nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

Requisitos de suporte a IPv6 para equipamentos de TIC.

Índice

Nota da versão em português

Este texto é a tradução do documento RIPE 772 - *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**, **Tim Chown**, **Tim Winters,** com o apoio da comunidade técnica europeia de operadores da Internet (RIPE), pode ser encontrado no seguinte endereço:

- https://www.ripe.net/publications/docs/ripe-772

1 Introdução

Para garantir a adoção sem incidentes e de baixo custo do IPv6 em todas as redes, é importante que as grandes empresas, o setor público ou empresas de pesquisa e educação especifiquem requisitos de funcionalidade e compatibilidade para o IPv6 ao preparar 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*) para apoiar as organizações em tais processos de licitação, no entanto, o mesmo não especifica nenhum padrão ou política em si. Ele é uma atualização do documento ripe-554, que é a segunda versão do documento - *Requirements for IPv6 in ICT Equipment*.

Ele inclui diretrizes sobre quais especificações devem ser exigidas e destina-se a ser usado como um **modelo** que pode ser utilizado pelos governos, universidades, empresas de grande porte ou qualquer outra organização que necessite de apoio nas especificações do IPv6 em

suas licitações, ou requisitos de equipamento. 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, principalmente a IETF, que operam independentemente da comunidade RIPE, e que todos esses padrões estão sujeitos a mudanças ou substituição por versões mais recentes. Embora este documento tenha sido aprovado pelos membros do RIPE, principalmente por meio do IPv6 WG, a partir da data de publicação, seu conteúdo ficará desatualizado à medida que novas RFCs ou documentos relacionados forem publicados.

Poderá também ser necessário adequar as recomendações às suas necessidades locais específicas; novamente, este documento é puramente um modelo, e os elementos obrigatórios e opcionais sugeridos podem precisar serem ajustados para seu caso de uso específico.

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

https://www.nist.gov/programs-projects/usgv6-program

Para o qual existe uma versão mais recente em:

https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.500-267Ar1.pdf

Os autores modificaram o conteúdo desses documentos para torná-los mais universais. Esta opção inclui uma lista de padrões de especificações RFC que devem ser suportados, divididos em sete categorias de dispositivos. Observe que este documento remove a categoria 'dispositivo móvel', e inclui esses dispositivos como *hosts*.

Este documento também está em conformidade com o documento "Requisitos para nós IPv6" (*IPv6 Node requirements*, RFC8504), que atualiza a RFC6434. Essa RFC contém as instruções gerais e o consenso da IETF sobre que partes do IPv6 devem ser implementadas por dispositivos diferentes, e seu conteúdo geralmente é refletido neste documento.

1.1 Informações gerais sobre como usar este documento

Este documento não impõe tecnologias específicas a serem utilizadas, em vez disso, presume que um projeto/solução de redes foi produzido e que o projeto e os componentes que ele utiliza precisam ser mapeados para o documento de compra.

A certificação ***IPv6 Ready Logo*** pode ser solicitada para *hosts*, roteadores e roteadores nas instalações do cliente. Embora a certificação Logo tenha sido criada há cerca de 20 anos, ela se mantém atual com as atualizações do padrão IPv6 e é um programa globalmente aceito para que os fornecedores promovam seus equipamentos e garantam que eles atendem aos requisitos básicos do IPv6. As últimas atualizações da certificação *IPv6 Ready Logo* exigem que os dispositivos sejam testados em ambientes somente IPv6 e tenham o IPv6 ativado por padrão. 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.

Para mais informações sobre o programa *IPv6 Ready Logo*, consulte: http://www.ipv6ready.org/

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. Da mesma forma, se os recursos listados como opcionais forem necessários para o caso de uso específico do órgão que abrir a licitação, esses requisitos devem se tornar obrigatórios. Note que a entidade que abrir a licitação deve determinar as funções obrigatórias, não o fornecedor do equipamento; este documento é simplesmente um modelo.

1.2 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.

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 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 *.**

2 Texto genérico sugerido para a entidade que abrir a licitação

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

Todos os hardwares e softwares relacionados às TICs (ICT), pertinente a esta licitação, devem ser compatíveis com o protocolo IPv6 e DEVEM operar em um ambiente somente IPv6. Por exemplo, onde SNMP é usado, ele deve ser capaz de operar sobre transporte IPv6.

Se o IPv4 for suportado, o desempenho e capacidades deverão ser semelhantes para ambos os protocolos em termos de entrada, saída e performance do fluxo de dados, transmissão e processamento de pacotes. A diferença deverá ser imperceptível para os usuários.

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

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

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

3 Categorias de dispositivos no escopo deste documento

Os requisitos são divididos em equipamento de hardware e suporte a integradores.

Todos os requisitos impostos às capacidades de tráfego IPv4, como latência, largura de banda e taxa de transferência, ou para monitoramento e contabilidade, também devem ser exigidos para o tráfego IPv6.

3.1 Definições e descrições de diferentes categorias 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.

Observe que a categoria de dispositivo móvel incluída no documento ripe-554 foi removida. Esses dispositivos agora se enquadram na categoria de *host*, de modo que são considerados apenas a partir de sua conectividade com a infraestrutura local (via WiFi) e, portanto, os requisitos relacionados ao 3GPP estão fora do escopo deste documento.

***Host*:** *Host* é um participante da rede que envia e recebe pacotes, mas não os encaminha em nome de outros. Isso inclui dispositivos móveis conectados à infraestrutura de rede local.

Dispositivos *host* em uma empresa podem ser *multihomed*, dispositivos móveis sendo um exemplo e dispositivos com uma rede e interface de gerenciamento sendo outro. A IETF tem trabalhado por muitos anos em abordagens de *multihoming* para IPv6. Requisitos específicos da RFC4191 estão incluídos neste documento.

***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. Esta categoria é dividida em dispositivos para clientes (normalmente para uso doméstico) e em dispositivos para empresas/provedores de serviços de Internet.

Os pontos de acesso WiFi não são tecnicamente dispositivos de camada 2 puros, mas eles devem (possivelmente em cooperação com um controlador sem fio) executar a mesma

funcionalidade que um *switch* de camada 2 no que diz respeito aos recursos IPv6. Assim, o texto desta seção também pode ser usado para pontos de acesso WiFi.

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. Frequentemente, os CPEs precisam suportar mecanismos de transição IPv6; este documento se concentrará principalmente em métodos de transição para redes somente IPv6.

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.

3.2 O que está fora do escopo deste documento

Com intuito de chegar a um consenso para publicar uma atualização para o documento ripe-554 da forma mais eficiente possível, os autores minimizaram a inclusão de novos tipos de dispositivos. Estes podem ser adicionados em uma atualização futura ou como uma atualização separada.

Como mencionado acima, neste documento, os dispositivos móveis são considerados apenas em relação à sua conectividade com a infraestrutura corporativa (normalmente por WiFi) e, a esse respeito, são considerados *hosts*.

Observe que as "Máquinas Virtuais" (*Virtual Machines* - VMs) e contêineres estão fora do escopo deste documento; essas funções podem ser fornecidas em sistemas adquiridos como *hosts* (4.1 Requisitos para os equipamentos "*host*") por meio deste documento, mas não são "equipamentos de TICs" em si.

Embora a RFC8504 inclua uma seção sobre YANG para gerenciamento de rede, outros requisitos YANG não estão incluídos neste documento.

Certas novas funções de roteamento que surgiram recentemente também não foram adicionadas neste ponto do documento, como por exemplo o SRv6 da RFC8986.

4 Listas de padrões RFC exigidos para diferentes tipos de hardware

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

- *Host*: cliente (incluindo dispositivo móvel) ou servidor
- *Switch* de camada 2 para clientes
- *Switch* de camada 2 para empresas/provedores de serviços de Internet
- Roteador ou *Switch* de camada 3
- Equipamentos de segurança de rede (*firewalls*, IDS, IPS...)

- Equipamentos de CPE
- Balanceador de carga

Os seguintes requisitos estão divididos em dois tipos: 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 (*).

4.1 Requisitos para os equipamentos "*host*"

Suporte obrigatório:

- "Especificação Básica de IPv6" (*IPv6 Basic specification*, RFC8200/STD 86) *
- "Arquitetura de Endereçamento IPv6" (*IPv6 Addressing Architecture*, RFC4291) *
- "Seleção de Endereço Padrão para IPv6" (*Default Address Selection for IPv6*, RFC6724)
- "Endereços Unicast IPv6 Únicos" (*Unique Local IPv6 Unicast Addresses (ULA)*, RFC4193)
- ICMPv6 [RFC4443/STD89] *
- Se for necessário suporte para DHCPv6, o dispositivo deverá ter suporte para:
    - “Cliente DHCPv6 *Stateful*” (*Stateful DHCPv6 client*, RFC8415) *
    - “Cliente DHCPv6 *Stateless*” (*Stateless DHCPv6 client*, RFC8415) *

  - “Opções de configuração de DNS para Protocolo de Configuração Dinâmica de *Host* para IPv6” (*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, RFC3646)*
  - “Um Método para Gerar Identificadores de Interface Semanticamente Opacos (IIDs) com o Protocolo de Configuração Dinâmica de *Host* para IPv6” (*A Method for Generating Semantically Opaque Interface Identifiers (IIDs) with the Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, RFC7943)
- SLAAC [RFC4862] *
- "Descoberta de Caminho MTU" (*Path MTU Discovery*, RFC8201/STD87) *
- "Descoberta de Vizinhança" (*Neighbor Discovery*, RFC4861, RFC6980) *
- "Extensões de protocolo DNS para incorporação dos registros de recursos IPv6 DNS" (*DNS protocol extensions for incorporating IPv6 DNS resource records*, RFC3596/STD88)
- "Mecanismos de ampliação de mensagem DNS" (*DNS message extension mechanism*, RFC6891/STD75)
- "Requisitos de tamanho de mensagens DNS" (*DNS message size requirements*, RFC3226)
- “Transmissão de pacotes IPv6 em redes *Ethernet*” (*Transmission of IPv6 Packets over Ethernet Networks*, RFC2464)
- “Implicações de segurança da fragmentação IPv6 com descoberta de vizinhança IPv6” (*Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*, RFC6980)
- “Atualizações na arquitetura de endereçamento multicast IPv6” (*Updates to the IPv6 Multicast Addressing Architecture*, RFC7371)
- “Um Método para Gerar Identificadores de Interface Semanticamente Opacos com a Configuração Automática de Endereço Stateless para IPv6” (*A Method for Generating*

Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC), RFC7217)

- "Opções de Anúncios de Roteadores IPv6 para Configuração DNS" (*IPv6 Router Advertisement Options for DNS Configuration*, RFC8106)
- "Descoberta de ouvinte *multicast* versão 2" (*Multicast Listener Discovery version 2*, RFC3810) *
- "Preferências padrão do roteador e rotas mais específicas: funções de *host* do tipo A e B" (*Default Router Preferences and More-Specific Routes: Type A and B host roles*, RFC4191)
- 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)
- "Especificação de rótulo de fluxo IPv6" (*IPv6 Flow Label Specification*, RFC6437)

Suporte opcional:

- "ICMP estendido para mensagens multiparte" (*Extended ICMP for multi-part messages*, RFC4884)
- "Extensões de endereço temporário para configuração automática de endereço *stateless* no IPv6" (*Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6*, RFC8981)
- "(Classe de tráfego) DS" DS (*Traffic class*), RFC2474, RFC3140)
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79, RFC7619, RFC8221, RFC8247] *
- "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]
- "Detecção de MTU da camada de Empacotamento" (*Packetisation Layer Path MTU Discovery*, RFC4821, RFC8899)
- "Compartilhamento de Carga do *Host* ao Roteador IPv6" (*IPv6 Host-to-Router Load Sharing*, RFC4311)
- "Preferências padrão do roteador e rotas mais específicas: função de *host* do tipo C" (*Default Router Preferences and More-Specific Routes: Type C host role*, RFC4191)
- "Opção de sinalização de anúncio de roteador IPv6" (*IPv6 Router Advertisement Flags Option*, RFC5175)
- "A adição de notificação explícita de congestionamento para IP" (*The Addition of Explicit Congestion Notification (ECN) to IP*, RFC3168)
- "Seleção de roteador de primeiro salto por *hosts* em uma rede com vários prefixos" (*First-Hop Router Selection by Hosts in a Multi-Prefix Network*, RFC8028)
- "Distribuindo Política de Seleção de Endereço usando DHCPv6" (*Distributing Address Selection Policy Using DHCPv6*, RFC7078)
- Para a privacidade do endereço IPv6 melhorada, o suporte deve ser considerado para "Considerações de segurança e privacidade para mecanismos de geração de endereços IPv6" (*Security and Privacy Considerations for IPv6 Address Generation Mechanisms*, RFC7721) e "Recomendação sobre identificadores de interface IPv6 estáveis" (*Recommendation on Stable IPv6 Interface Identifiers*, RFC8064)
- MIPv6 [RFC6275, RFC5555] e "Operação IPv6 móvel com IKEv2 e a arquitetura IPsec revisada" (*Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture*, RFC4877)

- “Descobrindo PREF64 em anúncios de roteador” (*Discovering PREF64 in Router Advertisements*, RFC8781)

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

Suporte opcional (gerenciamento):

- *MLDv2 snooping* [RFC4541]
- "Especificação Básica de IPv6" (*IPv6 Basic specification*, RFC8200/STD86)*
- "Arquitetura de Endereçamento IPv6" (*IPv6 Addressing Architecture*, RFC4291) *
- "Seleção de Endereço Padrão" (*Default Address Selection for IPv6*, RFC6724)
- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- "Descoberta de Vizinhança" (Neighbor Discovery, RFC4861, RFC6980) *
- "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]
- “Transmissão de pacotes IPv6 em redes *Ethernet*” (T*ransmission of IPv6 Packets over Ethernet Networks*, RFC2464)

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

Suporte obrigatório (plano de encaminhamento):

- “Transmissão de pacotes IPv6 em redes *Ethernet*” (*Transmission of IPv6 Packets over Ethernet Networks*, RFC2464)
- *MLDv2 snooping* [RFC4541]

- “Guarda de anúncio de roteador” (*Router Advertisement (RA) Guard*, RFC6105) e [RFC7113]
- “Escudo DHCPv6: proteção contra servidores DHCPv6 desonestos” (*DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers*, RFC7610)
- “Inspeção dinâmica de "solicitação/anúncio de vizinhança IPv6” (*Dynamic "IPv6 Neighbor solicitation/advertisement" inspection*, RFC4861)
- “Filtro de detecção de inacessibilidade de vizinho” (*Neighbor Unreachability Detection (NUD) filtering*, RFC4861)
- “Rastreamento e filtragem de detecção de endereço duplicado” (*Duplicate Address Detection (DAD) snooping and filtering*, RFC4429)
- Se for necessário suporte para DHCPv6, o dispositivo deverá ter suporte para:
    - “Agente DHCPv6 *Relay Lightweight*” (*Lightweight DHCPv6 Relay Agent*, RFC6221)
    - “Opção de ID remoto do agente DHCPv6 *relay*” (*DHCPv6 Relay Agent Remote-ID Option*, RFC4649)
    - “Opção de ID de assinante do agente DHCPv6 *relay*” (*DHCPv6 Relay Agent Subscriber-ID Option*, RFC4580)
    - “Opção de endereço da camada de link do cliente DHCPv6” (*DHCPv6 Client Link-Layer Address Option*, RFC6939)

Suporte obrigatório (gerenciamento; o dispositivo deve funcionar como um *host* IPv6 para gerenciamento):

- "Especificação Básica de IPv6" (*IPv6 Basic specification*, RFC8200/STD86)*
- "Arquitetura de Endereçamento IPv6" (*IPv6 Addressing Architecture*, RFC4291) *
- "Seleção de Endereço Padrão" (*Default Address Selection for IPv6*, RFC6724)

- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- Se for necessário suporte para SNMP:
    - "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 [RFC8200, Valor do próximo Cabeçalho 43]" (*IPv6 Routing Header [RFC8200, Next Header value 43] filtering*) *

Suporte opcional:

- “Solução de melhoria de validação de endereço de origem para DHCP” (*Source Address Validation Improvement (SAVI) Solution for DHCP*, RFC7513)

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

Suporte obrigatório:

- "Especificação Básica de IPv6" (*IPv6 Basic specification*, RFC8200/STD86) *
- “Transmissão de pacotes IPv6 em redes Ethernet” (*Transmission of IPv6 Packets over Ethernet Networks*, RFC2464)
- "Arquitetura de Endereçamento IPv6" (*IPv6 Addressing Architecture*, RFC4291) *
- "Seleção de Endereço Padrão para IPv6" (*Default Address Selection for IPv6*, RFC6724)
- "Endereços Unicast IPv6 Únicos" (*Unique Local IPv6 Unicast Addresses (ULA)*, RFC4193)
- Se for necessário suporte para DHCPv6, o dispositivo deverá ter suporte para:
    - “Cliente/servidor/*relay* DHCPv6” (*DHCPv6 client/server/relay*, RFC8415) *

  - “Opção de ID remoto do agente DHCPv6 *relay*” (*DHCPv6 Relay Agent Remote-ID Option*, RFC4649)
  - “Opção de ID de assinante do agente DHCPv6 *relay*” (*DHCPv6 Relay Agent Subscriber-ID Option*, RFC4580)
  - “Opção de endereço da camada de link do cliente DHCPv6” (*DHCPv6 Client Link-Layer Address Option*, RFC6939)
- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- “Opções de Anúncios de Roteadores IPv6 para Configuração DNS” (*IPv6 Router Advertisement Options for DNS Configuration*, RFC8106) *
- *MLDv2 snooping* [RFC4541]
- “Descoberta de ouvinte *multicast* versão 2” (*Multicast Listener Discovery version 2*, RFC3810) *
- “Atualizações na arquitetura de endereçamento *multicast* IPv6” (*Updates to the IPv6 Multicast Addressing Architecture*, RFC7371)
- "Descoberta de Caminho MTU" (*Path MTU Discovery*, RFC8201/STD87) *
- "Descoberta de Vizinhança" (*Neighbor Discovery,* RFC4861, RFC6980) *
- “Prefixos IPv6 de 127 bits em links inter-roteadores” (*127-bit IPv6 Prefixes on Inter-Router Links*, RFC6164)
- “Recomendações de tamanho de prefixo IPv6 para encaminhamento” (*IPv6 Prefix Length Recommendations for Forwarding*, RFC7608) *
- Se for necessário suporte para SNMP:
  - "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]

- Se for solicitado um protocolo de roteamento interno (IGP) dinâmico, então será necessário suporte para RIPng [RFC2080], OSPFv3 [RFC5340] [RFC5613] 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) ou “Trailer de autenticação de suporte para OSPFv3” (*Supporting Authentication Trailer for OSPFv3*, RFC7166)
- Se for solicitado suporte para OSPFv3 e SNMP, o equipamento deverá oferecer suporte para “Base de informações de gerenciamento para OSPFv3” (*Management Information Base for OSPFv3*, RFC5643)
- Se for solicitado o protocolo BGP4, o equipamento deverá estar em conformidade com os requisitos em [RFC4271], [RFC1772], [RFC4760], [RFC1997], [RFC3392], [RFC2545], [RFC5492], [RFC6268], [RFC6608], [RFC6793], [RFC7606], [RFC7607], [RFC7705] e [RFC8212]
- Se for solicitado o protocolo VRRP, o equipamento deverá estar em conformidade com os requisitos em [RFC5798]
- Se for solicitado o protocolo PIM-SM, o equipamento deverá estar em conformidade com os requisitos em [RFC7761/STD83] e [RFC5059]
- 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 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 [RFC3775, RFC5555] e “Operação de IPv6 Móvel com IKEv2 e a Arquitetura IPsec Revisada" (*Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture*, RFC4877)
- 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 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)
- 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)

- “Especificação de rótulo de fluxo IPv6” (*IPv6 Flow Label Specification*, RFC6437)

Suporte opcional:

- “ICMP estendido para mensagens multiparte” (*Extended ICMP for multi-part messages*, RFC4884)
- “Extensões de privacidade SLAAC” (*SLAAC Privacy Extensions*, RFC4941)
- *Stateless DHCPv6* [RFC8415] *
- “Delegação de prefixo DHCPv6” (*DHCPv6 Prefix Delegation*, RFC8415) *
- *DHCPv6 Bulk Leasequery* [RFC5460]
- *DHCPv6 Active Leasequery* [RFC7653]
- "(QOS) Encaminhamento Assegurado" (*(QOS) Assured Forwarding*, RFC2597)
- "(QOS) Encaminhamento Acelerado" (*(QOS) Expedited Forwarding*, RFC3246)
- “(QOS) Suporte para gerenciamento de filas ativas” (*(QOS) Active Queue Management support*, RFC7567)
- "Encapsulamento de Roteamento Genérico" (*Generic Routing Encapsulation*, RFC2784)
- “IPsec/IKEv2 (Plano de Controle)” (IPsec/IKEv2 (*Control Plane*), RFC4301, RFC4303, RFC7268, RFC8221, RFC8247) *
- “IPsec/IKEv2 VPN (Plano de Dados)” (IPsec/IKEv2 VPN (*Data Plane*), [RFC4301, RFC4303], RFC7269, RFC8221) *
- "Uso de IPsec para Garantir túneis de IPv6-em-IPv4" (*Using IPsec to Secure IPv6-in-IPv4 tunnels*, RFC4891)

- "Extensões de protocolo DNS para incorporação dos registros de recursos IPv6 DNS" (*DNS protocol extensions for incorporating IPv6 DNS resource records*, RFC3596/STD88)
- "Mecanismos de ampliação de mensagem DNS" (*DNS message extension mechanism*, RFC6891/STD75)
- "Requisitos de tamanho de mensagens DNS" (*DNS message size requirements*, RFC3226)
- "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 padrão do roteador e rotas mais específicas” (*Default Router Preferences and More-Specific Routes*, RFC4191)
- “Descobrindo PREF64 em anúncios de roteador” (*Discovering PREF64 in Router Advertisements*, RFC8781)

4.5 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*, RFC8200/STD86) (FW, IPS, APFW) *
- "Arquitetura de Endereçamento IPv6" (*IPv6 Addressing Architecture*, RFC4291) (FW, IPS, APFW)
- "Seleção de Endereço Padrão para IPv6" (*Default Address Selection for IPv6*, RFC6724) (FW, IPS, APFW)
- ICMPv6 [RFC4443/STD89] (FW, IPS, APFW) *
- “Transmissão de pacotes IPv6 em redes Ethernet” (*Transmission of IPv6 Packets over Ethernet Networks*, RFC2464)
- SLAAC [RFC4862] (FW, IPS) *
- Se for necessário suporte para SNMP:
    - "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]
- “Opções de Anúncios de Roteadores IPv6 para Configuração DNS” (*IPv6 Router Advertisement Options for DNS Configuration*, RFC8106) (FW)
- "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)
- "Descoberta de Caminho MTU" (*Path MTU Discovery*, RFC8201/STD87) (FW, IPS, APFW) *
- "Descoberta de Vizinhança" (*Neighbor Discovery*, RFC4861) (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], OSPFv3 [RFC5340] ou IS-IS [RFC5308] . A autoridade contratante deverá especificar o protocolo exigido. (FW, IPS, APFW)
- 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) ou “Trailer de autenticação de suporte para OSPFv3” (*Supporting Authentication Trailer for OSPFv3*, RFC7166) (FW, IPS, APFW)
- Se for solicitado suporte para OSPFv3 e SNMP, o equipamento deverá oferecer suporte para “Base de informações de gerenciamento para OSPFv3” (*Management Information Base for OSPFv3*, RFC5643)
- 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:

- “Cliente/servidor/*relay* DHCPv6” (*DHCPv6 client/server/relay*, RFC8415) *
- *Stateless DHCPv6* [RFC8415] *
- “Delegação de prefixo DHCPv6” (*DHCPv6 Prefix Delegation*, RFC8415) *
- “ICMP estendido para mensagens multiparte” (*Extended ICMP for Multipart Messages*, RFC4884)
- “Extensões de privacidade SLAAC” (*SLAAC Privacy Extensions*, RFC4941)
- "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*, RFC3246)
- "Endereços Unicast IPv6 Únicos" (*Unique Local IPv6 Unicast Addresses (ULA)*, RFC4193)
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79] *
- "Uso de IPsec para Garantir túneis de IPv6-em-IPv4" (*Using IPsec to Secure IPv6-in-IPv4 tunnels*, RFC4891) (FW)
- OSPFv3 [RFC5340]
- "Autenticação/Confidencialidade para OSPF-v3" (*Authentication / Confidentiality for OSPF-v3*, RFC4552)
- "IPv6 e Tunelamento Genérico de Pacotes" (*Generic Packet Tunneling and IPv6*, RFC2473)
- “Extensões DNS para suportar IPv6” (*DNS extensions to support IPv6*, RFC3596)

- "Mecanismos de ampliação de mensagem DNS" (*DNS message extension mechanism*, RFC6891)
- "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) *
- *MLDv2 snooping* [RFC4541] (quando em modo camada 2 ou de passagem) *
- "Detecção de MTU da camada de Empacotamento" (*Packetisation Layer Path MTU Discovery*, RFC4821 e RFC8899)
- "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 padrão do roteador e rotas mais específicas" (*Default Router Preferences and More-Specific Routes*, RFC4191)
- "Transmissão e processamento de cabeçalhos de extensão IPv6" (*Transmission and Processing of IPv6 Extension Headers*, RFC7045)

4.6 Requisitos para equipamentos CPE

Suporte obrigatório:

- "Requisitos Básicos para Roteadores IPv6 de Borda para Clientes" (*Basic Requirements for IPv6 Customer Edge Routers*, RFC7084) *

- “Recursos de segurança simples recomendados em equipamentos das instalações do cliente para fornecer serviços residenciais de Internet IPv6” (*Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service*, RFC6092)
- Se for necessário suporte para mecanismos de transição IPv4 específicos, o equipamento precisa ter suporte aos requisitos relevantes, conforme podem ser obtidos em “Requisitos para roteadores de borda de cliente IPv6 para oferecer suporte a IPv4 como serviço” (*Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service*, RFC8585) e “Descobrindo PREF64 em anúncios de roteador” (*Discovering PREF64 in Router Advertisements*, RFC8781)
- Se for necessário suporte para SNMP:
    - "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]

Suporte opcional:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296, RFC7619, RFC8221, RFC8247] *
- MIPv6 [RFC6275, RFC5555] e “Operação IPv6 móvel com IKEv2 e a arquitetura IPsec revisada” (*Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture*, RFC4877)
- “ICMP estendido para mensagens multiparte” (*Extended ICMP for multi-part messages*, RFC4884)
- “Extensões de privacidade SLAAC” (*SLAAC Privacy Extensions*, RFC4941)

- “Transmissão de pacotes IPv6 em redes *Ethernet*” (*Transmission of IPv6 Packets over Ethernet Networks*, RFC2464)
- “(QOS) (Classe de tráfego) DS” ((QOS) DS (*Traffic class*), RFC2474, RFC3140)
- “(QOS) Suporte para gerenciamento de filas ativas” (*(QOS) Active Queue Management support*, RFC7567)
- “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 e RFC8899)
- “Requisitos para roteadores de borda de cliente IPv6 para oferecer suporte a IPv4 como serviço” (*Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service*, RFC8585)
- "Compartilhamento de Carga do *Host* ao Roteador IPv6" (*IPv6 Host-to-Router Load Sharing*, RFC4311)
- “Preferências padrão do roteador e rotas mais específicas” (*Default Router Preferences and More-Specific Routes*, RFC4191)

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

Suporte obrigatório:

- "Especificação Básica de IPv6" (*IPv6 Basic specification*, RFC8200/STD86) *
- "Arquitetura de Endereçamento IPv6" (*IPv6 Addressing Architecture*, RFC4291) *
- "Seleção de Endereço Padrão" (*Default Address Selection*, RFC6274)
- “Transmissão de pacotes IPv6 em redes *Ethernet*” (*Transmission of IPv6 Packets over Ethernet Networks*, RFC2464)
- "Endereços *Unicast* IPv6 Únicos" (*Unique Local IPv6 Unicast Addresses (ULA)*, RFC4193)
- ICMPv6 [RFC4443/STD89] *
- "Descoberta de Caminho MTU" (*Path MTU Discovery*, RFC8201/STD87) *
- "Descoberta de Vizinhança" (*Neighbor Discovery*, RFC4861) *
- “Opções de Anúncios de Roteadores IPv6 para Configuração DNS” (*IPv6 Router Advertisement Options for DNS Configuration*, RFC8106)

- "Extensões de protocolo DNS para incorporação dos registros de recursos IPv6 DNS" (*DNS protocol extensions for incorporating IPv6 DNS resource records*, RFC3596/STD88)
- "Mecanismos de ampliação de mensagem DNS" (*DNS message extension mechanism*, RFC6891)
- "Requisitos de tamanho de mensagens DNS" (*DNS message size requirements*, RFC3226)
- Se for necessário suporte para balanceamento de carga em camada 7 (nível aplicação/*proxy* reverso, definido como 'substituto' na seção 2.2 da RFC3040), o equipamento precisa ter suporte para "Extensão de HTTP encaminhada" (*Forwarded HTTP Extension*, RFC7239) para endereços de cliente IPv4 e IPv6
- Se for necessário suporte para balanceamento de carga em camada 7 (nível aplicação/*proxy* reverso, definido como 'substituto' na seção 2.2 da RFC3040), o equipamento precisa ter suporte para "Protocolo de Segurança da Camada de Transporte Versão 1.3" (*Transport Layer Security (TLS) Protocol Version 1.3*, RFC8446)
- Se for necessário suporte para IPsec, o dispositivo deverá suportar IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79]* 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 em 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)

Suporte opcional:

- “ICMP estendido para mensagens multiparte” (*Extended ICMP for Multipart Messages*, RFC4884)
- "(Classe de tráfego) DS" DS (*Traffic class*), RFC2474, RFC3140)
- "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]
- "Compartilhamento de Carga *Host* ao Roteador IPv6" (*IPv6 Host-to-Router Load Sharing*, RFC4311)
- “Preferências padrão do roteador e rotas mais específicas” (*Default Router Preferences and More-Specific Routes*, RFC4191)

5 Requisitos para suporte IPv6 em software

Todo software deve suportar o protocolo IPv6 e ser capaz de se comunicar 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 suportar configuração de parâmetros IPv6. O 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

O desenvolvedor/fornecedor de software deve, no mínimo, fazer o seguinte para garantir isso:

- 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*, RFC6724)
- É obrigatório ter suporte a todas as notações de endereço IPv6 válidas conforme especificado em "Arquitetura de Endereçamento IP versão 6" (*IP Version 6 Addressing Architecture*, RFC4291) em todos os locais no software no qual os endereços IP são manipulados (como em interfaces de usuário, interpretação de arquivos de configuração ou onde os dados são processados)
- É recomendado que seja seguido a especificação "Uma recomendação para representação de endereços IPv6 em texto" (*A Recommendation for IPv6 Address Text Representation*, RFC5952) na saída da notação IPv6 ou em todos os locais no qual os endereços IPv6 são exibidos
- A resolução de nomes de *host* do DNS deve ter suporte a respostas IPv6 (AAAA)
- Conectar a outros sistemas e receber conexões de outros sistemas deve ter suporte a conexões IPv6 utilizando os mecanismos de sistema apropriados (p.ex. soquetes de rede)
- Ao configurar uma conexão, o software deve seguir a “Seleção de Endereço Padrão para Protocolo de Internet Versão 6" (*Default Address Selection for Internet Protocol version 6*, RFC6724) ou “*Happy Eyeballs* versão 2: melhor conectividade usando

concorrência" (*Happy Eyeballs Version 2: Better Connectivity Using Concurrency*, RFC8305)

- Esses requisitos também devem ser verificados em qualquer biblioteca ou ferramenta utilizada pelo software

Esta lista não é exaustiva e cobre apenas os requisitos básicos.

O artigo "Dependência de versão de IP em software de aplicativos - Preparando o código-fonte para IPv6" (*IP-version dependency in application software - Preparing source code for IPv6*[1]) da Fundação IPv6 da Holanda pode ser utilizado como ponto de partida pelos desenvolvedores.

6 IPsec: obrigatório vs opcional

No padrão de "Requisitos para nós IPv6" (*IPv6 Node requirements*, RFC4294) original, a implementação do IPsec estava listada como 'OBRIGATÓRIA' para estar em conformidade com os padrões. A versão atualizada da RFC de "Requisitos para Nós" (*Node Requirements*, RFC6434) publicada em 2011 mudou a classificação do IPsec para 'DEVERIA' ser implementado. As justificativas para a mudança foram declaradas nessa RFC.

O "Grupo de Trabalho IPv6 RIPE" (*RIPE IPv6 Working Group*) discutiu se o suporte ao IPsec deveria ser obrigatório ou opcional. Ao finalizar o documento ripe-554, os seus membros mais comunicativos apoiaram a mudança do IPsec para as seções opcionais, o que também se refletiu neste documento atualizado.

Embora o consenso entre a comunidade tenha sido de que o IPsec deve ser opcional na maioria dos casos, a IETF confirmou em 2019 na última versão do padrão de "Requisitos para nós IPv6" (*IPv6 Node requirements*, RFC8504) que o IPsec 'DEVERIA' ser implementado (não 'OBRIGATÓRIO'). No contexto da IETF, 'DEVERIA' significa que pode haver motivos válidos

[1] https://www.stipv6.nl/wp-content/uploads/2013/09/ip-aspects-software-stipv6-white-paper-v12.pdf

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, RFC8221, RFC7296 RFC7619 and RFC8247]*

O atual conjunto de algoritmos de implementação obrigatória para a arquitetura IPsec é definido em “Requisitos de implementação de algoritmo criptográfico para ESP e AH” (*Cryptographic Algorithm Implementation Requirements for ESP and AH*, RFC8221). Nós IPv6 que implementam a arquitetura IPsec tem que estar OBRIGATORIAMENTE em conformidade com os requisitos em [RFC8221].

O atual conjunto de algoritmos de implementação obrigatória para a arquitetura IKEv2 é definido em “Requisitos de implementação de algoritmo criptográfico para ESP e AH” (*Cryptographic Algorithm Implementation Requirements for ESP and AH*, RFC8247). Nós IPv6 que implementam a arquitetura IKEv2 tem que estar OBRIGATORIAMENTE em conformidade com os requisitos em [RFC8247] e/ou em quaisquer atualizações ou substituições futuras da [RFC8247].

Embora o “Cabeçalho de Autenticação” (*Authentication Header*) especificado na RFC4302 fosse supostamente a forma de fornecer integridade e não repúdio, porque não podia atravessar NATs, tornou-se uma prática comum o uso de *ESP null*. Conforme declarado na Seção 13.1 da RFC8504, que é retirada da RFC4301, nós IPv6 que implementam a Arquitetura IPsec devem ‘OBRIGATORIAMENTE’ implementar ESP (RFC4303) e 'PODEM' implementar AH (RFC4302).

7 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. Além disso, esses funcionários devem ter conhecimentos gerais sobre o protocolo IPv6, planejamento de rede IPv6 e segurança em IPv6 (como 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 devem assinar o seguinte formulário que indica 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.

7.1 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 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.

8 Agradecimentos

A primeira versão (Eslovena) deste documento foi criada no *Go6 Expert Council* e no *Slovenian IPv6 working group* em 2009.

Os autores originais gostariam de agradecer a todos os envolvidos na criação e modificação da primeira versão deste documento (ripe-501, ano 2009). 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 realizado do *Slovenian IPv6 working group* por sua revisão e contribuições proveitosas, um reconhecimento especial vai para Ivan Pepelnjak, Andrej Kobal e Ragnar Us por seus esforços e trabalho realizado no documento. 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 do RIPE-NCC

por corrigir a nossa gramática e o texto deste documento. E a todos os outros que contribuíram com este trabalho.

Os autores da versão anterior do documento (ripe-554, ano 2012) gostariam de agradecer ao RIPE IPv6 WG 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 também 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.

Os autores da versão atual do documento gostariam de agradecer aos membros do Grupo de Trabalho RIPE IPv6 e seus líderes, e especialmente a Jens Link, Martin Schröder, Fernando Gont, Enno Rey, Dave Taht, Azalea Fernandez, Yannis Nikolopoulos e Eric Vyncke por seus comentários.

Sugestões para melhoria deste documento e outros comentários podem ser enviados para as listas de e-mails do RIPE IPv6 WG ou RIPE BCOP TF.

https://www.ripe.net/mailman/listinfo/ipv6-wg/

https://www.ripe.net/mailman/listinfo/bcop