nic.br
Núcleo de Informação
e Coordenação do
Ponto BR

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Requisitos de suporte a IPv6 para equipamentos de TIC.

Índice

Nota da versão em português 2

Introdução 2

Informações gerais sobre como usar este documento 3

Como especificar requisitos 3

Texto genérico sugerido para a entidade que abrir a licitação 4

Listas de especificações técnicas RFC/3GPP obrigatórias e opcionais de suporte para diversos hardware e software 4

IPsec: obrigatório ou opcional 4

Definições e descrições de diferentes tipos de dispositivos 5

Listas de padrões RFC/3GPP exigidos para diferentes tipos de hardware 6

Requisitos para os equipamentos “host” 6

Requisitos para equipamentos de "switch de camada 2" para clientes 8

Requisitos para equipamentos de "switch de camada 2" para empresas/provedores de serviços de Internet 8

Requisitos para equipamentos de "roteador ou switch de camada 3" 9

Requisitos para "equipamentos de segurança de redes" 13

Requisitos para equipamentos CPE 16

Requisitos para dispositivos móveis 17

Requisitos para balanceadores de carga 19

Requisitos para suporte IPv6 em software 21

Habilidades necessárias ao integrador de sistemas 22

Declaração de qualificação em IPv6 22

Agradecimentos 23

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Nota da versão em português.

Este texto é a tradução do documento RIPE 554 - Requirements for IPv6 in ICT Equipment. A tradução foi realizada como parte dos esforços de disseminação do IPv6 pelo NIC.br, no escopo da iniciativa conhecida como IPv6.br. O objetivo é que sirva como um guia para órgãos do governo e empresas brasileiras, para que possam incluir em suas licitações e processos de compra os requisitos necessários para que os novos equipamentos relacionados às Tecnologias de Informação e Comunicação suportem o protocolo IPv6.

A equipe técnica do IPv6.br endossa as recomendações presentes neste documento.

O original, em inglês, elaborado por **Merike Käo, Jan Žorž, Sander Steffann,** com o apoio da comunidade técnica européia de operadores da Internet (RIPE), pode ser encontrado no seguinte endereço:

- http://www.ripe.net/ripe/docs/current-ripe-documents/ripe-554

Introdução

Para garantir a adoção sem incidentes e de baixo custo do IPv6 em todas as redes, é importante que os governos e as grandes empresas especifiquem requisitos de compatibilidade para o IPv6 ao abrir licitações para compra de equipamentos e serviços de suporte relacionados às "Tecnologias de Informação e Comunicação" (Information and Communication Technologies - ICT). O objetivo deste documento é apresentar as melhores práticas na área (Best Current Practice - BCP), sendo que o mesmo não especifica nenhum padrão ou política em si.

Ele pode servir de modelo para governos, empresas de grande porte e qualquer outra organização que necessite de apoio na implantação do IPv6, ou com equipamentos relacionados em suas licitações, e inclui diretrizes sobre o que deve ser exigido. Ele também pode auxiliar indivíduos ou organizações que queiram submeter propostas para licitações governamentais ou de grandes empresas.

É importante notar que os padrões aqui listados são provenientes de diversos órgãos, que operam independentemente da comunidade RIPE, e que todos esses padrões estão sujeitos a mudanças ou substituição por versões mais recentes. Poderá também ser necessário adequar as recomendações às suas necessidades locais específicas.

Algumas partes desta seção têm ressonância no perfil NIST/USGv6 desenvolvido pelo governo americano: [1]

http://www.antd.nist.gov/usgv6/

Os autores modificaram esses documentos para torná-los mais universais. Esta opção

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

inclui uma lista de padrões de especificações RFC que devem ser suportados, divididos em oito categorias de dispositivos.

Este documento também está em conformidade com o documento “Requisitos para nós IPv6” (IPv6 Node requirements, RFC 6463). Essa RFC contém as instruções gerais da IETF sobre que partes do IPv6 devem ser implementadas por dispositivos diferentes.

Informações gerais sobre como usar este documento

A certificação **IPv6 Ready Logo** pode ser solicitada para qualquer dispositivo. Essa é a maneira mais fácil de os fornecedores de equipamentos provarem que o mesmo está em conformidade com os requisitos básicos do IPv6. O órgão que abrir a licitação também deverá especificar as RFCs obrigatórias e opcionais, de modo a não excluir os fornecedores que ainda não certificaram os seus dispositivos com a certificação IPv6 Ready Logo. Deste modo, não se poderá acusar as licitações públicas de favorecer qualquer tipo de fornecedor de equipamentos.

Ao especificar a lista de RFCs exigidos, é preciso listar todos os requisitos obrigatórios, exceto os itens iniciados com: "Se for solicitado [função]...". Os últimos são obrigatórios somente se o órgão que abrir a licitação exigir determinada função. Note que a entidade que abrir a licitação deve determinar as funções obrigatórias, não o fornecedor do equipamento.

Certos recursos inclusos na seção "opcional" deste documento podem ser necessários no seu caso e/ou da sua organização em particular. Nesses casos a entidade que abrir a licitação deverá colocar o item na seção "obrigatório" no seu edital.

Como especificar requisitos

Conforme discutido acima, o programa de certificação IPv6 Ready Logo não engloba todos os equipamentos que têm suporte adequado para o IPv6; portanto, excluir tais equipamentos pode não ser desejável. Este documento recomenda que a entidade que abrir a licitação especifique que os equipamentos devem ser certificados no programa IPv6 Ready ou estar em conformidade com as RFCs listadas na seção abaixo.

Sobre o programa **IPv6 Ready Logo:** http://www.ipv6ready.org/

Note também que existe um projeto, chamado BOUNDv6, cujo objetivo é criar um ambiente de rede permanente com vários fornecedores, conectando laboratórios aprovados, de modo que a comunidade possa testar os aplicativos e dispositivos habilitados para IPv6 em cenários de teste significativos. Recomenda-se que as entidades que abrirem licitações chequem e usem os resultados deste projeto.

Sobre o **BOUNDv6:** http://www.boundv6.org/

Observação importante para a entidade que abrir a licitação: A certificação IPv6 Ready Logo cobre os requisitos básicos do IPv6 e alguns recursos avançados, mas não todos. Se

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

houver necessidade de algum recurso não incluso na certificação IPv6 Ready Logo, solicite uma lista de RFCs que inclua essas necessidades específicas, além da Certificação IPv6 Ready Logo. **As RFCs nas listas abaixo que estão inclusas na certificação IPv6 Ready Logo foram indicados com um *** .

Texto genérico sugerido para a entidade que abrir a licitação

O texto a seguir deverá ser incluso em todos os editais:

Todo hardware relacionado às TIC (ICT), pertinente a esta licitação, deverá suportar os protocolos IPv4 e IPv6. O desempenho deverá ser semelhante para ambos os protocolos em termos de entrada, saída e rendimento do fluxo de dados, transmissão e processamento de pacotes.

O suporte ao protocolo IPv6 poderá ser evidenciado e comprovado através da certificação IPv6 Ready Logo.

Qualquer software que se comunique através do protocolo IP deverá suportar ambas as versões (IPv4 e IPv6). A diferença deverá ser imperceptível para os usuários.

Os equipamentos que não tiverem sido submetidos aos procedimentos de teste do programa IPv6 Ready, deverão estar em conformidade com as RFCs listadas abaixo:

[lista incluindo as RFCs obrigatórias e opcionais selecionadas das listas abaixo]

Listas de especificações técnicas RFC/3GPP obrigatórias e opcionais de suporte para diversos hardware e software

Os requisitos estão divididos em equipamentos de hardware e suporte a integradores.

Deve-se assumir que todo o tráfego IPv4 será migrado para IPv6. Todos os requisitos relativos às características do tráfego IPv4, como latência, largura de banda e rendimento deverão ser obrigatórios para o tráfego IPv6.

IPsec: obrigatório ou opcional

No padrão de “Requisitos para nós IPv6” (IPv6 Node requirements, RFC4294) original, a implementação do IPsec estava listada como 'OBRIGATÓRIA' para conformidade com os padrões. A versão atualizada da RFC (RFC6434) mudou a classificação do IPsec para 'DEVERIA' ser implementado. A justificativa para a mudança consta na nova RFC.

O "Grupo de Trabalho IPv6 RIPE" (RIPE IPv6 Working Group) discutiu se o suporte ao IPsec deveria ser obrigatório ou opcional. Os seus membros mais comunicativos apoiaram a mudança do IPsec para as seções opcionais, o que se refletiu neste documento.

Embora o consenso entre a comunidade tenha sido de que o IPsec deve ser opcional na

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

maioria dos casos, a IETF declarou que o IPsec 'DEVERIA' ser implementado na última versão do padrão de “Requisitos para nós IPv6” (IPv6 Node requirements, RFC6434). No contexto da IETF, DEVERIA significa que pode haver motivos válidos em certos casos que justificam ignorar determinado item, mas todas as consequências devem ser compreendidas e cuidadosamente avaliadas antes de se determinar uma alternativa.

Organizações que usam o IPsec, ou pretendem usá-lo no futuro, devem incluir a seguinte seção obrigatória no edital de abertura da licitação:

• IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *

Definições e descrições de diferentes tipos de dispositivos

As definições a seguir serão usadas para classificar diversos equipamentos de hardware. Apesar de alguns dos hardwares desempenharem funções coincidentes (p.ex. um switch de camada 2 pode atuar como roteador de camada 3, ou um roteador pode exercer algumas funções de firewall), assume-se que para quaisquer funções coincidentes, os requisitos para cada dispositivo específico sejam inclusos.

Host: Host é um participante da rede que envia e recebe pacotes, mas não os encaminha em nome de outros.

Switch, ou ‘Switch de camada 2’: Um switch ou ‘switch de camada 2’ é um dispositivo usado primordialmente para o encaminhamento de quadros Ethernet com base nos seus atributos. No geral, trocar informações Ethernet com outros switches Ethernet faz parte da sua função.

Roteador ou 'Switch de camada 3': Um roteador ou ‘switch de camada 3’ é um dispositivo usado primordialmente para o encaminhamento de pacotes IP com base nos seus atributos. No geral, trocar informações de roteamento com outros Roteadores faz parte da sua função.

Equipamentos de Segurança de Rede: Os equipamentos de segurança de rede são dispositivos cuja função primordial é permitir, negar e/ou monitorar o tráfego entre interfaces, de modo a detectar ou prevenir possíveis atividades maliciosas. As referidas interfaces também podem incluir VPNs (SSL ou IPsec). Um Equipamento de Segurança de Rede comumente também é um switch de camada 2 ou Roteador/switch de camada 3.

Equipamento das Instalações do Cliente (Customer Premise Equipment - CPE): Um dispositivo CPE consiste em um roteador residencial ou de um pequeno escritório usado para conectar usuários domiciliares e/ou escritórios pequenos a milhares de configurações. Embora um CPE seja geralmente um roteador, os requisitos são diferentes para um switch roteador de camada 3 de uma Empresa/Provedor de Serviços de Internet.

Dispositivo Móvel: No contexto deste documento, um dispositivo móvel é um nó que conecta a um sistema 3GPP definido usando algumas tecnologias específicas de acesso 3GPP (como 2G, 3G ou LTE). Em casos em que a lógica da rede estiver sendo fornecida

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

somente por um dispositivo dedicado A conectado a outro dispositivo B, a especificação será aplicável ao dispositivo A e não ao dispositivo B. Se a lógica do protocolo for distribuída (p.ex. computador com interface Ethernet externa que faz TCP checksum offloading), refere-se ao sistema como um todo.

Balanceador de Carga: Um balanceador de carga é um dispositivo de rede que distribui a carga de trabalho entre vários computadores, servidores e outros recursos para maximizar ou atingir o plano de uso de recursos, maximizar o rendimento, minimizar o tempo de resposta e evitar sobrecarga.

As referências a seguir são relevantes para este documento BCP. À data da publicação, as edições indicadas estavam em vigor. Todas as referências estão sujeitas a revisão. Recomenda-se, portanto, que os usuários deste documento BCP analisem a possibilidade de usar a edição mais atualizada das referências citadas abaixo.

Listas de padrões RFC/3GPP exigidos para diferentes tipos de hardware

Os equipamentos de hardware de TIC (ICT) são divididos em sete grupos funcionais:

- Host: cliente ou servidor
- Switch de camada 2
- Roteador ou Switch de camada 3
- Equipamentos de segurança de rede (firewalls, IDS, IPS...)
- CPE
- Dispositivo móvel
- Balanceador de carga

Os seguintes requisitos estão divididos em duas categorias: "obrigatórios" e "opcionais". O equipamento deve estar em conformidade com a lista de padrões exigidos. Ser capaz de suportar requisitos opcionais poderá render pontos adicionais ao licitante, se assim especificado pela organização responsável pela abertura da licitação.

Todo o hardware que não esteja em conformidade com todos os padrões obrigatórios deverá ser classificado como inadequado pelo avaliador.

Os padrões inclusos nos procedimentos de teste do IPv6 Ready Logo, geralmente realizados por laboratórios credenciados, estão indicados com um asterisco (*).

Requisitos para os equipamentos "host"

Suporte obrigatório:

- "Especificação Básica de IPv6" (IPv6 Basic specification, RFC2460) *

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

- "Arquitetura de Endereçamento IPv6" (IPv6 Addressing Architecture, RFC4291) *
- "Seleção de Endereço Padrão" (Default Address Selection, RFC3484)
- "Endereços Unicast IPv6 Únicos" (Unique Local IPv6 Unicast Addresses (ULA), RFC4193)
- ICMPv6 [RFC4443] *
- "Cliente DHCPv6" (DHCPv6 client, RFC3315) *
- SLAAC [RFC4862] *
- "Descoberta de Caminho MTU" (Path MTU Discovery, RFC1981) *
- "Descoberta de Vizinho" (Neighbor Discovery, RFC4861) *
- Se for necessário suporte para tunelamento e pilha dupla, o dispositivo deverá oferecer suporte para Mecanismos de Transição Básicos para Hosts e Roteadores IPv6 (Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC4213)
- Se for necessário suporte para IPv6 móvel, o dispositivo deverá ter suporte para “MIPv6” [RFC6275, RFC5555] e “Operação de IPv6 Móvel com IKEv2 e Arquitetura IPsec Revisada" (“Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture,” RFC4877)
- "Extensões de protocolo DNS para incorporação dos registros de recursos IPv6 DNS" (DNS protocol extensions for incorporating IPv6 DNS resource records, RFC3596)
- "Mecanismos de ampliação de mensagem DNS" (DNS message extension mechanism, RFC2671)
- "Requisitos de tamanho de mensagens DNS" (DNS message size requirements, RFC3226)
- "Deprecação de Cabeçalhos de Roteamento 0 em IPv6" (Deprecation of Type 0 Routing Headers in IPv6, RFC5095) *

Suporte opcional:

- "Opções de Anúncios para Roteadores IPv6 com Configuração DNS" (IPv6 Router Advertisement Options for DNS Configuration, RFC6106)
- "ICMP ampliado para mensagens com diversas partes" (Extended ICMP for multi-part messages, RFC4884)
- SeND [RFC3971]
- "Extensões de Privacidade SLAAC" (SLAAC Privacy Extensions, RFC4941)

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

- Stateless DHCPv6 [RFC3736] *
- "(Classe de tráfego) DS" (DS (Traffic class), RFC2474, RFC3140)
- "Endereços Gerados Criptograficamente" (Cryptographically Generated Addresses, RFC3972)
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- "Protocolo SNMP" (SNMP protocol, RFC3411)
- "Funções SNMP" (SNMP capabilities, RFC3412, RFC3413, RFC3414)
- "MIBs SNMP para IP" (SNMP MIBs for IP, RFC4293) "Encaminhamento" (Forwarding, RFC4292) e DiffServ [RFC3289]
- "Descoberta de Ouvinte Multicast versão 2" (Multicast Listener Discovery version 2, RFC3810) *
- "Detecção de MTU da camada de Empacotamento" (Packetisation Layer Path MTU Discovery, RFC4821)
- "Compartilhamento de Carga do Host ao Roteador IPv6" (IPv6 Host-to-Router Load Sharing, RFC4311)
- "Preferências de Roteador Padrão e Rotas Mais Específicas" (Default Router Preferences and More-Specific Routes, RFC4191)

Requisitos para equipamentos de "switch de camada 2" para clientes

Suporte opcional (gerenciamento)

- MLDv2 snooping [RFC4541]
- "Especificação Básica de IPv6" (IPv6 Basic specification, RFC2460) *
- "Arquitetura de Endereçamento IPv6" (IPv6 Addressing Architecture, RFC4291) *
- "Seleção de Endereço Padrão" (Default Address Selection, RFC3484)
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- "Protocolo SNMP" (SNMP protocol, RFC3411)
- "Funções SNMP" (SNMP capabilities, RFC3412, RFC3413, RFC3414)
- "MIBs SNMP para IP" (SNMP MIBs for IP, RFC4293) "Encaminhamento" (Forwarding, RFC4292) e DiffServ [RFC3289]

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Requisitos para equipamentos de "switch de camada 2" para empresas/provedores de serviços de Internet

Suporte obrigatório:

- MLDv2 snooping [RFC4541]
- "Filtragem DHCPv6" (DHCPv6 filtering, RFC3315) *
- "Filtragem de Anúncio de Roteador (RA)" (Router Advertisement (RA) filtering, RFC4862)
- Inspeção dinâmica de "solicitação/anúncio de Vizinho IPv6" (Dynamic "IPv6 Neighbor solicitation/advertisement" inspection, RFC4861)
- "Filtragem de Detecção de Inacessibilidade de Vizinho" (Neighbor Unreachability Detection [NUD, RFC4861] filtering)
- "Investigação e filtragem de Detecção de Endereço Repetido" (Duplicate Address Detection [DAD, RFC4429] snooping and filtering). [2]

Suporte opcional (gerenciamento):

- "Especificação Básica de IPv6" (IPv6 Basic specification, RFC2460) *
- "Arquitetura de Endereçamento IPv6" (IPv6 Addressing Architecture, RFC4291) *
- "Seleção de Endereço Padrão" (Default Address Selection, RFC3484)
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- "Protocolo SNMP" (SNMP protocol, RFC3411)
- "Funções SNMP" (SNMP capabilities, RFC3412, RFC3413, RFC3414)
- "MIBs SNMP para IP" (SNMP MIBs for IP, RFC4293) "Encaminhamento" (Forwarding, RFC4292) e DiffServ [RFC3289]
- "Filtragem de cabeçalho de Roteamento IPv6 [RFC2460, Valor do próximo Cabeçalho 43]" (IPv6 Routing Header [RFC2460, Next Header value 43] filtering) *
- "Deprecação de Cabeçalhos de Roteamento 0 em IPv6" (Deprecation of Type 0 Routing Headers in IPv6, RFC5095) *
- "Filtragem UPnP" (UPnP filtering)

Requisitos para equipamentos de "roteador ou switch de camada 3"

Suporte obrigatório:

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

- "Especificação Básica de IPv6" (IPv6 Basic specification, RFC2460) *
- "Arquitetura de Endereçamento IPv6" (IPv6 Addressing Architecture, RFC4291) *
- "Seleção de Endereço Padrão" (Default Address Selection, RFC3484)
- "Endereços Unicast IPv6 Únicos" (Unique Local IPv6 Unicast Addresses (ULA), RFC4193)
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- MLDv2 snooping [RFC4541]
- "Descoberta de Ouvinte Multicast versão 2" (Multicast Listener Discovery version 2, RFC3810) *
- "Opção de Alerta de Roteador" (Router-Alert option, RFC2711)
- "Descoberta de Caminho MTU" (Path MTU Discovery, RFC1981) *
- "Descoberta de Vizinho" (Neighbor Discovery, RFC4861) *
- "Deprecação de Cabeçalhos de Roteamento 0 em IPv6" (Deprecation of Type 0 Routing Headers in IPv6, RFC5095) *
- Se for solicitado um protocolo de roteamento interno (IGP) dinâmico, então será necessário suporte para RIPng [RFC2080], OSPF-v3 [RFC5340] ou IS-IS [RFC5308]. A autoridade contratante deverá especificar o protocolo exigido.
- Se for solicitado OSPF-v3, o equipamento deverá estar em conformidade com o requisito de "Autenticação/Confidencialidade para OSPF-v3" ("Authentication/Confidentiality for OSPF-v3," RFC4552)
- Se for solicitado o protocolo BGP4, o equipamento deverá estar em conformidade com os requisitos RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 e RFC2545
- Suporte para QoS [RFC2474, RFC3140]
- Se for necessário suporte para tunelamento e pilha dupla, o dispositivo deverá oferecer suporte para Mecanismos de Transição Básicos para Hosts e Roteadores IPv6 (Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC4213)
- Se for necessário suporte para tunelamento e pilha dupla, o dispositivo deverá oferecer suporte para "IPv6 e Tunelamento Genérico de Pacotes" (Generic Packet Tunneling and IPv6, RFC2473)
- Se for solicitado 6PE, o equipamento deverá oferecer suporte para "Conexão de

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Ilhas IPv6 sobre IPv4 MPLS Usando Roteadores de Borda de Provedor IPv6 (6PE)" ("Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)," RFC4798)

- Se for solicitado suporte para IPv6 móvel, o dispositivo deverá ter suporte para MIPv6 [RFC6275, RFC5555] e "Operação de IPv6 Móvel com IKEv2 e Arquitetura IPsec Revisada" ("Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture," RFC4877)
- Se for solicitado o protocolo de roteamento IS-IS, o equipamento deverá ter suporte para "M-ISIS: Roteamento em Diversas Topologias em Sistema Intermediário a Sistema Intermediário (IS-IS)" ("M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120])
- Se for solicitada a função MPLS (p.ex. roteador central sem BGP, MPLS TE, MPLS FRR), os roteadores PE e os refletores de rota deverão oferecer suporte para "Conexão de Ilhas IPv6 sobre IPv4 MPLS Usando Roteadores de Borda de Provedor IPv6 (6PE)" ("Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)," RFC4798)
- Se for necessária uma função VPN de camada 3, os roteadores PE e os refletores de rota deverão suportar "Extensão BGP-MPLS IP para Rede Privada Virtual (VPN) para IPv6 VPN" ("BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN," RFC4659)
- Se for utilizada Engenharia de Tráfego MPLS com o protocolo de roteamento IS-IS, o equipamento deverá oferecer suporte para "M-ISIS: Roteamento em Diversas Topologias em Sistema Intermediário a Sistema Intermediário (IS-IS)" ("M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120])

Suporte opcional:

- "Opções de Anúncios para Roteadores IPv6 com Configuração DNS" (IPv6 Router Advertisement Options for DNS Configuration, RFC6106)
- "Cliente/servidor/repetidor DHCPv6" (DHCPv6 client/server/relay, RFC3315) *
- "ICMP ampliado para mensagens com diversas partes" (Extended ICMP for multi-part messages, RFC4884)
- SeND [RFC3971]
- "Extensões de Privacidade SLAAC" (SLAAC Privacy Extensions, RFC4941)
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

- "Atualização de Rota para Funções BGP-4" (Route Refresh for BGP-4 Capabilities, RFC2918)
- "Atributo de Comunidades Estendidas de BGP" (BGP Extended Communities Attribute, RFC4360)
- "(QOS) Encaminhamento Assegurado" ((QOS) Assured Forwarding, RFC2597)
- "(QOS) Encaminhamento Acelerado" ((QOS) Expedited Forwarding, RFC2597)
- "Encapsulamento de Roteamento Genérico" (Generic Routing Encapsulation, RFC2784)
- "Endereços Gerados Criptograficamente" (Cryptographically Generated Addresses, RFC3972)
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- "Uso de IPsec para Garantir túneis de IPv6-em-IPv4" (Using IPsec to Secure IPv6-in-IPv4 tunnels, RFC4891)
- "Protocolo SNMP" (SNMP protocol, RFC3411)
- "Funções SNMP" (SNMP capabilities, RFC3412, RFC3413, RFC3414)
- "MIBs SNMP para IP" (SNMP MIBs for IP, RFC4293) "Encaminhamento" (Forwarding, RFC4292) e DiffServ [RFC3289]
- "Extensões de protocolo DNS para incorporação dos registros de recursos IPv6 DNS" (DNS protocol extensions for incorporating IPv6 DNS resource records, RFC3596)
- "Mecanismos de ampliação de mensagem DNS" (DNS message extension mechanism, RFC2671)
- "Requisitos de tamanho de mensagens DNS" (DNS message size Requirements, RFC3226)
- "Prefixos de IPv6 de 127 bits em Enlaces Entre Roteadores" (127-bit IPv6 Prefixes on Inter-Router Links, RFC6164)
- "Detecção de MTU da camada de Empacotamento" (Packetisation Layer Path MTU Discovery, RFC4821)
- "Compartilhamento de Carga Host ao Roteador IPv6" (IPv6 Host-to-Router Load Sharing, RFC4311)
- "Preferências de Roteador Padrão e Rotas Mais Específicas" (Default Router Preferences and More-Specific Routes, RFC4191)

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

Requisitos para "equipamentos de segurança de redes"

Os equipamentos nesta seção estão divididos em três subgrupos:

- Firewall (FW)
- "Dispositivo de prevenção de intrusão" (Intrusion prevention device, IPS)
- "Firewall de Aplicativo" (Application firewall, APFW)

Para cada padrão obrigatório os subgrupos aplicáveis foram indicados entre parênteses no final da linha.

Suporte obrigatório:

- "Especificação Básica de IPv6" (IPv6 Basic specification, RFC2460) (FW, IPS, APFW) *
- "Arquitetura de Endereçamento IPv6" (IPv6 Addressing Architecture, RFC4291) (FW, IPS, APFW)
- "Seleção de Endereço Padrão" (Default Address Selection, RFC3484) (FW, IPS, APFW)
- ICMPv6 [RFC4443] (FW, IPS, APFW) *
- SLAAC [RFC4862] (FW, IPS) *
- "Deprecação de Cabeçalhos de Roteamento 0 em IPv6" (Deprecation of Type 0 Routing Headers in IPv6, RFC5095) *
- "Inspeção de tráfego protocolo-41 de IPv6-em-IPv4" (Inspecting IPv6-in-IPv4 protocol-41 traffic), especificado em: "Mecanismos Básicos de Transmissão para Hosts e Roteadores IPv6" (Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC4213) (IPS)
- "Opção de Alerta de Roteador" (Router-Alert option, RFC2711) (FW, IPS)
- "Descoberta de Caminho MTU" (Path MTU Discovery, RFC1981) (FW, IPS, APFW) *
- "Descoberta de Vizinho" (Neighbor Discovery, RFC4443) (FW, IPS, APFW) *
- Se for solicitado o protocolo BGP4, o equipamento deverá estar em conformidade com os requisitos RFC4271, RFC1772, RFC4760 e RFC2545 (FW, IPS, APFW)
- Se for solicitado um protocolo de roteamento interno (IGP) dinâmico, então será necessário suporte para RIPng [RFC2080], OSPF-v3 [RFC5340] ou IS-IS [RFC5308]. A autoridade contratante deverá especificar o protocolo exigido. (FW, IPS, APFW)

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

- Se for solicitado OSPF-v3, o dispositivo deverá ter suporte para "Autenticação/Confidencialidade para OSPF-v3" ("Authentication/Confidentiality for OSPF-v3," RFC4552) (FW, IPS, APFW)
- Suporte para QoS [RFC2474, RFC3140] (FW, APFW)
- Se for necessário tunelamento, o dispositivo deverá oferecer suporte para "Mecanismos de Transição Básicos para Hosts e Roteadores IPv6" (Basic Transition Mechanisms for IPv6 Hosts and Routers, RFC4213) (FW)

No geral, um Dispositivo de Segurança de Rede é colocado no lugar de um switch de camada 2 ou de um roteador/switch de camada 3. Dependendo dessa colocação, os requisitos pertinentes deverão ser incluídos.

Funções e recursos suportados no IPv4 deverão ser comparáveis às funções e recursos suportados no IPv6. Por exemplo, se um sistema de prevenção de intrusão é capaz de operar no modo camada 2 e camada 3 no protocolo IPv4, então esta função deve também estar disponível para o protocolo IPv6. Alternativamente, se um firewall está operando em um aglomerado capaz de sincronizar sessões de IPv4 entre todos os membros do aglomerado, então isso deve ser possível também para as sessões de IPv6.

Suporte opcional:

- "Opções de Anúncios para Roteadores IPv6 com Configuração DNS" (IPv6 Router Advertisement Options for DNS Configuration, RFC6106)
- "Cliente/servidor/relé DHCPv6" (DHCPv6 client/server/relay, RFC3315) *
- "ICMP ampliado para mensagens com diversas partes" (Extended ICMP for Multipart Messages, RFC4884)
- SeND [RFC3971]
- "Extensões de Privacidade SLAAC" (SLAAC Privacy Extensions, RFC4941)
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- "Atributo de Comunidades de BGP" (Communities Attribute, RFC1997)
- "Funções de Anúncio WITH-4 de BGP" (BGP Capabilities Advertisement WITH-4, RFC3392)
- "(QOS) Encaminhamento Assegurado" ((QOS) Assured Forwarding, RFC2597)
- "(QOS) Encaminhamento Acelerado" ((QOS) Expedited Forwarding, RFC2597)
- "Endereços Unicast IPv6 Únicos" (Unique Local IPv6 Unicast Addresses (ULA), RFC4193)

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

- "Endereços Gerados Criptograficamente" (Cryptographically Generated Addresses, RFC3972)
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- "Uso de IPsec para Garantir túneis de IPv6-em-IPv4" (Using IPsec to Secure IPv6-in-IPv4 Tunnels, RFC4891)
- OSPF-v3 [RFC5340]
- "Autenticação/Confidencialidade para OSPF-v3" ("Authentication/Confidentiality for OSPF-v3," RFC4552)
- "Tunelamento e IPv6 de Pacote Genérico" (Generic Packet Tunneling and IPv6, RFC2473)
- "Protocolo SNMP" (SNMP protocol, RFC3411)
- "Funções SNMP" (SNMP capabilities, RFC3412, RFC3413, RFC3414)
- "MIBs SNMP para IP" (SNMP MIBs for IP, RFC4293) "Encaminhamento" (Forwarding, RFC4292) e DiffServ [RFC3289]
- "Extensões DNS para suportar o IPv6" (DNS extensions to support IPv6, RFC3596)
- "Mecanismos de ampliação de mensagem DNS" (DNS message extension mechanism, RFC2671)
- "Requisitos de tamanho de mensagens DNS" (DNS message size requirements, RFC3226)
- "Uso de IPsec para Garantir túneis de IPv6-em-IPv4" (Using IPsec to Secure IPv6-in-IPv4 Tunnels, RFC4891)
- "Descoberta de Ouvinte Multicast versão 2" (Multicast Listener Discovery version 2, RFC3810) *
- "Investigação MLDv2" (MLDv2 snooping, RFC4541) (quando em modo camada 2 ou de passagem) *
- "Detecção de MTU da camada de Empacotamento" (Packetisation Layer Path MTU Discovery, RFC4821)
- "Configuração IPv6 em Protocolo de Troca de Chave da Internet Versão 2 (IKEv2)" (IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2), RFC5739)
- "Compartilhamento de Carga Host ao Roteador IPv6" (IPv6 Host-to-Router Load Sharing, RFC4311)

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

- "Preferências de Roteador Padrão e Rotas Mais Específicas" (Default Router Preferences and More-Specific Routes, RFC4191)

Requisitos para equipamentos CPE

Suporte obrigatório:

- RFC6204 "Requisitos Básicos para Roteadores IPv6 de Borda para Clientes" (Basic Requirements for IPv6 Customer Edge Routers) *

Suporte opcional:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Se for necessário suporte para IPv6 móvel, o dispositivo precisa ter suporte para "MIPv6" [RFC6275, RFC5555] e "Operação de IPv6 Móvel com IKEv2 e Arquitetura IPsec Revisada" ("Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture," RFC4877)
- "ICMP ampliado para mensagens com diversas partes" (Extended ICMP for multi-part messages, RFC4884)
- SeND [RFC3971]
- "Extensões de Privacidade SLAAC" (SLAAC Privacy Extensions, RFC4941)
- "(classe de tráfego) DS" (DS (Traffic class), RFC2474, RFC3140)
- "Endereços Gerados Criptograficamente" (Cryptographically Generated Addresses, RFC3972)
- "Protocolo SNMP" (SNMP protocol, RFC3411)
- "Funções SNMP" (SNMP capabilities, RFC3412, RFC3413, RFC3414)
- "MIBs SNMP para IP" (SNMP MIBs for IP, RFC4293) "Encaminhamento" (Forwarding, RFC4292) e DiffServ [RFC3289]
- "Descoberta de Ouvinte Multicast versão 2" (Multicast Listener Discovery version 2, RFC3810) *
- "Detecção de MTU da camada de Empacotamento" (Packetisation Layer Path MTU Discovery, RFC4821)
- "IPv6 de Instalação Rápida em Infraestruturas IPv4 (6rd)" (IPv6 Rapid Deployment on IPv4 Infrastructures (6rd), RFC5969)
- Instalações de Banda Larga Lite em Duas Pilhas após Exaustão do IPv4 (Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, RFC6333). Se

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

houver suporte para o último, deverá haver suporte para o "Protocolo de Configuração de Host Dinâmico para IPv6 (DHCPv6) com Opção para Lite em Duas Pilhas" (Dynamic Host Configuration protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite, RFC6334)

- "A Abordagem A+P à Falta de endereços IPv4" (The A+P Approach to the IPv4 Address Shortage, RFC6346)
- "Configuração IPv6 em Protocolo de Troca de Chave da Internet Versão 2 (IKEv2)" (IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2), RFC5739)
- "Compartilhamento de Carga Host ao Roteador IPv6" (IPv6 Host-to-Router Load Sharing, RFC4311)
- "Preferências de Roteador Padrão e Rotas Mais Específicas" (Default Router Preferences and More-Specific Routes, RFC4191)

Requisitos para dispositivos móveis

Suporte obrigatório:

- "Especificação Básica de IPv6" (IPv6 Basic specification, RFC2460) *
- "Descoberta de Vizinho para IPv6" (Neighbor Discovery for IPv6, RFC4861) *
- “Autoconfiguração de Endereço IPv6 Stateless” (IPv6 Stateless Address Autoconfiguration, RFC4862) *
- "Arquitetura de Endereçamento IPv6" (IPv6 Addressing Architecture, RFC4291) *
- ICMPv6 [RFC4443] *
- "IPv6 sobre PPP" (IPv6 over PPP, RFC2472)
- "Descoberta de Ouvinte Multicast versão 2" (Multicast Listener Discovery version 2, RFC3810) *
- "Opção de Alerta de Roteador IPv6" (IPv6 Router Alert option, RFC2711)
- "Extensões de protocolo DNS para incorporação dos registros de recursos IPv6 DNS" (DNS protocol extensions for incorporating IPv6 DNS resource records, RFC3596)

Suporte opcional:

- "Extensões de Privacidade para Autoconfiguração de Endereços Stateless em IPv6" (Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC4941)

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

- "Descoberta de Caminho MTU para IPv6" (Path MTU Discovery for IPv6, RFC1981) *
- "Tunelamento de Pacote Genérico para IPv6" (Generic Packet Tunneling for IPv6, RFC2473)
- DHCPv6 [RFC3315] *
- Stateless DHCPv6 [RFC3736]
- "Opção DHCP para servidores SIP" (DHCPv6 option for SIP servers, RFC3319)
- "Opções de Prefixos IPv6 para DHCPv6" (IPv6 Prefix Options for DHCPv6, RFC3633)
- "Opção de Exclusão de Prefixo para Delegação de Prefixos com base no DHCPv6" (Prefix Exclude Option for DHCPv6-based Prefix Delegation) [draft-ietf-dhc-pd-exclude]
- "Seleção de Endereço Padrão" (Default Address Selection, RFC3484)
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- “Protocolo MOBIKE de Mobilidade e Multihoming IKEv2” (IKEv2 Mobility and Multihoming Protocol MOBIKE, RFC 4555)
- "Compartilhamento de Carga Host ao Roteador IPv6" (IPv6 Host-to-Router Load Sharing, RFC4311)
- "Preferências de Roteador Padrão e Rotas Mais Específicas" (Default Router Preferences and More-Specific Routes, RFC4191)

Referências:

- 3GPP
- "Conexão em rede Entre Rede Móvel Terrestre Pública (PLMN), com suporte para serviços à base de pacotes, e Redes de Pacotes de Dados (PDN)" (Internetworking Between Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)) [3GPP TS 29.061]
- "Descrição de Serviço GPRS" (GPRS Service Description) [3GPP TS 23.060]
- "Melhorias no Serviço de Rádio de Pacote Geral (GPRS) para Acesso a Rede de Acesso de Rádio Universal Terrestre Evoluído (E-UTRAN)" (General Packet Radio Service, (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access) [3GPP TS 23.401]
- "Fluxos de Sinalização para IP de controle de Ligações multimídia com base no SIP e SDP" (Signaling flows for IP multimedia Call control based on SIP and SDP)

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

[3GPP TS 24.228]

- "Protocolo IP de controle de ligação multimídia com base no SIP e SDP" (IP multimedia call control protocol based on SIP and SDP) [3GPP TS 24.229]
- "Estrutura Multimídia com Base em protocolo IP" (IP Based Multimedia Framework) [3GPP TS 22.941]
- "Requisitos Arquitetônicos" (Architectural Requirements) [3GPP TS 23.221]
- "Domínio de pacotes; Estações Móveis (MS) com Suporte para Serviço de Troca de Pacotes" (Packet domain; Mobile Stations (MS) Supporting Packet Switching Service) [3GPP TS 27.060]
- "Diretrizes de migração para o IPv6" (IPv6 migration guidelines) [3GPP TR 23.975]
- IETF
- "IPv6 para Alguns Hospedeiros de Celulares de Segunda e Terceira Geração" (IPv6 for Some Second and Third Generation Cellular Hosts, RFC3316)
- "Recomendações para IPv6 em Padrões 3GPP" (Recommendations for IPv6 in 3GPP Standards, RFC3314)
- "IPv6 em Projeto de Parceria de 3a Geração (3GPP)" (IPv6 in 3rd Generation Partnership Project (3GPP), RFC6459)

Requisitos para balanceadores de carga

Um balanceador de carga distribui as solicitações que entram e/ou as conexões de clientes para diversos servidores. Os balanceadores de carga devem ter suporte para diversas combinações de IPv4 e IPv6:

- É obrigatório ter suporte para balanceamento de carga de clientes IPv6 para servidores IPv6 (6 para 6)
- É obrigatório ter suporte para balanceamento de carga de clientes IPv6 para servidores IPv4 (6 para 4)
- É recomendado ter suporte para balanceamento de carga de clientes IPv4 para servidores IPv4 (4 para 4)
- É recomendado ter suporte para balanceamento de carga de clientes IPv4 para servidores IPv6 (4 para 6)
- É recomendado ter suporte para balanceamento de carga de um único endereço IPv4 externo/virtual para um conjunto misto de servidores IPv4 e IPv6.
- É recomendado ter suporte para balanceamento de carga de um único endereço

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

IPv6 externo/virtual para um conjunto misto de servidores IPv4 e IPv6.

Se um balanceador de carga tiver suporte para balanceamento de carga de camada 7 (nível de aplicativos / proxy reversa, definido como 'substituto' na seção 2.2 da RFC3040), então é obrigatório ter suporte para o cabeçalho X-forwarded-for (ou equivalente) em HTTP para tornar o endereço IP fonte do cliente visível para os servidores.

Suporte obrigatório:

- "Especificação Básica de IPv6" (IPv6 Basic specification, RFC2460) *
- "Arquitetura de Endereçamento IPv6" (IPv6 Addressing Architecture, RFC4291) *
- "Seleção de Endereço Padrão" (Default Address Selection, RFC3484)
- "Endereços Unicast IPv6 Únicos" (Unique Local IPv6 Unicast Addresses (ULA), RFC4193)
- ICMPv6 [RFC4443] *
- "Descoberta de Caminho MTU" (Path MTU Discovery, RFC1981) *
- "Descoberta de Vizinho" (Neighbor Discovery, RFC4861) *
- "Extensões de protocolo DNS para incorporação dos registros de recursos IPv6 DNS" (DNS protocol extensions for incorporating IPv6 DNS resource records, RFC3596)
- "Mecanismos de ampliação de mensagem DNS" (DNS message extension mechanism, RFC2671)
- "Requisitos de tamanho de mensagens DNS" (DNS message size requirements, RFC3226)
- "Deprecação de Cabeçalhos de Roteamento 0 em IPv6" (Deprecation of Type 0 Routing Headers in IPv6, RFC5095) *

Suporte opcional:

- "Opções de Anúncios para Roteadores IPv6 com Configuração DNS" (IPv6 Router Advertisement Options for DNS Configuration, RFC6106)
- "ICMP ampliado para mensagens com diversas partes" (Extended ICMP for multi-part messages, RFC4884)
- SeND [RFC3971]
- "(classe de tráfego) DS" (DS (Traffic class), RFC2474, RFC3140)
- "Endereços Gerados Criptograficamente" (Cryptographically Generated Addresses,

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

RFC3972)

- "Protocolo SNMP" (SNMP protocol, RFC3411)
- "Funções SNMP" (SNMP capabilities, RFC3412, RFC3413, RFC3414)
- "MIBs SNMP para IP" (SNMP MIBs for IP, RFC4293) "Encaminhamento" (Forwarding, RFC4292) e DiffServ [RFC3289]
- "Descoberta de Ouvinte Multicast versão 2" (Multicast Listener Discovery version 2, RFC3810) *
- "Detecção de MTU da camada de Empacotamento" (Packetisation Layer Path MTU Discovery, RFC4821)
- NAT64/DNS64 [RFC6146, RFC6147]
- Se for necessário suporte para IPsec, o dispositivo deverá suportar IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] * e o "Mecanismo de Redirecionamento para o Protocolo de Troca de Chave da Internet Versão 2.0" (Redirect Mechanism for the Internet Key Exchange Protocol Version 2, IKEv2) [RFC5685]
- Se for necessário suporte para o protocolo BGP4, o equipamento deverá estar em conformidade com os requisitos RFC4271, RFC1772, RFC4760 e RFC2545
- Se for necessário suporte para um protocolo de roteamento interno (IGP) dinâmico, deverá haver suporte para RIPng [RFC2080], OSPF-v3 [RFC5340] ou IS-IS [RFC5308]. A autoridade contratante deverá especificar o protocolo exigido.
- Se for solicitado OSPF-v3, o dispositivo deverá ter suporte para "Autenticação/Confidencialidade para OSPF-v3" ("Authentication/Confidentiality for OSPF-v3," RFC4552) (FW, IPS, APFW)
- "Compartilhamento de Carga Host ao Roteador IPv6" (IPv6 Host-to-Router Load Sharing, RFC4311) (FW)
- "Preferências de Roteador Padrão e Rotas Mais Específicas" (Default Router Preferences and More-Specific Routes, RFC4191) (FW)

Requisitos para suporte IPv6 em software

Todo software deve suportar os protocolos IPv4 e IPv6 e ser capaz de se comunicar somente em IPv4, somente em IPv6 ou em redes em pilha dupla. Se um software incluir parâmetros de rede nas suas configurações de servidor local ou remoto, o mesmo também deverá suporta configuração de parâmetros IPv6.

Todos os recursos oferecidos em IPv4 deverão estar também disponíveis em IPv6. O

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

usuário não deve notar nenhuma diferença quando o software estiver se comunicando através de IPv4 ou IPv6, exceto quando isso for diretamente benéfico para o usuário.

É altamente recomendável que não sejam usados endereços literais nos códigos de software, conforme descrito no documento "Seleção de Endereço Padrão para Protocolo de Internet Versão 6" (Default Address Selection for Internet Protocol version 6, RFC3484).

Habilidades necessárias ao integrador de sistemas

Os fornecedores e revendedores que oferecerem serviços de integração de sistemas devem ter pelo menos três funcionários com certificados válidos de qualificação dos fabricantes do equipamento vendido como parte da concorrência. Esses funcionários deverão também ter conhecimentos gerais sobre o protocolo IPv6, planejamento de rede IPv6 e segurança em IPv6 (também comprovados por certificados dessas habilidades). Se ficar claro durante a instalação e integração do equipamento que o conhecimento do integrador, sua competência e experiência não são suficientes para instalar e configurar o equipamento adequadamente para comunicar-se normalmente por IPv4 e IPv6 com a rede, o contrato deverá ser rescindido, anulado e invalidado.

A definição de integração adequada, tempo e interrupção na rede durante a instalação deverá ser determinada contratualmente entre o cliente e o integrador de sistemas.

Recomenda-se também que um integrador de sistemas e seus funcionários tenham amplos conhecimentos em IPv6 e certificados genéricos em IPv6, além dos oferecidos especificamente pelos fabricantes de equipamentos. Esses certificados podem ser obtidos de instituições de ensino independentes. Tais conhecimentos poderão render pontos extras no processo de licitação.

Todos os licitantes no processo de licitação deverão assinar uma declaração indicando que a empresa e seus funcionários foram aprovados em treinamento técnico para design, construção e integração de equipamentos TIC (ICT) em redes IPv4 e IPv6. Segue abaixo um modelo desta declaração.

Declaração de qualificação em IPv6

As entidades que abrirem licitação deverão exigir uma declaração de qualificação técnica em IPv6 do fornecedor do equipamento ou integrador. É necessário ter experiência e conhecimentos em IPv6 para garantir a instalação e integração adequada do IPv6 no ambiente TIC (ICT).

A declaração deve dizer que o fornecedor do equipamento ou integrador do sistema declara, sob pena de responsabilização criminal e material:

- Que possui número suficiente de funcionários para realizar os serviços oferecidos;
- Que tais funcionários têm qualificações profissionais para realizar o seu trabalho: design, construção e integração de equipamentos TIC (ICT) em redes e ambientes

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

IPv4 e IPv6;

- Que a qualidade dos serviços oferecidos está em conformidade com os requisitos exigidos nos documentos da licitação, e que esses requisitos se aplicam tanto a IPv4 quanto a IPv6.

Note que esse tipo de declaração pode variar dependendo da legislação local. Portanto, tradutores e entidades que abrirem licitações deverão obter aconselhamento jurídico para determinar o texto exato desses requisitos.

Agradecimentos

A primeira versão deste documento foi feita no Go6 Expert Council e no Slovenian IPv6 working group.

Os autores gostariam de agradecer a todos os envolvidos na criação e modificação da versão anterior deste documento. Em primeiro lugar, gostaríamos de agradecer a Janez Sterle, Urban Kunc, Matjaz Straus, Simeon Lisec, Davor Sostaric e Matjaz Lenassi do Go6 Expert Council por coordenarem com entusiasmo este documento. Reconhecemos o trabalho do Slovenian IPv6 working group de revisão e suas contribuições proveitosas. Gostaríamos de reconhecer especialmente os esforços e trabalho no documento de Ivan Pepelnjak, Andrej Kobal e Ragnar Us. Agradecemos também aos co-Líderes do Grupo de Trabalho RIPE IPv6, David Kessens, Shane Kerr e Marco Hogewoning por seu apoio e encorajamento. Gostaríamos também de agradecer a Patrik Fältström, Torbjörn Eklöv, Randy Bush, Matsuzaki Yoshinobu, Ides Vanneuville, Olaf Maennel, Ole Trøan, Teemu Savolainen e membros do Grupo de Trabalho RIPE IPv6 (João Damas, S.P. Zeidler, Gert Doering, dentre outros) por suas contribuições, comentários e análise do documento. Por último, mas não menos importante, gostaríamos de agradecer a Chris Buckridge e à Equipe de Comunicações da RIPE NCC por corrigir a nossa gramática e o texto deste documento. E a todos os outros que contribuíram com este trabalho.

Os autores deste documento gostariam de agradecer o Grupo de Trabalho RIPE IPv6 e seus líderes por todo o seu apoio e encorajamento no desenvolvimento de uma versão atualizada do documento. Agradecemos em especial a Ole Trøan, editor da RFC6204, por sua ajuda na seção CPE e por sugerir outras mudanças em todo o documento. Agradecemos a Marco Hogewoning, Ivan Pepelnjak e S.P. Zeidler por suas valiosas ideias sobre como melhorar a estrutura e o conteúdo do documento, a Timothy Winters e Erica Johnson (ambos do comitê IPv6 Ready Logo, UNH) por sua ajuda indicando as RFCs testadas por eles e por suas sugestões construtivas. Somos gratos a Yannis Nikolopoulos e Frits Nolet. Agradecemos em especial a Jouni Korhonen, Jari Arkko, Eric Vyncke, David Freedman, Tero Kivinen e Michael Richardson por seus comentários e sugestões extremamente pertinentes, que tornaram este documento infinitamente melhor.

Sugestões para melhoria deste documento e outros comentários podem ser enviados para a lista de e-mails do Grupo de Trabalho RIPE IPv6 <ipv6-wg@ripe.net>

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.nic.br

[1] As especificações USGv6 estão sendo revisadas e atualizadas no momento, e espera-se que sejam concluídas no início de 2012.

[2] O "Grupo de Trabalho para Melhorias na Validação de Endereço-Fonte IETF" (IETF Source Address Validation Improvements (SAVI) Working Group) está trabalhando nas RFCs que especificam a estrutura de validação de endereços-fonte. Quando essas RFCs tiverem sido publicadas, as referências de filtragem NUD e DAD poderão sofrer alterações de acordo com as mesmas.