Network Working Group
Internet-Draft
Intended status: BCP
Expires: May 3, 2009

H. Singh
W. Beebee
Cisco Systems, Inc.

October 30, 2008

IPv6 CPE Router Recommendations
draft-wbeebee-ipv6-cpe-router-03

Status of this Memo

Abstract

This document recommends IPv6 behavior for Customer Premises Equipment (CPE) routers in Internet-enabled homes and small offices. The CPE Router may be a standalone device. The CPE Router may also be embedded in a device such as a cable modem, DSL modem, cellular phone, etc. This document describes the router portion of such a device. The purpose behind this document is to provide minimal functionality for interoperability and create consistency in the customer experience and satisfy customer expectations for the device. Further, the document also provide some guidance for implementers to expedite availability of IPv6 CPE router products in the marketplace.

Table of Contents

1. Introduction

This document defines IPv6 features for a residential or small office router referred to as a CPE Router. Typically, CPE Router devices support IPv4, as discussed in the "IPv4 Support" section. Also, this document does not go into configuration details for the CPE Router. A CPE Router is an IPv6 Node and, therefore, MUST follow IPv6 Node Requirements draft-ietf-6man-node-req-bis-01 [I-D.ietf-6man-node-req-bis].

The document discusses IPv6 implications for the attached Service Provider network. The document notes that the CPE Router may be deployed in home in one of two ways. Either the Service Provider or the home user may manage this device. When the CPE Router is managed by the Service Provider, the router may need additional management and routing properties like a new MIB definition and routing protocols communicating between the CPE Router and the Service Provider network. The CPE router has one or more WAN interface(s) to connect to the Service Provider and zero or more LAN interfaces to the home network devices. The WAN interface is preferred to be Ethernet encapsulated but it may support other encapsulations such as PPP.

2. Terminology and Abbreviations

Host - this is a personal computer or any other network device in a home that connects to the Internet via the CPE Router.

LAN interface(s) - an optional set of network interfaces on the CPE Router that are used to connect hosts in the home. This set of ports could be switched, bridged, or routed. If no LAN interface is present, then there is no need for the CPE router to provide LAN side services such as DHCPv6 PD or ULA's.

WLAN interface - an optional wireless access point interface on the CPE Router used to connect wireless hosts in the home in either managed or ad-hoc modes.

WAN interface - usually a single physical network interface on the standalone CPE Router that is used to connect the router to the access network of the Service Provider. When the CPE Router is embedded in a device that connects to the WAN, this interface is a logical network interface that bridges the device to the CPE Router. Some devices which can have an embedded CPE router are: a cable or DSL modem, or a cellular telephone, etc. A CPE router with more than one WAN interface will need a more complicated provisioning and multicast model than is described in this

document.

GRE tunnel - Generic Routing Encapsulation tunnel.

SLAAC - StateLess Address Auto Configuration.

IPTV - Internet Protocol TeleVision.

mDNS - Multicast Domain Name System - see http://www.zeroconf.org.

3. Operational Behavior

The CPE Router is a gateway to the Internet for a home. The router is also intended to provide home networking functionality. The CPE Router may have a console or web interface for configuration. This document defines the core set of features that are supported by the CPE Router, however individual implementations may include value-added features such as WLAN capability.

The core set of IPv6 features for the CPE Router includes provisioning the CPE Router for IPv6, IPv6 data forwarding including IPv6 multicast, CPE Router provisioning hosts on its LAN interface(s), firewall, and QoS behavior. An IPv6 firewall is discussed briefly in the Firewall section where the section refers the draft-ietf-v6ops-cpe-simple-security [I-D.ietf-v6ops-cpe-simple-security] for more details.

3.1. Conceptual Configuration Variables

The CPE Router maintains such a list of conceptual optional configuration variables.

1. Loopback interface enable.

2. PPPOE enable.

3. Softwire enable.

4. 6to4

5. RIPng enable.

6. If DHCPv6 fails, the CPE Router may initiate PPPOE, L2TPv2 Softwire tunnel, or 6to4 [RFC3056] operation.

4. Router Initialization

Before the CPE Router is initialized, the device must have IPv6 enabled. The CPE Router SHOULD support the ability to disable its IPv6 stack. The CPE Router also has the ability to block or forward IPv6 traffic to and from the router's LAN interface(s). [RFC2669] includes a MIB definition to block the IPv4 or IPv6 Ethertype in the upstream or downstream interface(s) of a device such as the CPE Router. Some portion of this MIB may need to be modified for use with the CPE Router.

The CPE Router supports at least one of two modes of initialization: either the LAN interface(s) become operational first or the WAN interface becomes operational first. More details have been provided in the Basic IPv6 Provisioning section.

5. Basic IPv6 Provisioning

The CPE Router MUST support at least one of two WAN interface models, one of which will be active on the CPE Router at any given time. In the Numbered model, the WAN interface acquires a global unicast address (GUA) using a combination of SLAAC and stateful DHCPv6 for IA_PD (no IA_NA) or uses only stateful DHCPv6 for GUA (IA_NA) and IA_PD. IA_PD is acquired using stateful DHCPv6 as described in [RFC3633]. A Loopback interface (which can be used as a stable peering point for routing protocols or to respond to the anycast address) is optional. If stateful DHCPv6 is not used to obtain other IPv6 configuration, then stateless DHCPv6 [RFC3736] must be initiated by the WAN interface to obtain other IPv6 configuration. Further, in the numbered model, we recommend the CPE Router WAN interface acquire its global IPv6 address using stateful DHCPv6 for administrative control of the router. Manual configuration may be supported by the CPE router for IPv6 address configuration of the WAN interface. However, manual configuration is beyond the scope of this document.

In the Unnumbered model, the WAN interface only constructs a LLA, then the WAN interface initiates stateful DHCPv6 for IA_PD. The IA_PD is sub-delegated to the LAN interface(s) and an optional Loopback interface (or the addresses for the LAN/Loopback interfaces could come from IA_NAs). Either the Loopback or the LAN interface can be used to source WAN-facing traffic. Other IPv6 configuration information is obtained using stateless DHCPv6.

The CPE Router acquires its IPv6 addresses from the Service Provider along with any other IPv6 configuration any time the WAN interface is connected to the Service Provider network. Thereafter the CPE Router provisions its LAN interface(s) for IPv6 router functionality

including provisioning global IPv6 addresses on the LAN interface(s). Even if LAN interface(s) have been operational and provisioned earlier, the global IPv6 configuration of LAN interface(s) is still required. More details for provisioning the CPE Router are given in the following sections.

5.1. Construct Link-Local Address

If an interface of the CPE Router is configured for IPv6, when the interface initializes itself, as per [RFC4862], the CPE Router must create a link-local address for the interface. We recommend the CPE Router use the EUI-64 identifier as a link-local address for each of its interfaces. Refer to EUI-64 details in [RFC4291]. Further, as per [RFC4862], the CPE Router must perform Duplicate Address Detection (DAD) on all unicast addresses unless a layer 2-specific document specifies that DupAddrDetectTransmits is zero for that linktype. If the CPE Router detects a duplicate address assigned to an interface, the CPE Router must not send IPv6 packets from the interface.

5.2. Process RAs

The CPE Router must process incoming RAs received on the WAN interface as specified in section 6.3 of [RFC4861]. The CPE Router locates routers that reside on the attached WAN link from the received RAs.

5.3. Acquire IPv6 Address and Other Configuration Parameters

The CPE Router must process RAs received on the WAN interface. As per [RFC4861] if the M bit is set in the RA, the WAN interface must perform stateful DHCPv6- if the O bit is set in the RA, the WAN interface acquires other configuration information. If stateful DHCPv6 is not used to obtain other IPv6 configuration, then stateless must be initiated by the WAN interface to obtain other IPV6 configuration. If the A bit in the RA is clear or the RA does not include any Prefix Information Option (PIO), the WAN interface must not perform SLAAC. IPv6 deployments that configure RA to not include any PIO are discussed in draft-ietf-6man-ipv6-subnet-model [I-D.ietf-6man-ipv6-subnet-model].

5.3.1. Numbered Model

As instructed by the RA message, the WAN interface acquires global IPv6 address using stateful DHCPv6.

5.3.2. Unnumbered Model

When the CPE router is configured for Unnumbered model, the WAN interface only constructs a LLA, then the WAN interface initiates stateful DHCPv6 for IA_PD. Then the IA_PD is sub-delegated to the LAN interface(s) and an optional Loopback interface (or the addresses for the LAN/Loopback interfaces could come from IA_NAs). Either the Loopback or the LAN interface can be used to source WAN-facing traffic. When the Loopback or the LAN interface is used to source WAN-facing traffic, both the CPE Router and the Service Provider Router must consider the traffic to be off-link to the link connecting the CPE Router with the Service Provider Router. Other IPv6 configuration information is obtained using stateless DHCPv6. The Unnumbered model is incompatible with the strong host model on the CPE router. The unnumbered model may be inappropriate for use with certain deployments where a device that uses the strong host model can operate as a CPE Router.

5.3.3. Both Models

At any instance in time of the CPE Router operation, the router does not forward any traffic between its WAN and LAN interface(s) if the router has not completed IPv6 provisioning process that involves the acquisition of a global IPv6 address by the WAN or if the WAN is unnumbered and there is no GUA available to source WAN packets. The LAN interface(s) must also be provisioned for a global or Unique Local Address.

5.4. Details for DHCPv6 Address Acquisition

If the WAN interface uses stateful DHCPv6, the interface sends a DHCPv6 Solicit message as described in section 17.1.1 of [RFC3315]. The Solicit message must include an IA_NA option as specified by [RFC3315]. If the WAN interfaces uses stateless DHCPv6, the WAN interface sends an Information Request. Both the DHCPv6 SOLICIT and Information Request also include other options like a Reconfigure Accept option to inform the server that client is willing to accept Reconfigure message from server, and the Options Request option that includes the DNS Recursive Name server option as specified in [RFC3646]. The Solicit may also include the Rapid Commit option if the CPE Router is willing to accept a 2-message DHCPv6 exchange with the server.

When the CPE Router processes a DHCPv6 response from the server, if the response message (e.g. ADVERTISE or REPLY) received does not include an IA_PD option (if stateful DHCPv6 was initiated), or Reconfigure Accept option, then the CPE Router has failed DHCPv6 address acquisition. If stateful DHCPv6 succeeds, the CPE Router

must perform DAD for any IPv6 address acquired from DHCPv6. If the CPE Router detects a duplicate, the CPE Router must send a DHCPv6 Decline message to the DHCPv6 server.

The CPE Router may support the Reconfigure Key Authentication Protocol, as described in section 21.5 of [RFC3315]. The CPE Router may also support prefix sub-delegation. Prefix sub-delegation involves DHCPv6 server support with IA_PD on the CPE router and the ability to provision the server from a DHCPv6 REPLY with IA_PD option received on the WAN interface.

5.5. IPv6 Provisioning of Home Devices

The CPE Router may include a stateful DHCPv6 server to assign addresses to home devices connected via the LAN interface(s) of the CPE Router. The home devices can also acquire addresses via SLAAC.

If the LAN interface(s) are switched or bridged ports, then the CPE Router assigns a single global IPv6 address to a conceptual virtual interface serving all the LAN interface(s). If each LAN interface is a routed port, then the CPE router will assign a global IPv6 address and unique subnet to each LAN interface. In either case, when the CPE Router needs to assign a single IPv6 address to LAN interface(s) or multiple IPv6 addresses, the CPE Router redistributes the addresses and subnets from the prefix received in IA_PD option by the WAN interface. If the IA_PD changes, the CPE Router must reconfigure the LAN interface(s) with new IPv6 addresses derived from the new IA_PD and then also renumber the IPv6 ND RA configuration on the LAN interface(s).

This document recommends the RA sent out by LAN Interface(S) to be configured for SLAAC so that the prefix advertised in the RA is derived from the IA_PD assigned to the CPE Router by the Service Provider; the O-bit is also set so that the CPE Router can pass Domain Name Server(s) IPv6 address(es) to home devices. The CPE Router obtained the Domain Name Server(s) in OPTION_DNS_SERVERS option from the DHCPv6 server when the CPE Router WAN interface completed DHCPv6.

5.5.1. LAN Initialization before WAN Initialization

On power up, the LAN interface(s) of the CPE Router may become operational before the WAN interface. This mode is appropriate for manual user configuration of the CPE Router. After any LAN interface has constructed a link-local address, the address can be used for user configuration via the network. The interface can assign itself a Unique Local Address automatically through the pseudo-random number generation algorithm described in [RFC4193]. Note that the ULA must

have a larger subnet than a /64 if multiple routers are cascaded behind the CPE router and prefix sub-delegation is used (see the Cascading of Routers behind the CPE Router section below). Once the IPv6 address configuration of the LAN interface(s) is complete with a ULA, as per [RFC4862], the CPE Router sends Router Advertisements (RA) to devices in the home. Hosts receiving the RA from LAN interface(s) will process the RA and perform IPv6 address acquisition. After all the LAN interface(s) have become operational, if the WAN interface is connected to the Service Provider network, then the WAN interface provisions itself and may acquire an IA_PD. If an IA_PD is acquired, it may be sub-delegated to any cascaded routers or used for SLAAC provisioning of hosts in the home. Based on the IA_PD, the CPE Router configures global address(es) on the LAN interface(s) and sends an RA containing the global address and unique local prefixes out the LAN interface(s). After this process, every LAN interface has a link-local unicast address, a ULA, and a GUA. Therefore, the interface has to apply source address selection to determine which address to use as a source for outgoing packets. Since the GUA has a larger scope than the link-local address, or the ULA (rule #2 of [RFC3484]), the GUA will be used as a source address of outgoing packets that are not subject to rule #1. If a user desires to keep CPE Router configuration traffic local to the home network, the user can do the following:

- Use the ULA of the CPE Router as the destination of the configuration traffic.

- Use access control lists (ACL)s to block any ULA sourced packet from being sent out the WAN interface.

Rule #1 of [RFC3484] and the ACLs ensure that the traffic does not escape the home network.

After the WAN interface initializes, then the LAN interface(s) can acquire global unicast addresses.

5.5.2. WAN initialization before LAN Initialization

On power up, the WAN interface of the CPE Router may become operational before the LAN interface(s). This mode is appropriate for Service Provider configuration of the CPE Router. After the IPv6 address configuration for WAN interface is completed, the CPE Router configures IPv6 address for LAN interface(s).

Once IPv6 address configuration of the LAN interface(s) is complete, as per [RFC4862], the CPE Router sends Router Advertisements (RA) to devices in the home. Hosts receiving the RA from LAN interface(s) will process the RA and perform IPv6 address acquisition.

5.6. IPv6 over PPP

In some deployments IPv6 over PPP is preferred to connect the home to the Service Provider. For such a deployment, another configuration variable on the CPE Router enables optional IPv6 over PPP support. After IPv6CP negotiates IPv6 over PPP and the WAN interface has constructed a LLA, steps mentioned in the "Acquire IPv6 Address and Other Configuration Parameters" section above are followed to acquire a GUA for WAN interface and also an IA_PD. If an IA_PD is acquired by the WAN interface, the CPE Router assigns global address(es) to its LAN interface(s) and sub-delegates the IA_PD to hosts connected to the LAN interface(s). IPv6 over PPP follows [RFC5072]. As per [RFC5072], the CPE router does not initiate any DAD for unicast IPv6 addresses since DupAddrDetectTransmits variable from [RFC4862] is zero for IPv6 over PPP.

If the Service Provider deployment supports dual-stack PPP support, then the CPE Router WAN interface may initiate one PPP logical channel and support NCP IPv4 and IPv6 control protocols over one PPP logical channel. [RFC4241] describes such behavior. The IPv4 and IPv6 NCP's are independent of each other and start and terminate independently.

5.6.1. Softwire Support

If the CPE Router is deployed in a deployment where the home includes IPv6 hosts but the Service Provider network does not support IPv6, an optional softwire feature may be enabled on the CPE Router. The softwire draft-ietf-softwire-hs-framework-l2tpv2 [I-D.ietf-softwire-hs-framework-l2tpv2] initiates L2TPv2 tunnel from the CPE Router to tunnel IPv6 data from the home over an IPv4 network. The feature is enabled before any IPv6 host in the home is connected to the CPE Router or the WAN interface of the CPE Router is operational. If the CPE Router supports the Softwire feature, then the CPE Router must support the deployment scenario of Router CPE as Softwire Initiator described in section 3.1.2 of draft-ietf-softwire-hs-framework-l2tpv2 [I-D.ietf-softwire-hs-framework-l2tpv2]. IPV6CP negotiates IPv6 over PPP which also provides the capability for the Service Provider to assign the 64-bit Interface-Identifier to the WAN interface of the CPE Router. After the WAN interface has acquired an IA_PD option, global addresses from the IA_PD are assigned to the LAN interface(s) and the IA_PD is also sub-delegated to clients connected to the LAN interface(s).

5.7. Stateful DHCPv6 Server

The CPE Router may support a stateful DHCPv6 server to serve clients on the CPE Router LAN interface(s). If the CPE Router needs to support a stateful DHCPv6 server, then more details will be added to this section specifying the minimal functionality that the stateful DHCPv6 server needs to support.

6. Cascading of Routers behind the CPE Router

To support cascading routers behind the CPE Router this document recommends using prefix sub-delegation of the prefix obtained either via IA_PD from WAN interface or a ULA from the LAN interface. The network interface of the downstream router may obtain an IA_PD either via stateful DHCPv6 or stateless DHCPv6. If the CPE router supports cascading of routers through automatic prefix sub-delegation, the CPE router MUST support a DHCPv6 server or DHCPv6 relay agent. If an IA_PD is used, the Service Provider or user MUST allocate an IA_PD or ULA prefix short enough to be sub-delegated and subsequently used for SLAAC. Therefore, a prefix length shorter than /64 is needed. The CPE Router MAY support RIPng in the home network.

7. IPv6 Data Forwarding

Each of the WAN and LAN interface(s) of the CPE Router must have its own L2 (e.g. MAC) address. The CPE Router supports ND protocol on both the WAN interface and LAN interface(s) to advertise itself as a router to neighbors in the Service Provider and home networks.

The CPE Router forwards packets between the Service Provider and the home network. To do this, the CPE Router looks up the destination address of the packet in the routing table and decide which route to use to forward the packet. The CPE Router routing table will be initialized during CPE Router initialization. The routing table is filled by directly connected, static, and routing protocol routes.

The CPE Router consumes any packet destined to its WAN or LAN interface. The CPE Router forwards other packets destined to hosts attached to CPE Router LAN interface(s). Any packet that is not routable by the CPE Router must be dropped.

The CPE Router must support the ND protocol specified by [RFC4861]. Proxy Neighbor Advertisements as described in Section 7.2.8 of [RFC4861] are not applicable to the CPE Router. Also note, as per section 6.2.8 of [RFC4861] the link-local address on a router should rarely change, if ever. As per [RFC2460], the CPE Router decrements

the Hop Limit by 1 for any packet it forwards. The packet is discarded if Hop Limit is decremented to zero and the CPE Router also sends an ICMP Time Exceeded message to the source of the packet.

A route SHOULD be added to the routing table (to prevent routing loops) that is lower priority than any route except the default route. The choice to drop the packet or send an ICMPv6 Destination Unreachable to the source address of the packet is implementation-dependent. The installation of the null route MAY be automatic.

7.1. IPv6 Multicast

The CPE Router SHOULD follow the model described for MLD Proxy in [RFC4605] to implement multicast. The MLD Proxy model was chosen because it is simpler to implement than more complicated multicast routing functionality.

Querier Election rules as described in section 7.6.2 of [RFC3810] do not apply to the CPE Router (even when the home has multiple cascaded routers) since every CPE Router in the cascade is the only router in its own multicast domain. Every CPE Router in the cascade will send MLDv2 Reports with aggregated multicast Group Membership information to the next upstream router.

If the CPE Router hardware includes a network bridge between the WAN interface and the LAN interface(s), then the CPE Router MUST support MLDv2 snooping as per [RFC4541].

Consistent with [RFC4605], the CPE Router must not implement the router portion of MLDv2 for the WAN interface. Likewise, the LAN interfaces on the CPE router must not implement an MLDv2 Multicast Listener. However, if a user at home wants to create a new multicast group and send multicast data to other nodes on the Service Provider network, then Protocol Independent Multicast-Source Specific Multicast (PIM-SSM) [RFC3569] is recommended to handle multicast traffic flowing in the upstream direction as a one-to-many multicast flow.

8. Other IPv6 Features

8.1. Path MTU Discovery Support

GRE tunnels, such as IPv6 to IPv4 tunnels (which may be terminated on the CPE Router), can modify the default Ethernet MTU of 1500 bytes. Also, in the future, Ethernet Jumbo frames (9000+ bytes) may also be supported. Since the MTU can vary, a newly initiated TCP stream must detect the largest packet that can be sent to the destination without

fragmentation. This can be detected using Path MTU Discovery [RFC1981]. Routers which may encounter a packet too large to be forwarded from source to destination may drop the packet and send an ICMPv6 Packet Too Big message to the source. The CPE Router must route back to the source any ICMPv6 Packet Too Big messages generated anywhere on this path.

8.2. Optional RIPng Support

The CPE Router may support RIPng routing protocol [RFC2080] so that RIPng operates between the CPE Router and the Service Provider network. RIPng has scaling and security implications for the Service Provider network where one Service Provider router may terminate several tens of thousands of CPE routers. However, RIPng does provide one solution from the CPE Router to the Service Provider network for prefix route injection.

8.3. Firewall

The CPE Router must support an IPv6 Firewall feature. The firewall may include features like access-control lists. The firewall may support interpretation or recognition of most IPv6 extension header information including inspecting fragmentation header. The firewall must support stateful and stateless Packet Filters as follows.

8.3.1. Packet Filters

The CPE Router must support packet filtering based on IP headers, extended headers, UDP and TCP ports etc. There are numerous filters mentioned (section 3.2) in draft-ietf-v6ops-cpe-simple-security [I-D.ietf-v6ops-cpe-simple-security], like some that allow IKE, IPSec packets while another filter may block Teredo packets.

8.4. Zero Configuration Support

The CPE Router MAY support manual configuration via the web using a URL string like http://router.local as per mDNS described in the Terminology and Abbreviations section. Note that mDNS is a link-local protocol, so extra functionality is required if configuration is to be supported over cascaded routers. Support of configuration through cascaded routers is beyond the scope of this document.

8.5. 6to4 Automated Tunneling

If the IPv4 address assigned to the WAN interface of the CPE Router is a non-[RFC1918] IPv4 address, and the CPE Router fails to acquire an IPv6 address, then the 6to4 tunneling protocol [RFC3056] MAY be enabled automatically, allowing tunneling of IPv6 packets over IPv4

without requiring user configuration.

6to4 can be useful in the scenario where the Service Provider does not yet support IPv6, but devices in the home use IPv6. An IPv6 address is constructed automatically from the IPv4 address (V4ADDR) configured on the interface using the prefix 2002:V4ADDR::/48. A 6to4 tunnel can be automatically created using a pre-configured 6to4 gateway end-point for the tunnel.

8.6. Emerging IPv6 Transition Mechanisms Support

Several proposals are being considered by IETF related to the problem of IPv4 address depletion, but have not yet achieved working group consensus for publication as an RFC. Dual-stack lite durand-softwire-dual-stack-lite-00 [I-D.durand-softwire-dual-stack-lite] will require the CPE Router to support features such as v4 in v6 encapsulation and softwires. When the Dual-stack lite work becomes an RFC this section will be revisited.

8.7. DNS Support

For local DNS queries for configuration, the CPE Router may include a DNS server to handle local queries. Non-local queries can be forwarded unchanged to a DNS server specified in the DNS server DHCPv6 option. The CPE Router may also include DNS64 functionality. In that case, the prefix used is either a well-known prefix or configured through DHCPv6 or SNMP. An A record is simply passed through untouched. An AAAA record is relayed to the server. If the CPE Router receives no response, then an A query is used. If the A query returns a response, then an AAAA record is synthesized using the prefix and sent to the host. If DNSSEC is used, then both an A record (authenticated with DNSSEC), and the synthesized AAAA record (possibly tagged as synthetic with an EDNS0 option, IDENT bit(s), or using a well-known prefix) is returned. This allows unmodified hosts to simply use the synthetic AAAA record (without DNSSEC). Modified hosts can look at the DNSSEC A record, authenticate it, then synthesize its own AAAA record in a stub resolver located in the host. Therefore, unmodified hosts can get connectivity, but modified hosts can also authenticate DNS records.

8.8. Quality Of Service(QoS)

The CPE router MAY support differentiated services [RFC2474].

9. IPv4 Support

IPv4 support is largely out of scope for this document. However, a

brief overview of current practice in the market may be helpful since the CPE Router may support both IPv4 and IPv6. This section does NOT require the CPE Router to support IPv4. For background information on IPv4 routing capabilities, please refer to [RFC1812]. Typically, CPE Routers which support IPv4, also support IPv4 NAT for translating private [RFC1918] addresses (e.g. 192.168.x.x) into a single non-[RFC1918] WAN address assigned through DHCPv4 or manually configured. In addition to NAT, CPE Routers that support IPv4 typically also support Application Layer Gateway functionality (ALG), such as the FTP ALG. The IPv4 NAT functionality typically has a built-in DHCPv4 server. A CPE Router which supports IPv4 also supports ARP and basic unicast IPv4 forwarding. Some CPE Routers which support IPv4 also support IPv4 multicast forwarding ([RFC5135]) and basic firewall capabilities. A stateful firewall can enhance security by examining the state of each connection and only allow traffic which conforms to an expected packet flow.

10. Security Considerations

Security considerations of a CPE router are covered by draft-ietf-v6ops-cpe-simple-security [I-D.ietf-v6ops-cpe-simple-security].

11. IANA Considerations

None.

12. Acknowledgements

Thanks (in alphabetical order) to Antonio Querubin, Bernie Volz, Carlos Pignataro, Dan Wing, David Miles, Francois-Xavier, Fred Baker, James Woodyatt, Mark Townsley, Mikael Abrahamsson, Ole Troan, Remi Denis-Courmont, Shin Miyakawa, and Tony Hain for their input on the document.

13. References

13.1. Normative References

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

13.2. Informative References

[I-D.durand-softwire-dual-stack-lite]
Durand, A., Droms, R., Haberman, B., and J. Woodyatt, "Dual-stack lite broadband deployments post IPv4 exhaustion", draft-durand-softwire-dual-stack-lite-00 (work in progress), September 2008.

[I-D.ietf-6man-ipv6-subnet-model]
Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet Model: the Relationship between Links and Subnet Prefixes", draft-ietf-6man-ipv6-subnet-model-02 (work in progress), October 2008.

[I-D.ietf-6man-node-req-bis]
Loughney, J., "IPv6 Node Requirements RFC 4294-bis", draft-ietf-6man-node-req-bis-01 (work in progress), February 2008.

[I-D.ietf-softwire-hs-framework-l2tpv2]
Storer, B., Pignataro, C., Santos, M., Stevant, B., and J. Tremblay, "Softwire Hub & Spoke Deployment Framework with L2TPv2", draft-ietf-softwire-hs-framework-l2tpv2-10 (work in progress), October 2008.

[I-D.ietf-v6ops-cpe-simple-security]
Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service", draft-ietf-v6ops-cpe-simple-security-03 (work in progress), July 2008.

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[RFC2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

[RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, November 1998.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC2669] St. Johns, M., "DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems", RFC 2669, August 1999.

[RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC3569] Bhattacharyya, S., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC3646] Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC3769] Miyakawa, S. and R. Droms, "Requirements for IPv6 Prefix Delegation", RFC 3769, June 2004.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4241] Shirasaki, Y., Miyakawa, S., Yamasaki, T., and A. Takenouchi, "A Model of IPv6/IPv4 Dual Stack Internet Access Service", RFC 4241, December 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.

[RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC5072] S.Varada, Haskin, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, September 2007.

[RFC5135] Wing, D. and T. Eckert, "IP Multicast Requirements for a Network Address Translator (NAT) and a Network Address Port Translator (NAPT)", BCP 135, RFC 5135, February 2008.

Appendix A. CHANGE HISTORY

[NOTE TO RFC EDITOR: PLEASE REMOVE THIS SECTION UPON PUBLICATION.]

Changes in draft-wbeebee-ipv6-cpe-router-03.txt since -02.txt are:

- Added new text to the Abstract to clarify what our vision of the CPE Router is.
- Clarified the WAN interface definition in the "Terminology and Abbreviations" section. Also changed Introduction section to allow more than one WAN interface.
- Added text for zero LAN to Introduction section and also changed LAN interface definition in the "Terminology and Abbreviations" section.
- Removed last sentence in Introduction section for LAN interfaces being only Ethernet encapsulation. "Each LAN interface is Ethernet encapsulated."

- Changed "Acquire" to "Construct" for use with link-local addresses.

- Changed first sentence of the "Basic IPv6 Provisioning" section from "The CPE Router needs to support two WAN interface models, one of which will be active on the CPE Router at any given time." to "The CPE Router MUST support at least one of two WAN interface models, one of which will be active on the CPE Router at any given time."

- Added following text to the "Unnumbered Model" section: "When the Loopback or the LAN interface is used to source WAN-facing traffic, both the CPE Router and the Service Provider Router must consider the traffic to be off-link to the link connecting the CPE Router with the Service Provider Router."

- Added following text to the end of the "Unnumbered Model" section: "The unnumbered model is incompatible with the strong host model on the CPE router. The unnumbered model may be inappropriate for use with certain broadband deployments where a device that uses the strong host model can operate as a CPE Router."

- Re-wrote the multicast section to mostly reference RFC4605.

- Added a short paragraph for null route towards the end of "IPv6 Data Forwarding" section.

- Added a Zeroconf section.

- Added a DNS Support section.

- Cleaned up "Basic IPv6 Provisioning" section to reflect what was presented as cleanup to IETF 72.

- Added text to the "IPv6 over PPP" section to reference section 5.3 for SLAAC/DHCPv6 and IA_PD acquisition.

- Language in first paragraph of the "IPv6 Provisioning of Home Devices" section has been toned down for DHCPv6 vs SLAAC for address acquisition by home devices.

- Add new section called "6to4 Automated Tunneling".

- Added a new section called "Emerging IPv6 Transition Mechanisms Support" to track SNAT and dual-stack lite draft.

- Added a new section called "IPv4 Support", which documents observations about current practice for IPv4 CPE Routers.

Changes in draft-wbeebee-ipv6-cpe-router-02.txt since -01.txt are:

- Added a new section called Conceptual Configuration Variables to list optional configuration variables.

- Removed the following sentence from the LAN initialization before WAN initialization section. "Note that if the home does not cascade CPE routers, then ULA's are not needed for the LAN interfaces, since link-local addresses are sufficient for configuration."

- Removed the following sentence from IPv6 Data Forwarding Section. "Each protocol that the CPE Router can forward packets for must have a separate routing table."

- Removed the following sentence from IPv6 Data Forwarding Section because once it was explained what the sentence is describing, reviewers said the facts are obvious for a router. "Before forwarding a packet in any direction from CPE router, the CPE Router will perform a MAC rewrite operation that rewrites the source L2 address of the packet with CPE Router's WAN or LAN interface MAC address."

- Reworded the QoS section and added a reference to [RFC2474].

- Changed hyphenated 6-to-4 text in the Path MTU Discovery Support section to IPv6 to IPv4.

- Added a new IPv6 over PPP section.

- Added a new Softwires section.

- Added one new sentence at the end of second paragraph of the IPv6 Provisioning of Home Devices for renumbering behavior for the CPE Router network interfaces.

- Added a new section called "Emerging IPv6 Transition Mechanisms Support.

- Added a new section called "IPv4 Support".

- Some text int the "Path MTU Discovery Support" section was changed to clarify text.

Changes in draft-wbeebee-ipv6-cpe-router-01.txt since -00.txt are:

- Added to Abstract to explain better what is the scope of the CPE Router document.

- In Introduction section, changed WAN port from only Ethernet encapsulation to also support other encapsulation types like PPP.

- Added another router initialization mode of LAN first before WAN to Router Initialization section.

- Split up Acquire IPv6 address and other configuration parameters section into two sub-sections to support no global IPV6 address assigned to WAN interface. Added details as to how WAN interface works without a global IPv6 address.

- IPv6 Provisioning of Home Devices section was split up into two sections called LAN initialization before WAN initialization and WAN initialization before LAN initialization. Details have been provided for workings of the CPE Router in such initialization modes.

- New section called Cascading of Routers behind the CPE Router was added.

- Text of draft between sections 4-5 has a lot of shuffling around to accommodate new initialization modes and two different kind of WAN interface address support.

Authors' Addresses

Hemant Singh
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Phone: +1 978 936 1622
Email: shemant@cisco.com
URI: http://www.cisco.com/

Wes Beebee
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Phone: +1 978 936 2030
Email: wbeebee@cisco.com
URI: http://www.cisco.com/

Full Copyright Statement

Intellectual Property