White Paper

Using PPPoE and IPoE in Ethernet Broadband Networks

Comparing the Protocols for Service Delivery and Subscriber Management

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Part Number: 200187-002 Jan 2008

Table of Contents

Executive Overview

Point-to-Point Protocol (PPP) has been a dominant session control protocol in wireline broadband networks, first in dial-up networks and then evolving to support DSL. Until recently, PPP was the only transport mechanism allowed by the DSL Forum[1]. The DSL Forum[2] now also allows using IP over Ethernet (IPoE). IPoE relies on Dynamic Host Configuration Protocol (DHCP) to provide many of the capabilities provided by Point-to-Point Protocol over Ethernet (PPPoE).

The connection-oriented PPP is the most widely deployed method for providing many broadband services, but the connection-less IPoE has been enhanced to allow its use in many broadband networks. This paper reviews the capabilities of PPP and IPoE relevant to broadband networks. Related protocols used to provide the overall connection are also included.

Introduction: Broadband Session Requirements

The most fundamental requirement for offering broadband service is the establishment of a network connection for each subscriber that can be used to control network access. Establishing this connection consists of several phases:

1. User authentication—once the link is established, the identity of the user must be validated (authenticated) before the subscriber has access to the network.
2. Address assignment—once authenticated, the user must be assigned an IP address so that he/she can access the applications.
3. Access control—the network must authorize which network resources (services) the user can use. This can be as simple as limiting Internet access speed based on what the subscriber has signed up for.
4. Monitor the connection—each connection must be monitored to ensure that the subscriber is still connected to the network.

PPPoE and IPoE are the two primary techniques available for performing these tasks. IPoE is also sometimes referred to as "DHCP" since that protocol plays a key role in the overall IPoE connection establishment.

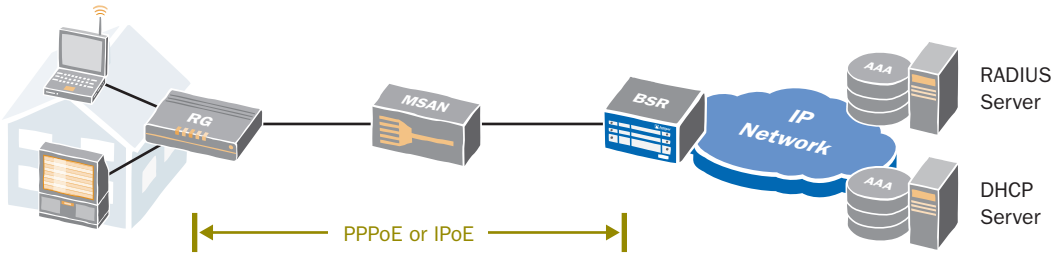

Figure 1: Broadband Network Overview

Figure 1 depicts a simple broadband network. A device that terminates only PPPoE sessions is called a Broadband Remote Access Server (BRAS). A Broadband Services Router (BSR) supports IPoE sessions in addition to PPPoE[3].

[1]DSL Forum TR-025 *Core Network Architecture for Access to Legacy Data Network over ADSL and TR-059 DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services* can be downloaded from http://www.dslforum.org/techwork/treports.shtml

[2]DSL Forum's Technical Report 101 (TR-101), Migration to Ethernet-Based DSL Aggregation.

[3]Buyer beware: Some BSRs do not terminate PPPoE traffic but instead only support non-PPPoX implementations.

Introduction to PPPoE

PPP is used for communications between two nodes, such as between a client and a server. Originally defined for a direct connection between devices over a leased line using ISO 3309 framing, several methods have been defined to establish PPP connections across other media. These include PPP over ATM (PPPoA), PPPoE, and PPP over SONET/SDH (POS).

PPPoA was the connection method originally specified by the DSL Forum, and is the most prevalent method for connecting broadband users into the network. At an intermediate point such as a multiservice access node (MSAN), such as a digital subscriber line access multiplexer (DSLAM) or edge router, the individual subscriber sessions are aggregated onto a single ATM uplink. As networks transition to Ethernet, PPPoE is the successor to PPPoA. As depicted in Figure 2, PPPoE is used between the residential gateway and the BSR.

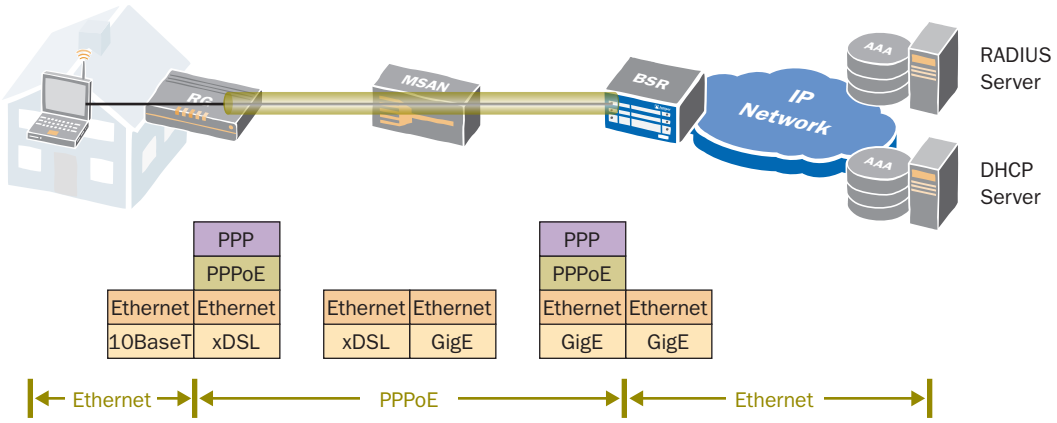

Figure 2: PPPoE Protocol Stack Overview

Since PPP supports switched connections such as dial-in users, it is well suited to support individual broadband-attached subscribers.

Figure 3 provides an overview of the PPPoE session establishment process, plus the periodic monitoring for session aliveness. First, the PPPoE connection is established per RFC2516. Second, the link connection is established using PPP's Link Control Protocol (LCP). This optional phase negotiates link-level parameters such as the authentication method and whether compression will be used. Third, the subscriber is authenticated as part of the connection establishment, typically using Challenge Handshake Authentication Protocol (CHAP[4]). Alternatively, other authentication protocols can be negotiated using Extensible Authentication Protocol (EAP[5]). Finally, Internet Protocol Control Protocol (IPCP[6]) is used to assign an IP address. At this point the subscriber can access the network. In addition, PPP includes a means of monitoring link availability. Each of these steps is discussed below in more detail.

[4]RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP)

[5]RFC 3748, Extensible Authentication Protocol (EAP)

[6]RFC 1332, The PPP Internet Protocol Control Protocol (IPCP)

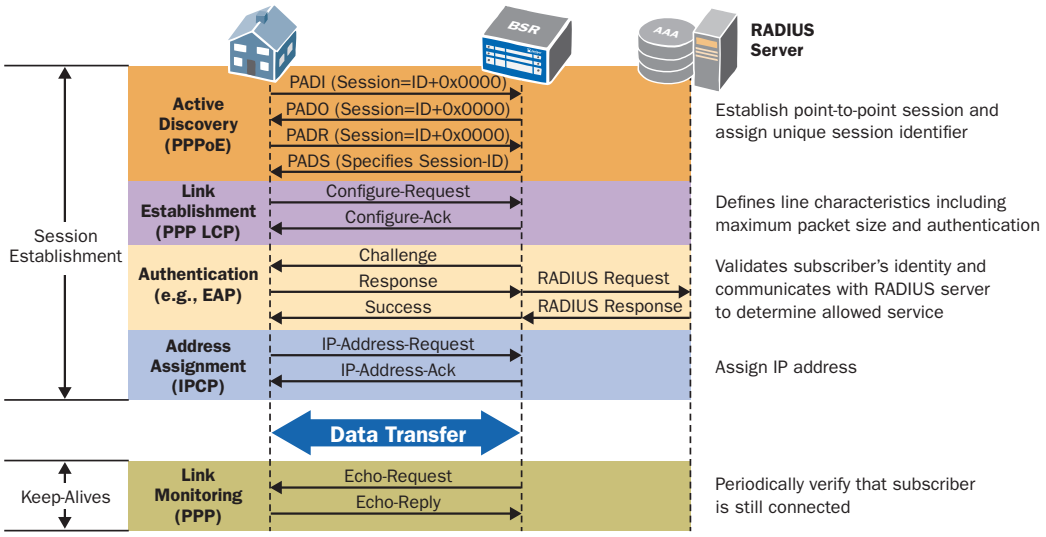

Figure 3: PPPoE Connection Establishment

PPPoE Session Establishment and PPP Link Establishment

PPPoE includes a straightforward mechanism for the host to find a PPPoE server with which to communicate. The host broadcasts a request to "initiate" a session (PADI); all potential PPPoE servers respond with an "offer" (PADO) to be the termination point; the host indicates which offer will be accepted by "requesting" a session (PADR); and the PPPoE server responds by assigning a "session identifier (*session-id*)" (PADS).

The PPP session identifier uniquely identifies the subscriber, which does not change for the life of the session. Once the session establishment phase is complete, it can be used to track which services can be used by each subscriber.

PPPoE flows may also include the PPP link establishment phase. Originally used to establish the dial-up connection, this phase negotiates line characteristics such as the maximum transmission unit (MTU) size and the authentication protocol to be used.

PPPoE Subscriber Authentication

PPP authenticates users before allowing them access to the network, typically by requiring that the user log into the network using an assigned user id and password[7].

Subscriber Management Server: Tight RADIUS Integration

During this authentication phase, the network assigns attributes to individual subscribers by forwarding the login request to a RADIUS server. The RADIUS server returns information that specifies how to treat traffic for this subscriber, including information such as:

- What services the subscriber can access, such as the Internet access tier (upload/download speeds allowed) or whether he/she has signed up to receive IPTV service.
- Appropriate quality of service (QoS) markings. For example, a subscriber who has signed up for a VoIP service will have this traffic marked as high priority, while subscribers that have not signed up for this service will have VoIP traffic marked for "best effort" delivery.

[7]In broadband networks, this information is often programmed into the PC or Residential Gateway (RG) during network setup. The subscriber is unaware that this information is being sent. In addition, many service providers no longer authenticate the user and instead authorize network access based on the physical DSLAM port to which the user is connected.

Once the session gets successfully established, RADIUS accounting will start, allowing the provider to do either time-based or volume-based billing. When the session gets disconnected, either explicitly or by means of missing keep-alives, RADIUS accounting for the session will be closed. The tight RADIUS integration allows for centralized policy and QoS control as well as detailed accounting information on a per subscriber basis. Lawful interception (on a per subscriber basis) can also be enabled via RADIUS.

Wholesale Support

Having a separate login before IP address allocation allows the network to assign different IP addresses based on the service or destination. This is most critical in a "wholesale" network in which each subscriber can select a different content provider (different ISPs to support Internet Access, for example). This powerful aspect of PPP is a key reason why it remains the predominant mechanism for providers offering wholesale services to third-party content providers.

DSL Forum's Technical Report TR-025 defines two models for broadband networks: PPP Terminated Aggregation (PTA) and L2TP Access Aggregation (LAA). PTA is used when the network "pipe" operator also provides the services (retail). LAA is used when the network transport and network services are provided by separate organizations (the "wholesale" model).

When using PTA, the PPP connection is controlled by the network operator. Each PPP session is terminated at the edge router. Forwarding between the edge router and the head-end is done using IP routing.. When using LAA, the PPP connection is controlled by the application service provider. PPP sessions are aggregated but not terminated at the edge router and forwarded to the application provider's data center using L2TP. Equally important, PPPoE allows the broadband operator to easily offer both retail and wholesale services over a single link, as depicted in Figure 4.

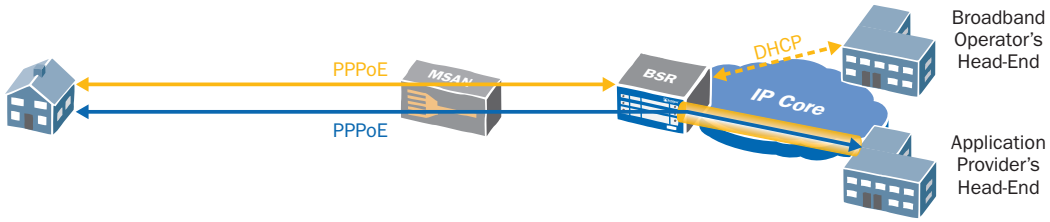

Figure 4: Delivering Retail and Wholesale Services Using PTA (top) and LAA (bottom)

PPPoE Address Assignment

After the subscriber is authenticated, PPP's IP Control Protocol (IPCP as defined in RFC 1332) sends an IP address to the PPPoE client. The PPPoE server may store a range of addresses that can be assigned to clients, or it may get the IP address from an external DHCP server.

PPPoE Session Monitoring

PPPoE typically assumes an "infinite" life for each connection. Session termination occurs only if the connection is lost, such as when the residential gateway is unplugged or an intermediate node gets re-booted. Using PPP keep-alive (echo) messages, both endpoints can monitor whether the session is still up and running. Upon missing a pre-defined number of keep-alives, the session will be terminated.

PPPoE Challenges

PPP has two drawbacks. First, using PPPoE (which also requires PPP) adds 8 bytes to every packet. This requires more processing to create, inspect and terminate each PPP packet than is required by IP over Ethernet (IPoE). Figure 5 depicts a PPPoE frame.

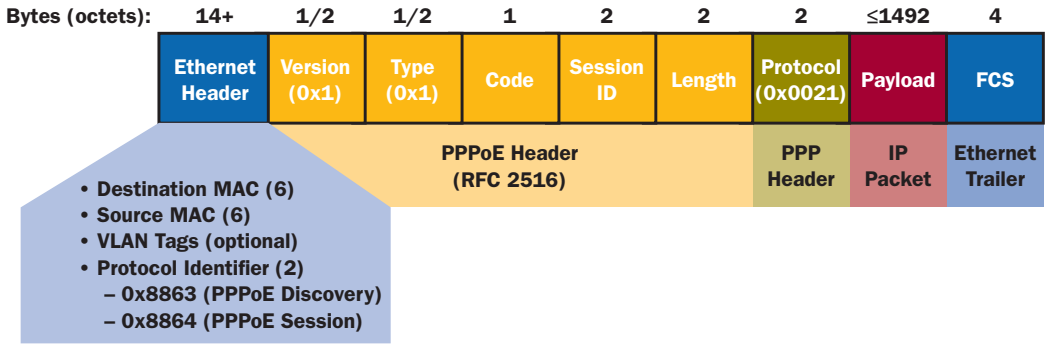

Figure 5: PPPoE Packet Format

The bigger issue is that PPP does not efficiently support multicast traffic. Broadcast television is the first major IP application that relies heavily on multicast delivery to multiple subscribers. Using PPPoE for multicast requires that the edge router terminate a PPP session for each subscriber watching television, as depicted in Figure 6. In this example, the same content (television channel) is sent three times to the MSAN across the same physical link, with each session having a unique PPP session-identifier. This prevents PPPoE from efficiently supporting IP multicast between the edge router and the DSLAM/OLT. This is one of the primary drivers for using IPoE on broadband networks.

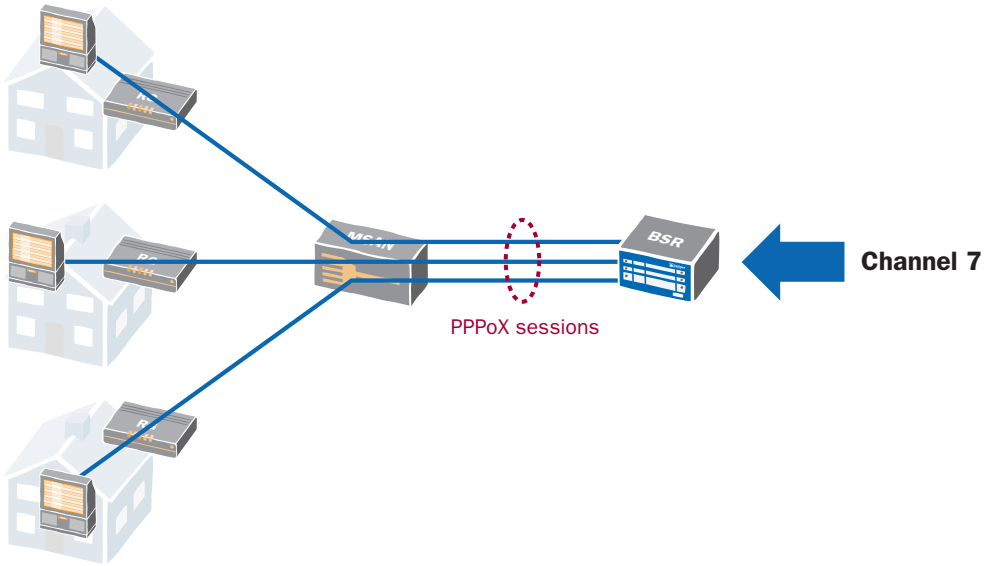

Figure 6: Broadcast Television Distribution Using PPPoE

IP over Ethernet

IPoE is a shorthand way of saying that the broadband traffic is delivered across an Ethernet network without using PPP encapsulation. This more recent alternative relies primarily on DHCP, which was designed to assign an IP address to a LAN-attached device. As such, it did not originally include support for link establishment, subscriber authentication or link monitoring. DHCP extensions and other protocols (such as Extensible Authentication Protocol) are combined with DHCP to provide capabilities similar to PPPoE. Figure 7 overviews the IPoE process when the BSR functions as the DHCP server and can therefore assign IP addresses.

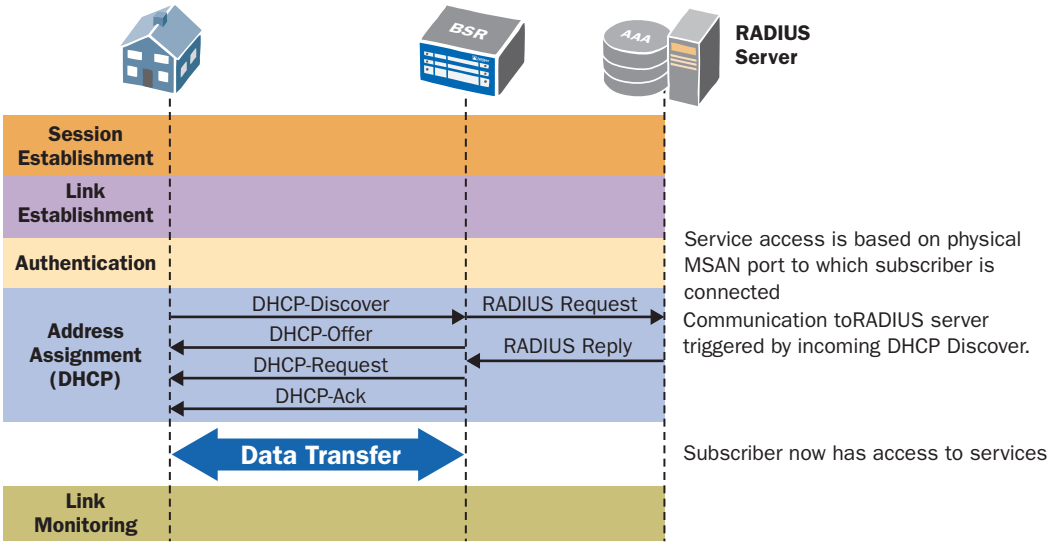

Figure 7: IPoE Connection Establishment (BSR functions as DHCP Server)

IPoE Session Establishment

IPoE does not establish a session between the endpoints, and therefore does not have a unique, permanent subscriber identifier. Therefore, the IP address must be used to identify the subscriber, and steps must be taken to ensure that the IP address assigned to a subscriber does not change, or that the network adapts as the IP address changes.

IPoE Subscriber Authentication

IPoE lacks a subscriber login procedure such as Challenge Handshake Authentication Protocol (CHAP) or Extensible Authentication Protocol (EAP). Therefore, the network uses information about the subscriber's network connection to determine the available services. This can be information passed up by the MSAN about the subscriber's physical connectivity (MSAN node id, slot and port), or can be based on the Ethernet VLAN/ATM VC from which the DHCP request was received.

IPoE advocates argue that there is no need for a separate user login since "always on" broadband users are always connected to a fixed physical port. There are two drawbacks to this approach:

- Recent trends no longer restrict a subscriber to accessing the network from a single location. Rather, broadband access can be from a Wi-Fi hot-spot or a 3G network as well as from the home. In this case, there is no mechanism to uniquely identify the subscriber regardless of how he is connected to the network.
- It prevents the subscriber from dynamically switching between different application service providers (such as ISPs). Using a login process, the subscriber can easily access any domain simply by logging in (for example, user123@domainxyz). In response, the network will assign an IP address appropriate to using that domain. In this case, the problem stems from the fact that the IP address is assigned before the network can check which services are being use.

The ideal solution to this is to use IEEE 802.1X, also known as Extensible Authentication Protocol over LAN (EAPoL). This allows the login mechanisms originally designed for use with PPP to be used across a LAN. However, most DHCP clients do not support this function. In contrast, IEEE 802.1X capability is an integral part of the IEE 802.11i[8] security used in Wi-Fi networks.

Specifying a Configuration File

DHCP includes the ability for the DHCP server to send the client the location of its configuration file, which the client can then download. This is particularly useful for television set-top boxes, since the STB's configuration determines what channels each subscriber can access. The configuration server sends the name of the appropriate configuration file to download, reflecting two key attributes:

- Channels that this subscriber is allowed to view: For example, a subscriber who does not subscribe to a premium tier will not be able to view HBO.
- Geography: For example, subscribers in New York and Boston viewing Channel 7 will see different content, reflecting the "local" television channels available in each market.

Subscriber Management Server

In addition to finalizing the IP address assignment, the DHCP messages from the DHCP server may also include DHCP options which describe how to treat traffic. These attributes are read and stored by the BSR or MSAN. Alternatively, some intermediary devices can serve as a RADIUS Proxy. Upon seeing the initial DHCP DISCOVER request, the device queries a RADIUS server asking for information about how to handle this subscriber's traffic. This allows a single database to support subscribers connected via either method. In addition, RADIUS supports per-subscriber accounting .

IPoE Address Assignment

As depicted in Figure 8, DHCP address assignment operates similarly to the PPPoE discovery phase. When a new device is powered on, it automatically broadcasts a request to be assigned an IP address. One or more DHCP servers respond by offering an IP address, the client responds to the offer it wishes to accept, and the appropriate DHCP server acknowledges that the request can be honored.

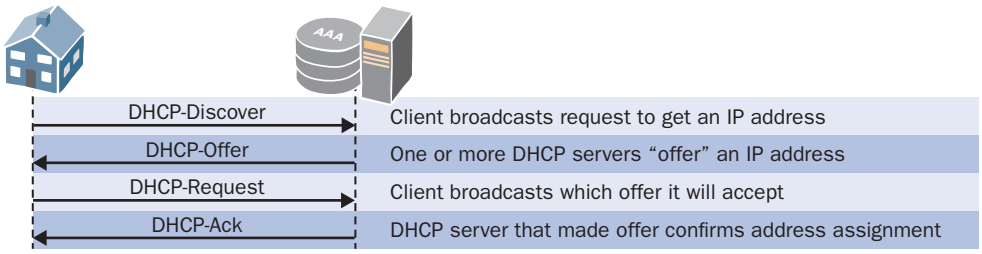

Figure 8: Address Assignment Using DHCP

DHCP across a WAN: DHCP Relay

One challenge is that DHCP packets are broadcast onto the network. The IP addresses may not actually be assigned by the BSR; rather it forwards DHCP flows to a DHCP server. A gateway device, called a DHCP Relay Agent, substitutes unicast IP addresses before forwarding the packet onto the WAN. This requires that the DHCP server's IP address be configured into the relay agent. Figure 9 illustrates how the DHCP relay agent modifies the DHCP packet, with the substitutions highlighted in red.

Alternatively, the BSR can serve as the AAA server, holding a pool of IP addresses to assign to subscribers.

[9]http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

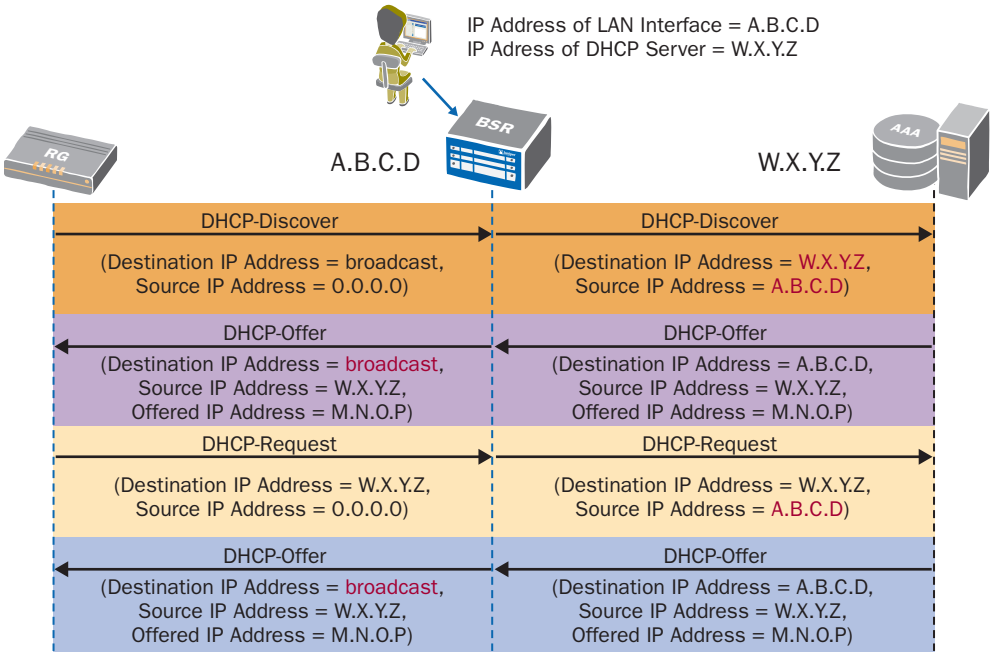

Figure 9: BSR as DHCP Relay Agent

Security Enhancement: DHCP Proxy

The DHCP Relay Agent can also hide the AAA server's address from downstream subscribers, minimizing the opportunity for attacks upon this server. To do this, the DHCP Relay agent substitutes its own IP address for that of the DHCP server as shown in Figure 10. Since the same device often provides both relay and proxy functions, it is a DHCP Proxy Relay Agent.

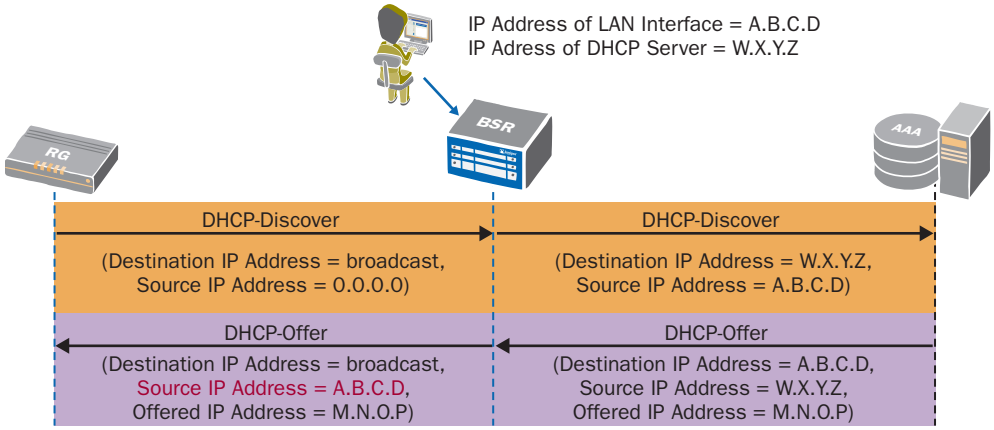

Figure 10: BSR as DHCP Proxy Relay Agent

Minimizing Authentication Requests: Caching of IP Addresses and Lease Information

Another challenge is that IP addresses assigned via DHCP expire after a specified amount of time. Each DHCP-assigned address has a "lease timer" that specifies how long this IP address is valid. When this expires, the client must ask for a new IP address. Since DHCP triggers the RADIUS communications, this is repeated every time a lease expires.

One solution is to ensure that the client does not need to request a new IP address. To do this, the DHCP server can be configured to provide very long leases (often one week or more) for "always on" broadband clients. In addition, DHCP allows clients to request a lease extension by sending a new DHCP REQUEST. Therefore, under normal operation, the broadband client will never need to request a new IP address.

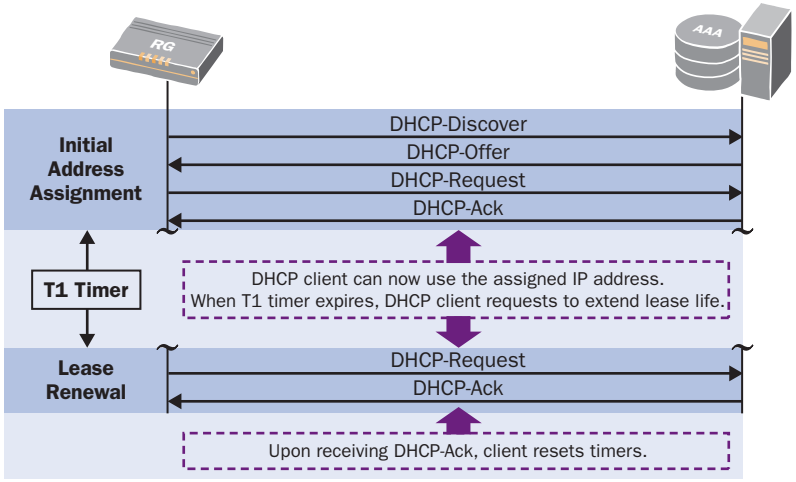

Figure 11: DHCP Lease Renewal

The outstanding issue is an extended network outage, especially for a large network, since there will be many simultaneous requests as soon as the network becomes available. To resolve this, the DHCP Proxy Relay Agent can cache the IP address for each subscriber, including the lease timer, in non-volatile memory. If the network fails, the DHCP Proxy Relay Agent can continue to respond to lease renewal requests. If the DHCP Proxy Relay Agent itself fails, it can respond to renewal requests upon its recovery, using the information cached in its non-volatile memory. Using this approach, only a very long network outage will cause the client's IP address to expire, minimizing the flow of DHCP DISCOVER requests across the network. This places DHCP on a par with PPP-based networks.

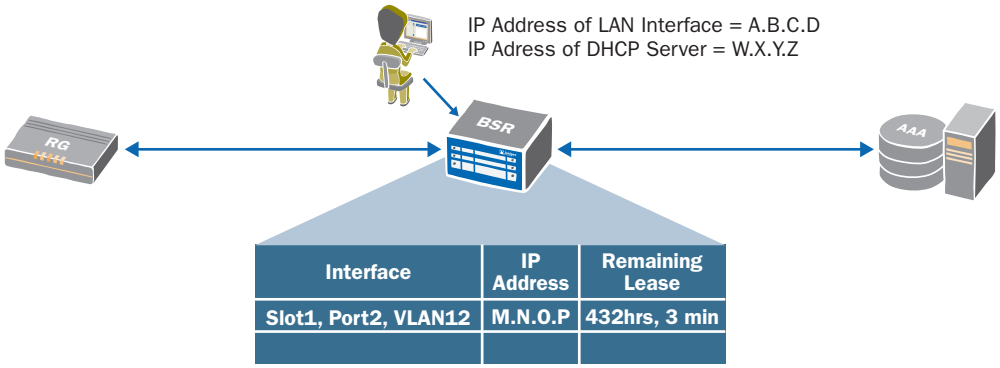

Figure 12: IP Address Cache in DHCP Proxy Relay Agent

IPoE Monitoring

Another benefit of DHCP Proxy Relay is that it allows the DHCP address renewal process to be used as a keep-alive mechanism. It does this by assigning a very short lease time to clients. Since the residential gateway sees a very short lease timer, it continually issues DHCP REQUEST messages to the BSR. If these packets are not received for a specified period, the BSR will assume that the device is down and flush any stored information.

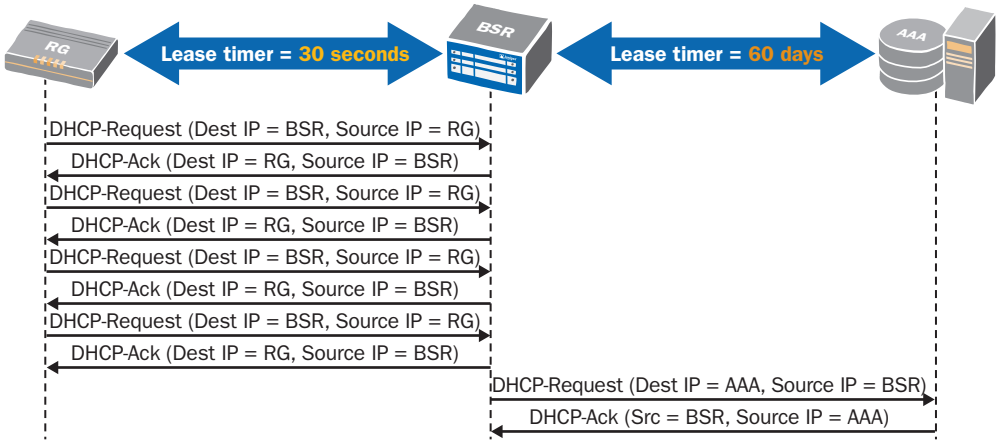

Figure 13: DHCP Proxy with Different Lease Timers

Of course, this means that the DHCP Proxy Relay Agent must modify the lease timers[10] carried in the DHCP flows. At the same time, a long lease continues to be used in the upstream connection.

Summary of Required Extensions to Support IPoE

Successfully supporting IPoE requires a "broadband gateway" device—typically either the MSAN or BSR—to provide the following functions:

- DHCP Relay
- DHCP Proxy, including:
  - Substituting the address of the AAA server
  - Caching of IP addresses and DHCP leases in non-volatile memory (typically in the DHCP Relay Proxy Agent)
  - The ability to generate and respond to DHCP lease renewal requests
- Learn about how to treat traffic to/from this subscriber, either by interpreting vendor-specific DHCP options or by communicating with the RADIUS server whenever a device requests a new IP address

Remaining IPoE Challenges

There are two remaining weaknesses with current DHCP implementations:

- Wholesale Support: For wholesale networks, the lack of a PPP session identifier makes it difficult to dynamically track which application provider each packet is destined for. Each third-party provider therefore requires a unique VLAN, or can be assigned a range of IP addresses.
- IPv6 Migration: PPP allows the service provider to create both IPv4 and IPv6 connections, each with its own session identifier, using the same VLAN. DHCP requires separate VLANs for this to occur.

[10]The DHCP lease timers are defined in RFC 2132. Option 51 (IP address lease time) specifies the lease life. Option 58 (T1 timer) indicates when the client should ask the DHCP server that assigned the lease to extend the lease life, and is typically set to 50% of the original lease life. Option 59 (T2 timer) indicates when the DHCP client should broadcast a request to extend the lease, in case the original server that assigned the lease does not respond. This is typically set to 87.5% of the original lease time.

Deploying PPPoX and DHCP

PPPoX and DHCP can, and often are, deployed to deliver different services on the same network. Typically this means using PPPoE to deliver unicast services such as VoIP and data, while using DHCP to deliver multicast IPTV. This dual approach is most commonly used in wholesale networks, as well as in networks that have already deployed PPPoX to support broadband traffic.

There are two common alternatives, as depicted in Figure 14. The top network has a separate logical connection for each service. Since each of the connections illustrated typically flows across a separate VLAN, this is called a "service VLAN" (or N:1, since there are multiple VLANs to each subscriber) model. In the bottom network, a single PPPoE connection carries all unicast traffic to a given subscriber, with the residential gateway acting as a local DHCP server and providing NAT functionality. This is the "customer VLAN" (or 1:1, since there is one VLAN per subscriber) model. In either case, multicast IPTV is carried using a separate DHCP-based service VLAN[11].

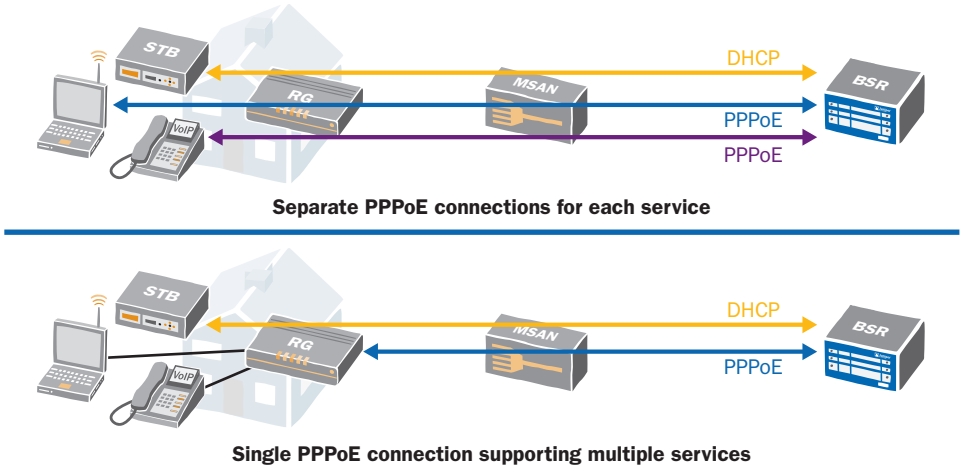

Figure 14: Network Connection using PPPoE and DHCP

Juniper Networks Broadband Support

Juniper Networks E-series Broadband Service Routing Platform (E-series) supports subscribers connected via PPP and/or IPoE. In addition to providing all of the functionality to support traditional PPPoX-based broadband networks, E-series routers provide extensive IPoE support that includes:

- Dynamically learning about new subscribers from DHCP requests
- Issuing requests to RADIUS servers based on received DHCP requests
- Serving as the network's DHCP server
- Implementing DHCP Relay and DHCP Proxy
- Supporting PTA and LAA

For a detailed discussion of how Juniper E-series supports DHCP, see http://www.juniper.net/solutions/literature/app_note/350086.pdf.

[11] For additional information on customer and service VLANs, see VLAN Design for Broadband Networks, www.juniper.net/solutions/literature/white_papers/200186.pdf

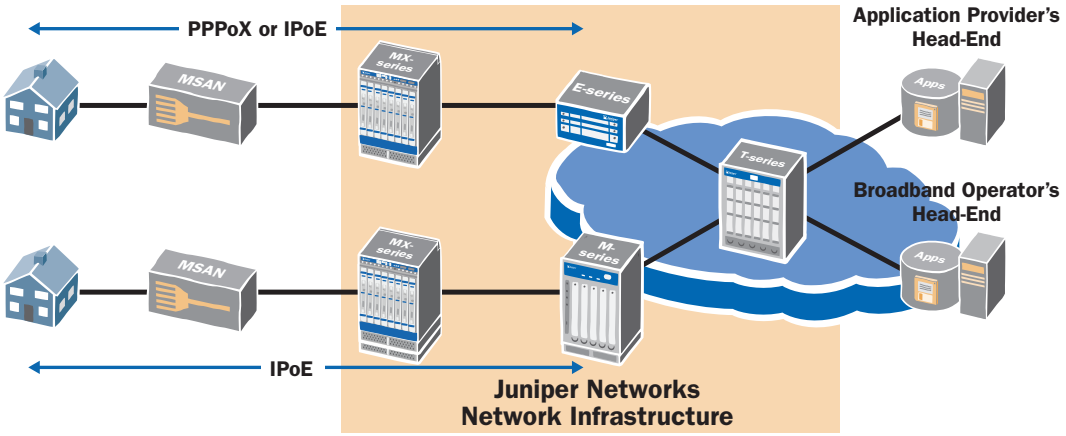

Figure 15: Juniper Networks Infrastructure for Wireline Broadband Networks

Summary

Table 1 provides a brief comparison of PPPoE and IPoE when supporting broadband networks. PPPoE remains the most powerful and dominant protocol for managing connections to individual subscribers. It remains the most mature method of supporting broadband users, and is the only method that can adequately support a wholesale environment. In addition, it simplifies the migration to IPv6 and supports integrated link quality monitoring.

DHCP has been enhanced to allow IPoE to be useful in specific circumstances, and today can be exclusively used in many broadband networks. In addition, IPoE can be incrementally introduced into a PPPoX-based network to support IPTV and/or new subscribers.

Table 1: Comparison of PPPoX and IPoE

Feature	PPPoX	IPoE
Session Establishment	PPP session-identifier uniquely identifies subscriber connection	Connectionless—use IP address as customer identifier
Subscriber Authentication	Triggered by automated login using CHAP, PAP or other EAP-supported method	Triggered by incoming DHCP Discover packet
Authentication Server	RADIUS	DHCP (some implementations allow use of RADIUS)
Address Assignment	DHCP (with DHCP Relay) based on subscriber login	DHCP (with DHCP Relay), based on physical port, VLAN or VC
Monitoring	LCP echo commands provide Integrated keep-alive mechanism	Using DHCP Proxy allows DHCP lease renewal requests to function as keep-alive
Additional Strengths	Wholesale support; IPv6 support	Point to multipoint support
Additional Weaknesses	Overhead on each packet (8 bytes)	Re-authenticate whenever IP address changes. (Using DHCP Proxy mitigates this issue)

References

Authentication

- *RFC 1334 - PPP Authentication Protocols:* http://www.faqs.org/rfcs/rfc1334.html
- *RFC 1994 - PPP Challenge Handshake Authentication Protocol:* http://www.faqs.org/rfcs/rfc1994.html
- *EAP: PPP EAP:* http://www.faqs.org/rfcs/rfc3748.html
  - EAP Authentication Methods: http://www.iana.org/assignments/eap-numbers
- *EAPoL (IEEE 802.1X): Port-Based Network Access Control:* http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

RADIUS

- *RFC 2865 - RADIUS:* http://www.faqs.org/rfcs/rfc2865.html
- *RFC 2866 - RADIUS Accounting:* http://www.faqs.org/rfcs/rfc2866.html
- *RFC 2869 - RADIUS Extension:* http://www.faqs.org/rfcs/rfc2869.html

PPP

- *RFC 1661 - The Point-to-Point Protocol:* http://www.faqs.org/rfcs/rfc1661.html
- *RFC 2364 - PPP over ATM AAL5:* http://www.faqs.org/rfcs/rfc2364.html
- *RFC 2516 - PPPoE:* http://www.faqs.org/rfcs/rfc2516.html
- *RFC 1570 - PPP LCP Extensions:* http://www.faqs.org/rfcs/rfc1570.html
- *RFC 1332 - PPP IP Control Protocol:* http://www.faqs.org/rfcs/rfc1332.html

DHCP

- *RFC 951 - Bootstrap Protocol:* http://www.faqs.org/rfcs/rfc951.html
- *RFC 2131 - DHCP:* http://www.faqs.org/rfcs/rfc2131.html
- *RFC 2132 - DHCP and BOOTP Vendor Extensions*: http://www.faqs.org/rfcs/rfc2132.html
  - Specifies DHCP Options 51 (lease timer), 58 (T1 timer) and 59 (T2 timer)

DHCP Relay Agent

- *RFC 1542 -* Clarifications and Extensions for the Bootstrap Protocol: http://www.faqs.org/rfcs/rfc1542.html
  - Describes the DHCP/BOOTP Relay Agent
- *RFC 3046 -* DHCP Relay Agent Information Option: http://www.faqs.org/rfcs/rfc3046.html
  - Specifies DHCP Option 82, which is added by the DHCP Relay Agent to identify the originator of this DHCP request. This allows the DHCP server to assign the appropriate attributes for this subscriber.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS FOR
NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44.(0).1372.385500
Fax: 44.(0).1372.385501

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978.589.5800
Fax: 978.589.0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803