Requerimientos de IPv6 para equipos de TIC

Esta es una traducción de RIPE-772 y la versión en inglés es la versión autoritativa

Autores:

- Merike Käo, <merike@doubleshotsecurity.com>
- Jan Žorž, <jan@go6.si>
- Sander Steffann, <sander@steffann.nl>
- Tim Chown <tim.chown@jisc.ac.uk>
- Tim Winters <tim@qacafe.com>

Grupos de Trabajo:

- Grupo de Trabajo de IPv6
- Grupo de Trabajo de Mejores Prácticas Operativas Actuales

(Carta constitutiva propuesta) ID del documento: ripe-772
Actualizaciones: ripe-554 Fecha: diciembre del 2021

Tabla de contenidos:

1 Introducción

A fin de asegurar una adopción del IPv6 sin problemas y rentable en todas sus redes, es importante que las grandes empresas comerciales, del sector público o de las áreas de investigación y educación especifiquen los requerimientos para la funcionalidad y compatibilidad con el IPv6 al elaborar las licitaciones de equipos y soportes de Tecnologías de la Información y Comunicación (TIC).

El presente documento pretende proporcionar las Mejores Prácticas Actuales (BCP) para apoyar a las organizaciones en los procesos de licitación, pero no especifica ningún estándar o política. Se trata de una actualización del documento ripe-554, que es la segunda versión de las pautas de "Requerimientos de IPv6 para equipos de TIC".

Brinda orientación sobre qué especificaciones solicitar y pretende servir como **plantilla** para su uso por parte de los gobiernos, las universidades, las grandes empresas o cualquier otra organización al momento de especificar los requerimientos para el soporte del IPv6 en sus licitaciones o solicitudes de equipos. También puede utilizarse como una guía para aquellas personas u organizaciones interesadas en licitaciones para contratos gubernamentales o empresariales.

Tenga en cuenta que los estándares que se incluyen en el presente provienen de distintos organismos, principalmente del IETF, que operan independientemente de la comunidad del RIPE, y que cualquiera de estos estándares puede modificarse o remplazarse por una nueva versión. Si bien este documento cuenta con la aprobación de los miembros del RIPE, principalmente a través del Grupo de Trabajo (WG) del IPv6, sus contenidos pueden quedar desactualizados a medida que se elaboran nuevas RFC o documentos similares.

Además, es posible que deba ajustar las recomendaciones según sus necesidades locales específicas. Como mencionamos, este documento es meramente una plantilla, y los aspectos obligatorios u opcionales sugeridos puede que deban modificarse según su(s) caso(s) de uso específico(s).

Algunos fragmentos de esta sección están ligeramente basados en el perfil NIST/USGv6 elaborado por el Gobierno de EE. UU.:

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

Puede encontrar la versión más reciente en:

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

Los autores han modificado el contenido de estos documentos para que sean más aplicables de manera universal. Esta opción incluye una lista de estándares de especificación RFC, que deben tener soporte, y se divide en siete categorías de dispositivos. Tenga en cuenta que el presente documento no incluye la categoría "dispositivo móvil", sino que incorpora dichos dispositivos en la categoría de "hosts".

Aquí también se aplica el documento de requerimientos de nodos de IPv6: RFC8504 (la actualización de la RFC6434). Esta RFC contiene pautas y consensos generales del IETF sobre qué partes del IPv6 deben implementar los distintos dispositivos, y su contenido se refleja en este documento a grandes rasgos.

1.1 Información general sobre cómo utilizar el presente documento

Este documento no impone el uso de tecnologías específicas, sino que supone que se ha producido un diseño o una solución de red y que dicho diseño, y los componentes que utiliza, deben estar correlacionados con el documento de adquisición.

Puede que los hosts, enrutadores y enrutadores CPE deban contar con un certificado IPv6 Ready Logo. Si bien la certificación Logo se diseñó hace aproximadamente 20 años, sigue vigente en las actualizaciones de estándares de IPv6 y es un programa con aceptación mundial que permite que los proveedores promuevan sus equipos y garanticen el cumplimiento de los requerimientos básicos del IPv6 por parte de dichos equipos. Las últimas actualizaciones de IPv6 Ready Logo exigen que los dispositivos se prueben en entornos exclusivamente del IPv6 y que tengan el IPv6 habilitado como valor predeterminado. El iniciador de la licitación también debe proporcionar una lista de RFC obligatorias y opcionales para evitar excluir a proveedores cuyos equipos aún no realizaron las pruebas de certificación de IPv6 Ready Logo. De este modo, los licitadores públicos no pueden ser acusados de favorecer ningún tipo ni proveedor de equipos.

Para obtener más información acerca del programa IPv6 Ready Logo, visite: http://www.ipv6ready.org/

Al especificar la lista de RFC requeridas, debemos enumerar todos los requerimientos obligatorios, excepto las entradas que comienzan con: “Si se solicita [cierta funcionalidad]...”. Estas entradas son obligatorias únicamente si el iniciador de la licitación solicita una funcionalidad determinada. Asimismo, si las características que se incluyen como opcionales son necesarias para el caso de uso específico del iniciador de la licitación, dichos requerimientos entonces se volverán obligatorios. Tenga en cuenta que es el iniciador de la licitación, no el proveedor de equipos, quien debe decidir qué funcionalidad se requiere. El presente documento es simplemente una plantilla.

1.2 Cómo especificar los requerimientos

Como mencionamos anteriormente, el programa IPv6 Ready Logo no cubre todos los equipos que son compatibles correctamente con el IPv6, por lo que no sería conveniente afirmar que tales equipos no son elegibles. El presente documento recomienda que el iniciador de la licitación especifique que los equipos elegibles tengan la certificación del programa IPv6 Ready Logo o bien cumplan con las RFC aplicables incluidas en la sección de más abajo.

Nota importante para el iniciador de la licitación:
La certificación de IPv6 Ready Logo cubre los requerimientos básicos de IPv6 y algunas funciones avanzadas, pero no todas. Si necesita una función avanzada que no está cubierta por la certificación de IPv6 Ready Logo, solicite una lista de RFC que cubra sus necesidades específicas además de la certificación de IPv6 Ready Logo. En las listas de más abajo, las RFC que están cubiertas por la

certificación de IPv6 Ready Logo están marcadas con un asterisco (*).

2 Texto genérico propuesto para el iniciador de la licitación

El siguiente texto debe incluirse en toda licitación:

Todo el hardware y el software de TIC que sea objeto de esta licitación debe ser compatible con el protocolo IPv6, y DEBE operar en un entorno exclusivamente de IPv6. Por ejemplo, cuando se use el SNMP, este debe ser capaz de operar sobre el transporte del IPv6.

Si el IPv4 es compatible, se debe brindar un rendimiento y capacidades similares para ambos protocolos en términos de entrada, salida o rendimiento del flujo de datos del caudal, transmisión y procesamiento de paquetes. La diferencia debe pasar desapercibida para los usuarios.

La compatibilidad con el IPv6 se puede verificar y certificar mediante el certificado de IPv6 Ready Logo.

Los equipos que no se hayan probado a través de los procedimientos de prueba de IPv6 Ready Logo deben cumplir, según corresponda, con las siguientes RFC obligatorias y opcionales:

[Insertar la lista correspondiente de RFC obligatorias y opcionales de las listas que se incluyen más abajo]

3 Categorías de dispositivos alcanzados en el presente documento

Los requerimientos se dividen en equipos de hardware y soporte del integrador.

Todos los requerimientos impuestos en las capacidades de tráfico del IPv4, como la latencia, el ancho de banda y el caudal, o para el monitoreo y la contabilización, también serán obligatorios para el tráfico del IPv6.

3.1 Definiciones y descripciones de las diferentes categorías de dispositivos

Las siguientes definiciones se utilizarán para clasificar los diversos equipos de hardware. Si bien algunos tipos de hardware pueden tener funcionalidades que se superponen (p. ej., un switch capa 2 puede funcionar como un enrutador capa 3 o un enrutador puede tener las capacidades de un cortafuegos), se espera que, cuando haya funcionalidades superpuestas, se combinen los requerimientos de cada dispositivo específico.

Tenga en cuenta que la categoría de “dispositivo móvil” incluida en el ripe-554 ha sido eliminada. Dichos dispositivos ahora entran en la categoría de “host”, ya que solo se los considera por su conectividad a la infraestructura local (a través de Wi-Fi) y, por lo tanto, los requerimientos relacionados con el 3GPP no están alcanzados en este documento.

Host: es una red participante que envía y recibe paquetes, pero no los reenvía en nombre de otros. Aquí se incluyen los dispositivos móviles que se conectan a la infraestructura de red local.

Los dispositivos host en una empresa pueden ser múltiples (p. ej., los dispositivos móviles) o pueden ser dispositivos con una red e interfaz de administración distinta. El IETF lleva varios años trabajando para desarrollar enfoques que contemplen el *multihoming* para el IPv6. En este documento, se incluyen requerimientos específicos [RFC4191].

Switch o switch capa 2: es un dispositivo que se usa principalmente para reenviar tramas de Ethernet en base a sus atributos. Generalmente, el intercambio de información de Ethernet con otros switches de Ethernet es parte de su función. Esta categoría, además, se divide en el nivel de usuario (para el uso doméstico, por lo general) y el nivel de empresa/ISP.

Técnicamente, los puntos de acceso a Wi-Fi no son dispositivos puros de capa 2, pero deberían desempeñar (en lo posible, en cooperación con un controlador inalámbrico) las mismas funcionalidades que un switch capa 2 en lo que respecta a las funcionalidades del IPv6. Por lo tanto, el texto de esta sección también podría usarse para los puntos de acceso a Wi-Fi.

Enrutador o switch capa 3: es un dispositivo que se usa principalmente para reenviar paquetes IP en base a sus atributos. Generalmente, el intercambio de información de enrutamiento con otros enrutadores es parte de su función.

Equipos de seguridad de red: son dispositivos cuya función principal es permitir, denegar o monitorear el tráfico entre interfaces con el fin de detectar o prevenir posibles actividades maliciosas. Tales interfaces también pueden incluir las VPN (SSL o IPsec). Los equipos de seguridad de red son también, a menudo, switches capa 2 o enrutadores/switches capa 3.

Equipo local del cliente (CPE): un dispositivo CPE es un enrutador de oficinas pequeñas u hogares que se usa para conectar a los usuarios en sus viviendas u oficinas en una gran variedad de configuraciones. Si bien un CPE usualmente es un enrutador, los requerimientos son diferentes de los de un enrutador empresarial/ISP o un switch capa 3. Los CPE, por lo general, deben soportar mecanismos de transición al IPv6. Este documento se enfocará fundamentalmente en los métodos de transición para redes exclusivamente de IPv6.

Balanceador de carga: es un dispositivo de red que distribuye la carga de trabajo de múltiples computadoras, servidores u otros recursos, para lograr una utilización de recursos óptima o planificada, maximizar el caudal, minimizar el tiempo de respuesta y evitar la sobrecarga.

Las siguientes referencias tienen relevancia en este documento de BCP. Al momento de su publicación, las ediciones indicadas eran válidas. Todas las referencias están sujetas a revisión. Se recomienda a los usuarios de este documento de BCP, por lo tanto, que investiguen si existe una edición más reciente de las referencias enumeradas más abajo.

3.2 Qué está fuera del alcance del presente documento

En aras de llegar al consenso para publicar una actualización del ripe-554 tan eficientemente como fuera posible, los autores minimizaron la incorporación de nuevos tipos de dispositivos. Puede que se los incorpore en una actualización futura o en una actualización por separado.

Como señalamos anteriormente, los dispositivos móviles se tienen en cuenta en este documento solo con respecto a su conectividad a una infraestructura empresarial (usualmente por Wi-Fi) y, en este aspecto, son considerados hosts.

Tenga en cuenta que las máquinas virtuales (VM) y los contenedores no se contemplan aquí. Estas funciones pueden ser provistas en sistemas adquiridos como hosts mediante esta guía, pero no son "equipos de TIC" en sí mismos.

Si bien la RFC8504 contiene una sección sobre YANG para la administración de la red, no se incluyen otros requerimientos de YANG en este documento.

Ciertas funciones nuevas de enrutamiento que emergieron recientemente tampoco se incorporaron hasta el momento, tales como SRv6 [RFC8986].

4 Listas de estándares RFC para las diferentes categorías de hardware

En el presente documento, el hardware de TIC se divide en siete grupos funcionales:

- Host: cliente (incluidos los dispositivos móviles) o servidor
- Switch capa 2 a nivel del consumidor
- Switch capa 2 a nivel empresarial/ISP
- Enrutador o switch capa 3
- Equipos de seguridad de red (cortafuegos, IDS, IPS, etc.)
- Equipos CPE
- Balanceador de carga

Hemos dividido los requerimientos a continuación en dos tipos: obligatorios y opcionales. Los equipos deben cumplir los requerimientos obligatorios de los estándares de la lista. El cumplimiento de los requerimientos opcionales puede otorgarle al licitador puntos adicionales, si así lo especifica el iniciador de la licitación.

El hardware que no cumpla **todos** los estándares obligatorios debe ser calificado como "inadecuado" por parte del evaluador de la licitación.

Los estándares que son parte de los procedimientos de prueba de IPv6 Ready Logo, usualmente llevados a cabo por laboratorios acreditados, están marcados con un asterisco (*).

4.1 Requerimientos para equipos “host”

Soporte obligatorio:

- Especificación básica de IPv6 [RFC8200/STD86] *
- Arquitectura de direcciones IPv6 [RFC4291] *
- Selección de direcciones predeterminadas para IPv6 [RFC6724]
- Direcciones Unicast IPv6 locales únicas (ULA) [RFC4193]
- ICMPv6 [RFC4443/STD89] *
- Si se solicita soporte para DHCPv6, el dispositivo debe ser compatible con:
    - Cliente DHCPv6 con estado [RFC8415] *
    - Cliente DHCPv6 sin estado [RFC8415] *
    - Opciones de configuración del DNS para el Protocolo de configuración dinámica de host para IPv6 (DHCPv6) [RFC3646] *
    - Un método para generar identificadores de interfaz (IID) semánticamente opacos con el Protocolo de configuración dinámica de host para IPv6 (DHCPv6) [RFC7943]
- SLAAC [RFC4862] *
- Descubrimiento de MTU de ruta [RFC8201/STD87] *
- Descubrimiento de vecinos [RFC4861] [RFC6980] *
- Extensiones del protocolo DNS para incorporar registros de recurso de DNS para IPv6 [RFC3596/STD88]
- Mecanismo de extensión de mensajes del DNS [RFC6891/STD75]
- Requerimientos de tamaño de mensajes del DNS [RFC3226]
- Transmisión de paquetes IPv6 sobre redes Ethernet [RFC2464]
- Implicancias de seguridad de la fragmentación IPv6 con descubrimiento de vecinos IPv6 [RFC6980]
- Actualizaciones de la arquitectura de direcciones Multicast IPv6 [RFC7371]
- Un método para generar identificadores de interfaz semánticamente opacos con autoconfiguración de direcciones sin estado IPv6 (SLAAC) [RFC7217]
- Opciones de anuncios de enrutador IPv6 para la configuración del DNS [RFC8106]
- Descubrimiento de receptores Multicast, versión 2 [RFC3810] *
- Preferencias de enrutador predeterminadas y rutas más específicas: Roles de host tipo A y B [RFC4191]
- Si se solicita soporte para túnel o pila doble, el dispositivo debe ser compatible con los Mecanismos de transición básicos de hosts y enrutadores IPv6 [RFC4213]
- Especificación de etiqueta de flujo de IPv6 [RFC6437]

Soporte opcional:

- ICMP extendido para mensajes multiparte [RFC4884]
- Extensiones de direcciones temporarias para la autoconfiguración de direcciones sin estado en IPv6 [RFC8981]
- DS (clase de tráfico) [RFC2474, RFC3140]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79, RFC7619, RFC8221, RFC8247] *
- Protocolo SNMP [RFC3411]

- Capacidades del SNMP [RFC3412, RFC3413, RFC3414]
- MIB del SNMP para IP [RFC4293] Reenvío [RFC4292] y DiffServ [RFC3289]
- Descubrimiento de MTU de ruta de la capa de paquetización [RFC4821] [RFC8899]
- Compartición de carga entre host y enrutador IPv6 [RFC4311]
- Preferencias de enrutador predeterminadas y rutas más específicas: Roles de host tipo C [RFC4191]
- Opción de marcadores de anuncios de enrutador IPv6 [RFC5175]
- La incorporación de Notificación de congestión explícita (ECN) a IP [RFC3168]
- Selección de enrutador de primer salto por hosts en una red de prefijos múltiples [RFC8028].
- Política de selección de distribución de direcciones usando DHCPv6 [RFC7078]
- Para una mayor privacidad de direcciones IPv6, se debe considerar la compatibilidad con las "Consideraciones de seguridad y privacidad para los mecanismos de generación de direcciones IPv6" [RFC7721] y las "Recomendaciones sobre identificadores de interfaz IPv6 estables" [RFC8064]
- "MIPv6" [RFC6275, RFC5555] y "Operación IPv6 móvil con IKEv2 y la arquitectura IPsec modificada" [RFC4877]
- Descubrimiento de PREF64 en anuncios de enrutadores [RFC8781]

4.2 Requerimientos para equipos "switch capa 2" a nivel de usuario

Soporte opcional (administración):

- MLDv2 snooping [RFC4541]
- Especificación básica de IPv6 [RFC8200/STD86] *
- Arquitectura de direcciones IPv6 [RFC4291] *
- Selección de direcciones predeterminadas para IPv6 [RFC6724]
- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- Descubrimiento de vecinos [RFC4861] [RFC6980] *
- Protocolo SNMP [RFC3411]
- Capacidades del SNMP [RFC3412, RFC3413, RFC3414]
- MIB del SNMP para IP [RFC4293] Reenvío [RFC4292] y DiffServ [RFC3289]
- Transmisión de paquetes IPv6 sobre redes Ethernet [RFC2464]

4.3 Requerimientos para equipos "switch capa 2" a nivel de empresa/ISP

Soporte obligatorio (plano de reenvío de datos):

- Transmisión de paquetes IPv6 sobre redes Ethernet [RFC2464]
- MLDv2 snooping [RFC4541]
- Guardia de anuncios de enrutador (RA) [RFC6105] y [RFC7113]
- DHCPv6-Shield: Protección contra servidores DHCPv6 falsos [RFC7610]
- Inspección dinámica de "solicitud/anuncios de vecinos IPv6" [RFC4861]
- Filtrado de detección de vecinos inalcanzables [NUD, RFC4861]
- Snooping y filtrado de detección de direcciones duplicadas [DAD, RFC4429]
- Si se solicita soporte para DHCPv6, el dispositivo debe ser compatible con:
    - Agente de retransmisión DHCPv6 ligero [RFC6221]

    - Opción de identificación remota de agente de retransmisión DHCPv6 [RFC4649]
    - Opción de identificación de suscriptor de agente de retransmisión DHCPv6 [RFC4580]
    - Opción de dirección de capa de enlace del cliente DHCPv6 [RFC6939]

Soporte obligatorio (administración; el dispositivo debe funcionar como host IPv6 para la administración):

- Especificación básica de IPv6 [RFC8200/STD86] *
- Arquitectura de direcciones IPv6 [RFC4291] *
- Selección de direcciones predeterminadas para IPv6 [RFC6724]
- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- Si se requiere soporte para el SNMP:
    - Protocolo SNMP [RFC3411]
    - Capacidades del SNMP [RFC3412, RFC3413, RFC3414]
    - MIB del SNMP para IP [RFC4293] Reenvío [RFC4292] y DiffServ [RFC3289]
- Filtrado de encabezado de enrutamiento IPv6 [RFC8200, próximo valor de encabezado 43] *

Soporte opcional:

- Solución de mejora de validación de la dirección de origen (SAVI) para DHCP [RFC7513]

4.4 Requerimientos para equipos “enrutador o switch capa 3”

Soporte obligatorio:

- Especificación básica de IPv6 [RFC8200/STD86] *
- Transmisión de paquetes IPv6 sobre redes Ethernet [RFC2464]
- Arquitectura de direcciones IPv6 [RFC4291] *
- Selección de direcciones predeterminadas para IPv6 [RFC6724]
- Direcciones Unicast IPv6 locales únicas (ULA) [RFC4193]
- Si se solicita soporte para DHCPv6, el dispositivo debe ser compatible con:
    - Cliente/servidor/retransmisión DHCPv6 [RFC8415] *
    - Opción de identificación remota de agente de retransmisión DHCPv6 [RFC4649]
    - Opción de identificación de suscriptor de agente de retransmisión DHCPv6 [RFC4580]
    - Opción de dirección de capa de enlace del cliente DHCPv6 [RFC6939]
- ICMPv6 [RFC4443/STD89] *
- SLAAC [RFC4862] *
- Opciones de anuncios de enrutador IPv6 para la configuración del DNS [RFC8106] *
- MLDv2 snooping [RFC4541]
- Descubrimiento de receptores Multicast, versión 2 [RFC3810] *
- Actualizaciones de la arquitectura de direcciones Multicast IPv6 [RFC7371]
- Descubrimiento de MTU de ruta [RFC8201/STD87] *
- Descubrimiento de vecinos [RFC4861] [RFC6980] *
- Prefijos IPv6 de 127 bits en enlaces entre enrutadores [RFC6164]
- Recomendaciones de longitud de prefijos IPv6 para el reenvío [RFC7608] *
- Si se requiere soporte para el SNMP:
    - Protocolo SNMP [RFC3411]
    - Capacidades del SNMP [RFC3412, RFC3413, RFC3414]

    - MIB del SNMP para IP [RFC4293] Reenvío [RFC4292] y DiffServ [RFC3289]
- Si se solicita un protocolo de gateway interior (IGP) dinámico, se debe tener compatibilidad con RIPng [RFC2080], OSPFv3 [RFC5340] [RFC5613] o IS-IS [RFC5308]. La autoridad contratante debe especificar el protocolo requerido.
- Si se solicita OSPFv3, los equipos deben cumplir la "Autenticación/confidencialidad para OSPFv3" [RFC4552] o el "Trailer de autenticación de soporte para OSPFv3" [RFC7166].
- Si se solicitan OSPFv3 y SNMP, el dispositivo debe ser compatible con la "Base de información para gestión para OSPFv3" [RFC5643].
- Si se solicita el protocolo BGP4, los equipos deben ser compatibles con [RFC4271], [RFC1772], [RFC4760], [RFC1997], [RFC3392], [RFC2545], [RFC5492], [RFC6268], [RFC6608], [RFC6793], [RFC7606], [RFC7607], [RFC7705] y [RFC8212].
- Si se solicita el protocolo VRRP, los equipos deben cumplir con [RFC5798].
- Si se solicita el protocolo PIM-SM, los equipos deben cumplir con [RFC 7761/STD83] y [RFC5059].
- Soporte para QoS [RFC2474, RFC3140]
- Si se solicita soporte para túnel o pila doble, el dispositivo debe ser compatible con los Mecanismos de transición básicos de hosts y enrutadores IPv6 [RFC4213]
- Si se solicita soporte para túnel o pila doble, el dispositivo debe ser compatible con los Túneles de paquetes genéricos e IPv6 [RFC2473]
- Si se solicita 6PE, los equipos deben soportar la "Conexión de islas IPv6 sobre IPv4 MPLS usando enrutadores Provider Edge IPv6 (6PE)" [RFC4798]
- Si se solicita IPv6 móvil, los equipos deben soportar MIPv6 [RFC3775, RFC5555] y la "Operación IPv6 móvil con IKEv2 y la arquitectura IPsec modificada" [RFC4877]
- Si se solicita la funcionalidad MPLS (por ejemplo, core sin BGP, MPLS TE, MPLS FRR), los enrutadores PE y los reflectores de ruta deben soportar la "Conexión de islas IPv6 sobre IPv4 MPLS usando enrutadores Provider Edge IPv6 (6PE)" [RFC4798]
- Si se usa ingeniería de tráfico MPLS junto con el protocolo de enrutamiento IS-IS, los equipos deben soportar "M-ISIS: Enrutamiento de tipología múltiple (MT) en sistema intermediario a sistema intermediario (IS-IS)" [RFC5120]
- Si se solicita la funcionalidad de VPN de capa 3, los enrutadores PE y los reflectores de ruta deben soportar la "Extensión de Red privada virtual (VPN) de BGP-MPLS IP para VPN IPv6" [RFC4659].
- Especificación de etiqueta de flujo de IPv6 [RFC6437]

Soporte opcional:

- ICMP extendido para mensajes multiparte [RFC4884]
- Extensiones de privacidad SLAAC [RFC4941]
- DHCPv6 sin estado [RFC8415] *
- Delegación de prefijos DHCPv6 [RFC8415] *
- LeaseQuery masivo DHCPv6 [RFC5460]
- LeaseQuery activo DHCPv6 [RFC7653]
- (QOS) Reenvío asegurado [RFC2597]
- (QOS) Reenvío acelerado [RFC3246]
- (QOS) Soporte de gestión de fila activa [RFC7567]

- Encapsulación de enrutamiento genérico [RFC2784]
- IPsec/IKEv2 (plano de control) [RFC4301, RFC4303, RFC7268, RFC8221, RFC 8247] *
- IPsec/IKEv2 VPN (plano de datos) [RFC4301, RFC4303], RFC7269, RFC8221] *
- Uso de IPsec para brindar seguridad a los túneles de IPv6 a IPv4 [RFC4891]
- Extensiones del protocolo DNS para incorporar registros de recurso de DNS para IPv6 [RFC3596/STD88]
- Mecanismo de extensión de mensajes del DNS [RFC6891/STD75]
- Requerimientos de tamaño de mensajes del DNS [RFC3226]
- Descubrimiento de MTU de ruta de la capa de paquetización [RFC4821]
- Compartición de carga entre host y enrutador IPv6 [RFC4311]
- Preferencias predeterminadas de enrutador y rutas más específicas [RFC4191]
- Descubrimiento de PREF64 en anuncios de enrutadores [RFC8781]

4.5 Requerimientos para equipos de “seguridad de red”

Los equipos en esta sección se dividen en tres subgrupos:

- Cortafuegos (FW)
- Sistemas de prevención de intrusos (IPS)
- Cortafuegos de aplicación (APFW)

Cada estándar obligatorio incluye, entre paréntesis y al final del renglón, los subgrupos a los que aplica.

Soporte obligatorio:

- Especificación básica de IPv6 [RFC8200/STD86] (FW, IPS, APFW) *
- Arquitectura de direcciones IPv6 [RFC4291] (FW, IPS, APFW)
- Selección de direcciones predeterminadas para IPv6 [RFC6724] (FW, IPS, APFW)
- ICMPv6 [RFC4443/STD89] (FW, IPS, APFW) *
- Transmisión de paquetes IPv6 sobre redes Ethernet [RFC2464]
- SLAAC [RFC4862] (FW, IPS) *
- Si se requiere soporte para el SNMP:
    - Protocolo SNMP [RFC3411]
    - Capacidades del SNMP [RFC3412, RFC3413, RFC3414]
    - MIB del SNMP para IP [RFC4293] Reenvío [RFC4292] y DiffServ [RFC3289]
- Opciones de anuncios de enrutador IPv6 para la configuración del DNS [RFC8106] (FW)
- Inspección del tráfico del protocolo-41 de IPv6 a IPv4, que se especifica en: Mecanismos de transición básicos para hosts y enrutadores IPv6 [RFC4213] (IPS)
- Descubrimiento de MTU de ruta [RFC8201/STD87] (FW, IPS, APFW) *
- Descubrimiento de vecinos [RFC4861] (FW, IPS, APFW) *
- Si se solicita el protocolo BGP4, los equipos deben cumplir con las siguientes solicitudes: RFC4271, RFC1772, RFC4760 y RFC2545 (FW, IPS, APFW)
- Si se solicita un protocolo de gateway interior (IGP) dinámico, se debe tener compatibilidad con RIPng [RFC2080], OSPFv3 [RFC5340] o IS-IS [RFC5308]. La autoridad contratante debe especificar el protocolo requerido. (FW, IPS, APFW)

- Si se solicita OSPFv3, los equipos deben cumplir la “Autenticación/confidencialidad para OSPFv3” [RFC4552] o el “Trailer de autenticación de soporte para OSPFv3” [RFC7166] (FW, IPS, APFW)
- Si se solicitan OSPFv3 y SNMP, el dispositivo debe ser compatible con la “Base de información para gestión para OSPFv3” [RFC5643]
- Soporte para QoS [RFC2474, RFC3140] (FW, APFW)
- Si se solicitan túneles, el dispositivo debe ser compatible con los Mecanismos de transición básicos de hosts y enrutadores IPv6 [RFC4213] (FW)

Los dispositivos de seguridad de red suelen ubicarse donde se ubicarían los switches capa 2 o enrutadores/switches capa 3. De dicha ubicación dependerán los requerimientos que deban cumplirse.

La funcionalidad y las funciones que sean compatibles con IPv4 deberán ser comparables con la funcionalidad compatible con IPv6. Por ejemplo, si un sistema de prevención de intrusos es capaz de operar sobre IPv4 en modo capa 2 y capa 3, también debería ofrecer esa funcionalidad sobre IPv6. Asimismo, si un cortafuegos opera en un clúster capaz de sincronizar sesiones IPv4 entre todos los miembros de un clúster, eso también debería ser posible con sesiones IPv6.

Soporte opcional:

- Cliente/servidor/retransmisión DHCPv6 [RFC8415] *
- DHCPv6 sin estado [RFC8415] *
- Delegación de prefijos DHCPv6 [RFC8415] *
- ICMP extendido para mensajes multiparte [RFC4884]
- Extensiones de privacidad SLAAC [RFC4941]
- Atributo de comunidades BGP [RFC1997]
- Anuncio de capacidades con BGP WITH-4 [RFC3392]
- (QOS) Reenvío asegurado [RFC2597]
- (QOS) Reenvío acelerado [RFC3246]
- Direcciones Unicast IPv6 locales únicas (ULA) [RFC4193]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79] *
- Uso de IPsec para brindar seguridad a los túneles de IPv6 a IPv4 [RFC4891] (FW)
- OSPFv3 [RFC5340]
- Autenticación/confidencialidad para OSPFv3 [RFC4552]
- Túneles de paquetes genéricos e IPv6 [RFC2473]
- Extensiones del DNS para dar soporte a IPv6 [RFC3596]
- Mecanismo de extensión de mensajes del DNS [RFC6891]
- Requerimientos de tamaño de mensajes del DNS [RFC3226]
- Uso de IPsec para brindar seguridad a los túneles de IPv6 a IPv4 [RFC4891]
- Descubrimiento de receptores Multicast, versión 2 [RFC3810] *
- MLDv2 snooping [RFC4541] (durante el modo capa 2 o passthrough) *
- Descubrimiento de MTU de ruta de la capa de paquetización [RFC4821] y [RFC8899]
- Configuración de IPv6 en el Protocolo de intercambio de claves de Internet, versión 2 (IKEv2) [RFC5739]

- Compartición de carga entre host y enrutador IPv6 [RFC4311]
- Preferencias predeterminadas de enrutador y rutas más específicas [RFC4191]
- Transmisión y procesamiento de encabezados de extensión IPv6 [RFC7045]

4.6 Requerimientos para equipos CPE

Soporte obligatorio:

- Requerimientos básicos para enrutadores Edge de cliente IPv6 [RFC7084] *
- Capacidades de seguridad simples recomendadas en los equipos locales del cliente (CPE) para la provisión del servicio de Internet residencial IPv6 [RFC6092]
- Si se solicita soporte para mecanismos de transición IPv4, el dispositivo debe soportar los requerimientos correspondientes, a partir de los Requerimientos para enrutadores Edge de cliente IPv6 para soportar IPv4 como servicio [RFC8585] y de Descubrimiento de PREF64 en anuncios de enrutadores [RFC8781]
- Si se requiere soporte para el SNMP:
    - Protocolo SNMP [RFC3411]
    - Capacidades del SNMP [RFC3412, RFC3413, RFC3414]
    - MIB del SNMP para IP [RFC4293] Reenvío [RFC4292] y DiffServ [RFC3289]

Soporte opcional:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296, RFC7619, RFC8221, RFC8247] *
- “MIPv6” [RFC6275, RFC5555] y “Operación IPv6 móvil con IKEv2 y la arquitectura IPsec modificada” [RFC4877]
- ICMP extendido para mensajes multiparte [RFC4884]
- Extensiones de privacidad SLAAC [RFC4941]
- Transmisión de paquetes IPv6 sobre redes Ethernet [RFC2464]
- (QOS) DS (clase de tráfico) [RFC2474, RFC3140]
- (QOS) Soporte de gestión de fila activa [RFC7567]
- Descubrimiento de receptores Multicast, versión 2 [RFC3810] *
- Descubrimiento de MTU de ruta de la capa de paquetización [RFC4821] y [RFC8899]
- Requerimientos para enrutadores Edge de cliente IPv6 para soportar IPv4 como servicio [RFC8585]
- Compartición de carga entre host y enrutador IPv6 [RFC4311]
- Preferencias predeterminadas de enrutador y rutas más específicas [RFC4191]

4.7 Requerimientos para balanceadores de carga

Los balanceadores de carga distribuyen las solicitudes o las conexiones entrantes de clientes a múltiples servidores. Los balanceadores de carga deberán soportar varias combinaciones de conexiones IPv4 e IPv6:

- Se **debe** soportar el balanceo de carga de clientes IPv6 a servidores IPv6 (6 a 6)
- Se **debe** soportar el balanceo de carga de clientes IPv6 a servidores IPv4 (6 a 4)
- Se **debe** soportar el balanceo de carga de clientes IPv4 a servidores IPv4 (4 a 4)
- Se **debe** soportar el balanceo de carga de clientes IPv4 a servidores IPv6 (4 a 6)

- Se **debe** soportar el balanceo de carga de una única dirección IPv4 externa/virtual a un conjunto mixto de servidores IPv4 e IPv6
- Se debe soportar el balanceo de carga de una única dirección IPv6 externa/virtual a un conjunto mixto de servidores IPv4 e IPv6

Soporte obligatorio:

- Especificación básica de IPv6 [RFC8200/STD86] *
- Arquitectura de direcciones IPv6 [RFC4291] *
- Selección de direcciones predeterminadas [RFC6274]
- Transmisión de paquetes IPv6 sobre redes Ethernet [RFC2464]
- Direcciones Unicast IPv6 locales únicas (ULA) [RFC4193]
- ICMPv6 [RFC4443/STD89] *
- Descubrimiento de MTU de ruta [RFC8201/STD87] *
- Descubrimiento de vecinos [RFC4861] *
- Opciones de anuncios de enrutador IPv6 para la configuración del DNS [RFC8106]
- Extensiones del protocolo DNS para incorporar registros de recurso de DNS para IPv6 [RFC3596/STD88]
- Mecanismo de extensión de mensajes del DNS [RFC6891]
- Requerimientos de tamaño de mensajes del DNS [RFC3226]
- Si se solicita balanceo de carga de capa 7 (a nivel de aplicación/proxy inverso, conocido como "subrogado" en la sección 2.2 de la RFC3040), los equipos deben soportar la "Extensión de HTTP reenviado [RFC7239]" tanto para direcciones de clientes IPv4 como IPv6
- Si se solicita balanceo de carga de capa 7 (a nivel de aplicación/proxy inverso, conocido como "subrogado" en la sección 2.2 de la RFC3040), los equipos deben soportar la "Versión 1.3 del Protocolo de seguridad de la capa de transporte (TLS) [RFC8446]"
- Si se solicita soporte para IPsec, el dispositivo debe soportar IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC7296/STD79] * y el Mecanismo de redirección para la versión 2 del Protocolo de intercambio de claves de Internet (IKEv2) [RFC5685]
- Si se solicita soporte para BGP4, los equipos deben cumplir con las siguientes: RFC4271, RFC1772, RFC4760 y RFC2545
- Si se solicita soporte para un protocolo de gateway interior (IGP) dinámico, se debe tener compatibilidad con RIPng [RFC2080], OSPFv3 [RFC5340] o IS-IS [RFC5308]. La autoridad contratante debe especificar el protocolo requerido.
- Si se solicita soporte para OSPFv3, el dispositivo debe ser compatible con la "Autenticación/confidencialidad para OSPFv3" [RFC4552]

Soporte opcional:

- ICMP extendido para mensajes multiparte [RFC4884]
- DS (clase de tráfico) [RFC2474, RFC3140]
- Protocolo SNMP [RFC3411]
- Capacidades del SNMP [RFC3412, RFC3413, RFC3414]
- MIB del SNMP para IP [RFC4293] Reenvío [RFC4292] y DiffServ [RFC3289]
- Descubrimiento de receptores Multicast, versión 2 [RFC3810] *
- Descubrimiento de MTU de ruta de la capa de paquetización [RFC4821]

- NAT64/DNS64 [RFC6146, RFC6147]
- Compartición de carga entre host y enrutador IPv6 [RFC4311]
- Preferencias predeterminadas de enrutador y rutas más específicas [RFC4191]

5 Requerimientos para el soporte de IPv6 en software

Todo software debe soportar IPv6 y ser capaz de comunicar sobre redes exclusivamente de IPv6 y redes de pila doble. Si el software incluye parámetros de red en los ajustes de servidores locales o remotos, debe soportar la configuración de parámetros IPv6. El usuario no debería percibir ninguna diferencia notable cuando el software se comunique sobre IPv4 o IPv6, a menos que hacerlo le brinde un beneficio evidente al usuario.

Los desarrolladores/proveedores de software deben llevar a cabo, como mínimo, las siguientes acciones para garantizarlo:

- Se recomienda explícitamente no usar direccionamiento literal en el código de software, tal como se describe en la "Selección de direcciones predeterminadas para el Protocolo de Internet, versión 6" [RFC6724].
- Donde se gestionen direcciones IP en el software (como en las interfaces de usuario, los análisis de configuración o donde se procesen datos), se deben soportar todas las notaciones de direcciones IPv6 válidas, tal como se especifica en la "Versión 6 del IP, Arquitectura de direcciones [RFC4291]".
- Donde se muestren o salgan direcciones IPv6, debe seguirse la notación especificada en la "Recomendación para la representación de texto de direcciones IPv6 [RFC5952]".
- La resolución de nombres de host en el DNS debe soportar respuestas IPv6 (AAAA).
- La conexión a otros sistemas y la recepción de conexiones de parte de otros sistemas debe soportar conexiones IPv6 usando los mecanismos de sistema correspondientes (p. ej., sockets de red).
- Al establecer una conexión, el software debe seguir la selección de direcciones predeterminadas para el protocolo de Internet, versión 6 [RFC6724] o la versión 2 de Happy Eyeballs: Mejor conectividad usando concurrencia [RFC8305].
- Estos requerimientos deben revisarse también en cualquier biblioteca o herramienta

utilizadas por el software. La lista brindada no es exhaustiva y solo cubre los requerimientos

básicos.

El libro blanco "Dependencia a la versión IP en software de aplicación: preparación del código fuente para IPv6"[1] de la Netherlands IPv6 Foundation puede utilizarse como puntapié para los desarrolladores.

6 IPsec: obligatorio u opcional

En la RFC de los Requerimientos de nodos IPv6 originales (RFC4294), IPsec era una implementación obligatoria para estar en cumplimiento con los estándares. La RFC de los Requerimientos de nodos actualizada (RFC6434), publicada en 2011, modificó dicha obligatoriedad y adquirió un carácter de implementación recomendada. En la RFC mencionada se indicaron los motivos de tal cambio.

El Grupo de Trabajo de IPv6 de RIPE ha analizado exhaustivamente si el soporte de IPsec debería ser obligatorio u opcional. Al finalizar el ripe-554, los integrantes más expresivos mostraron su apoyo por incluir el IPsec en la sección de los soportes opcionales, lo cual también se refleja en el documento actualizado.

Si bien el consenso de la comunidad fue hacer que el IPsec fuera opcional en la mayoría de los casos, el IETF confirmó en el 2019, en la versión más reciente del estándar de Requerimientos de nodos IPv6 (RFC8504), que debería implementarse como una recomendación, no como una obligación. En el contexto del IETF, una recomendación implica que pueden existir razones válidas en circunstancias particulares para ignorar un elemento específico, pero las implicancias totales deben comprenderse y sopesarse detenidamente antes de elegir un camino distinto.

Las organizaciones que usan IPsec o tienen pensado hacerlo en un futuro deberían incluir lo siguiente en la sección de soporte obligatorio al iniciar la licitación:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC8221, RFC7296 RFC7619 y RFC 8247] *

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

El conjunto actual de algoritmos que deben implementarse obligatoriamente para la arquitectura IPsec se define en los Requerimientos de implementación de algoritmos criptográficos para ESP y AH [RFC8221]. Los nodos IPv6 que implementen la arquitectura IPsec DEBEN cumplir obligatoriamente los requerimientos establecidos en [RFC8221].

El conjunto actual de algoritmos que deben implementarse obligatoriamente para IKEv2 se define en los Requerimientos de implementación de algoritmos criptográficos para ESP y AH [RFC8247]. Los nodos IPv6 que implementen IKEv2 DEBEN cumplir obligatoriamente los requerimientos establecidos en [RFC8247] o en cualquier actualización o reemplazo de [RFC8247] en el futuro.

Si bien se suponía que el encabezado de autenticación especificado en la RFC4302 debía brindar integridad y no repudio, debido a que no pudo atravesar las NAT, el uso de ESP nulo (null) se volvió una práctica común. Como se indica en la Sección 13.1 de la RFC8504, que deviene de la RFC4301, los nodos IPv6 que implementen arquitectura IPsec “DEBEN” implementar ESP (RFC4303) y “PUEDEN” implementar AH (RFC4302).

7 Requerimientos de habilidades del integrador de sistemas

Los proveedores y distribuidores que ofrecen servicios de integración de sistemas deben contar con, al menos, tres empleados que tengan una certificación válida de competencia emitida por los fabricantes de los equipos para todos los equipos que se vendan como parte de la licitación. Además, dichos empleados deben contar con conocimiento general del protocolo IPv6, la planificación de red IPv6 y la seguridad del IPv6 (p. ej., como lo indica la certificación de estas habilidades). Si resulta obvio durante la instalación e integración de los equipos que el conocimiento, las competencias y la experiencia del integrador no son suficientes para instalarlos y configurarlos satisfactoriamente para obtener una comunicación IPv4 e IPv6 normal con la red, el acuerdo procederá a cancelarse y declararse nulo.

La definición de qué implica la integración, la sincronización y el grado de disrupción adecuados de la red durante la instalación debe ser producto de un acuerdo entre el cliente y el integrador de sistemas.

También se recomienda que el integrador de sistemas y sus empleados tengan amplio conocimiento sobre el IPv6 y los certificados IPv6 genéricos más allá de aquellos ofrecidos específicamente por los fabricantes de los equipos. Estos certificados se pueden obtener de proveedores de educación independientes. Dicho conocimiento puede adjudicar puntos extra en el proceso de licitación.

Todos los licitadores en el proceso de licitación deben firmar el siguiente formulario, el cual indica que la empresa y sus empleados han aprobado la capacitación técnica para el diseño, la construcción y la integración de los equipos de TIC en las redes IPv4 e IPv6.

7.1 Declaración de competencia en IPv6

Los iniciadores de la licitación deben exigir una declaración de competencia técnica en IPv6 al proveedor o integrador de los equipos. Se exige conocimiento y experiencia en IPv6 para garantizar una instalación e integración adecuadas de los equipos en el entorno TIC del IPv6.

La declaración debe manifestar que el proveedor de los equipos o el integrador de sistemas declara bajo responsabilidad penal y material que:

- cuenta con una cantidad suficiente de personal para prestar los servicios que ofrece;
- dichos empleados están capacitados profesionalmente para cumplir sus tareas de diseño, construcción e integración de equipos de TIC en redes y entornos de IPv4 e IPv6;
- la calidad de los servicios ofrecidos cumple los requerimientos impuestos en los documentos de licitación, y que dichos requerimientos se aplican tanto al IPv4 como al IPv6.

Tenga en cuenta que las declaraciones de este estilo pueden variar según la legislación local. Por lo tanto, los iniciadores y traductores de la licitación deberían recibir asesoramiento legal para la redacción de dichos requerimientos.

8 Agradecimientos

La primera versión (eslovena) de este documento se creó en el consejo experto Go6 y el grupo de trabajo de IPv6 esloveno en el 2009.

Los autores originales desean agradecer a todos aquellos que formaron parte de la creación y modificación de la primera versión de este documento (ripe-501, año 2009). En primer lugar, queremos agradecer a Janez Sterle, Urban Kunc, Matjaz Straus, Simeon Lisec, Davor Sostaric y Matjaz Lenassi del consejo de expertos Go6 por su apasionada gestión del presente documento. Reconocemos el trabajo realizado por el grupo de trabajo de IPv6 esloveno en materia de revisión y contribuciones útiles y dedicamos un reconocimiento especial a Ivan Pepelnjak, Andrej Kobal y Ragnar Us por su trabajo y esfuerzo puesto en este documento. Agradecemos también a los copresidentes del grupo de trabajo de IPv6 de RIPE, David Kessens, Shane Kerr y Marco Hogewoning, por su apoyo y aliento. También queremos agradecer a Patrik Fältström, Torbjörn Eklöv, Randy Bush, Matsuzaki Yoshinobu, Ides Vanneuville, Olaf Maennel, Ole Trøan, Teemu Savolainen y a los integrantes del WG de IPv6 de RIPE (Joao Damas, S.P. Zeidler, Gert Doering, entre otros) por sus contribuciones, comentarios y revisión del documento. Por último, pero no menos importante, queremos dar las gracias a Chris Buckridge de RIPE-NCC por la corrección de la gramática y la redacción del presente documento. Y gracias también a todas las demás personas que contribuyeron en este trabajo.

Los autores de la versión anterior del documento (ripe-554, año 2012) agradecen al WG de IPv6 de RIPE y a sus presidentes por todo el apoyo y la motivación para elaborar la versión actualizada del documento. Agradecemos especialmente a Ole Trøan, editor de la RFC6204, por su ayuda en la sección sobre CPE y por sugerir otros cambios a lo largo del documento. Gracias a Marco Hogewoning, Ivan Pepelnjak y S.P. Zeidler por sus valiosas contribuciones e ideas sobre cómo estructurar el documento y presentar el contenido de una mejor manera, y a Timothy Winters y Erica Johnson (ambos del Comité de IPv6 Ready Logo, UNH) por su ayuda en la identificación de las RFC que ellos testean y por sus críticas constructivas. Agradecemos también a Yannis Nikolopoulos y Frits Nolet. Gracias especiales a Jouni Korhonen, Jari Arkko, Eric Vyncke, David Freedman, Tero Kivinen y Michael Richardson por sus valiosos aportes y sugerencias, que nos ayudaron a mejorar este documento.

Los autores de la versión actual del documento agradecen también a los miembros del WG de IPv6 de RIPE y sus presidentes y, en especial, a Jens Link, Martin Schröder, Fernando Gont, Enno Rey, Dave Taht, Azalea Fernandez, Yannis Nikolopoulos y Eric Vyncke por sus comentarios.

Cualquier sugerencia o comentario que contribuya a la mejora del documento actual puede enviarse a las listas de correo electrónico del WG de IPv6 de RIPE o de TF de BCOP de RIPE.
https://www.ripe.net/mailman/listinfo/ipv6-wg/
https://www.ripe.net/mailman/listinfo/bcop