, além de outros campos, os endereços de origem e destino para o IPv4, e envia o pacote que transitará em um segmento de rede IPv4 (ver Figura 4). No destino, ao verificar que se trata de um pacote identificado como 6in4, será removido o cabeçalho IPv4 e o pacote será tratado como IPv6. Também é possível, de forma análoga, encapsular pacotes IPv4 em pacotes IPv6, técnica conhecida como *4in6*.

Figura 04 - Funcionamento do tunelamento *6in4*



Uma das formas de se utilizar túneis é criando-os manualmente. A técnica *6over4* utiliza um túnel manual estabelecido entre dois nós IPv4 para enviar o tráfego IPv6. Atente para a diferença entre a técnica de encapsulamento *6in4* (que inclusive pode ser utilizada com outras técnicas de transição) e o túnel *6over4*.

Existem outras técnicas, além das baseadas em túneis descritas nesta seção, como o GRE e o Teredo. O Comitê Gestor da Internet no Brasil (cgi.br) detalha esses métodos no seu portal sobre IPv6.

Tradução

Por fim, outras classes de métodos que podem ser empregados no período de transição são as baseadas em tradução de pacotes. Esses mecanismos podem atuar de diversas formas e em camadas distintas, traduzindo cabeçalhos IPv4 em cabeçalhos IPv6 e vice-versa, além de realizar conversões de endereços.

Atividade 02

---

1. Pesquise e cite outras técnicas de transição além das descritas no material.
2. Analise e pesquise se seu dispositivo é compatível com ambos os protocolos IP, podendo suportar o *dual stack*.

Clique aqui para visualizar as respostas

Respostas

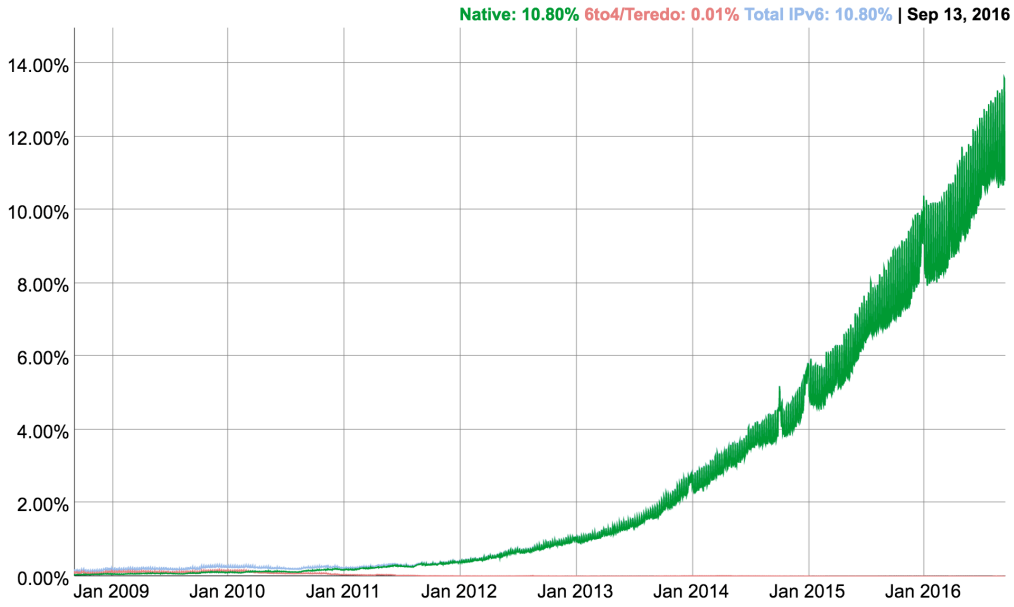
1. Entre as diferentes estratégias de transição podemos citar: Túneis GRE, Tunnel Broker, NAT64 e DNS64, 464XLAT, Teredo, DL-Lite, 4rd, 6rd, entre outros.
2. A depender do equipamento.

Status do IPv6

É possível analisar estatísticas sobre a adoção do IPv6 na Internet continuamente. Um dos principais responsáveis por essa métrica é o Google, medindo a disponibilidade de conectividade IPv6 entre seus usuários.

A Figura 5 demonstra um gráfico relativo à tendência de utilização do IPv6 em serviços associados ao Google. É notório que nos últimos anos a adoção vem crescendo exponencialmente, apesar de ainda ser bastante baixa.

Figura 05 - Adoção do IPv6 no mundo (Google).

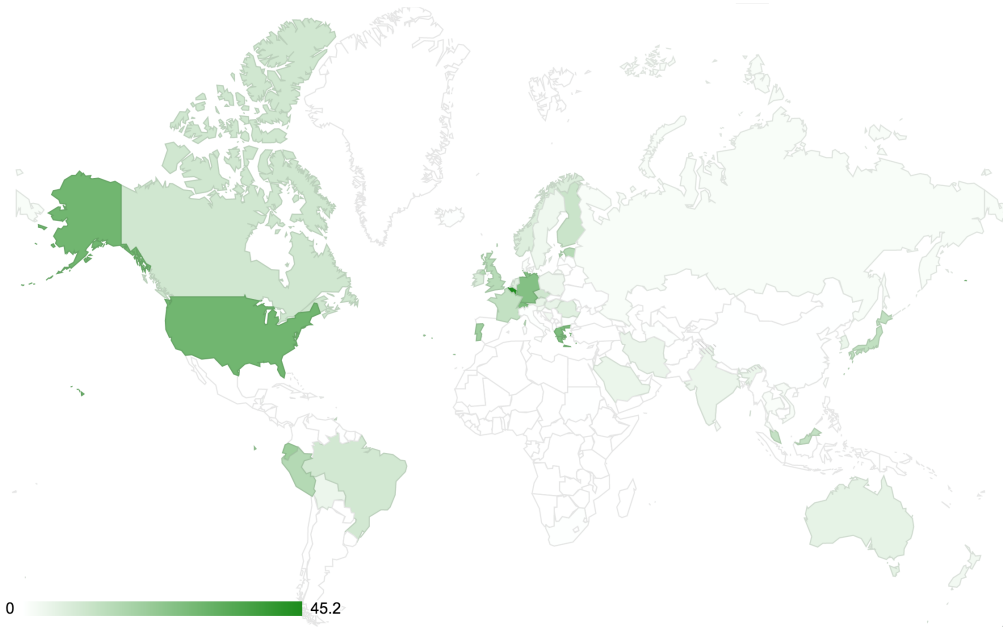


Fonte: https://www.google.com/intl/en/ipv6/statistics.html. Acesso em: 29 set. 2016

Outra grande parceira e entusiasta na adoção do IPv6 é o Núcleo de Informação e Coordenação do Ponto BR, ou simplesmente *nic.br*, entidade responsável pelas funções administrativas e operacionais relativas ao domínio *.br*. Em seu site (*www.ipv6.br*) é possível encontrar uma ampla gama de informações relativas à adoção do protocolo em território nacional.

O projeto *6lab* (*www.6lab.cisco.com*), endossado pela Cisco, também provê ferramentas *web* para análise do *status* do IPv6 em diferentes países do mundo. Uma das funcionalidades disponíveis permite visualizar um mapa interativo ilustrando a utilização do protocolo em diferentes países, como ilustrado na Figura 6.

Figura 06 - Adoção do IPv6 por país (Cisco).



Fonte: http://6lab.cisco.com/. Acesso em: 29 set. 2016

Por fim, é importante destacar que a adoção do IPv6 também acarreta a necessidade da implementação e adaptação de diversos outros recursos e serviços utilizados na Internet, como o protocolo de controle ICMP, o protocolo de alocação dinâmica de endereços DHCP e o serviço de nomes de domínio (DNS). Nos exemplos citados, foram implementadas versões conhecidas como ICMPv6 e DHCP6, além da adequação de uma nova entrada no registro (entrada AAAA) de recursos no DNS original.

Resumo

Nesta aula, estudamos que o protocolo IPv6, utilizado na camada de rede, vem como uma solução robusta e eficiente para um dos problemas que estão afetando a rede mundial de computadores: o esgotamento dos endereços IPv4. Você aprendeu a estrutura desse novo protocolo, o formato de seu pacote e a utilização dos cabeçalhos de extensão. Viu, também, a questão da compatibilidade entre as duas versões do IP e foi apresentado às principais técnicas de transição. Por fim, você descobriu como se desenvolve a implantação do IPv6 no mundo.

Autoavaliação

1. Pesquise o percentual de adoção do IPv6 no Brasil e faça um paralelo comparando a tendência de adoção desse protocolo nos últimos 5 anos.
2. Estudamos, anteriormente, alguns dos endereços reservados do IPv4. Pesquise, agora, os endereços reservados do IPv6.

Clique aqui para visualizar as respostas

Respostas

1. Como visto na aula, pelo site da Cisco 6lab é possível monitorar o percentual de usuários compatíveis com o protocolo IPv6. Pode-se filtrar por país e analisar um histórico detalhado dos últimos anos.
2. Existem diversos endereços reservados para diferentes propósitos no IPv6. Um deles é o endereço de *loopback*, que sabemos ser denotado no IPv4 por 127.0.0.1. No IPv6, o endereço de *loopback* é o ::1, ou seja, 0000:0000:0000:0000:0000:0000:0000:0001.

Referências

KUROSE, J.; ROSS, K. **Redes de computadores e a internet.** 5. ed. São Paulo: Addison Wesley, 2010.

STALLINGS, W.; CASE T. **Redes e sistemas de comunicação de dados.** 7 ed. Elsevier 2016.

WETHERALL, D; TANENBAUM, A, S. **Redes de computadores.** 5. ed. Rio de Janeiro: Editora Pearson Education, 2011.

SANTOS, R; MOREIRAS, A; REIS, E; ROCHA, A. **IPv6 básico.** Núcleo de Informação e Coordenação do ponto BR (nic.br), São Paulo, 2010.