

Redes de Computadores Av IPv6 para Concursos de TI

Prof. Walter Cunha

falecomigo@waltercunha.com

Redes de Computadores Av O Professor

Professor



- Natural: Fortaleza-CE
- Cargo: AFC-CGUT I (2009)
- Graduação: Engenharia Eletrônica ITA 2000
- Pós: Ger. Projetos FGV 2007
- <https://about.me/waltercunha>

Curriculum – Experiência

- Prof. de TI p/ Concursos (dsd 2007)
 - Redes de Computadores
 - Gerenciamento de Projetos
 - Licitações e Contratos de TI
- AFC/CGU – TI (dsd2009)
- ATRFB-TI (2006 a 2009)
- 1 Tem Eng Eln FAB (2000 a 2006)

Currículo – Realizações

- Criação da Lista TImasters (2007)
- Criação da Rede Social de Estudos ITnerante (2009)
- Coordenador Pedagógico dos Sites Preparatórios Provas de TI e Gabaritou TI
- Criação/Coordenação da Equipe de Professores ITenerante

Contato

- <http://www.itnerante.com.br/profile/WalterCunha>
- falecomigo@waltercunha.com

Seguir

- <http://www.waltercunha.com/blog/>
- <http://twitter.com/TIMasters/>
- <https://www.facebook.com/walter.cunha.7>
- <https://www.youtube.com/user/portalprovas>

Redes de Computadores Av O Módulo

Escopo

Abordar todos os aspectos de IPv6 que já foram cobrados até hoje (ou, pelo menos, nos últimos tempos) em Concurso Públicos de Tecnologia da Informação.

Para quem quer se “aprofundar” no assunto:

Cursos Moodle do NIC.br:

<http://saladeaula.nic.br/moodle/>

Agenda

- Histórico e Cenário Atual
- Vantagens/Funcionalidades
- Datagrama IPv6
- Endereço IPv6
- Tipos e Endereços Especiais
- Protocolos e Serviços (Componentes e Auxiliares)
- Estratégias de Migração (/Transição)

Referências

- Site do IPv6br:

<http://ipv6.br>

- Google:

<https://www.google.com/intl/en/ipv6/statistics.html>

- Cisco:

<http://6lab.cisco.com/stats/>

- Gabaritou:

<http://gabaritou.com.br/>

MasterMind WC

Você possui todos os módulos do Prof. WC?

falecomigo@waltercunha.com

- Então, pode solicitar participação e contar com as seguintes vantagens:
 - Orientação sobre planejamento de Estudos
 - Apoio na elaboração de recursos
 - Conferências Online
 - Materiais Extras
 - E muito mais!



MasterMind WC

Você possui todos os módulos do Prof. WC?

falecomigo@waltercunha.com

- Então, pode solicitar participação e contar com as seguintes vantagens:
 - Orientação sobre planejamento de Estudos
 - Apoio na elaboração de recursos
 - Conferências Online
 - Materiais Extras
 - E muito mais!



IPv6 para Concurso de TI

Histórico e Cenário Atual

IPv6 – Contexto

- A Internet não foi originalmente projetada para lidar com um número extremamente grande de usuários
- A alternativa de curto prazo para corrigir o problema de esgotamento de endereços IP foi o NAT (RFC 3022)
- O IPv6 surgiu como um solução mais enxuta e otimizada, em relação ao IPv4, tendo como finalidade a melhoria do desempenho e a correção dos erros presentes no antigo projeto

IPv6 – Linha do Tempo

- 1969 – Início da ARPANET
- 1981 – Definição do IPv4 na RFC 791
- 1983 – ARPANET adota o TCP/IP
- 1990 – Primeiros estudos sobre o esgotamento dos endereços
- 1992 – IETF cria o grupo IPng (IP Next Generation)
- 1993 – Internet passa a ser explorada comercialmente, intensificando a discussão sobre o possível esgotamento dos endereços livres e do aumento da tabela de roteamento.

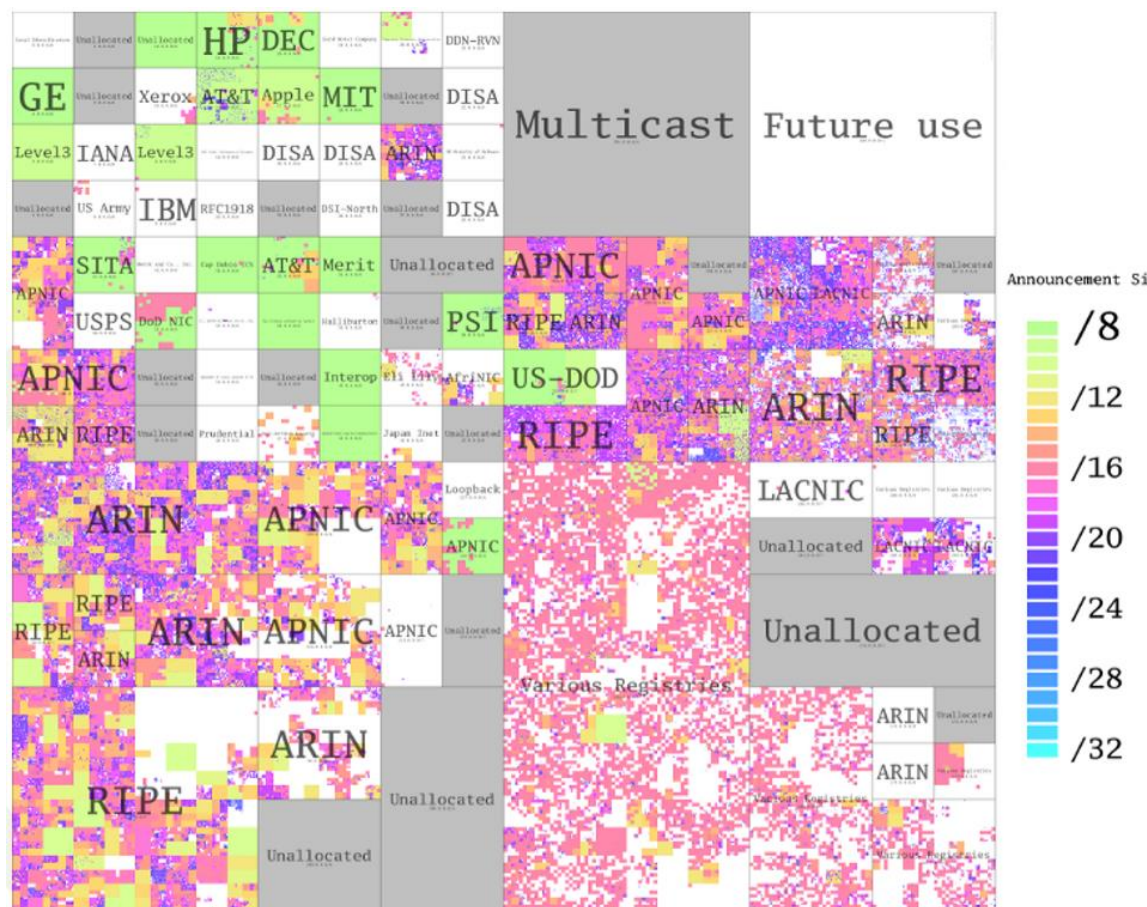
IPv6 – Distribuição Inicial

- IPv4 = 4.294.967.296 endereços.
- Política inicial de distribuição de endereços (caracterizada pelo desperdício)
- Ninguém tinha noção da dimensão que ia tomar
- Classe A
- Classe B
- Classe C
- Endereços reservados

Classe A

- IBM
- HP
- AT&T
- MIT
- DoD
- US Army USPS
- ...

IPv6 – Esgotamento do IPv4



IPv6 – Soluções Paliativas

1992 - IETF cria o grupo ROAD (ROuting and ADdressing)

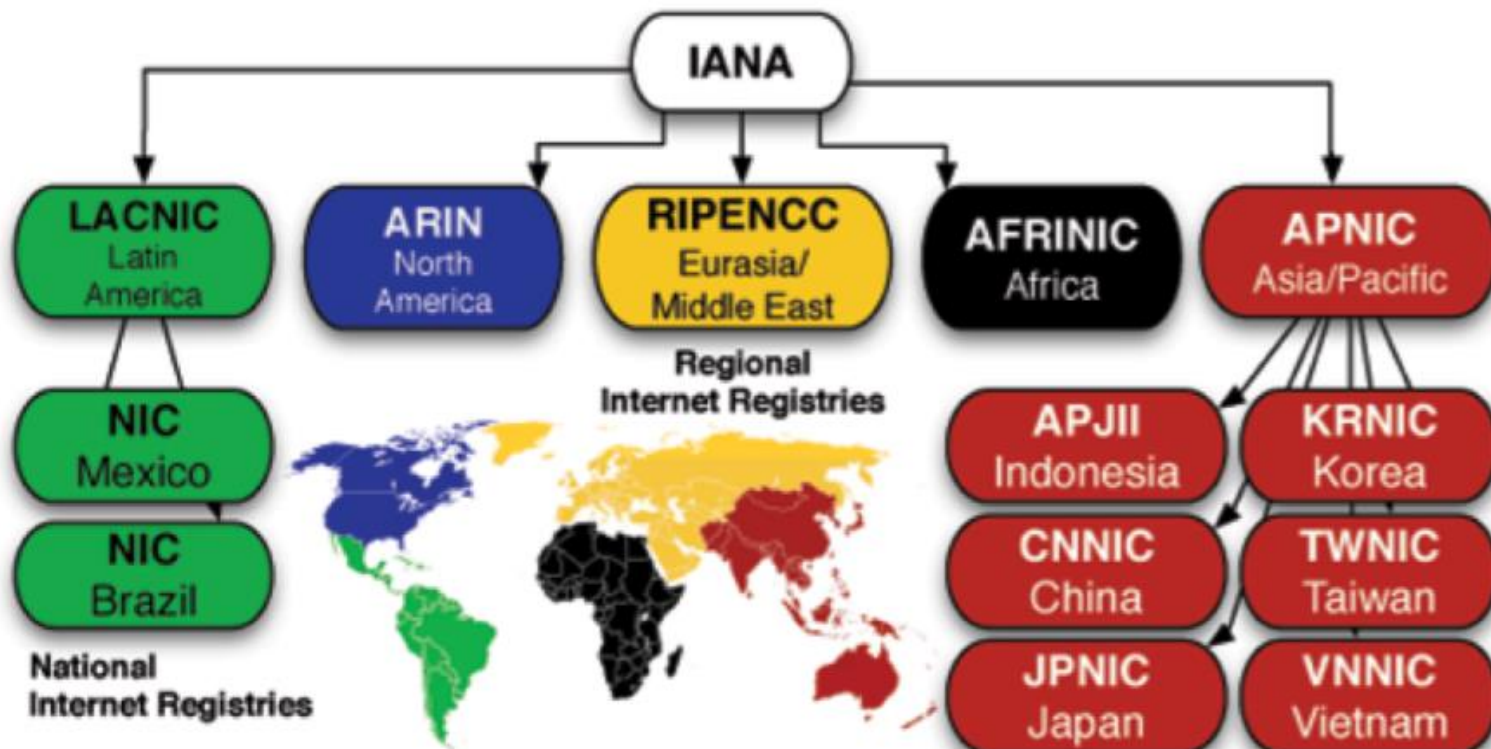
CIDR (RFC 4632):

- Fim do uso de classes = blocos de tamanho apropriado
- Endereço de rede = prefixo/comprimento
- Agregação das rotas = reduz o tamanho da tabela de rotas

DHCP - Alocações dinâmicas de endereços

NAT + RFC 1918 - Permite conectar toda uma rede de computadores usando apenas um endereço válido na Internet, porém com várias restrições

IPv6 – Regional Internet registry



IPv6 – Cenário Atual IPv4

(Ao tempo da publicação deste curso) no NIC.br:

- Ainda existem poucos blocos IPv4 disponíveis
- No NIC.BR, você pode pedir no máximo o /22
 - Se pedir mais, não vai ter
- Só pode pedir de novo depois de 6 (seis) meses

IPv6 - Cenário Atual IPv4

A Internet continua crescendo...

Mundo

- 1.966.514.816 usuários de Internet
- 28,7% da população
- Crescimento de 444,8% nos últimos 10 anos
- Em 2014, soma de celulares, smartphones, netbooks e modems 3G deve chegar a 2,25 bilhões de aparelhos

* Internet das Coisas!

IPv6 - Cenário Atual IPv4

A Internet continua crescendo...

Brasil

- 27% de domicílios com acesso à Internet
- 3,8 milhões de conexões em banda larga móvel
- 12 milhões de conexões em banda larga fixa

*** Internet vem sendo considerada um Direito Fundamental**

IPv6 – Solução Definitiva

- 1998 – IPv6 definido pela RFC 2460
- 128 bits para endereçamento
- Cabeçalho base simplificado
- Cabeçalhos de extensão
- Identificação de fluxo de dados (QoS)
- Mecanismos de IPSec incorporados ao protocolo.
- Realiza a fragmentação e remontagem dos pacotes apenas na origem e no destino (fragmentação nas pontas)
- Não requer o uso de NAT, permitindo conexões fim-a-fim.
- Mecanismos que facilitam a configuração de redes...

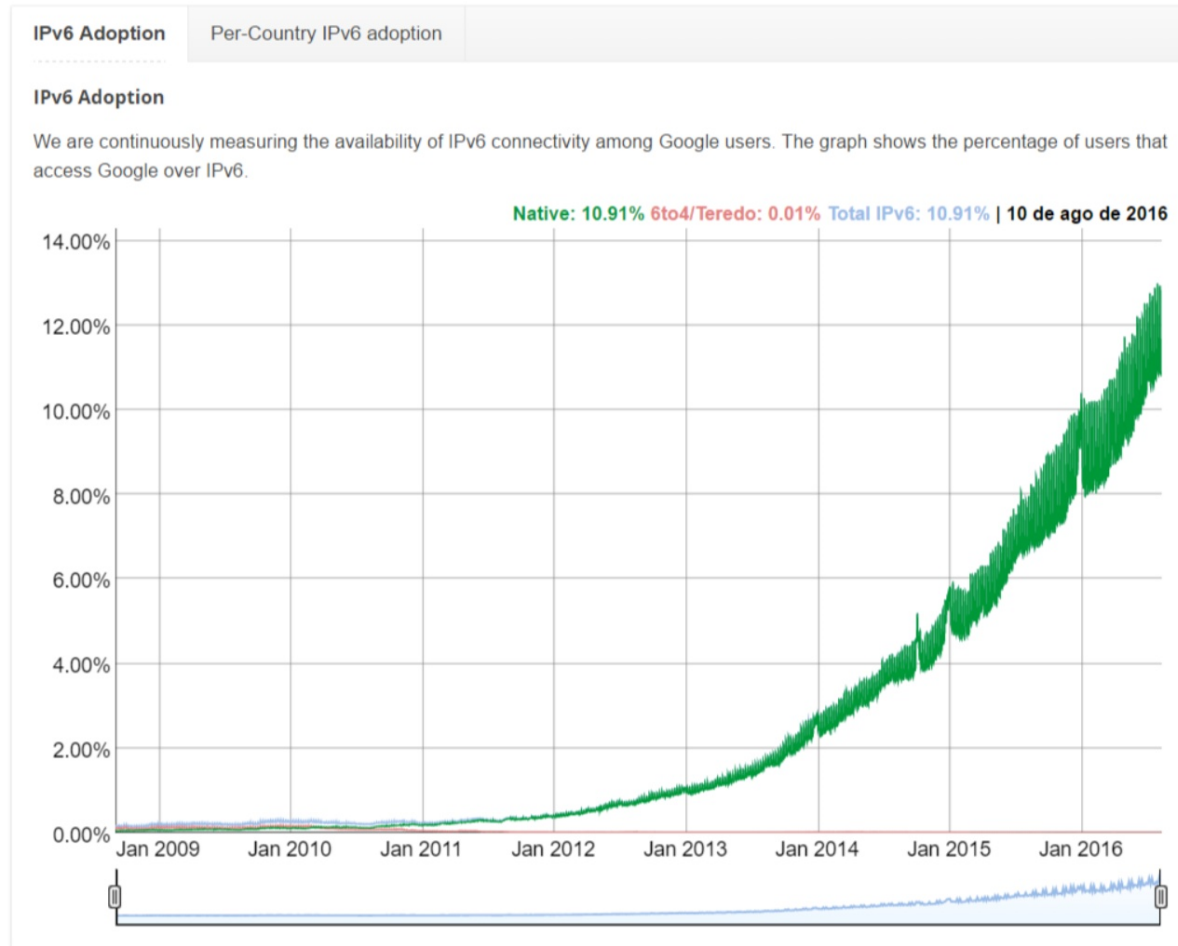
IPv6 – Cenário Atual IPv6

- ~15% dos ASs trabalham sobre IPv6
- ~3% dos 1.000.000 de sítios web mais visitados da Internet são acessíveis via IPv6
- 0,51% de clientes da Google possuem IPv6 ativado
- World IPv6 Day”. Durante 24 horas, os maiores portais da internet convertem seus servidores para o IPV6 a fim de avaliar possíveis problemas e corrigi-los antes da implementação definitiva

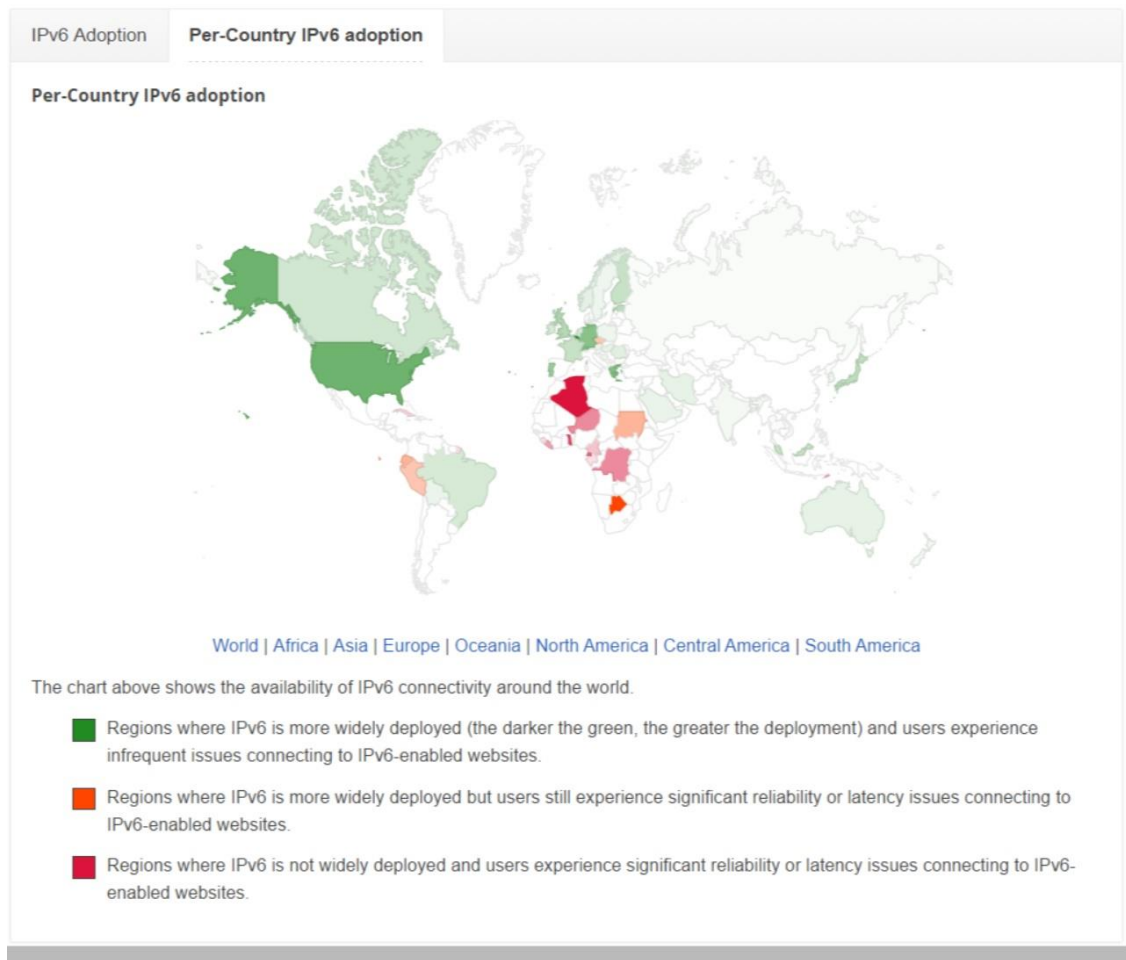
IPv6 – Cenário Atual IPv6

- Agências federais dos EUA foram ordenadas a atualizarem seus backbones para o IPv6 antes de 2008
- Grandes trechos da Internet em regiões em desenvolvimento como a China adotaram IPV6 desde o início
- ISPs de Broadband como a Comcast estão se preparando (ao tempo da publicação desse curso) para migrar para o IPV6 e quando eles virarem o interruptor algo em torno de 14 milhões de assinantes se tornarão pontos terminais IPV6

IPv6 – Estatísticas Google



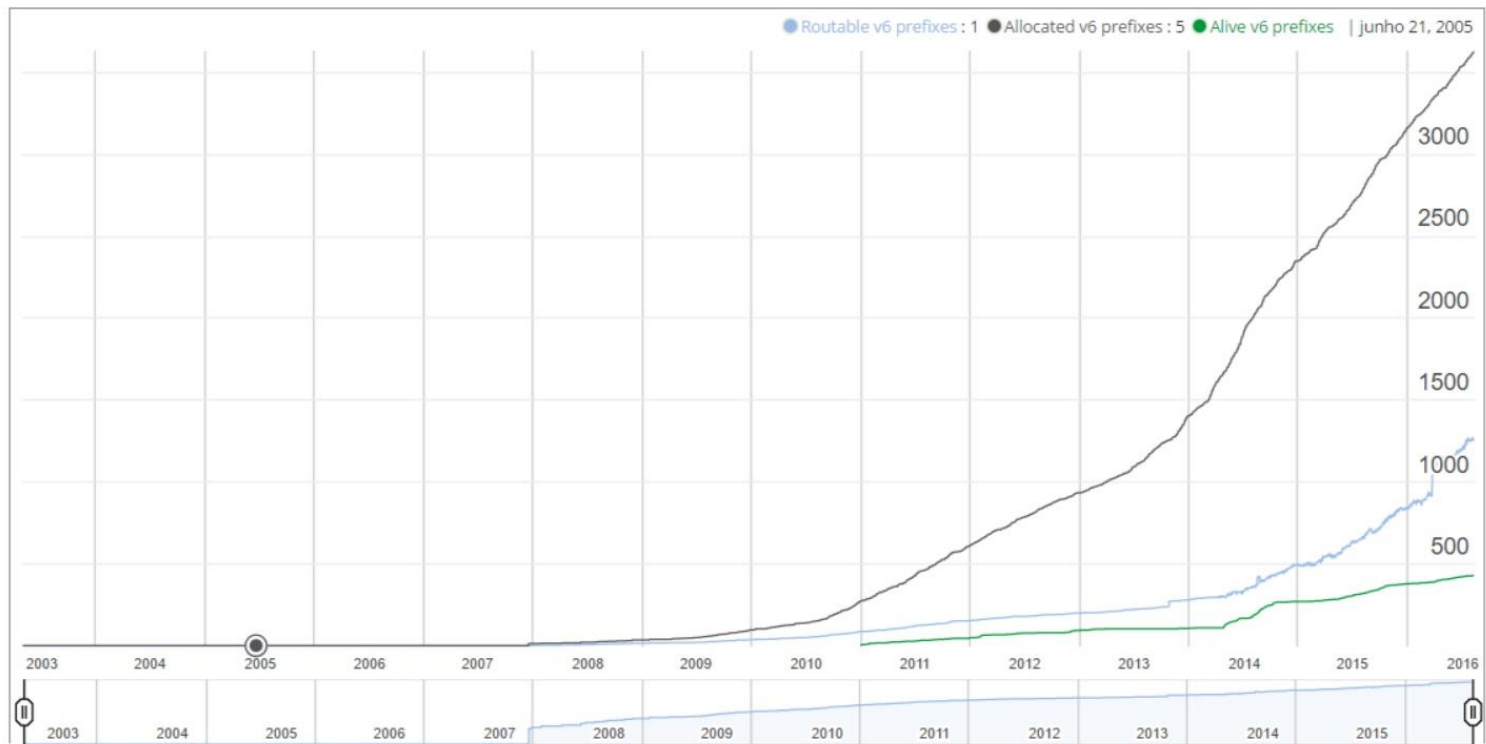
IPv6 – Estatísticas Google



IPv6 – Estatísticas Cisco

Brazil

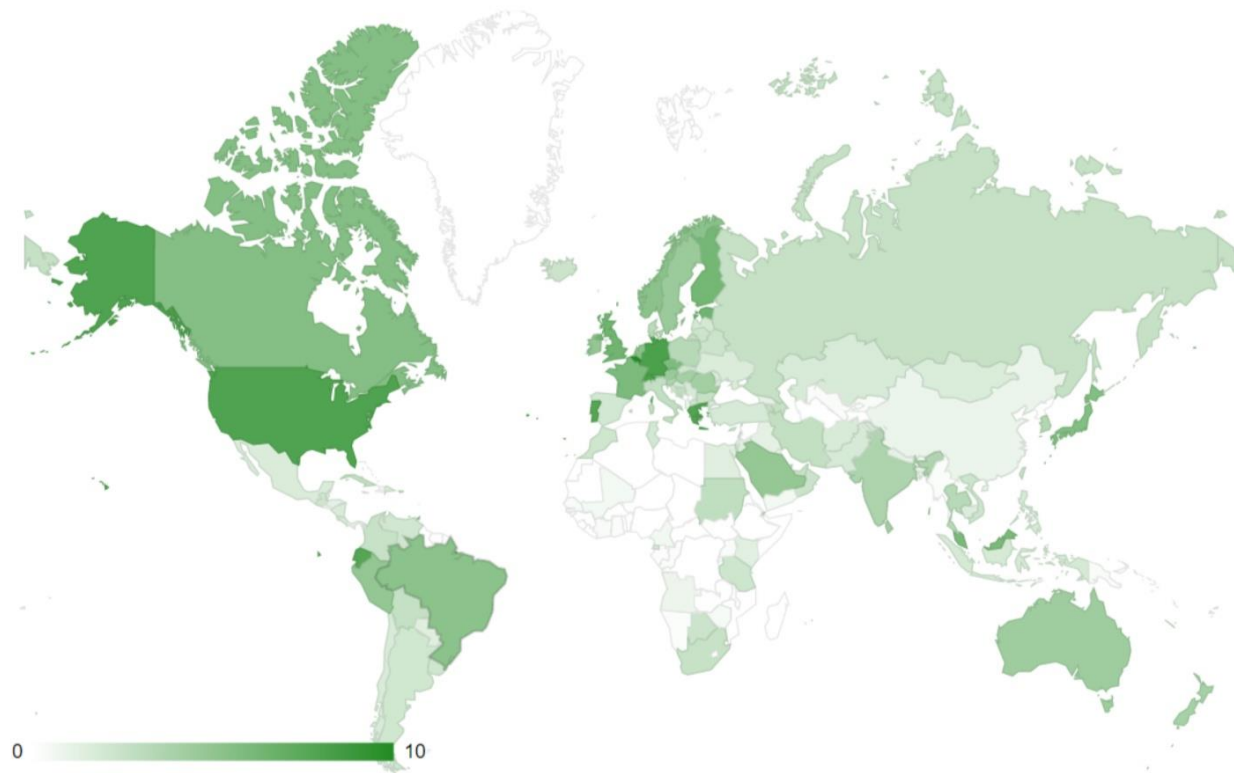
Display IPv6 Prefixes Data ⓘ



IPv6 – Estatísticas Cisco

Display global data 

[World](#) | [Africa](#) | [Asia](#) | [America](#) | [Europe](#) | [Oceania](#)



IPv6 – E quem não implantar?

A não implementação do IPv6 irá:

- Dificultar o surgimento de novas redes
- Diminuir o processo de inclusão digital, reduzindo o número de novos usuários
- Dificultar o surgimento de novas aplicações
- Aumentar a utilização de técnicas como a NAT (processamento)
- O custo de não implementar o IPv6 será maior que o custo de implementá-lo
- Provedores Internet precisam inovar e oferecer novos serviços a seus clientes
- ...

IPv6 – E quem não implantar?

- A maior dificuldade para adoção de IPv6 está no usuário final. Tem vários conteúdos na Internet em IPv6: netflix, akamai, etc
- Operadoras brasileiras já começaram a oferecer IPv6. Isso deu um gás no tráfego IPv6
- Os mais “atrasados” são os bancos na implantação, por questão de segurança. Mas a febraban já tem cronograma de implantação

Questões

(FCC/TRT-MS 2011) Os espaços de endereçamento dos protocolos IPv4 e IPv6 são, respectivamente,

- (A) 32 bits e 64 bits.
- (B) 48 bits e 96 bits.
- (C) 32 bits e 128 bits.
- (D) 64 bits e 128 bits.
- (E) 64 bits e 256 bits.

Questões

(FCC/TRT-MS 2011) Os espaços de endereçamento dos protocolos IPv4 e IPv6 são, respectivamente,

- (A) 32 bits e 64 bits.
- (B) 48 bits e 96 bits.
-  (C) 32 bits e 128 bits.
- (D) 64 bits e 128 bits.
- (E) 64 bits e 256 bits.

Questões

(FCC/TRF-2 2007) A alternativa de curto prazo para corrigir o problema de esgotamento de endereços IP, descrita na RFC 3022, é:

- (A) CIDR - Classless InterDomain Router.
- (B) NAT - Network Address Translation.
- (C) IPv6 - Internet Protocol Version 6.
- (D) ADSL - Asymmetric Digital Subscriber Line.
- (E) ICANN - Internet Corporation for Assigned Names and Numbers.

Questões

(FCC/TRF-2 2007) A alternativa de curto prazo para corrigir o problema de esgotamento de endereços IP, descrita na RFC 3022, é:

(A) CIDR - Classless InterDomain Router.



(B) NAT - Network Address Translation.

(C) IPv6 - Internet Protocol Version 6.

(D) ADSL - Asymmetric Digital Subscriber Line.

(E) ICANN - Internet Corporation for Assigned Names and Numbers.

Questões

(FGV/TJ-GO 2014) Uma empresa migrou todo o seu ambiente de IPv4 para IPv6, porque precisava de mais endereços IP válidos para se comunicar externamente. Com isso, seria possível abandonar o uso de um protocolo que era necessário, pela falta de IPs válidos, quando usavam IPv4. Esse protocolo é o:

A ICMP

B L2TP

C NAT

D SMTP

E BGP

Questões

(FGV/TJ-GO 2014) Uma empresa migrou todo o seu ambiente de IPv4 para IPv6, porque precisava de mais endereços IP válidos para se comunicar externamente. Com isso, seria possível abandonar o uso de um protocolo que era necessário, pela falta de IPs válidos, quando usavam IPv4. Esse protocolo é o:

A ICMP

B L2TP



C NAT

D SMTP

E BGP

IPv6 para Concurso de TI

Vantagens/Funcionalidades

IPv6 - Vantagens

- Maior espaço de endereçamento para os *hosts*
- Maior flexibilidade (cabeçalhos sob demanda)
- Maior sumarização
- *Multihoming*
- Auto-configuração e “*plug-and-play*”
- Renumeração

IPv6 - Vantagens

- Optar por continuar utilizando o IPv4 seria muito caro e complexo.
 - Os roteadores teriam que ter um poder de processamento muito maior para lidar com todo o overhead.
- Uma das inúmeras vantagens do IPv6 é justamente desonerar os roteadores
 - O cálculo do MTU, por exemplo, passa a ser feito na origem do pacote e não mais nos roteadores
- Além disso tem a questão da segurança, o IPSEC não funciona bem com NAT. No IPv6, ele funciona sem restrições

IPv6 – Maior Endereçamento

- A nova versão do IP define 128 bits (16 bytes) para endereçamento dos hosts, enquanto que a versão anterior define apenas 32 bits (4 bytes)
- As informações do endereço IP origem e destino devem ser transportadas no cabeçalho do pacote, o que define no mínimo 256 bits apenas para o endereçamento
- O IPv6 pode fornecer 2^{128} endereços IP, o que equivale a 79 trilhões de vezes o espaço disponível no IPv4 ou $3,4 \times 10^{27}$ endereços por habitante do planeta

IPv6 - *Multihoming*

- Quando um site é anexado a n provedores, cada um desses hosts receberá n diferentes endereços IPv6
- Isso reduz o tamanho das tabelas de roteamento BGP ao evitar alertar os prefixos IPv6 utilizados por domínios *stub* (*stub domains*) e fornece muitos outros benefícios adicionais em termos de diversidade de caminhos, além do quesito performance
- Entretanto, isso requer a implementação de novos protocolos e mecanismos a fim de coordenar a utilização desses diferentes endereços IPv6 para cada host, evitando os problemas relacionados à segurança e detectando as falhas de forma eficaz

IPv6 – Mobilidade

- Este método consiste basicamente em todo *host* móvel possuir um endereço fixo em sua rede local original, conhecido como *home address*
- Deste modo, ao se autoconfigurar em uma rede qualquer, o *host* móvel envia uma mensagem a sua rede local "avisando" seu novo endereço na rede na qual é visitante
- Assim, todos os pacotes destinados ao seu endereço original serão roteados para o seu endereço visitante, permitindo assim a recepção de pacotes de forma transparente

IPv6 - Renumeração

- Em alguns cenários, a autoconfiguração stateless simplifica muito o processo de renumeração de endereços de rede, exigindo somente que a interface de rede seja capaz de enviar e receber pacotes multicast
- Os hosts IPv6 (hosts e roteadores) criam, automaticamente, endereços link-local únicos para todas as interfaces de rede, combinando o endereço da camada de enlace no formato EUI-64 com os 64 bits do prefixo local

** O endereço EUI-64 de 64 bits é definido pelo Instituto de Engenheiros Elétricos e Eletrônicos (IEEE)*

IPv6 – Auto-Configuração

- Possibilidade de toda uma rede de computadores se autoconfigurar sem a necessidade de utilização de um serviço de DHCP ativo em algum servidor
- Essa forma de autoconfiguração é denominada *Stateless Address Autoconfiguration*, mais conhecida como SLAAC
- Esse método não mantém nenhum registro dos endereços atribuídos (stateless) e é automaticamente atribuído nos hosts (autoconfiguration), daí a origem do seu nome

IPv6 – Auto-Configuração

- O processo de autoconfiguração dos endereços em redes baseadas no IPv6 consiste basicamente em duas etapas: (i) configuração do prefixo e (ii) configuração do sufixo de host
- A primeira etapa é possível porque os hosts aprendem o prefixo da rede através das mensagens ICMPv6 Tipo 134 (RA) anunciadas pelos roteadores
- O sufixo de host é automaticamente gerado a partir do endereço físico (MAC) da interface de rede

IPv6 – Auto-Configuração

- O detalhe é que o MAC tem apenas 48 bits, por isso é aplicada uma função de expansão denominada IEEE EUI-64 (*Extended Unique Identifier*) no endereço físico que preenche os demais 16 bits através de um algoritmo padronizado
- Antes do endereço automaticamente gerado ser efetivamente atribuído à interface é aplicada a funcionalidade de detecção de endereços duplicados do NDP

IPv6 – Fragmentação

- No IPv6, a fragmentação é realizada entre os hosts comunicantes por meio dos cabeçalhos extensíveis e não mais pelos roteadores
- Caso um roteador receba um pacote com um tamanho maior do que ele pode suportar, em vez de fragmentá-lo, ele encaminha uma mensagem ICMP ao host transmissor contendo seu tamanho máximo suportado para que seja realizada a fragmentação do pacote pelo host
- Dessa forma, o campo *Fragment Offset* do IPv4 foi descartado no IPv6

Questões

(CESPE/PCF 2002) O suporte a IPSec é opcional em IPv4 e IPv6.

Questões



(CESPE/PCF 2002) O suporte a IPSec **é opcional** em IPv4 e IPv6.

Questões

(CESGRANRIO/TRANSPETRO 2012) O Protocolo da Internet (IP) é responsável pelo repasse e endereçamento de pacotes.

Dentre as características mais importantes introduzidas no protocolo IPv6, está a(o)

A expansão da capacidade de endereçamento

B flexibilização do comprimento do cabeçalho

C compatibilização com o HTTPS

D acomodação do IMAP

E acoplamento ao protocolo TCP

Questões

(CESGRANRIO/TRANSPETRO 2012) O Protocolo da Internet (IP) é responsável pelo repasse e endereçamento de pacotes. Dentre as características mais importantes introduzidas no protocolo IPv6, está a(o)



A expansão da capacidade de endereçamento

B flexibilização do comprimento do cabeçalho

C compatibilização com o HTTPS

D acomodação do IMAP

E acoplamento ao protocolo TCP

Questões

(CESPE/ANCINE 2013) Em comparação ao IPv4, o IPv6 é maior no que se refere à parte obrigatória do cabeçalho e ao número de campos.

Questões



(CESPE/ANCINE 2013) Em comparação ao IPv4, o IPv6 é maior no que se refere à parte obrigatória do cabeçalho e ao número de campos.

Questões

(FCC/MPE-MA 2013) Em relação ao IPv4, é INCORRETO afirmar que o IPv6

- a) apresenta mais flexibilidade por meio dos cabeçalhos adicionais.
- b) apresenta mais eficiência reduzindo o overhead do processamento dos pacotes.
- c) ainda mantém a limitação de não permitir pacotes maior do que 64 KB.
- d) adiciona mecanismo de suporte a mobilidade através do cabeçalho Routing.
- e) adiciona mecanismos de autenticação, de integridade e de confidencialidade.

Questões

(FCC/MPE-MA 2013) Em relação ao IPv4, é INCORRETO afirmar que o IPv6

- a) apresenta mais flexibilidade por meio dos cabeçalhos adicionais.
- b) apresenta mais eficiência reduzindo o overhead do processamento dos pacotes.
- c) ainda mantém a limitação de **não permitir pacotes maior do que 64 KB.**
- d) adiciona mecanismo de suporte a mobilidade através do cabeçalho Routing.
- e) adiciona mecanismos de autenticação, de integridade e de confidencialidade.



IPv6 para Concurso de TI

Datagrama IPv6

IPv6 - Datagrama

- Diferentemente do IPv4, todos os campos deste novo cabeçalho possuem tamanho fixo
- O fato de possuir um tamanho fixo acelera bastante o processamento dos pacotes pelos roteadores, visto que não há necessidade de calcular a extensão de certos campos, e nem o tamanho do cabeçalho como um todo
- Além disso, ocorreu uma redução do número de campos utilizados, por meio da exclusão de campos de pouca utilidade prática. Este fato também contribui para a diminuição do tempo gasto em processamento pelos roteadores

IPv6 - Datagrama

O cabeçalho IPv4 é composto por 12 campos fixos, podendo conter ou não opções, fazendo com que seu tamanho possa variar entre 20 e 60 Bytes.

Mais simples:

- 40 Bytes (tamanho fixo)
- Apenas duas vezes maior que o da versão anterior
- Mais flexível
- Extensão por meio de cabeçalhos adicionais
- Mais eficiente
- Minimiza o overhead nos cabeçalhos
- Reduz o custo do processamento dos pacotes
- ...

IPv6 - Datagrama

IPv4 Header

0	4	8	12	16	20	24	28	31
Version	IHL	Type of Service	Total Length					
Identification				Flags	Fragment Offset			
Time to Live		Protocol		Header Checksum				
Source Address								
Destination Address								

IPv6 Header

0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	63
Version	Traffic Class		Flow Label						Payload Length				Next Header		Hop Limit	
Source Address																
Destination Address																

IPv6 - Datagrama

Seis campos do cabeçalho IPv4 foram removidos

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)			Flags	Deslocamento do Fragmento (Fragment Offset)
Tempo de Vida (TTL)	Protocolo (Protocol)		Soma de verificação do Cabeçalho (Checksum)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)	
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)
Endereço de Origem (Source Address)			
Endereço de Destino (Destination Address)			

IPv6 - Datagrama

Quatro campos tiveram seus nomes alterados e seus posicionamentos modificados

Versão (Version)	Tamanho do Cabeçalho (H/L)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)			Flags	Deslocamento do Fragmento (Fragment Offset)
Tempo de Vida (TTL)	Protocolo (Protocol)		Soma de verificação do Cabeçalho (Checksum)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)		
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				

IPv6 - Datagrama

O campo Identificador de Fluxo foi acrescentado.

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)			Flags	Deslocamento do Fragmento (Fragment Offset)
Tempo de Vida (TTL)		Protocolo (Protocol)	Soma de verificação do Cabeçalho (Checksum)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)	
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)
Endereço de Origem (Source Address)			
Endereço de Destino (Destination Address)			

IPv6 - Datagrama

Três campos foram mantidos.

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)		Flags	Deslocamento do Fragmento (Fragment Offset)	
Tempo de Vida (TTL)	Protocolo (Protocol)	Soma de verificação do Cabeçalho (Checksum)		
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)	
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)
Endereço de Origem (Source Address)			
Endereço de Destino (Destination Address)			

IPv6 - Datagrama

O cabeçalho do pacote IP versão 6 contém um número menor de campo obrigatórios, podendo ser:

- Versão (4 bits) - Identifica a versão do protocolo utilizado. No caso, o valor desse campo é 6
- Classe de Tráfego (8 bits) – Identifica os pacotes por classes de serviços ou prioridade. Ele provê as mesmas funcionalidades e definições do campo “Tipo de Serviço do IPv4”
- Identificador de Fluxo (20 bits) – Identifica pacotes do mesmo fluxo de comunicação. Idealmente esse campo é configurado pelo endereço de destino para separar os fluxos de cada uma das aplicações e os nós intermediários de rede podem utiliza-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes

IPv6 - Datagrama

O cabeçalho do pacote IP versão 6 contém um número menor de campo obrigatórios, podendo ser:

- **Tamanho do Dados (16 bits)** – Indica o tamanho, em Bytes, apenas dos dados enviados junto ao cabeçalho IPv6. Substituiu o campo Tamanho Total do IPv4, que indicava o tamanho do cabeçalho mais o tamanho dos dados transmitidos. Contudo, o tamanho dos cabeçalhos de extensão também são somado nesse novo campo
- **Próximo Cabeçalho (8 bits)** – Identifica o cabeçalho de extensão que segue o atual. Ele foi renomeado (no IPv4 chamava-se Protocolo) para refletir a nova organização dos pacotes IPv6, uma vez que ele deixou de conter os valores referentes a outros protocolos, para indicar os tipos dos cabeçalhos de extensão.

IPv6 - Datagrama

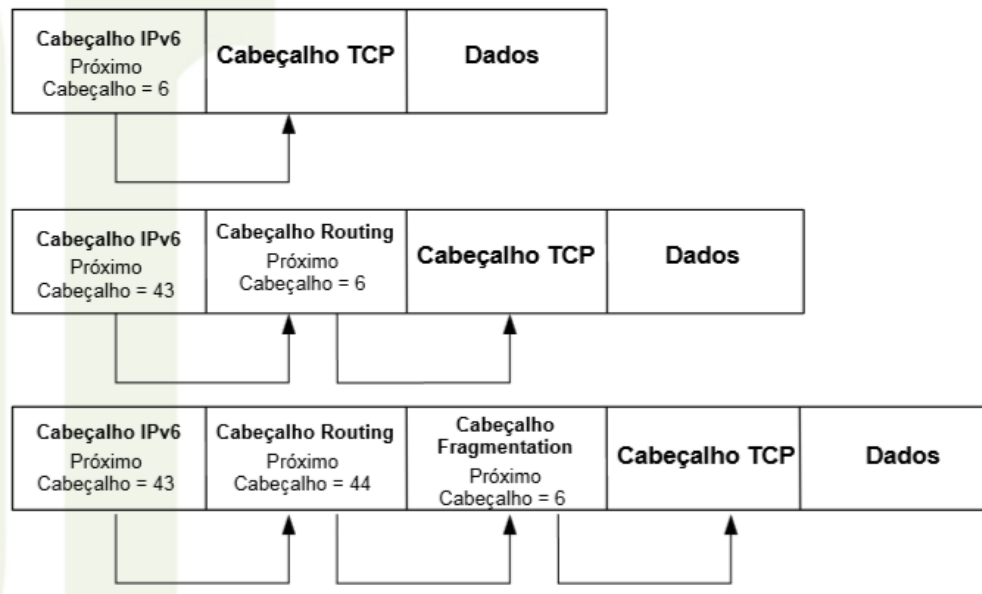
O cabeçalho do pacote IP versão 6 contém um número menor de campo obrigatórios, podendo ser:

- **Limite de Encaminhamento (8 bits)** – Esse campo é decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes de ser descartado. Ele padronizou o modo como o campo Tempo de Vida (TTL) do IPv4 vinha sendo utilizado, o qual diferia significativamente da descrição original que o definia como o tempo, em segundos, para o pacote ser descartado caso não chegasse à seu destino
- **Endereço de origem (128 bits)** – Indica o endereço de origem do pacote
- **Endereço de Destino (128 bits)** – Indica o endereço de destino do pacote

IPv6 - Datagrama

No IPv6, opções adicionais são tratadas por meio de cabeçalhos de extensão.

- Localizam-se entre o cabeçalho base e o cabeçalho da camada de transporte
- Não há nem quantidade, nem tamanho fixo para estes cabeçalhos



IPv6 - Datagrama

Quando houver mais de um cabeçalho de extensão, recomenda-se que eles apareçam na seguinte ordem:

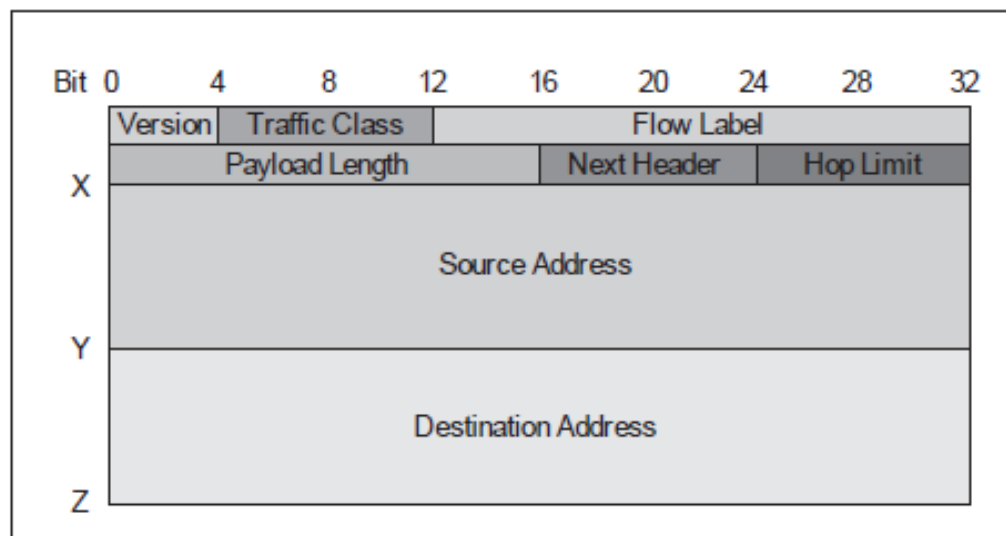
- Hop-by-Hop Options (0) – Processados por todos os nós
- Routing (43) - Mobilidade do IPv6 (atualmente)
- Fragmentation (44) – Fragmentação
- Authentication Header (51) – IPSec
- Encapsulating Security Payload (52) – IPSec
- Destination Options (60) – Processados no destino

IPv6 - Datagrama

- Se o campo Endereço de Destino tiver um endereço multicast, os cabeçalhos de extensão serão examinados por todos os nós do grupo
- Pode ser utilizado o cabeçalho de extensão Mobility pelos nós que possuírem suporte a mobilidade IPv6

Questões

(FCC/TRT-15 2015) A figura abaixo apresenta o formato do cabeçalho do datagrama IPv6, em que a numeração horizontal representa a posição sequencial dos bits e as letras X, Y e Z identificam os bits iniciais dos quadros Source Address, Destination Address e Data (ausente na figura), respectivamente.



Questões

(FCC/TRT-15 2015) ...

Os valores ou as posições dos bits representados pelas letras X, Y e Z na figura, são, respectivamente,

A 64, 128 e 192.

B 64, 192 e 320.

C 48, 112 e 176.

D 128, 256 e 384.

E 48, 128 e 192.

Questões

(FCC/TRT-15 2015) ...

Os valores ou as posições dos bits representados pelas letras X, Y e Z na figura, são, respectivamente,

A 64, 128 e 192.



B 64, 192 e 320.

C 48, 112 e 176.

D 128, 256 e 384.

E 48, 128 e 192.

Questões

(CONSULPLAN/HOB 2015) O IPv6 é o novo protocolo da internet. Com o crescimento dos dispositivos conectados à internet, o esgotamento dos endereços IPv4 é fato. Restam poucos blocos para serem comercializados, mas, mesmo assim, pertencem a algumas empresas, que podem ou não comercializarem. Comparando o cabeçalho do IPv6 com o do IPv4, algumas diferenças podem ser percebidas como, por exemplo, a renomeação de alguns campos. Um dos campos renomeados do IPv4 no IPv6 foi o de nome Protocolo. Sobre o correspondente ao campo Protocolo no cabeçalho IPv6, assinale a alternativa correta.

- A Limite de hops.
- B Próximo cabeçalho.
- C Classe de tráfego (TC).
- D Tamanho do payload de dados.

Questões

(CONSULPLAN/HOB 2015) O IPv6 é o novo protocolo da internet. Com o crescimento dos dispositivos conectados à internet, o esgotamento dos endereços IPv4 é fato. Restam poucos blocos para serem comercializados, mas, mesmo assim, pertencem a algumas empresas, que podem ou não comercializarem. Comparando o cabeçalho do IPv6 com o do IPv4, algumas diferenças podem ser percebidas como, por exemplo, a renomeação de alguns campos. Um dos campos renomeados do IPv4 no IPv6 foi o de nome Protocolo. Sobre o correspondente ao campo Protocolo no cabeçalho IPv6, assinale a alternativa correta.



- A Limite de hops.
- B Próximo cabeçalho.**
- C Classe de tráfego (TC).
- D Tamanho do payload de dados.

Questões

(FCC/TRT-PB 2014) É sabido que um dos motivantes para a proposição do IPv6 para substituir o IPv4 foi a capacidade limitada de endereçamento do IPv4. Entretanto, e aproveitando a oportunidade para melhorar a funcionalidade do protocolo IP, outros recursos foram modificados ou introduzidos no IPv6. Dentre eles,

- A a introdução do recurso de QoS (Qualidade de Serviço) utilizando o campo Flow Label.
- B o uso do ARP incorporado no campo EXT do cabeçalho IPv6.
- C a redução do tamanho dos fragmentos dos pacotes para minimizar os erros de transmissão.
- D a incorporação do serviço TCP para fragmentar os pacotes no roteador.
- E o uso de endereços Broadcast ao invés de Multicast para aumentar a eficiência.

Questões

(FCC/TRT-PB 2014) É sabido que um dos motivantes para a proposição do IPv6 para substituir o IPv4 foi a capacidade limitada de endereçamento do IPv4. Entretanto, e aproveitando a oportunidade para melhorar a funcionalidade do protocolo IP, outros recursos foram modificados ou introduzidos no IPv6. Dentre eles,



- A a introdução do recurso de QoS (Qualidade de Serviço) utilizando o campo Flow Label.
- B o uso do ARP incorporado no campo EXT do cabeçalho IPv6.
- C a redução do tamanho dos fragmentos dos pacotes para minimizar os erros de transmissão.
- D a incorporação do serviço TCP para fragmentar os pacotes no roteador.
- E o uso de endereços Broadcast ao invés de Multicast para aumentar a eficiência.

Questões

(CESPE/ANP 2012) O IPv4 utiliza 32 bits para endereçamento e hop limit para datagramas, enquanto que o IPv6 usa 256 bits para endereçamento e TTL (time to live) para datagramas.

Questões



(CESPE/ANP 2012) O IPv4 utiliza 32 bits para endereçamento e hop limit para datagramas, enquanto que o IPv6 usa 256 bits para endereçamento e TTL (time to live) para datagramas.

Questões

(FCC/TRT-MS 2011) Constitui uma característica comum nos protocolos IPv4 e IPv6:

- (A) Limite de número máximo de roteadores por onde o pacote poderá passar no percurso entre origem e destino.
- (B) Tamanho de cabeçalho.
- (C) Cabeçalho contendo 14 campos.
- (D) Distinção de cabeçalho de *host* e cabeçalho de rede.
- (E) Suporte a autenticação de dados, privacidade e confidencialidade.

Questões

(FCC/TRT-MS 2011) Constitui uma característica comum nos protocolos IPv4 e IPv6:



- (A) Limite de número máximo de roteadores por onde o pacote poderá passar no percurso entre origem e destino.
- (B) Tamanho de cabeçalho.
- (C) Cabeçalho contendo 14 campos.
- (D) Distinção de cabeçalho de *host* e cabeçalho de rede.
- (E) Suporte a autenticação de dados, privacidade e confidencialidade.

Questões

(CESGRANRIO/PETROBRAS 2010) Durante uma palestra sobre redes foram feitas três perguntas para o palestrante.

- 1) Por que não há mais o campo de checksum no cabeçalho do IPv6?
- 2) Os endereços IPv6 podem ser compatíveis com IPv4?
- 3) Como é tratado o QoS no IPv6?

Para as perguntas acima, o palestrante forneceu as respectivas respostas a seguir.

I - O objetivo de não utilizar o checksum com o IPv6 é processar mais rapidamente os datagramas no roteador, considerando-se, nesta versão, que o controle de erros das camadas do protocolo é confiável.

II - Os endereços IPv4 podem ser escritos por um par de dois pontos seguido da notação da versão 4 e o endereço 143.54.1.20 seria escrito como ::143.54.1.20.

III - Os campos Flow Label e Traffic Class do cabeçalho são usados para identificar aqueles pacotes que necessitam de uma maior qualidade de serviço, sendo pacotes originados de aplicações multimídia ou de tempo real, por exemplo.

Está(ão) correta(s) a(s) respostas(s)

- a) I, apenas. b) II, apenas. c) I e II, apenas. d) II e III, apenas. e) I, II e III.

Questões

(CESGRANRIO/PETROBRAS 2010) Durante uma palestra sobre redes foram feitas três perguntas para o palestrante.

- 1) Por que não há mais o campo de checksum no cabeçalho do IPv6?
- 2) Os endereços IPv6 podem ser compatíveis com IPv4?
- 3) Como é tratado o QoS no IPv6?

Para as perguntas acima, o palestrante forneceu as respectivas respostas a seguir.



I - O objetivo de não utilizar o checksum com o IPv6 é processar mais rapidamente os datagramas no roteador, considerando-se, nesta versão, que o controle de erros das camadas do protocolo é confiável.



II - Os endereços IPv4 podem ser escritos por um par de dois pontos seguido da notação da versão 4 e o endereço 143.54.1.20 seria escrito como ::143.54.1.20.



III - Os campos Flow Label e Traffic Class do cabeçalho são usados para identificar aqueles pacotes que necessitam de uma maior qualidade de serviço, sendo pacotes originados de aplicações multimídia ou de tempo real, por exemplo.

Está(ão) correta(s) a(s) respostas(s)

- a) I, apenas. b) II, apenas. c) I e II, apenas. d) II e III, apenas. e) I, II e III.



Questões

(FCC/TRT-23 2016) No IPv6, o cabeçalho do datagrama não possui o campo para a fragmentação como no cabeçalho do IPv4. A eliminação desse campo foi possível porque

- a) o datagrama IPv6 tem tamanho fixo de 1024 Mbytes o que é suficiente para a transferência de dados sem fragmentação.
- b) os roteadores compatíveis com o IPv6 gerenciam a fragmentação de datagramas de forma autônoma.
- c) as funções de checar e gerenciar a fragmentação foram inseridas no campo Checksum do datagrama IPv6.
- d) os hosts e os roteadores compatíveis com o IPv6 determinam o tamanho do datagrama de forma dinâmica.
- e) o cabeçalho do datagrama IPv6 possui o campo Next, utilizado para o tratamento de todos os casos opcionais

Questões

(FCC/TRT-23 2016) No IPv6, o cabeçalho do datagrama não possui o campo para a fragmentação como no cabeçalho do IPv4. A eliminação desse campo foi possível porque

- a) o datagrama IPv6 tem tamanho fixo de 1024 Mbytes o que é suficiente para a transferência de dados sem fragmentação.
- b) os roteadores compatíveis com o IPv6 gerenciam a fragmentação de datagramas de forma autônoma.
- c) as funções de checar e gerenciar a fragmentação foram inseridas no campo Checksum do datagrama IPv6.
- d) os hosts e os roteadores compatíveis com o IPv6 determinam o tamanho do datagrama de forma dinâmica.
- e) o cabeçalho do datagrama IPv6 possui o campo Next, utilizado para o tratamento de todos os casos opcionais



Dúvidas?

Fórum do EAD

IPv6 para Concurso de TI

Endereço IPv6

IPv6 – Endereço IPv6

- Um endereço IPv4 é formado por 32 bits
 - $2^{32} = 4.294.967.296$
- Um endereço IPv6 é formado por 128 bits
- $2^{128} =$
340.282.366.920.938.463.463.374.607.431.768.211.456 6
- ~ 56 octilhões ($5,6 \times 10^{28}$) de endereços IP por ser humano
- ~ 79 octilhões ($7,9 \times 10^{28}$) de vezes a quantidade de endereços IPv4

IPv6 – Endereço IPv6

- Os endereços IPv6 são normalmente escritos como oito grupos de 4 dígitos hexadecimais.
- A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por “:”, escritos com dígitos hexadecimais
- Zeros podem abreviado. Por exemplo,
2001:0db8:85a3:0000:0000:0000:0000:7344 é o mesmo
endereço IPv6 que: 2001:0db8:85a3::7344.

IPv6 – Endereço IPv6

- Na representação de um endereço IPv6, é permitido utilizar tanto caracteres maiúsculos quanto minúsculos.
- O endereço 2001:0DB8:0000:0000:130F:0000:0000:140B pode ser escrito como 2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B
- Neste exemplo é possível observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário poderá haver ambiguidades na representação do endereço

IPv6 - CIDR

- Outra representação importante é a dos prefixos de rede. Em endereços IPv6 ela continua sendo escrita do mesmo modo que no IPv4, utilizando a notação CIDR.
- Esta notação é representada da forma “endereço-IPv6/tamanho do prefixo”, onde “tamanho do prefixo” é um valor decimal que especifica a quantidade de bits contíguos à esquerda do endereço que compreendem o prefixo.
- O exemplo de prefixo de sub-rede apresentado indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a red/sub-rede.
 - Prefixo: 2001:db8:3003:2::/64
 - Prefixo global: 2001:db8::/32
 - ID da sub-rede: 3003:2

IPv6 - CIRD

- Esta representação também possibilita a agregação dos endereços de forma hierárquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da sub-rede, etc
- Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes (sumarização)
- Os endereços IPv4 podem ser escritos por um par de dois pontos seguido da notação da versão 4 e o endereço 143.54.1.20 seria escrito como ::143.54.1.20

IPv6

- Com relação a representação dos endereços IPv6 em URLs (Uniform Resource Locators), estes agora passam a ser representados entre colchetes.
- Deste modo, não haverá ambiguidades caso seja necessário indicar o número de uma porta juntamente com a URL.
- Observe os exemplos a seguir:
 - [http://\[2001:12ff:0:4::22\]/index.html](http://[2001:12ff:0:4::22]/index.html)
 - [http://\[2001:12ff:0:4::22\]:8080](http://[2001:12ff:0:4::22]:8080)

Questões

(FGV/TCE-SE 2015) Em um ambiente IPv6, um usuário deseja acessar o endereço IPv4 192.168.100.1, de forma mapeada. Nessa situação, o usuário deve digitar esse endereço com a sintaxe:

A :192:168:100:1

B ::ffff:192.168.100.1

C 192.168.100.1::

D 192.168.100.1::ffff:

E ::0000:192.168.100.1

Questões

(FGV/TCE-SE 2015) Em um ambiente IPv6, um usuário deseja acessar o endereço IPv4 192.168.100.1, de forma mapeada. Nessa situação, o usuário deve digitar esse endereço com a sintaxe:

A :192:168:100:1



B ::ffff:192.168.100.1

C 192.168.100.1::

D 192.168.100.1::ffff:

E ::0000:192.168.100.1

Questões

(MP-RS/MP-RS 2015) Uma organização recebe o bloco IPv6 2001:DB8::/48 e deseja dividi-lo igualmente entre suas 16 filiais.

Qual é a máscara que deve ser empregada?

A /44

B /52

C /60

D /68

E 255.255.255.240

Questões

(MP-RS/MP-RS 2015) Uma organização recebe o bloco IPv6 2001:DB8::/48 e deseja dividi-lo igualmente entre suas 16 filiais. Qual é a máscara que deve ser empregada?

A /44



B /52

C /60

D /68

E 255.255.255.240

Questões

(FCC/TJ-AP 2014) O IPv6 estabelece o uso de 128 bits para indicar o endereço, enquanto o IPv4 utiliza 32 bits, o que lhe confere uma capacidade extremamente elevada de endereços IP. Considerando os endereços IPv6, NÃO é uma representação permitida:

A 1001:AB8::120C::240D

B 1001:ab8:0:0:120c::

C 1001:ab8::120c:0:0:240d

D 1001:ab8:0:0:120c::240d

E 1001:AB8:0:0:120C::240D

Questões

(FCC/TJ-AP 2014) O IPv6 estabelece o uso de 128 bits para indicar o endereço, enquanto o IPv4 utiliza 32 bits, o que lhe confere uma capacidade extremamente elevada de endereços IP. Considerando os endereços IPv6, NÃO é uma representação permitida:



A 1001:AB8::120C::240D

B 1001:ab8:0:0:120c::

C 1001:ab8::120c:0:0:240d

D 1001:ab8:0:0:120c::240d

E 1001:AB8:0:0:120C::240D

Questões

(CESGRANRIO/LIQUIGÁS 2012) Para ajudar a tornar os endereços IPv6 mais fáceis de serem manipulados, o padrão permite fazer a representação desses endereços de forma compacta, sem que se produza interpretação ambígua. A forma mais compacta de representação do endereço

FE80:0000:0000:0000:0202:BEFF:0000:8329 é

A FE80:0:0202:BEFF:0000:8329

B FE80:0:0202:BEFF:0:8329

C FE80:0:202:BEFF:0:8329

D FE80::202:BEFF:0:8329

E FE80::202:BEFF::8329

Questões

(CESGRANRIO/LIQUIGÁS 2012) Para ajudar a tornar os endereços IPv6 mais fáceis de serem manipulados, o padrão permite fazer a representação desses endereços de forma compacta, sem que se produza interpretação ambígua. A forma mais compacta de representação do endereço

FE80:0000:0000:0000:0202:BEFF:0000:8329 é

A FE80:0:0202:BEFF:0000:8329

B FE80:0:0202:BEFF:0:8329

C FE80:0:202:BEFF:0:8329



D FE80::202:BEFF:0:8329

E FE80::202:BEFF::8329

Questões

(CESGRANRIO/PETROBRAS 2012) O protocolo IPv6 possui um espaço de endereçamento de 128 bits, bem maior do que os 32 bits do IPv4.

Um exemplo de endereço IPv6 válido é

- a) 2001.0015.000A.0000.0000.0001.0003
- b) 2001.0015::000A.0001.0003
- c) 2001:0015::A:1:3
- d) 2003:0021:C:1:1:3
- e) 2003:0021::0065::0001:0003

Questões

(CESGRANRIO/PETROBRAS 2012) O protocolo IPv6 possui um espaço de endereçamento de 128 bits, bem maior do que os 32 bits do IPv4.

Um exemplo de endereço IPv6 válido é

a) 2001.0015.000A.0000.0000.0001.0003

b) 2001.0015::000A.0001.0003



c) 2001:0015::A:1:3

d) 2003:0021:C:1:1:3

e) 2003:0021::0065::0001:0003

Questões

(IDECAN/BANESTES 2012) Observe o seguinte endereço IPv6 em sua forma abreviada: 0:15::1:12:1213. Identifique qual das alternativas encontrase a forma expandida desse endereço.

A 0:15:0:0:1:12:1213

B 0:15:0:1:12:1213

C 0000:0015:0000:0000:0000:0001:0012:1213

D 0000:15:0000:0000:0000:1:12:1213

E 0:0015:0:0:0:0001:0012:1213

Questões

(IDECAN/BANESTES 2012) Observe o seguinte endereço IPv6 em sua forma abreviada: 0:15::1:12:1213. Identifique qual das alternativas encontrase a forma expandida desse endereço.

A 0:15:0:0:1:12:1213

B 0:15:0:1:12:1213



C 0000:0015:0000:0000:0000:0001:0012:1213

D 0000:15:0000:0000:0000:1:12:1213

E 0:0015:0:0:0:0001:0012:1213

Dúvidas?

Fórum do EAD

IPv6 para Concurso de TI

Tipos e Endereços Especiais

IPv6 – Tipos de Endereços

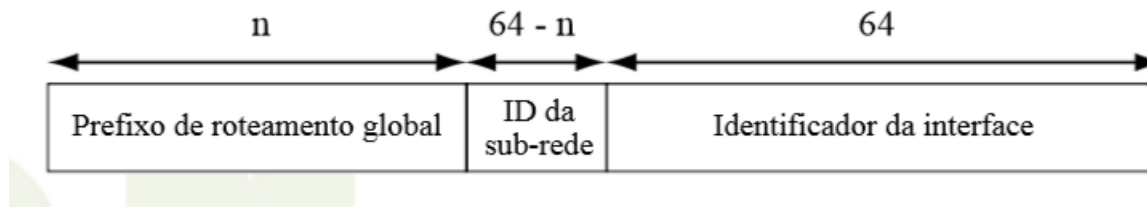
Há ainda no IPv6, tipos especiais de endereços:

- Unicast – Identificação Individual
- Multicast – Identificação Seletiva
- anycast – Identificação em Grupos

IPv6 – Unicast

Global Unicast

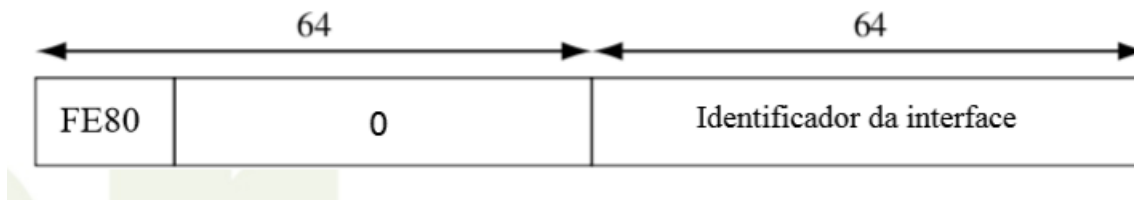
- 2000::/3
- Globalmente roteável (similar aos endereços públicos IPv4)
- 13% do total de endereços possíveis
- $2^{(45)} = 35.184.372.088.832$ redes / 48 distintas



IPv6 – Unicast

Unicast Link local

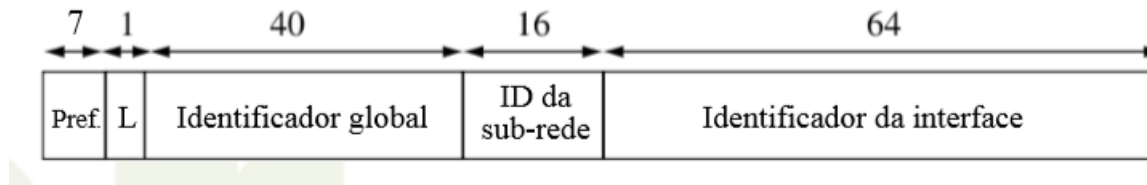
- FE80::/64
- Deve ser utilizado apenas localmente
- Atribuído automaticamente (autoconfiguração stateless)



IPv6 – Unicast

Unicast Unique local

- FC00::/7
- Prefixo globalmente único (com alta probabilidade de ser único)
- Utilizado apenas na comunicação dentro de um enlace ou entre um conjunto limitado de enlaces
- Não é esperado que seja roteado na Internet



IPv6 – Identificador da Interface (IID)

- Devem ser únicos dentro do mesmo prefixo de sub-rede
- O mesmo IID pode ser usado em múltiplas interfaces de um único nó, desde que estejam associadas a sub-redes diferentes
- Normalmente utiliza-se um IID de 64 bits, que pode ser obtido:
 - Manualmente
 - Autoconfiguração stateless
 - DHCPv6 (stateful)
 - A partir de uma chave pública (CGA)
- IID pode ser temporário e gerado randomicamente
- Normalmente é baseado no endereço MAC (Formato EUI-64)

IPv6 – Unicast Não-Especificado (Unspecified)

- É representado pelo endereço 0:0:0:0:0:0:0:0 ou ::0 (equivalente ao endereço IPv4 unspecified 0.0.0.0)
- Nunca deve ser atribuído a nenhum nó, indicando apenas a ausência de um endereço
- Ele pode, por exemplo, ser utilizado no campo Endereço de Origem de um pacote IPv6 enviado por um host durante o processo de inicialização, antes que este tenha seu endereço exclusivo determinado
- Não deve ser utilizado como endereço de destino de pacotes IPv6

IPv6 – Unicast Loopback (localhost)

- Representado pelo endereço unicast 0:0:0:0:0:0:0:1 ou ::1 (equivalente ao endereço IPv4 loopback 127.0.0.1)
- Utilizado para referenciar a própria máquina, sendo muito utilizado para teste internos
- Não deve ser atribuído a nenhuma interface física, nem usado como endereço de origem em pacotes IPv6 enviados para outros nós
- Um pacote IPv6 com um endereço loopback como destino não pode ser enviado por um roteador IPv6, e caso um pacote recebido em uma interface possua um endereço loopback como destino, este deve ser descartado

IPv6 – Unicast IPv4-mapeado

- Representado por 0:0:0:0:0:FFFF:wxyz ou ::FFFF:wxyz
- É usado para mapear um endereço IPv4 em um endereço IPv6 de 128-bit, onde xyzw representa os 32 bits do endereço IPv4, utilizando dígitos decimais.
- É aplicado em técnicas de transição para que nós IPv6 e IPv4 se comuniquem. Ex. ::FFFF:192.168.100.1

IPv6 – Endereços Especiais

Faixas Especiais

- 6to4 - 2002::/16
- Documentação - 2001:db8::/32
- Teredo - 2001:0000::/32

Obsoletos

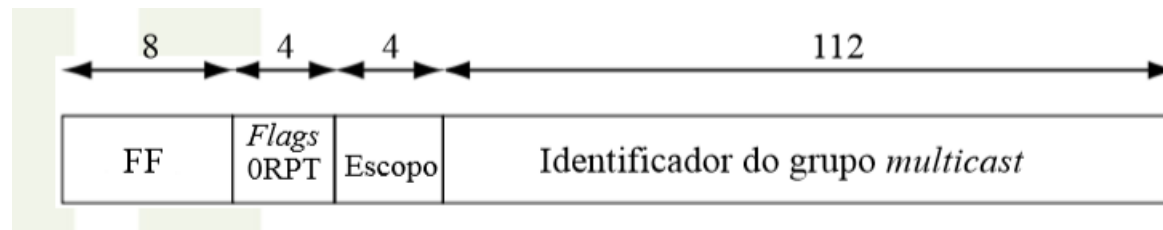
- Site local - FEC0::/10
- IPv4-compatível - ::wxyz
- 6Bone – 3FFE::/16 (rede de testes desativada em 06/06/06)

IPv6 – Anycast

- Identifica um grupo de interfaces
 - Entrega o pacote apenas para a interface mais perto da origem
- Atribuídos a partir de endereços unicast (são sintaticamente iguais).
- Possíveis utilizações:
 - Descobrir serviços na rede (DNS, proxy HTTP, etc.)
 - Balanceamento de carga
 - Localizar roteadores que forneçam acesso a uma determinada sub-rede
 - Utilizado em redes com suporte a mobilidade IPv6, para localizar os Agentes de Origem
- Subnet-Router

IPv6 – Multicast

- Identifica um grupo de interfaces.
- O suporte a multicast é obrigatório em todos os nós IPv6
- O endereço multicast deriva do bloco FF00::/8
- O prefixo FF é seguido de quatro bits utilizados como flags e mais quatro bits que definem o escopo do endereço multicast.
- Os 112 bits restantes são utilizados para identificar o grupo multicast.



IPv6 – Endereços Especiais

Endereço	Escopo	Descrição
FF01::1 FF01::2	Interface Interface	Todas as interfaces (<i>all-nodes</i>) Todos os roteadores (<i>all-routers</i>)
FF02::1 FF02::2 FF02::5 FF02::6 FF02::9 FF02::D FF02::1:2 FF02::1:FFXX:XXXX	Enlace Enlace Enlace Enlace Enlace Enlace Enlace Enlace	Todos os nós (<i>all-nodes</i>) Todos os roteadores (<i>all-routers</i>) Roteadores OSPF Roteadores OSPF designados Roteadores RIP Roteadores PIM Agentes DHCP <i>Solicited-node</i>
FF05::2 FF05::1:3 FF05::1:4	Site Site Site	Todos os roteadores (<i>all-routers</i>) Servidores DHCP em um site Agentes DHCP em um site
FF0X::101	Variado	NTP (<i>Network Time Protocol</i>)

IPv6 – Múltiplos Endereços

Do mesmo modo que no IPv4, os endereços IPv6 são atribuídos a interfaces físicas e não aos nós.

- Com o IPv6 é possível atribuir a uma única interface múltiplos endereços, independentemente do seu tipo
- Com isso, um nó pode ser identificado através de qualquer endereço de sua interfaces.
 - Loopback ::1
 - Link Local FE80:....
 - Unique local FD07:...
 - Global 2001:....
- A RFC 3484 determina o algoritmo para seleção dos endereços de origem e destino

Questões

(IADES/PCDF 2016) Assinale a alternativa que apresenta um endereço IPv6 Unicast da categoria Link Local.

A FE80::a00:27FF:FEC4:DEF0/64

B 2001:db8:cdaa::12/64

C ::1/64

D FC00::ECA:0DF/64

E 2000:ED00:0:FDC::1/64

Questões

(IADES/PCDF 2016) Assinale a alternativa que apresenta um endereço IPv6 Unicast da categoria Link Local.



A FE80::a00:27FF:FEC4:DEF0/64

B 2001:db8:cdaa::12/64

C ::1/64

D FC00::ECA:0DF/64

E 2000:ED00:0:FDC::1/64


Questões

(FCC/TCE-GO 2014) O principal motivo para a implantação do IPv6 é a necessidade de mais endereços, porque os endereços IPv4 disponíveis não são suficientes. No IPv6 os endereços

- A são representados por seis grupos de 16 bits separados por dois-pontos (:) e escritos com numeração hexadecimal.
- B anycast identificam uma única interface, de modo que um pacote enviado a um endereço anycast seja entregue a uma única interface.
- C broadcast não existem. No IPv4 eles eram responsáveis por direcionar um pacote para todos os nós de um mesmo domínio.
- D multicast identificam um conjunto de interfaces de forma que um pacote enviado a esse endereço sejam entregues a todas as interfaces associadas a esse endereço.
- E multicast são utilizados para identificar um grupo de interfaces, porém, com a propriedade de que um pacote enviado a um endereço multicast é encaminhado apenas à interface do grupo mais próxima da origem do pacote.

Questões

(FCC/TCE-GO 2014) O principal motivo para a implantação do IPv6 é a necessidade de mais endereços, porque os endereços IPv4 disponíveis não são suficientes. No IPv6 os endereços

- A são representados por seis grupos de 16 bits separados por dois-pontos (:) e escritos com numeração hexadecimal.
- B anycast identificam uma única interface, de modo que um pacote enviado a um endereço anycast seja entregue a uma única interface.
-  C broadcast não existem. No IPv4 eles eram responsáveis por direcionar um pacote para todos os nós de um mesmo domínio.
- D manycast identificam um conjunto de interfaces de forma que um pacote enviado a esse endereço sejam entregues a todas as interfaces associadas a esse endereço.
- E multicast são utilizados para identificar um grupo de interfaces, porém, com a propriedade de que um pacote enviado a um endereço multicast é encaminhado apenas à interface do grupo mais próxima da origem do pacote.

Questões

(FCC/TRT-1 2014) Diferentemente da designação de tipos de endereços no IPv4, no IPv6, devido à nova estrutura de endereços, são estabelecidos 5 tipos, que são

- A Broadcast, Multicast, de Retorno, não Especificados e Reservado.
- B Broadcast, Multicast, Simucast, Especificado e Reservado.
- C Unicast, Anycast, Multicast, de Retorno e não Especificados.
- D Broadcast, Unicast, Multicast, Especificado e de Retorno.
- E Unicast, Broadcast, Multicast, de Retorno e Reservado.

Questões

(FCC/TRT-1 2014) Diferentemente da designação de tipos de endereços no IPv4, no IPv6, devido à nova estrutura de endereços, são estabelecidos 5 tipos, que são

- A Broadcast, Multicast, de Retorno, não Especificados e Reservado.
- B Broadcast, Multicast, Simucast, Especificado e Reservado.
- C Unicast, Anycast, Multicast, de Retorno e não Especificados.
- D Broadcast, Unicast, Multicast, Especificado e de Retorno.
- E Unicast, Broadcast, Multicast, de Retorno e Reservado.



Questões

(CESPE/BASA 2012) Suponha que um computador que utilize IPv6 precise enviar uma mensagem a outro computador que também utilize IPv6, mas a mensagem precisa passar por uma parte da rede que esteja operando em IPv4. Nessa situação, deve ser usado um endereço compatível, cujo prefixo de tipo é 0000 0000.

Questões



(CESPE/BASA 2012) Suponha que um computador que utilize IPv6 precise enviar uma mensagem a outro computador que também utilize IPv6, mas a mensagem precisa passar por uma parte da rede que esteja operando em IPv4. Nessa situação, deve ser usado um endereço compatível, cujo prefixo de tipo é 0000 0000.

Questões

(CESPE/ANATEL 2014) No protocolo IPv6, não existe endereço broadcast, normalmente responsável por direcionar um pacote para todos os nós de um mesmo domínio. Nesse protocolo, essa função é atribuída a tipos específicos de endereços multicast.

Questões



(CESPE/ANATEL 2014) No protocolo IPv6, não existe endereço broadcast, normalmente responsável por direcionar um pacote para todos os nós de um mesmo domínio. Nesse protocolo, essa função é atribuída a tipos específicos de endereços multicast.

Dúvidas?

Fórum do EAD

IPv6 para Concurso de TI

Protocolos e Serviços

IPv6 – ICMPv6

Definido na RFC 4443

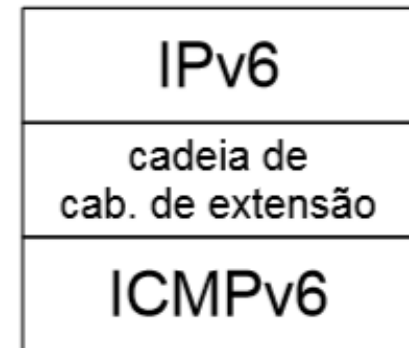
Mesmas funções do ICMPv4 (mas não são compatíveis):

- Informar características da rede
- Realizar diagnósticos
- Relatar erros no processamento de pacotes
- Assume as funcionalidades de outros protocolos:
 - ARP/RARP, IGMP
- Identificado pelo valor 58 no campo Próximo Cabeçalho
- Deve ser implementado em todos os nós

IPv6 – ICMPv6

É precedido pelos cabeçalhos de extensão, se houver, e pelo cabeçalho base do IPv6

- Protocolo chave da arquitetura IPv6
- Essencial em funcionalidades do IPv6:
 - Gerenciamento de grupos multicast
 - Descoberta de Vizinhaça (Neighbor Discovery)
 - Mobilidade IPv6
 - Descoberta do Path MTU



IPv6 – ICMPv6

Possui duas classes de mensagens:

Mensagens de Erro

- Destination Unreachable
- Packet Too Big
- Time Exceeded
- Parameter Problem

IPv6 – ICMPv6

Possui duas classes de mensagens:

Mensagens de Informação:

- Echo Request e Echo Reply
- Multicast Listener Query
- Multicast Listener Report
- Multicast Listener Done
- Router Solicitation e Router Advertisement
- Neighbor Solicitation e Neighbor Advertisement
- Redirect...

IPv6 – MLD

- Com a chegada do protocolo IPv6, o IGMP deu lugar a um novo protocolo chamado Multicast Listener Discovery (MLD), que possui diversas semelhanças e é derivado das versões 1 e 2 de seu antecessor
- A principal diferença entre o MLD e o IGMP se encontra no formato das mensagens e no formato do endereçamento.
- O MLD utiliza mensagens ICMPv6 (Internet Control Management Protocol version 6), ao contrário do IGMP, que possui mensagens independentes do protocolo ICMP

IPv6 – MLD

- O IPv6 faz uso intenso do MLD para descobrir nós que desejam receber pacotes multicast pertencentes a um grupo específico

** Internet Group Management Protocol (IGMP) A utilização de multicast IP em redes TCP/IP é definida como uma norma TCP/IP no RFC 1112, "Internet Group Management Protocol (IGMP)*

IPv6 – NDP

- Definido na RFC 4861
- Assume as funções de protocolos ARP, ICMP Router Discovery e ICMP Redirect, do IPv4
- Adiciona novos métodos não existentes na versão anterior do protocolo IP

IPv6 – NDP

Torna mais dinâmico alguns processos de configuração de rede:

- determinar o endereço MAC dos nós da rede
- encontrar roteadores vizinhos
- determinar prefixos e outras informações de configuração da rede
- detectar endereços duplicados
- determinar a acessibilidades dos roteadores
- redirecionamento de pacotes
- autoconfiguração de endereços

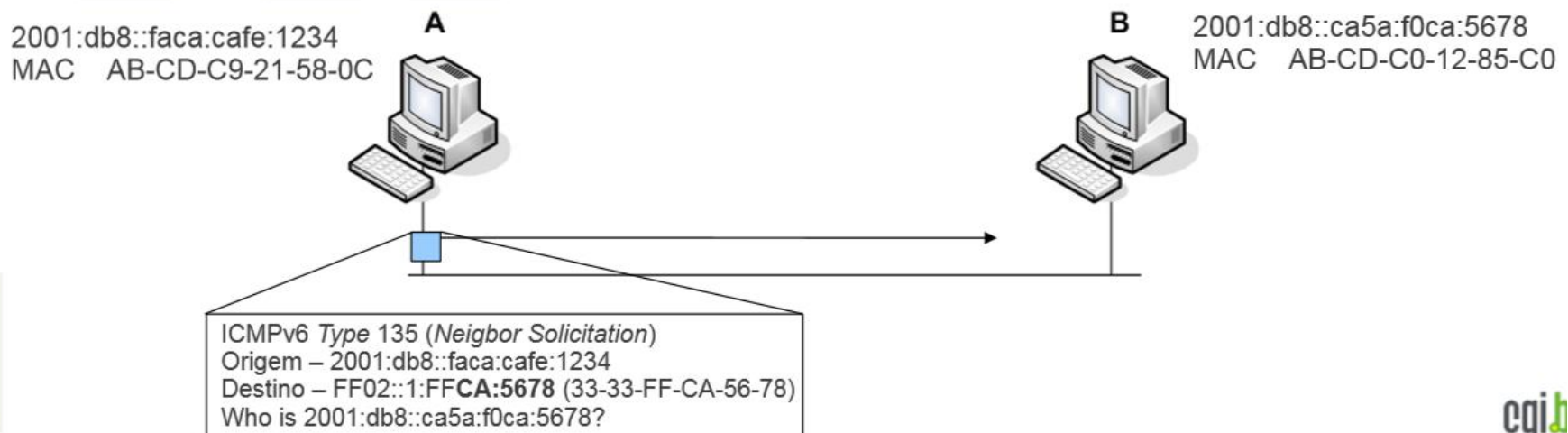
IPv6 – NDP

Utiliza 5 tipos de mensagens ICMPv6:

- Router Solicitation (RS) – ICMPv6 Tipo 133
- Router Advertisement (RA) – ICMPv6 Tipo 134
- Neighbor Solicitation (NS) – ICMPv6 Tipo 135
- Neighbor Advertisement (NA) – ICMPv6 Tipo 136
- Redirect – ICMPv6 Tipo 137

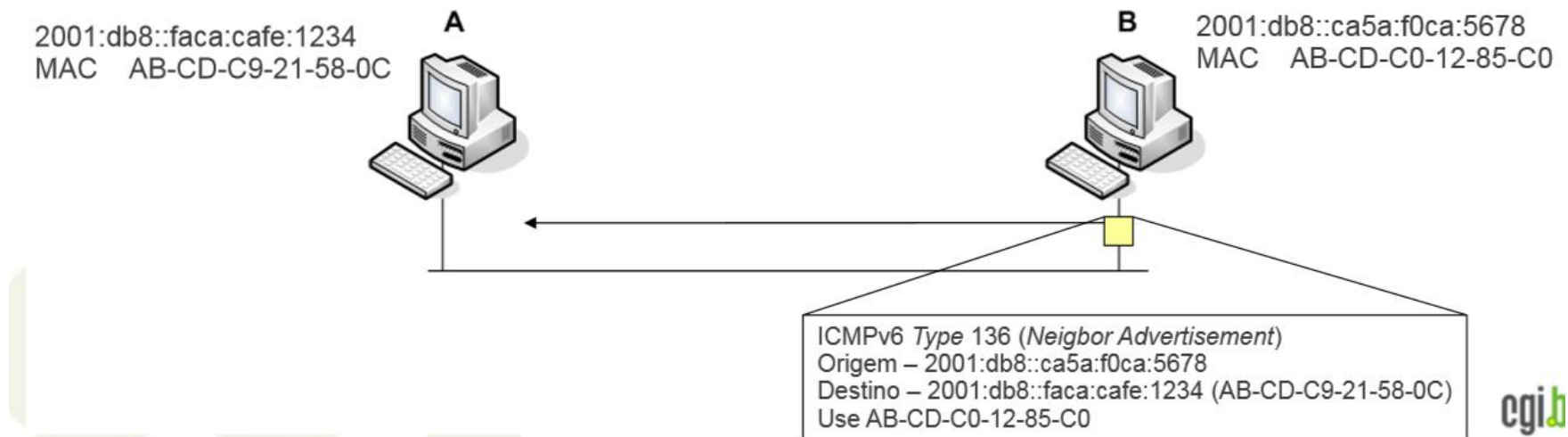
IPv6 – Descoberta de Endereços da Camada de Enlace

- Determina o endereço MAC dos vizinhos do mesmo enlace.
- Substitui o protocolo ARP
- Utiliza o endereço multicast solicited-node em vez de broadcast
 - O host envia uma mensagem NS informando seu endereço MAC e solicita o endereço MAC do vizinho



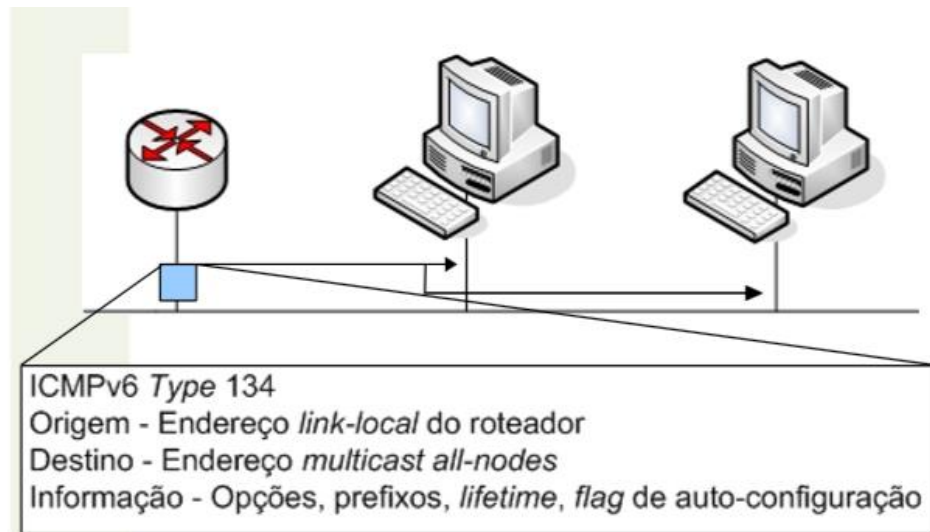
IPv6 – Descoberta de Endereços da Camada de Enlace

- Determina o endereço MAC dos vizinhos do mesmo enlace.
- Substitui o protocolo ARP
- Utiliza o endereço multicast solicited-node em vez de broadcast
 - O vizinho responde enviando uma mensagem NA informando seu endereço MAC



IPv6 – Descoberta de Roteadores e Prefixos

- Localizar roteadores vizinhos dentro do mesmo enlace
- Determina prefixos e parâmetros relacionados à autoconfiguração de endereço
- No IPv4, esta função é realizada pelas mensagens ARP Request.
- Roteadores enviam mensagens RA para o endereço multicast all-nodes



IPv6 – Detecção de Endereços Duplicados

- Verifica a unicidade dos endereços de um nó dentro do enlace
- Deve ser realizado antes de se atribuir qualquer endereço unicast a uma interface
- Consiste no envio de uma mensagem NS pelo host, com o campo target address preenchido com seu próprio endereço
- Caso alguma mensagem NA seja recebida como resposta, isso indicará que o endereço já está sendo utilizado

IPv6 – Detecção de Vizinhos Inacessíveis

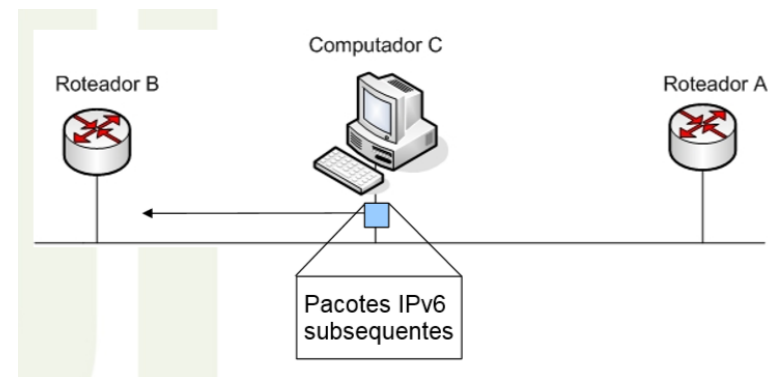
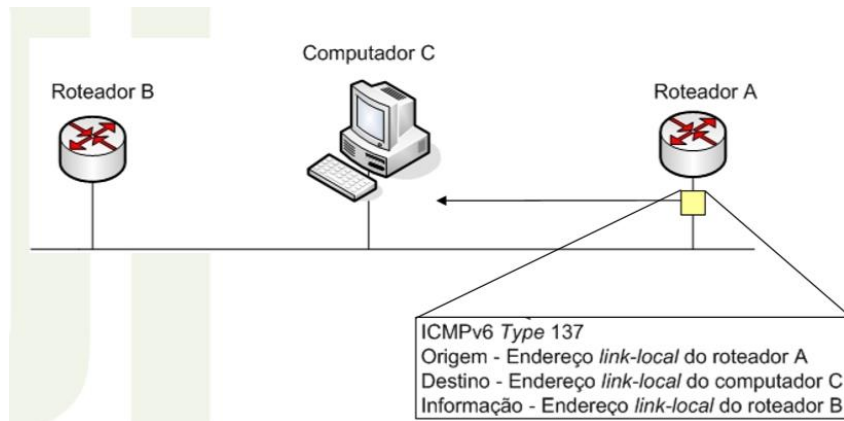
- Utilizado para rastrear a acessibilidade dos nós ao longo do caminho
- Um nó considera um vizinho acessível se ele recebeu recentemente a confirmação de entrega de algum pacote a esse vizinho

- Pode ser uma resposta a mensagens do protocolo de Descoberta de Vizinhança ou algum processo da camada de transporte que indique que uma conexão foi estabelecida

- Executado apenas para endereços unicast
- Neighbor Cache (similar a tabela ARP)
- Destination Cache

IPv6 – Redirecionamento

- Envia mensagens Redirect
- Redireciona um host para um roteador mais apropriado para o primeiro salto
- Informar ao host que destino encontra-se no mesmo enlace
- Este mecanismo é igual ao existente no IPv4



IPv6 – Autoconfiguração de Endereços Stateless

- Um endereço link-local é gerado
 - Prefixo FE80::/64 + identificador da interface.
- Endereço adicionado aos grupos *multicast solicited-node* e *all-node*
- Verifica-se a unicidade do endereço
 - Se já estiver sendo utilizado, o processo é interrompido, exigindo uma configuração manual
 - Se for considerado único e válido, ele será atribuído à interface
- Host envia uma mensagem RS para o grupo *multicast all-routers*
- Todos os roteadores do enlace respondem com mensagem RA

IPv6 – Path MTU Discovery

Assume que o MTU máximo do caminho é igual ao MTU do primeiro salto

- Pacote maiores do que o suportado por algum roteador ao longo do caminho, são descartados
 - Uma mensagem ICMPv6 packet too big é retornada
- Após o recebimento dessa mensagem, o nó de origem reduz o tamanho dos pacotes de acordo com o MTU indicado na mensagem packet too big
- O procedimento termina quando o tamanho do pacote for igual ou inferior ao menor MTU do caminho
- Essas interações podem ocorrer diversas vezes até se encontrar o menor MTU
- Pacotes enviados a um grupo multicast utilizam tamanho igual ao menor PMTU de todo o conjunto de destinos.

IPv6 – Jumbograms

- IPv6 permite o envio de pacotes que possuam entre 65.536 e 4.294.967.295 Bytes de comprimento
- Um jumbograms é identificado utilizando:
 - O campo Tamanho dos Dados com valor 0 (zero)
 - O campo Próximo Cabeçalho indicando o cabeçalho Hop-by-Hop.
- O cabeçalho de extensão Hop-by-Hop trará o tamanho do pacote
- Devem ser realizadas alterações também nos cabeçalhos TCP e UDP, ambos limitados a 16 bits para indicar o tamanho máximo dos pacotes

IPv6 – DNS e NAT

- O Registo de DNS AAAA executa a mesma função de **A**, porém, para um endereço IPv6.
- A faixa de endereços instituída para uso na conversão IPv6 em IPv4 é 192.88.99.0/24 ou 192.88.99.0 até 192.88.99.255 (RFC 3068).

IPv6 – DHCP

- Autoconfiguração de Endereços Stateful
- Usado pelo sistema quando nenhum roteador é encontrado
- Usado pelo sistema quando indicado nas mensagens RA
- Fornece:
 - Endereços IPv6
 - Outros parâmetros (servidores DNS, NTP...)
- Clientes utilizam um endereço link-local para transmitir ou receber mensagens DHCP
- Servidores utilizam endereços multicast para receber mensagens dos clientes (**FF02::1:2** ou **FF05::1:3**).

IPv6 – DHCP

- Permite um controle maior na atribuição de endereços aos host
- Os mecanismos de autoconfiguração de endereços **stateful** e **stateless** podem ser utilizados simultaneamente
 - Por exemplo: utilizar autoconfiguração stateless para atribuir os endereços e DHCPv6 para informar o endereço do servidor DNS
- DHCPv6 e DHCPv4 são independentes. Redes com Pilha Dupla precisam de serviços DHCP separados

Questões

(FCC/TRT-14 2011) A faixa de endereços usada para conversão *Ipv6* em *Ipv4* é

- (A) 0.0.0.0 a 0.255.255.255
- (B) 127.0.0.0 a 127.255.255.255
- (C) 169.254.0.0 a 169.254.255.255
- (D) 172.16.0.0 a 192.0.2.255
- (E) 192.88.99.0 a 192.88.99.255

Questões

(FCC/TRT-14 2011) A faixa de endereços usada para conversão *Ipv6* em *Ipv4* é

(A) 0.0.0.0 a 0.255.255.255

(B) 127.0.0.0 a 127.255.255.255

(C) 169.254.0.0 a 169.254.255.255

(D) 172.16.0.0 a 192.0.2.255

(E) 192.88.99.0 a 192.88.99.255



Questões

(CESPE/ANATEL 2014) Um dos avanços significativos do protocolo IPv6 com relação ao IPv4 é o suporte à autoconfiguração automática de endereços IP, o que torna o uso de servidor DHCP totalmente desnecessário.

Questões



(CESPE/ANATEL 2014) Um dos avanços significativos do protocolo IPv6 com relação ao IPv4 é o suporte à autoconfiguração automática de endereços IP, o que torna o uso de servidor DHCP totalmente desnecessário.


Questões

(FCC/TRT-5 2013) É uma característica do protocolo IPv6:

- (A) Address Resolution Protocol – ARP que utiliza requisitos do tipo broadcast.
- (B) endereço de 32 bits.
- (C) Multicast Listener Discovery – MLD.
- (D) suporte opcional de IPSec.
- (E) cabeçalho que inclui campos de opção.

Questões

(FCC/TRT-5 2013) É uma característica do protocolo IPv6:

- (A) Address Resolution Protocol – ARP que utiliza requisitos do tipo broadcast.
- (B) endereço de 32 bits.
-  (C) Multicast Listener Discovery – MLD.
- (D) suporte opcional de IPSec.
- (E) cabeçalho que inclui campos de opção.

Questões

(VUNESP/TJ-PA 2014) No serviço DNS, os registros de recurso _____ e _____ associam um nome de domínio a endereços IPv4 e IPv6, respectivamente.

Assinale a alternativa que preenche, correta e respectivamente, as lacunas da sentença apresentada.

- A AAAA ... NS
- B AAAA ... A
- C CNAME ... MX
- D A ... AAAA
- E AAAA ... CNAME

Questões

(VUNESP/TJ-PA 2014) No serviço DNS, os registros de recurso _____ e _____ associam um nome de domínio a endereços IPv4 e IPv6, respectivamente.

Assinale a alternativa que preenche, correta e respectivamente, as lacunas da sentença apresentada.

A AAAA ... NS

B AAAA ... A

C CNAME ... MX

 D A ... AAAA

E AAAA ... CNAME


Questões

(IADES/PCDF 2016) O processo de detecção de endereços duplicados em uma rede IPv6 é chamado de duplicate address detection (DAD). Assinale a alternativa que descreve as etapas desse processo.

- A Após configurar o endereço IPv6 em qualquer interface, o equipamento informa na rede esse endereço IPv6 e o respectivo endereço físico da interface. As tabelas (cache) de mapeamento de endereços IP e MAC são preenchidas em todos os nós da rede. Caso seja detectada uma duplicação de endereço, o equipamento envia uma mensagem Neighbor Advertisement (NA) e suspende a respectiva transmissão por essa interface
- B Ao se conectar a uma rede IPv6, o equipamento envia uma mensagem Router Solicitation (RS). O roteador da rede responde com uma mensagem Router Advertisement (RA), contendo parâmetros de configuração, como o prefixo da rede. O equipamento então gera o respectivo endereço IPv6 combinando o prefixo informado com o endereço físico da respectiva interface, resultando, assim, em um endereço único não duplicado
- C Primeiro, o equipamento envia uma mensagem Neighbor Discovery Protocol (NDP), recebendo, em seguida, uma resposta de um roteador da rede habilitado para informar parâmetros como default route e servidor DNS. Em seguida, o equipamento procura na rede pelo servidor DHCPv6 para solicitar seu endereço IPv6 e demais parâmetros de rede necessários para o respectivo funcionamento
- D Ao ser atribuído um endereço IPv6 a uma interface, ela envia uma mensagem Neighbor Solicitation (NS) para tentar descobrir o endereço físico do próprio endereço IPv6. Nessa mensagem, o campo de endereço de origem é :: (não especificado). Caso receba de volta uma mensagem Neighbor Advertisement (NA), tal endereço é bloqueado nessa interface, e o nó que já possuía o endereço duplicado continua funcionando normalmente
- E Ao se conectar a uma rede IPv6, o equipamento envia um pacote Neighbor Discovery ao endereço multicast solicited-node (FF02::1:ff00:0000), informando seu endereço IPv6 e MAC. Um servidor DHCPv6 da rede responde diretamente ao nó requisitante com uma mensagem Neighbor Advertisement, podendo ser uma resposta positiva (endereço disponível) ou negativa (endereço já utilizado).

Questões

(IADES/PCDF 2016) O processo de detecção de endereços duplicados em uma rede IPv6 é chamado de duplicate address detection (DAD). Assinale a alternativa que descreve as etapas desse processo.

- A Após configurar o endereço IPv6 em qualquer interface, o equipamento informa na rede esse endereço IPv6 e o respectivo endereço físico da interface. As tabelas (cache) de mapeamento de endereços IP e MAC são preenchidas em todos os nós da rede. Caso seja detectada uma duplicação de endereço, o equipamento envia uma mensagem Neighbor Advertisement (NA) e suspende a respectiva transmissão por essa interface
- B Ao se conectar a uma rede IPv6, o equipamento envia uma mensagem Router Solicitation (RS). O roteador da rede responde com uma mensagem Router Advertisement (RA), contendo parâmetros de configuração, como o prefixo da rede. O equipamento então gera o respectivo endereço IPv6 combinando o prefixo informado com o endereço físico da respectiva interface, resultando, assim, em um endereço único não duplicado
- C Primeiro, o equipamento envia uma mensagem Neighbor Discovery Protocol (NDP), recebendo, em seguida, uma resposta de um roteador da rede habilitado para informar parâmetros como default route e servidor DNS. Em seguida, o equipamento procura na rede pelo servidor DHCPv6 para solicitar seu endereço IPv6 e demais parâmetros de rede necessários para o respectivo funcionamento
-  D Ao ser atribuído um endereço IPv6 a uma interface, ela envia uma mensagem Neighbor Solicitation (NS) para tentar descobrir o endereço físico do próprio endereço IPv6. Nessa mensagem, o campo de endereço de origem é :: (não especificado). Caso receba de volta uma mensagem Neighbor Advertisement (NA), tal endereço é bloqueado nessa interface, e o nó que já possuía o endereço duplicado continua funcionando normalmente
- E Ao se conectar a uma rede IPv6, o equipamento envia um pacote Neighbor Discovery ao endereço multicast solicited-node (FF02::1:ff00:0000), informando seu endereço IPv6 e MAC. Um servidor DHCPv6 da rede responde diretamente ao nó requisitante com uma mensagem Neighbor Advertisement, podendo ser uma resposta positiva (endereço disponível) ou negativa (endereço já utilizado).

Questões

(CESPE/MEC 2015) Para o IPv6 definiu-se uma nova versão do ICMP que incorpora funções do protocolo IGMP com o propósito de gerenciar adesões de grupos multicast.

Questões



(CESPE/MEC 2015) Para o IPv6 definiu-se uma nova versão do ICMP que incorpora funções do protocolo IGMP com o propósito de gerenciar adesões de grupos multicast.

Dúvidas?

Fórum do EAD

IPv6 para Concurso de TI

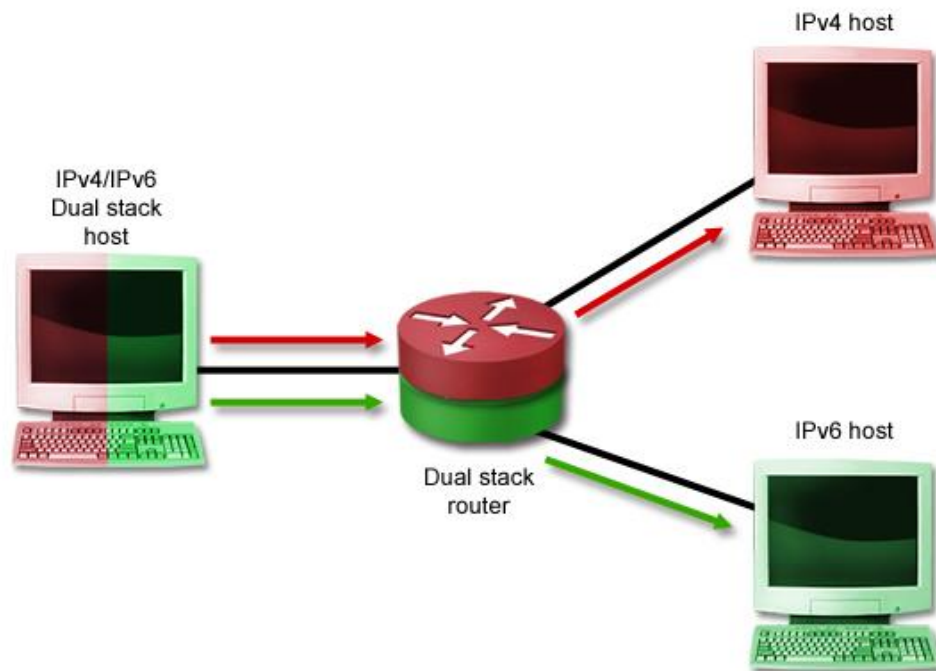
Estratégias de Migração

Transição

- A transição do endereçamento IP versão 4 para versão 6 não requer a migração simultânea de todos os *hosts* da rede.
- Existem vários mecanismos de transição que permitem comunicação entre hosts com IP versão 4 com *hosts* com IPv6.
- Os mecanismos mais comuns para a transição de tecnologia são:
 - **Dual Stack (lado a lado).**
 - **Túnel Ipv6 para Ipv4 (6to4)**
 - **NAT**

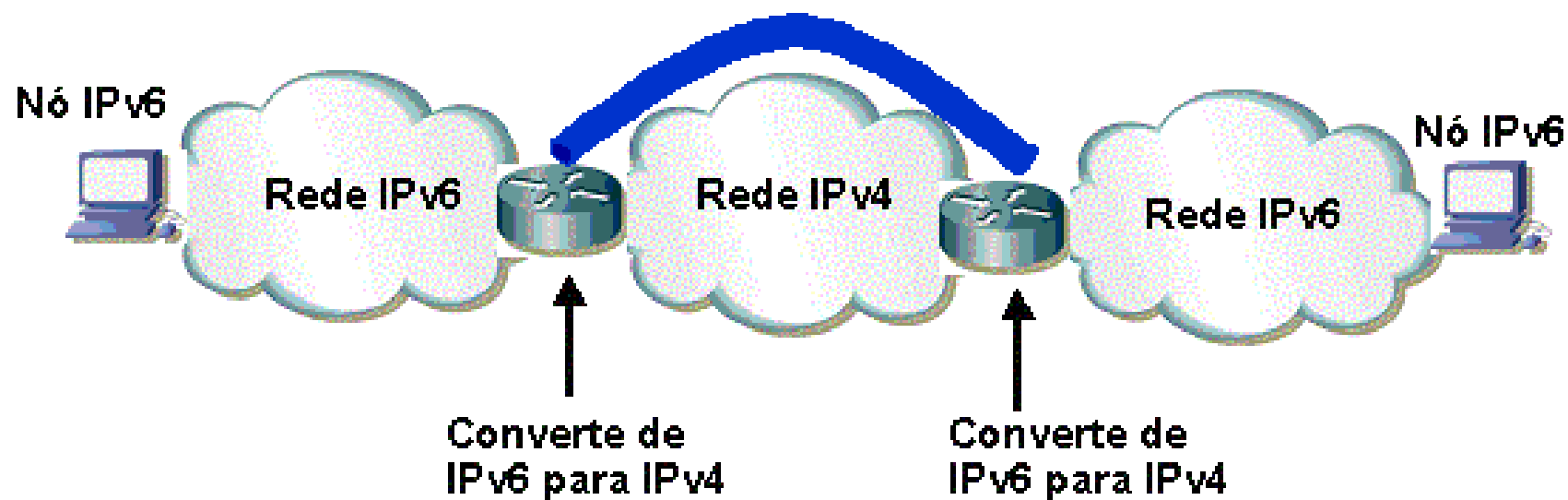
Transição

- Dual Stack



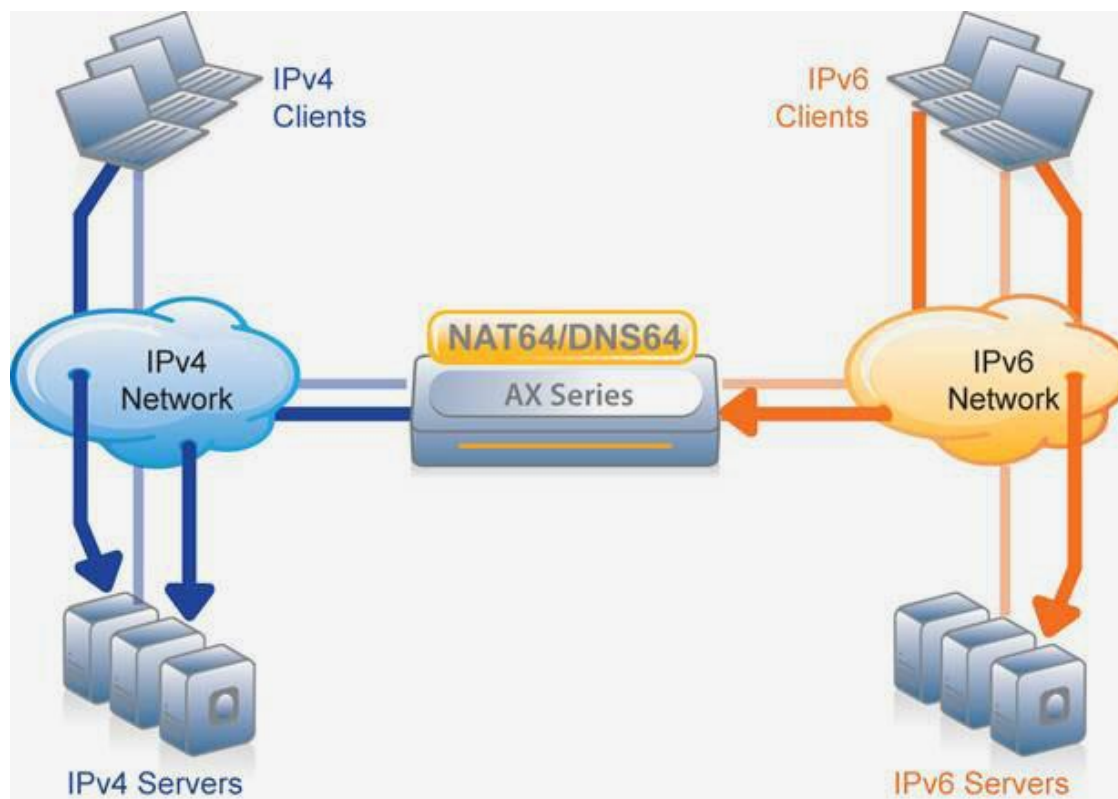
Transição

- Túnel Ipv6 para Ipv4 (6to4)



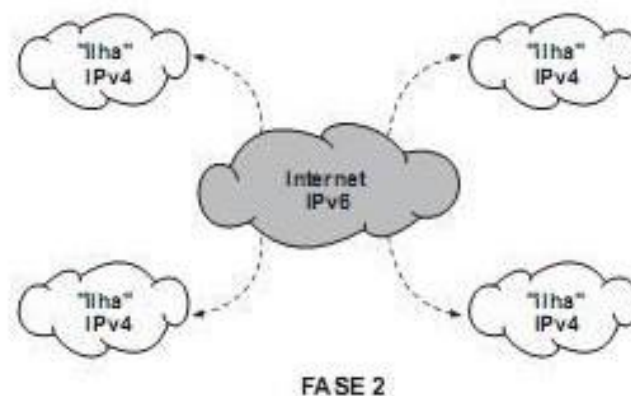
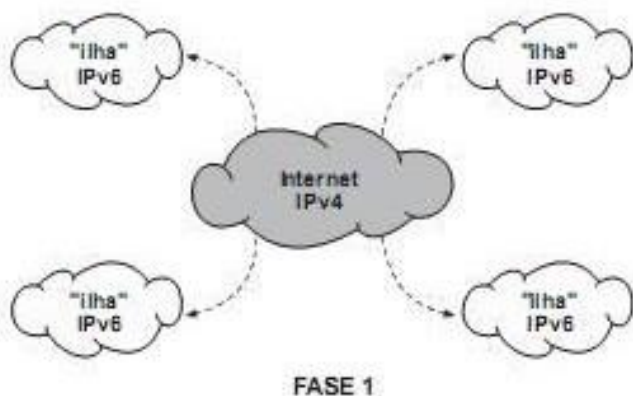
Transição

- NAT



Questões


(FCC/TRT-15 2013) As figuras abaixo sugerem como deveria se dar a transição do protocolo IPv4 para IPv6. Em relação aos protocolos IPv4 e IPv6 e a transição sugerida nas figuras acima é correto afirmar:



Questões

- a) A IETF - Internet Engineering Task Force recomenda que, para agilizar o processo de migração, é necessário que haja 2 Internets diferentes e todos os hosts conectados a elas possuam as duas pilhas de protocolos IPv4 e IPv6 funcionando separadamente. Esta estratégia é chamada de dual-protocol.
- b) As figuras sugerem que cada host pode ter acesso aos 2 protocolos utilizados em 2 Internets diferentes, enquanto durar a transição. A vantagem é que uma aplicação IPv4 consegue dialogar diretamente com uma aplicação IPv6 e vice-versa.
- c) Como os diagramas da transição mostram, haveria técnicas auxiliares de transição, inicialmente para interconectar ilhas IPv6 em uma Internet majoritariamente IPv4 e, depois de algum tempo, para fazer o contrário. Há necessidade de se implantar o IPv6 numa Internet sempre crescente, na qual novos usuários ainda precisam de conectividade IPv4, mas não há mais endereços IPv4 livres para atendê-los.
- d) O IPv6 utiliza endereços maiores e acrescenta alguns novos recursos, mas mantém o formato de datagrama do IPv4 para facilitar a transição dos novos endereços IP.
- e) O IPv4 utiliza endereços de 32 bits; o IPv6 duplica este tamanho, usando endereços de 64 bits, tornando o espaço tão grande que não possa ser esgotado em um futuro previsível. Além disso, o IPv6 mantém o mesmo esquema de fragmentação de datagramas em roteadores intermediários. Este tipo de fragmentação do IPv4 é denominado fim-a-fim.

Questões

- a) A IETF - Internet Engineering Task Force recomenda que, para agilizar o processo de migração, é necessário que haja 2 Internets diferentes e todos os hosts conectados a elas possuam as duas pilhas de protocolos IPv4 e IPv6 funcionando separadamente. Esta estratégia é chamada de dual-protocol.
- b) As figuras sugerem que cada host pode ter acesso aos 2 protocolos utilizados em 2 Internets diferentes, enquanto durar a transição. A vantagem é que uma aplicação IPv4 consegue dialogar diretamente com uma aplicação IPv6 e vice-versa.
-  c) Como os diagramas da transição mostram, haveria técnicas auxiliares de transição, inicialmente para interconectar ilhas IPv6 em uma Internet majoritariamente IPv4 e, depois de algum tempo, para fazer o contrário. Há necessidade de se implantar o IPv6 numa Internet sempre crescente, na qual novos usuários ainda precisam de conectividade IPv4, mas não há mais endereços IPv4 livres para atendê-los.
- d) O IPv6 utiliza endereços maiores e acrescenta alguns novos recursos, mas mantém o formato de datagrama do IPv4 para facilitar a transição dos novos endereços IP.
- e) O IPv4 utiliza endereços de 32 bits; o IPv6 duplica este tamanho, usando endereços de 64 bits, tornando o espaço tão grande que não possa ser esgotado em um futuro previsível. Além disso, o IPv6 mantém o mesmo esquema de fragmentação de datagramas em roteadores intermediários. Este tipo de fragmentação do IPv4 é denominado fim-a-fim.

Questões

(FCC/MPE-MA 2013) Com o intuito de facilitar o processo de transição entre as duas versões do protocolo IP (IPv4 e IPv6), algumas técnicas foram desenvolvidas. Cada uma dessas técnicas apresenta uma característica específica, podendo ser utilizada individualmente ou em conjunto com outras técnicas, de modo a atender as necessidades de cada situação. As técnicas:

I. Um nó IPv6/IPv4, ao se comunicar com um nó IPv6, se comporta como um nó IPv6 e na comunicação com um nó IPv4, se comporta como nó IPv4.

II. Permite transmitir pacotes IPv6 através da infraestrutura IPv4 já existente, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento.

III. Possibilita roteamento transparente na comunicação entre nós que apresentem suporte apenas a uma versão do protocolo IP.

Referem-se, respectivamente, a utilização da técnica de

- a) Pilha dupla - Tradução - Tunelamento.
- b) Pilha dupla - Tunelamento - Tradução.
- c) Tradução - Tunelamento - Pilha dupla.
- d) Tradução - Pilha dupla - Tunelamento.
- e) Tunelamento - Pilha dupla - Tradução.

Questões

(FCC/MPE-MA 2013) Com o intuito de facilitar o processo de transição entre as duas versões do protocolo IP (IPv4 e IPv6), algumas técnicas foram desenvolvidas. Cada uma dessas técnicas apresenta uma característica específica, podendo ser utilizada individualmente ou em conjunto com outras técnicas, de modo a atender as necessidades de cada situação. As técnicas:

- I. Um nó IPv6/IPv4, ao se comunicar com um nó IPv6, se comporta como um nó IPv6 e na comunicação com um nó IPv4, se comporta como nó IPv4.
- II. Permite transmitir pacotes IPv6 através da infraestrutura IPv4 já existente, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento.
- III. Possibilita roteamento transparente na comunicação entre nós que apresentem suporte apenas a uma versão do protocolo IP.

Referem-se, respectivamente, a utilização da técnica de

- a) Pilha dupla - Tradução - Tunelamento.
- b) Pilha dupla - Tunelamento - Tradução.
- c) Tradução - Tunelamento - Pilha dupla.
- d) Tradução - Pilha dupla - Tunelamento.
- e) Tunelamento - Pilha dupla - Tradução.



Dúvidas?

Fórum do EAD

IPv6

Questões Atualização 2019 - I

Prof. Walter Cunha

falecomigo@waltercunha.com

[Professor]



Natural: Fortaleza – CE

Cargo: AFFC-CGU TI (2009)

Graduação: Engenharia Eletrônica
ITA 2000

Pós: Ger. Projetos FGV 2007

Emerging Leaders: Harvard
Kennedy School Nov/2018



Outros Cursos no Provas de TI:

<http://bit.ly/2RsnuhF>

Tlmasters:

<https://br.groups.yahoo.com/neo/groups/tlmasters/info>

Orientação para Concursos:

<https://www.patreon.com/tlmasters>

Outros:

<https://about.me/waltercunha>

[Questão 01]

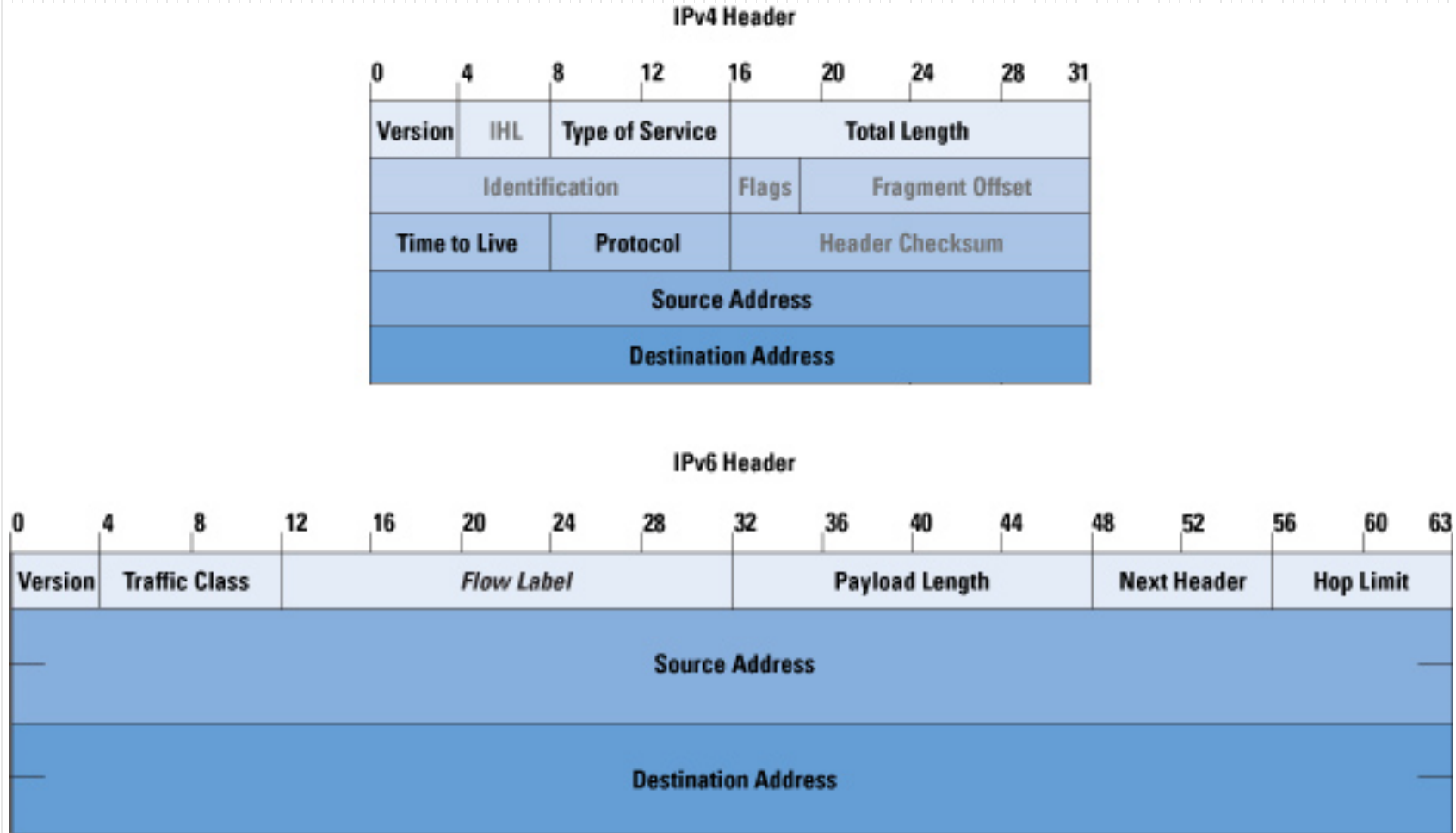
(CESPE/EMAP 2018) Comparativamente ao IPv4, o IPv6, além de aumentar o endereçamento de 32 bites para 128 bites, também aumentou a quantidade de campos no cabeçalho: de 7 para 13.

[Questão 01]

(CESPE/EMAP 2018) Comparativamente ao IPv4, o IPv6, além de aumentar o endereçamento de 32 bites para 128 bites, também aumentou a quantidade de campos no cabeçalho: de 7 para 13.

ERRADA

[Questão 01] – Comentários...



[Questão 02]

(CESPE/PF 2018) No IPv4, um endereço IP é composto por 32 bites, enquanto no IPv6, um endereço IP tem 128 bites. Em comparação com o modelo de referência OSI, tanto o IPv4 quanto o IPv6 encontram-se na camada de rede.

[Questão 02]

(CESPE/PF 2018) No IPv4, um endereço IP é composto por 32 bites, enquanto no IPv6, um endereço IP tem 128 bites. Em comparação com o modelo de referência OSI, tanto o IPv4 quanto o IPv6 encontram-se na camada de rede.

CERTA

[Questão 02] – Comentários...

Camada	Protocolo
7.Aplicação	HTTP, RTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, Ping ...
6.Apresentação	XDR, TLS ...
5.Sessão	NetBIOS ...
4.Transporte	NetBEUI, TCP, UDP, SCTP, DCCP, RIP ...
3.Redes	IP (IPv4, IPv6), IPsec, ICMP, ARP, RARP, NAT ...
2.Enlace <ul style="list-style-type: none">• Subcamada LLC• Subcamada MAC	Ethernet, IEEE 802.1Q, HDLC, Token ring, FDDI, PPP, Switch, Frame relay, ATM ...
1.Física	Modem, , 802.11 Wi-Fi, RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB, 10BASE-T, 100BASE-TX, ISDN, SONET, DSL ...

[Questão 03]

(CESPE/SEDf 2017) A utilização do IPv6 permite o controle do congestionamento do tráfego por meio do campo prioridade; assim, se um de dois datagramas consecutivos tiver de ser descartado em virtude do congestionamento, será eliminado o datagrama assinalado com prioridade de pacote menor.

[Questão 03]

(CESPE/SEDf 2017) A utilização do IPv6 permite o controle do congestionamento do tráfego por meio do campo prioridade; assim, se um de dois datagramas consecutivos tiver de ser descartado em virtude do congestionamento, será eliminado o datagrama assinalado com prioridade de pacote menor.

CERTA

[Questão 03] – Comentários...

Classe de Tráfego (8 bits) – Identifica os pacotes por classes de serviços ou prioridade. Ele provê as mesmas funcionalidades e definições do campo “Tipo de Serviço do IPv4”

[Questão 04]

(CESPE/STJ 2018) No IPv6, o tráfego não controlado por congestionamento é usado quando a eliminação de pacotes é indesejável e, por essa razão, não são atribuídas prioridades aos pacotes.

[Questão 04]

(CESPE/STJ 2018) No IPv6, o tráfego não controlado por congestionamento é usado quando a eliminação de pacotes é indesejável e, por essa razão, não são atribuídas prioridades aos pacotes.

[Questão 04] – Comentários...

Tráfego não Controlado por Congestionamento

Este se refere a um tipo de tráfego com expectativa de atraso mínimo. A eliminação de pacotes é indesejável. A retransmissão, na maioria dos casos, impossível. Em outras palavras, a origem não se adapta a situações de congestionamento. Áudio e vídeo em tempo real são exemplos desse tipo de tráfego. Níveis de prioridade de 8 a 15 são atribuídos ao tráfego não controlado por congestionamento. Embora ainda não existam quaisquer atribuições-padrão particulares para esse tipo de dados, as prioridades normalmente se baseiam em quanto a qualidade dos dados recebidos é afetada pela eliminação de pacotes. Dados contendo menos redundância (como áudio ou vídeo de baixa fidelidade) podem receber maior prioridade (15). Dados contendo maior redundância (como áudio ou vídeo de alta fidelidade) recebem menor prioridade (8). Ver a Tabela 20.8.

Fonte: *pág. 600 do livro Comunicação de Dados e Redes de Computadores, Forouzan, 4ª edição.*

[Questão 05]

(CESPE/BNB 2018) No caso do DNSSEC, o suporte ao protocolo IPv6 depende do IPSEC, pois a troca de cache de zonas é por túnel.

[Questão 05]

(CESPE/BNB 2018) No caso do DNSSEC, o suporte ao protocolo IPv6 depende do IPSEC, pois a troca de cache de zonas é por túnel.

[Questão 05] – Comentários...

DNS SEC

O que garante?

- Origem (Autenticidade)
- Integridade
- A não existência de um nome ou tipo

O que não garante?

Confidencialidade

Proteção contra ataques de negação de serviço (DOS)

DNSSEC utiliza o conceito de chaves assimétricas – chave pública e chave privada

Dúvidas

Prof. Walter Cunha

falecomigo@waltercunha.com

<https://www.patreon.com/timasters>

<https://www.facebook.com/walter.cunha.7>

<https://www.instagram.com/walter.cunha.7/>

<https://twitter.com/timasters>

<https://www.linkedin.com/in/walter-cunha-19a90721>



PROVAS DE TI
TUDO PARA VOCÊ PASSAR

IPv6 (FCC)

Questões Atualização 2019 - I

Prof. Walter Cunha

falecomigo@waltercunha.com

[Questão 01]

(FCC/SEMEF-AM 2019) Sobre o protocolo IPv6, é correto afirmar que
A a sua implantação só ocorrerá após a substituição total do IPv4.

B ele prevê cinco classes: A, B, C, D e E.

C o endereçamento que ele prevê envolve 256 bits

D o endereço IPv6 2011:0fef:ba43::1234 é o mesmo que
2011:0fef:ba43:0000:0000:0000:0000:1234.

E um endereço IPv6 é normalmente escrito como oito grupos de três dígitos hexadecimais

[Questão 01] – Comentários...

(FCC/SEMEF-AM 2019) Sobre o protocolo IPv6, é correto afirmar que
A a sua implantação ~~só ocorrerá após a substituição total do IPv4~~.

B ele ~~prevê cinco classes~~: A, B, C, D e E.

C o endereçamento que ele prevê envolve ~~256 bits~~

D o endereço IPv6 2011:0fef:ba43::1234 é o mesmo que
2011:0fef:ba43:0000:0000:0000:1234.

E um endereço IPv6 é normalmente escrito como oito grupos de ~~três dígitos
hexadecimais~~

RESP D

[Questão 02]

(FCC/SEFAZ-BA 2019) Solicitou-se a um Auditor analisar os endereços IP listados abaixo.

Sufixo DNS específico de conexão: Endereço IPv6 :

2804:14c:122:86k6::1008 Endereço IPv6 :

2804:14c:122:86b6:9d9d:91c0:a266:c8b8 Endereço IPv6 Temporário..... :

2804:14c:122:86b6:6157:ba6e:cb64:37e2 Endereço IPv6 de link local :

fe80::9d9d:91c0:a266:c8b8%7 Endereço IPv4.....: 192.168.0.21

Máscara de Sub-rede : 255.255.255.0 Gateway

Padrão..... : fe80::ea20:e2ff:fe0f:c832%7

Ele concluiu corretamente que o endereço

[Questão 02]

(FCC/SEFAZ-BA 2019) Solicitou-se a um Auditor analisar os endereços IP listados abaixo.

(...)

A 192.168.0.21 está incorreto, pois um endereço IPv4 precisa ter sempre 3 algarismos separados por pontos.

B 255.255.255.0 está incorreto, pois os valores do endereço IPv4 não podem passar de 192.

C 2804:14c:122:86k6::1008 está incorreto, pois as letras possíveis em um endereço IPv6 vão de a até f.

D 2804:14c:122:86b6:6157:ba6e:cb64:37e2 está incorreto, pois um endereço IPv6 deve iniciar por 2019, que é o ano atual.

E fe80::9d9d:91c0:a266:c8b8%7 está incorreto, pois possui o sinal dois-pontos duplicado.

[Questão 02]

(FCC/SEFAZ-BA 2019) Solicitou-se a um Auditor analisar os endereços IP listados abaixo.

(...)

A 192.168.0.21 está incorreto, pois um endereço IPv4 ~~precisa ter sempre 3 algarismos separados por pontos~~.

B 255.255.255.0 está incorreto, pois os valores do ~~endereço IPv4 não podem passar de 192~~.

C 2804:14c:122:86k6::1008 está incorreto, pois as letras possíveis em um endereço IPv6 vão de a até f.

D 2804:14c:122:86b6:6157:ba6e:cb64:37e2 está incorreto, pois um ~~endereço IPv6 deve iniciar por 2019, que é o ano atual~~.

E fe80::9d9d:91c0:a266:c8b8%7 está incorreto, ~~pois possui o sinal dois pontos duplicado~~.

[Questão 03]

(FCC/SEFAZ-SC 2018) Um Administrador de um computador com interface de rede compatível com IPv6 deseja saber se a interface está em funcionamento. Para essa verificação ele deve utilizar o comando ping para o endereço:

A FC00::

B ::0

C FD00::

D ::1

E E00::

[Questão 03] – Comentários...

Loopback

IPV6

Endereço de Loopback é 0:0:0:0:0:0:0:1

IPV4

Endereços de Loopback (127.0.0.0/8)

[Questão 03]

(FCC/SEFAZ-SC 2018) Um Administrador de um computador com interface de rede compatível com IPv6 deseja saber se a interface está em funcionamento. Para essa verificação ele deve utilizar o comando ping para o endereço:

A FC00::

B ::0

C FD00::

D ::1

E E00::

[Questão 04]

(FCC/TRT-2 2018) Na internet o modelo de serviços diferenciados (DiffServ) tem sido aplicado para diferenciar e priorizar vários tipos de tráfego. Quando o fluxo entra na rede, no primeiro roteador, os pacotes são classificados de acordo com a prioridade sinalizada pela aplicação. A partir daí, cada roteador que recebe um pacote inspeciona seu cabeçalho IPv6 e obtém seu nível de prioridade no campo Class-of-Service (CoS) tomando ações para encaminhamento. A prioridade é definida principalmente pelos bits mais significativos do campo CoS, conhecidos como precedence bits. Se um roteador recebe um pacote cujo campo CoS possui o valor 10100000, ele reconhece corretamente que o IP Precedence é

A Routine. B Priority. C Critical.
D Immediate. E Flash.

[Questão 04] – Comentários...

8 bits reservados ao campo TOS, os primeiros 3 bits mais significativos (MSB - Most Significant Bit), são os bits utilizados para classificar ao pacote.

000- Routine

001- Priority

101 - Critical

010- Immediate

011 - Flash

<https://www.coffeeip.com/single-post/2017/08/31/Entendendo-QOS-em-3-posts---2-de-3>

[Questão 04]

(FCC/TRT-2 2018) Na internet o modelo de serviços diferenciados (DiffServ) tem sido aplicado para diferenciar e priorizar vários tipos de tráfego. Quando o fluxo entra na rede, no primeiro roteador, os pacotes são classificados de acordo com a prioridade sinalizada pela aplicação. A partir daí, cada roteador que recebe um pacote inspeciona seu cabeçalho IPv6 e obtém seu nível de prioridade no campo Class-of-Service (CoS) tomando ações para encaminhamento. A prioridade é definida principalmente pelos bits mais significativos do campo CoS, conhecidos como precedence bits. Se um roteador recebe um pacote cujo campo CoS possui o valor 10100000, ele reconhece corretamente que o IP Precedence é

A Routine. B Priority. C Critical.
D Immediate. E Flash.

[Questão 05]

(FCC/SABESP 2018) Um Técnico da SABESP entrou no site https://test-ipv6.com/index.html.pt_BR para verificar a adequação do navegador e da conexão ao IPv6 e obteve algumas informações como as listadas abaixo.

- Seu endereço IPv4 parece ser 189.100.255.119
- Seu endereço IPv6 parece ser ...I...
- Seu ..II.... parece ser CLARO S.A.
- Como você possui IPv6, estamos incluindo uma guia que mostra o quão bem você pode alcançar outros sites IPv6.

[Questão 05]

(FCC/SABESP 2018) (...)

Com base nestas informações, é correto afirmar que

A o endereço IPv4 é da classe C, que possui máscara 255.0.0.0

B a lacuna I pode ser preenchida com: 2804:14c:20:807b:89ac:e6e1:ac78:a99d, pois os 128 bits são divididos em grupos escritos com dígitos hexadecimais maiúsculos ou minúsculos e separados por:

C a lacuna I pode ser preenchida com: 2804::20:807b:89ac:e6e1::a99d, pois é permitido omitir os zeros à esquerda de cada bloco de 8 bits, além de substituir uma sequência longa de zeros por ::

D a lacuna II pode ser preenchida com: fornecedor de protocolos TCP/IP (ISP)

E o endereço IPv4 é da classe A. Os dois primeiros bytes identificam o host e os dois últimos identificam a rede: 255.119

[Questão 05]

(FCC/SABESP 2018) (...)

Com base nestas informações, é correto afirmar que

A ~~o endereço IPv4 é da classe C~~, que possui máscara 255.0.0.0

B a lacuna I pode ser preenchida com: 2804:14c:20:807b:89ac:e6e1:ac78:a99d, pois os 128 bits são divididos em grupos escritos com dígitos hexadecimais maiúsculos ou minúsculos e separados por:

C a lacuna I pode ser preenchida com: 2804::20:807b:89ac:e6e1::a99d, pois é permitido omitir os zeros à esquerda de cada bloco de 8 bits, além de substituir uma sequência longa de zeros por :: (só uma vez)

D a lacuna II pode ser preenchida com: ~~fornecedor de protocolos TCP/IP (ISP)~~

E ~~o endereço IPv4 é da classe A~~. Os dois primeiros bytes identificam o host e os dois últimos identificam a rede: 255.119

[Questão 06]

(FCC/SABESP 2018) Com a introdução e uso do IPv6, o DNS se tornou extremamente importante para facilitar o acesso aos recursos da internet. Dentre os tipos de registro DNS, o utilizado para vincular um domínio ou subdomínio a um endereço IPv6 é o

A AFSDB.

B AAAA.

C CNAME.

D A.

E SOA.

[Questão 06] – Comentários...

A (Address) – Contém o endereço IPv4 de um registro

AAAA (Quad-A) – Contém o endereço IPv6 de um registro

CNAME (Canonical Name) – É o segundo nome ou apelido (alias) de um registro de domínio

[Questão 06]

(FCC/SABESP 2018) Com a introdução e uso do IPv6, o DNS se tornou extremamente importante para facilitar o acesso aos recursos da internet. Dentre os tipos de registro DNS, o utilizado para vincular um domínio ou subdomínio a um endereço IPv6 é o

A AFSDB.

B AAAA.

C CNAME.

D A.

E SOA.

[Questão 07]

(FCC/DPE-AM 2018) Considere a representação do seguinte endereço IPv6:

1010:7AB:56::B

O endereço, em sua forma completa é:

A 1010:07AB:0056:0000:0000:0000:0000:000B

B 1010:07AB:0056:0000:0000:0000:0000:0000:B000

C 1010:07AB:0056:0000:0000:0000:000B

D 1010:07AB:0056:0000:0000:0000:0000:0000:000B

E 1010:7AB0:5600:0000:0000:0000:0000:B000

[Questão 07]

(FCC/DPE-AM 2018) Considere a representação do seguinte endereço IPv6:

1010:7AB:56::B

O endereço, em sua forma completa é:

A 1010:07AB:0056:0000:0000:0000:0000:000B

B 1010:07AB:0056:0000:0000:0000:0000:0000:B000

C 1010:07AB:0056:0000:0000:0000:000B

D 1010:07AB:0056:0000:0000:0000:0000:0000:000B

E 1010:7AB0:5600:0000:0000:0000:0000:B000

Dúvidas

Prof. Walter Cunha

falecomigo@waltercunha.com

<https://www.patreon.com/timasters>

<https://www.facebook.com/walter.cunha.7>

<https://www.instagram.com/walter.cunha.7/>

<https://twitter.com/timasters>

<https://www.linkedin.com/in/walter-cunha-19a90721>



PROVAS DE TI
TUDO PARA VOCÊ PASSAR