Requerimientos de IPv6 para equipos de TIC

Fecha: 27/01/2016

Tutor: Jan Zörz

Documentos de Referencia: RIPE-554

Traductores: Azael Fernández Alcántara, Ernesto Pérez Estévez, Ariel Weher, otros (agregar)

Expertos en la materia (SME):

Estado: BCOP

Asunto del BCOP: Requerimientos de IPv6 para equipos de TIC

Best Current Operational Practice (BCOP)

==

1. Resumen del BCOP

Para asegurar la inserción suave y rentable de IPv6 en sus redes, es importante que los gobiernos y las grandes corporaciones especifiquen requerimientos de compatibilidad de IPv6 en la búsqueda de ofertas de equipamiento y soporte de TIC (Tecnologías de Información y Comunicaciones). Este documento tiene como objeto proporcionar una "Mejor Práctica Actual" Best Current Practice (BCP) y no especifica ninguna norma ni política por sí mismo.

Puede servir como una plantilla que puede ser utilizada por los gobiernos, las grandes empresas y todas las demás organizaciones en la búsqueda de la compatibilidad con IPv6 en sus ofertas o requerimientos de equipo y ofrecerle orientación sobre qué especificaciones para pedir. También puede servir como una ayuda para aquellas personas u organizaciones interesadas en la licitación de contratos gubernamentales o empresariales.

Tenga en cuenta que las normas mencionadas anteriormente, tienen su origen en diversos organismos, que operan independientemente de la comunidad RIPE, y que cualquiera de estos estándares podrían ser cambiados o ser reemplazados por una versión más nueva. También puede ser necesario ajustar las recomendaciones a sus necesidades locales específicas.

Algunas partes de esta sección se basan libremente en el perfil NIST / USGv6 desarrollado por el gobierno de Estados Unidos:[1]

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

Los autores han modificado estos documentos para hacerlos más aplicables universalmente. Esta opción incluye una lista de las los estándares de especificación RFC que deben ser soportados, divididos en ocho categorías de dispositivos.

Este documento también sigue el documento de requisitos de Nodos IPv6, RFC6434. Este RFC es la guía general de IETF sobre qué partes de IPv6 deben ser implementadas en los distintos dispositivos.

==

2. Trasfondo del BCOP/ Historia

Los certificados IPv6 Ready Logo pueden ser requeridos para cualquier dispositivo. Esta es la forma más fácil para que los proveedores que ofrecen equipos puedan demostrar que cumplen con los requisitos básicos de IPv6. El iniciador de la licitación también proporcionará la lista de RFCs obligatorios y opcionales requeridos con el fin de no excluir a los proveedores que aún no exponen sus equipos a la prueba de certificación del programa IPv6 Ready Logo. De esta forma los licitadores públicos no pueden ser acusados de preferir cualquier tipo de proveedor de equipamiento.

Cuando especificamos la lista de RFCs requeridos, debemos enumerar todos los requisitos obligatorios, con excepción de las entradas que comienzan con: "Si [funcionalidad] Se solicita ..." Estas entradas son obligatorias sólo si el iniciador de de la licitación requiere cierta funcionalidad. Tenga en cuenta que el iniciador de licitación debe decidir qué funcionalidad se requiere, no el proveedor de equipos.

Algunas de las funciones que se encuentran en la sección "opcional" en este documento pueden ser importantes para su caso y / u organización específica. En tales casos, el iniciador de licitación debe mover el requisito hacia la sección “necesaria” en su solicitud de licitación.

==

3. Texto del BCOP

Cómo especificar los requisitos

Como se mencionó anteriormente, el programa IPv6 Ready Logo no abarca todo el equipamiento que soporta correctamente IPv6; por lo que declarar esos equipos como no elegibles puede no ser deseable. Este documento recomienda que el iniciador de de la licitación especifique que los equipos elegibles serán ya sea certificados bajo el programa IPv6 Ready o serán compatibles con los RFCs apropiados que se enumeran en la sección siguiente.

Acerca del programa “IPv6 Ready Logo”:

http://www.ipv6ready.org/

Tenga en cuenta que existe el proyecto BOUNDv6 cuyo objetivo es crear un entorno de red permanente de múltiples proveedores conectando laboratorios autorizados donde la comunidad puede probar las aplicaciones y los dispositivos habilitados para IPv6 en escenarios de prueba significativos. Se anima a los iniciadores de licitación a echar un vistazo y también utilizar los resultados de este proyecto.

Acerca de BOUNDv6:

http://www.boundv6.org/

Nota importante para el iniciador de oferta:

La certificación "IPv6 Ready Logo" cubre los requisitos básicos de IPv6 y algunas características avanzadas, pero no todos ellos. Si usted requiere alguna característica avanzada que no está cubierta por la certificación IPv6 Ready Logo, por favor solicite una lista de RFCs que cubran esas necesidades específicas, además de las comprendidas por la certificación IPv6 Ready Logo. En las listas siguientes, los RFCs que se tratan en dicha certificación están marcados con *.

Texto genérico propuesto para el iniciador de la licitación

En cada licitación, deberá incluirse el siguiente texto:

"Todo el hardware de TIC objeto de esta licitación debe apoyar tanto los protocolos IPv4 e IPv6. Similar comportamiento se debe proporcionar para ambos protocolos de entrada, salida y / o el rendimiento de flujo de datos de rendimiento, la transmisión y el procesamiento de paquetes.

El soporte de IPv6 puede ser verificado y certificado por el certificado IPv6 Ready Logo.

Cualquier software que se comunica a través del protocolo IP debe ser compatible con ambas versiones del protocolo (IPv4 e IPv6). La diferencia no debe ser perceptible para los usuarios.

El equipo que no se ha puesto a través de los procedimientos de pruebas IPv6 Ready deben cumplir con las RFC se enumeran a continuación:"

[lista apropiada de los RFCs obligatorios y opcionales seleccionados de las listas a continuación]

Lista de especificaciones técnicas RFC/3GPP obligatorias y opcionales soportadas en variedades de hardware y software

Los requisitos se dividen por equipos de hardware y soporte del integrador.

Se debe asumir que todo el tráfico de IPv4 migrará a IPv6. Todos los requisitos impuestos a las capacidades de tráfico IPv4 como latencia, ancho de banda y throughput también se debería exigir para el tráfico IPv6.

IPsec: obligatorio u opcional

En el estándar original Requisitos de Nodos IPv6 (RFC4294), IPsec fue listado como un "DEBE" para ser compatible con los estándares. El RFC actualizado (RFC6434) cambió

IPsec a "DEBERÍA" ponerse en práctica. Las razones para el cambio se expresan en este nuevo RFC.

El Grupo de Trabajo RIPE IPv6 ha debatido ampliamente si es necesario hacer el soporte IPsec obligatorio u opcional. Los constituyentes más participativos mostraron apoyo para mover IPsec para las secciones opcionales, que es lo que se refleja en este documento.

Mientras que el consenso de la comunidad era hacer IPsec opcional en la mayoría de los casos, el IETF ahora ha declarado que IPsec 'DEBERÍA' ser implementado en la versión más reciente del estándar Requisitos de Nodos IPv6 (RFC6434). En el contexto del IETF, un 'DEBERÍA' significa que pueden existir razones válidas en circunstancias particulares para ignorar un tema en particular, pero todas las consecuencias deben entenderse y valorarse cuidadosamente antes de elegir un camino diferente.

Las organizaciones que utilizan IPsec o tengan intención de utilizar en el futuro deberían incluir lo siguiente en la sección obligatoria al iniciar su oferta:

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

Definiciones y descripciones de diferentes tipos de dispositivos

Las siguientes definiciones se utilizarán para clasificar los distintos equipamientos de hardware. Mientras algún hardware pueda tener funcionalidades superpuestas (por ejemplo, un switch Capa 2 puede operar como un router Capa 3 o un router puede tener algunas capacidades de firewall), se espera que para cada funcionalidad superpuesta, se combinen los requerimientos de cada dispositivo específico.

Host: Un host es un participante de una red que recibe y envía paquetes pero no los conmuta en nombre de otros.

Conmutador, Switch, o 'Switch Capa 2': Un conmutador, switch o 'switch Capa 2' es un dispositivo que es usado principalmente para el reenvío de tramas Ethernet basándose en sus atributos. El intercambio de información Ethernet con otros switches Ethernet suele también ser parte de sus funciones.

Enrutador, router or 'Switch Capa 3': Un router o 'switch Capa 3' es un dispositivo que es usado principalmente para realizar el reenvío de paquetes IP basándose en sus atributos. El intercambio de información de ruteo con otros Routers suele también ser parte de sus funciones.

Equipos de Seguridad de Red: Los Equipos de Seguridad de Red son dispositivos cuya función primaria es permitir, denegar y/o monitorear el tráfico entre interfaces con el fin de detectar o prevenir potenciales actividades maliciosas. Estas interfaces además pueden incluir las VPNs (SSL o IPsec). El Equipamiento de Seguridad de Red es a menudo también un switch Capa 2 o un Router/switch Capa 3.

Customer Premise Equipment (CPE): Un dispositivo CPE es un router de pequeña oficina o bien un router residencial que es usado para conectar a los usuarios finales hogareños o pequeñas empresas usando una amplia cantidad de configuraciones diferentes. A pesar que un CPE es usualmente un dispositivo llamado router, los requerimientos son diferentes desde el punto de vista de un Router o Switch Capa 3 en una empresa o ISP, dado que estos suelen ser más complejos al estar compuestos por un hardware y software más avanzado.

Dispositivo Móvil: En el contexto de este documento, un dispositivo móvil es un nodo que se conecta a un sistema 3GPP definido utilizando alguna tecnología de acceso 3GPP específica (tal como 2G, 3G, o LTE). En las situaciones donde la lógica de red se compone únicamente por un dispositivo dedicado A conectado a otro dispositivo B, la especificación se referirá al dispositivo A y no al dispositivo B. Si la lógica de protocolos está distribuida (por ejemplo una computadora con una interfaz ethernet externa que realiza TCP checksum offloading), el sistema agregado será referido.

Balanceador de Carga: Un balanceador de carga es un dispositivo de red que distribuye la carga de trabajo a través de múltiples computadoras, servidores u otros recursos, con el fin de lograr la utilización óptima o prevista de recursos, maximizar el rendimiento, minimizar el tiempo de respuesta y evitar la sobrecarga.

Las siguientes referencias son de relevancia a este documento BCP. En el momento de la publicación, las ediciones indicadas eran válidas. Todas las referencias son objetos de revisiones; Por lo que los usuarios de este documento BCP deben animarse a investigar la posibilidad de aplicar las ediciones más recientes de las referencias citadas a continuación.

Listado de normas RFC/3GPP requeridas para diferentes tipos de hardware

El equipamiento para TIC está dividido en siete grupos funcionales:

- Host: cliente o servidor
- Conmutador o Switch Capa 2
- Router o Switch Capa 3
- Equipos de seguridad de red (firewalls, IDS, IPS...)
- CPE
- Dispositivo móvil
- Balanceador de carga

Hemos dividido los siguientes requisitos en dos categorías, “obligatorias” y “opcionales”. El equipo debe cumplir con la lista de requisitos de los estándares obligatorios. El soporte de requisitos opcionales pueden ganar puntos adicionales en la licitación, si esto fuera especificado por el iniciador.

Cualquier hardware que no cumpla con **todos** los estándares obligatorios debe ser marcados como no apropiado por el evaluador de la licitación.

Las normas que son parte de los procedimientos de prueba del “IPv6 Ready Logo”, y son llevados a cabo típicamente por laboratorios acreditados, están marcados con un asterisco *.

Requerimientos para equipo "host"

Soporte obligatorio:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- DHCPv6 client [RFC3315] *
- SLAAC [RFC4862] *
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- Si se requiere soporte para túneles y doble pila, el dispositivo debe soportar “Basic Transition Mechanisms for IPv6 Hosts y Routers” [RFC4213]
- Si se requiere soporte para IPv6 móvil, , el dispositivo debe soportar “MIPv6” [RFC6275, RFC5555] y “Mobile IPv6 Operation With IKEv2 y el Revised IPsec Architecture” [RFC4877]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *

Soporte opcional:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] y DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences y More-Specific Routes [RFC4191]

Requerimientos para equipo "consumer grade Layer 2 switch"

Soporte opcional: (administración)

- MLDv2 snooping [RFC4541]
- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] y DiffServ [RFC3289]

Requerimientos para equipo "enterprise/ISP grade "Layer 2 switch"

Soporte obligatorio:

- MLDv2 snooping [RFC4541]
- DHCPv6 filtering [RFC3315]
- Router Advertisement (RA) filtering [RFC4862]
- Dynamic "IPv6 Neighbor solicitation/advertisement" inspection [RFC4861]
- Neighbor Unreachability Detection [NUD, RFC4861] filtering
- Duplicate Address Detection [DAD, RFC4429] snooping y filtering.[2]

Soporte opcional: (administración):

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] y DiffServ [RFC3289]
- IPv6 Routing Header [RFC2460, Next Header value 43] filtering *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
- UPnP filtering

Requerimientos para equipo "router or Layer 3 switch"

Soporte obligatorio:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]

- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- MLDv2 snooping [RFC4541]
- Multicast Listener Discovery version 2 [RFC3810] *
- Router-Alert option [RFC2711]
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
- Si se requiere un “dynamic interior gateway protocol (IGP)” , entonces deben ser soportados RIPng [RFC2080], OSPF-v3 [RFC5340] o IS-IS [RFC5308]. La entidad de contratación deberá especificar el protocolo requerido.
- Si se requiere OSPF-v3 , el equipo debe cumplir con "Authentication/Confidentiality para OSPF-v3" [RFC4552]
- Si se requiere el protocolo BGP4 , el equipo debe cumplir con RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 y RFC2545
- Soporte para QoS [RFC2474, RFC3140]
- Si se requiere soporte para encapsulamiento y pila dual, el dispositivo debe soportar “Basic Transition Mechanisms for IPv6 Hosts y Routers” [RFC4213]
- Si se requiere soporte para encapsulamiento y pila dual, el dispositivo debe soportar “Generic Packet Tunneling y IPv6” [RFC2473]
- Si se requiere 6PE, el equipo debe soportar "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)” [RFC4798]
- Si se requiere IPv6 móvil, el equipo debe soportar MIPv6 [RFC6275, RFC5555] y "Mobile IPv6 Operation With IKEv2 y el Revised IPsec Architecture” [RFC4877]
- Si se requiere “IS-IS routing protocol” el equipo debe soportar "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]
- Si se requiere funcionalidad MPLS (por ejemplo, BGP-free core, MPLS TE, MPLS FRR) , los PE-routers y route reflectors deben soportar "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- Si se requiere funcionalidad “Layer 3 VPN” , los PE-routers y route reflectors deben soportar "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN" [RFC4659]
- Si “MPLS Traffic Engineering” es usado en combinación con “IS-IS routing protocol”, el equipo debe soportar "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]

Soporte opcional:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]

- DHCPv6 client/server/relay [RFC3315] *
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- Route Refresh for BGP-4 Capabilities [RFC2918]
- BGP Extended Communities Attribute [RFC4360]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Generic Routing Encapsulation [RFC2784]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 tunnels [RFC4891]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] y DiffServ [RFC3289]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size Requirements [RFC3226]
- 127-bit IPv6 Prefixes on Inter-Router Links [RFC6164]
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences y More-Specific Routes [RFC4191]

Requisitos para "equipamiento de seguridad en la red"

El equipamiento en esta sección se divide en tres subgrupos:

- Cortafuegos o Firewalls (FW)
- Sistema de prevención de intrusos (IPS)
- Firewalls de aplicación (APFW)

Para cada norma obligatoria los subgrupos aplicables se especifican entre paréntesis al final de la línea.

Soporte obligatorio:

- IPv6 Basic specification [RFC2460] (FW, IPS, APFW) *
- IPv6 Addressing Architecture [RFC4291] (FW, IPS, APFW)
- Default Address Selection [RFC3484] (FW, IPS, APFW)
- ICMPv6 [RFC4443] (FW, IPS, APFW) *
- SLAAC [RFC4862] (FW, IPS) *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *

- Inspecting IPv6-in-IPv4 protocol-41 traffic, que está especificado en: “Basic Transition Mechanisms for IPv6 Hosts y Routers” [RFC4213] (IPS)
- Router-Alert option [RFC2711] (FW, IPS)
- Path MTU Discovery [RFC1981] (FW, IPS, APFW) *
- Neighbor Discovery [RFC4861] (FW, IPS, APFW) *
- Si la petición es para el protocolo BGP4, el equipo debe cumplir con RFC4271, RFC1772, RFC4760 y RFC2545 (FW, IPS, APFW)
- Si la petición es para “dynamic internal gateway protocol (IGP)”, entonces se deben soportar RIPng [RFC2080], OSPF-v3 [RFC5340] o IS-IS [RFC5308]. La entidad de contratación especificará el protocolo requerido. (FW, IPS, APFW)
- Si se requiere OSPF-v3 , el dispositivo debe soportar "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- Soprte para QoS [RFC2474, RFC3140] (FW, APFW)
- Si se requiere encapsulamiento, el dispositivo debe soportar “Basic Transition Mechanisms for IPv6 Hosts and Routers” [RFC4213] (FW)

Un dispositivo de seguridad de red a menudo se coloca donde lo haría un switch de capa 2/capa 3. En función de su colocación esos requisitos deberìan ser incluidos .

La funcionalidad y características que se soportan para IPv4 deben ser comparables con la funcionalidad soportada para IPv6. Por ejemplo, si un sistema de prevención de intrusiones es capaz de operar en IPv4 en modos de capa 2 y capa 3, entonces también debe ofrecer esta funcionalidad en IPv6. O si un Firewall se está ejecutando en un clúster capaz de sincronizar sesiones IPv4 entre todos los miembros del cluster, entonces esto también debe ser posible con sesiones IPv6.

Soporte opcional:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client/server/relay [RFC3315] *
- Extended ICMP for Multipart Messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- BGP Communities Attribute [RFC1997]
- BGP Capabilities Advertisement WITH-4 [RFC3392]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- Cryptographically Generated Addresses [RFC3972]

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW)
- OSPF-v3 [RFC5340]
- Authentication/Confidentiality for OSPF-v3 [RFC4552]
- Generic Packet Tunneling y IPv6 [RFC2473]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] y DiffServ [RFC3289]
- DNS extensions to support IPv6 [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Using IPSec to Secure IPv6-in-IPv4 Tunnels [RFC4891]
- Multicast Listener Discovery version 2 [RFC3810] *
- MLDv2 snooping [RFC4541] (when in L2 or passthrough mode) *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5739]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences y More-Specific Routes [RFC4191]

Requerimientos para equipo CPE

Soporte obligatorio:

- RFC6204 (Basic Requirements for IPv6 Customer Edge Routers) *

Soporte opcional:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Si se requiere el soporte para IPv6 móvil, el dispositivo necesita cumplir con “MIPv6” [RFC6275, RFC5555] y “Mobile IPv6 Operation With IKEv2 y el Revised IPsec Architecture” [RFC4877]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] y DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) [RFC5969]
- Si se soporta “Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion” [RFC6333] entonces también se debe soportar la opción “Dynamic

Host Configuration protocol for IPv6 (DHCPv6)" para "Dual-Stack Lite" [RFC6334]

- The A+P Approach to el IPv4 Address Shortage [RFC6346]
- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5739]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences y More-Specific Routes [RFC4191]

Requerimientos para dispositivos móviles

Soporte obligatorio:

- IPv6 basic specification [RFC2460] *
- Neighbor Discovery for IPv6 [RFC4861] *
- IPv6 Stateless Address Autoconfiguration [RFC4862] *
- IPv6 Addressing Architecture [RFC4291] *
- ICMPv6 [RFC4443] *
- IPv6 over PPP [RFC2472]
- Multicast Listener Discovery version 2 [RFC3810] *
- IPv6 Router Alert Option [RFC2711]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]

Soporte opcional:

- Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [RFC4941]
- Path MTU Discovery for IPv6 [RFC1981] *
- Generic Packet Tunneling for IPv6 [RFC2473]
- DHCPv6 [RFC3315] *
- Stateless DHCPv6 [RFC3736]
- DHCPv6 option for SIP servers [RFC3319]
- IPv6 Prefix Options for DHCPv6 [RFC3633]
- Prefix Exclude Option for DHCPv6-based Prefix Delegation [draft-ietf-dhc-pd-exclude]
- Default Address Selection [RFC3484]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- IKEv2 Mobility y Multihoming Protocol MOBIKE [RFC 4555]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences y More-Specific Routes [RFC4191]

Referencias:

- 3GPP

- Internetworking Between Public Land Mobile Network (PLMN) supporting packet based services y Packet Data Networks (PDN) [3GPP TS 29.061]
- GPRS Service Description [3GPP TS 23.060]
- General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access [3GPP TS 23.401]
- Signaling flows for IP multimedia Call control based on SIP y SDP [3GPP TS 24.228]
- IP multimedia call control protocol based on SIP y SDP [3GPP TS 24.229]
- IP Based Multimedia Framework [3GPP TS 22.941]
- Architectural Requirements [3GPP TS 23.221]
- Packet domain; Mobile Stations (MS) Supporting Packet Switching Service [3GPP TS 27.060]
- IPv6 migration guidelines [3GPP TR 23.975]
- IETF
- IPv6 for Some Second y Third Generation Cellular Hosts [RFC3316]
- Recommendations for IPv6 in 3GPP Standards [RFC3314]
- IPv6 in 3rd Generation Partnership Project (3GPP) [RFC6459]

Requerimientos para balanceadores de carga

Un balanceador de carga distribuye las solicitudes entrantes y/o las conexiones de clientes a varios servidores. Los balanceadores de carga tendrán que soportar varias combinaciones de conexiones IPv4 e IPv6:

- **Debe** ser soportado el balanceo de carga de clientes IPv6 a servidores IPv6 (6-a-6)
- **Debe** ser soportado el balanceo de carga de clientes IPv6 a servidores IPv4 (6-a-4)
- **Debería** ser soportado el balanceo de carga de clientes IPv4 a servidores IPv4 (4-a-4)
- **Debería** ser soportado el balanceo de carga de clientes IPv4 a servidores IPv6 (4-a-6)
- **Debería** ser soportado el balanceo de carga una sola dirección externa / virtual IPv4 a un conjunto mixto de servidores IPv4 e IPv6
- **Debería** ser soportado el balanceo de carga una sola dirección externa / virtual IPv6 a un conjunto mixto de servidores IPv4 e IPv6

Si un balanceador de carga provee balanceo en capa 7 (A nivel de aplicación / proxy reverso, definido como ‘surrogate’ en la sección 2.2 de la RFC3040) entonces el soporte para el header X-forwarded-for (o equivalente) en HTTP **tiene** que ser provisto con la finalidad de hacer la dirección IP del cliente visible a los servidores.

Soporte obligatorio:

- IPv6 Basic specification [RFC2460] *

- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *

Soporte opcional:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] y DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- NAT64/DNS64 [RFC6146, RFC6147]
- Si el soporte para IPsec es requerido, el dispositivo debe soportar IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] * y el Mecanismo de Redireccionamiento para el Protocolo Key Exchange Version 2 (IKEv2) [RFC5685]
- Si se requiere soporte para BGP4, el equipo debe cumplir con RFC4271, RFC1772, RFC4760 y RFC2545
- Si se requiere soporte para el dynamic internal gateway protocol (IGP), el RIPng [RFC2080], OSPF-v3 [RFC5340] o IS-IS [RFC5308] tiene que ser soportada. La autoridad contratante debe especificada el protocolo requerido.
- Si se requiere OSPF-v3, el dispositivo debe soportar "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- IPv6 Host-to-Router Load Sharing [RFC4311] (FW)
- Default Router Preferences and More-Specific Routes [RFC4191] (FW)

Requerimientos para el soporte IPv6 en software

Todo el software debe soportar IPv4 e IPv6 y ser capaz de comunicarse sobre redes sólo IPv4, sólo IPv6 y doble pila. Si el software incluye parámetros de red en su configuración de servidor local o remoto este debe además permitir la configuración de parámetros en IPv6.

Todas las características que se ofrecen sobre IPv4 deben estar disponibles también en IPv6. El usuario no debe experimentar ninguna diferencia notable tanto si el software se comunica por IPv4 o por IPv6 excepto cuando esto provea un beneficio apreciable al usuario.

Se recomienda encarecidamente no utilizar ninguna dirección en el código del software, como está descrito en "Default Address Selection for Internet Protocol version 6" [RFC3484].

Requerimientos de habilidades del integrador de sistemas

Vendedores y revendedores que ofrecen servicios de integración de sistemas deben tener al menos tres empleados con certificaciones válidas de competencia del fabricante del equipamiento para equipos que sean provistos al comprador. Estos empleados deben además tener conocimiento general del protocolo IPv6, planificación de redes en IPv6 y seguridad en IPv6 (como se sugiere por la certificación de estas habilidades). Si resulta obvio durante el proceso de instalación e integración que el conocimiento, competencias y experiencias del integrador no son suficientes para instalar y configurar satisfactoriamente el equipamiento para obtener una comunicación IPv4 e IPv6 apropiada con la red, el acuerdo debe ser cancelado y declarado nulo.

La definición de una integración apropiada, tiempos y grados de disrupción en la red durante el proceso de instalación deben ser producto de un acuerdo entre el cliente y el integrador del sistema.

Además se recomienda que los integradores de sistemas y sus empleados tengan un amplio conocimiento de IPv6 y certificados de IPv6 genéricos fuera de aquellos ofrecidos por los fabricantes de equipamiento. Estos certificados pueden ser obtenidos de sistemas de capacitación independientes. Este conocimiento debe recibir puntuación adicional en el proceso de contratación.

Todos los participantes en el proceso de contratación deben firmar una declaración la cual indicará que la compañía y sus empleados han cursado entrenamientos técnicos para el diseño, construcción e integración de equipamiento de las TIC en redes IPv4 e IPv6. Un ejemplo de esta declaración es mostrada a continuación.

Declaración de competencia en IPv6

Los contratantes deben requerir una declaración de competencias técnicas en IPv6 de parte del suministrador o integrador del equipamiento. Se requiere conocimiento y experiencia en IPv6 como forma de asegurar una apropiada instalación e integración de IPv6 en ambientes de las TIC.

La declaración debe decir que el suministrador de equipamiento o integrador de sistemas declara bajo juramento de ley:

- Que ellos tienen suficiente número de empleados para cumplir con los servicios ofertados.
- Que estos empleados han sido entrenados profesionalmente para su trabajo de diseño, integración y/o construcción de equipamiento de las TIC en ambientes IPv4 e IPv6;
- Que la calidad de los servicios ofertados cimplen todos los requerimientos definidos en los documentos de la contratación y que estos requerimientos aplican tanto para IPv4 como para IPv6.

Debe notarse que este tipo de declaraciones pueden variar en dependencia de la legislación local. Por tanto los traductores y los contratantes deben buscar apoyo legal respecto las palabras y textos a utilizar en estos documentos.

Reconocimientos

La primera versión de este documento fue realizada en el Go6 Expert Council y el Slovenian IPv6 working group.

Los autores quieren agradecer a todos los involucrados en la creación y modificación de versiones previas de este documento. Primero que todo, queremos agradecer a Janez Sterle, Urban Kunc, Matjaz Straus, Simeon Lisec, Davor Sostaric y Matjaz Lenassi del Go6 Expert Council por su guía a este documento. Reconocemos el trabajo hecho en el “Slovenian IPv6 working group” en la revisión y necesarias opiniones. Reconocimiento especial vaya a Ivan Pepelnjak, Andrej Kobal y Ragnar Us por sus esfuerzos y trabajo en aras de este documento. Gracias además a el co-Chairs del RIPE IPv6 Working Group, David Kessens, Shane Kerr y Marco Hogewoning por su apoyo y ánimos. Queremos agradecer a Patrik Fältström, Torbjörn Eklöv, Randy Bush, Matsuzaki Yoshinobu, Ides Vanneuville, Olaf Maennel, Ole Trøan, Teemu Savolainen y las personas del RIPE IPv6 Working Group (Joao Damas, S.P. Zeidler, Gert Doering entre otros) por sus sugerencias, comentarios y revisión del documento. Por último, pero no menos importante, queremos agradecer a Chris Buckridge y el “Communications Team de RIPE NCC” por corregir nuestra gramática y ortografía en el documento. Y a todos los demás que contribuyeron a este trabajo.

Los autores de este documento desean agradecer al RIPE IPv6 Working Group y sus directores por todo el apoyo y ánimos para desarrollar una versión mejorada del documento. Gracias especiales vayan a Ole Trøan, el editor de la RFC6204 por su ayuda en la sección de los CPE y por sugerir otros cambios en el documento. Gracias a Marco Hogewoning, Ivan Pepelnjak y S.P. Zeidler por sus valiosos aportes en ideas sobre cómo estructurar el documento y los contenidos de una mejor manera. A Timothy Winters y Erica Johnson (ambos del IPv6 Ready Logo committee, UNH) por su ayuda en anotar las RFCs que probaron y sus sugerencias constructivas. Gracias además a Yannis Nikolopoulos y Frits Nolet. Gracias especiales vayan a Jouni Korhonen, Jari Arkko, Eric Vyncke, David Freedman, Tero Kivinen y Michael Richardson por varios comentarios sumamente valiosos y sugerencias que hicieron a este documento mucho mejor.

Las sugerencias de mejoras a este documento y otros comentarios deben ser enviados a la lista de correos del RIPE IPv6 Working Group <ipv6-wg@ripe.net>.

---

[1]Las especificaciones USGv6 están siendo actualmente sometidas a una revisión para actualizarlas, la cual se espera esté lista para inicios del 2012.

[2] El IETF Source Address Validation Improvements (SAVI) Working Group está actualmente trabajando en las RFCs que especificarán un marco para la validación de direcciones de origen. Una vez sean publicadas estas RFC, las referencias al filtrado de NUD y DAD serán cambiadas de acuerdo a lo especificado.

==

4. Conclusión del BCOP

TBD