White Paper

Understanding PPPoE and DHCP

Marc Bernstein
IPTV Solutions

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200187-001 May 2006

Contents

Executive Overview

Point-to-Point Protocol (PPP) has been a dominant session control protocol in service provider networks, first in dial-up networks and then evolving to support broadband DSL. Until recently, PPP was the only transport mechanism allowed by the DSL Forum[1]. The DSL Forum now[2] also allows using IP over Ethernet (IPoE), which is based on DHCP. However, PPP remains the more mature and robust method for providing many broadband services.

PPP was designed to support subscriber authentication and address assignment while DHCP is more limited due to its heritage as a LAN IP address assignment protocol. These limitations have been appended with the introduction of protocols such as IEEE 802.1x for access security. Still, DHCP-based networks do not meet all the requirements of broadband networks.

This paper reviews the capabilities of PPP and DHCP relevant to broadband networks. Related protocols used to provide the overall connection are also included.

Session Requirements

Providing these capabilities requires that the network establish sessions between the subscriber and the application. This session can then be used to manage the subscriber's connection to the network. Establishing the session consists of several phases:

1. Establish the physical link. In broadband networks, this can be used to establish the connection bandwidth. This can be statically defined or dynamically determined.
2. Establish the session. There will be one or more logical sessions from the subscriber (or more specifically, from the subscriber's applications) to the network. Each session can be uniquely tracked and managed.
3. Authenticate and authorize the user. Once the link is established, the identity of the user must be validated (authenticated) before the subscriber has access to the network. Typically this is done by having the subscriber provide a user login and password. Once the subscriber's identity is validated, the network must authorize which network resources (services) the user can access.
4. Identify the user. Once authenticated, the user must be assigned a network address so that he/she can access the applications.
5. Monitor the network. Each portion of the network should be monitored to ensure that the network is available for use. Often the simplest way to do this is to monitor each logical connection.

There are two primary techniques available for performing these tasks. These mechanisms, PPPoE and IPoE, are described below. IPoE is also sometimes referred to as "DHCP" since that protocol plays a key role in the overall IPoE session.

[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.*

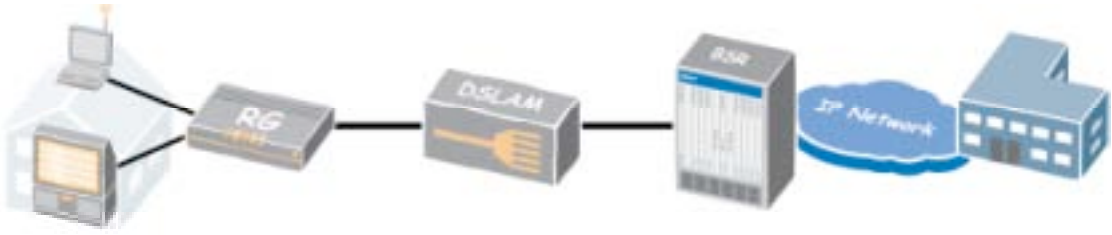

Figure 1: Broadband Network Overview

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

Introduction to PPPoE

Point-to-point Protocol (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), PPP over Ethernet (PPPoE), and PPP over SONET/SDH (POS).

PPP over ATM (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 DSLAM or edge router, the individual PPPoA sessions are aggregated onto a single ATM VC uplink. This allows the network to scale, since the backbone could not scale to support a unique ATM VC for each subscriber.

As networks transition to Ethernet, PPPoE has emerged as an alternative to PPPoA. There are several advantages to PPPoE. PPPoE can be implemented in software on PCs, while PPPoA requires a special ATM line card (or a DSL modem which supports PPPoA). In addition, PPPoA requires a separate ATM VC for each service, while PPPoE allows multiple services over the same connection.

[3] Buyer beware: Some BSRs do not terminate PPPoE traffic.

Figure 2 overviews a basic PPPoE network configuration. In PPPoE-based DSL networks, the Residential Gateway (RG) adds a PPP header which is then terminated at the BRAS. The PPP client resides at the subscriber site and can be a DSL modem or other routing gateway (RG).

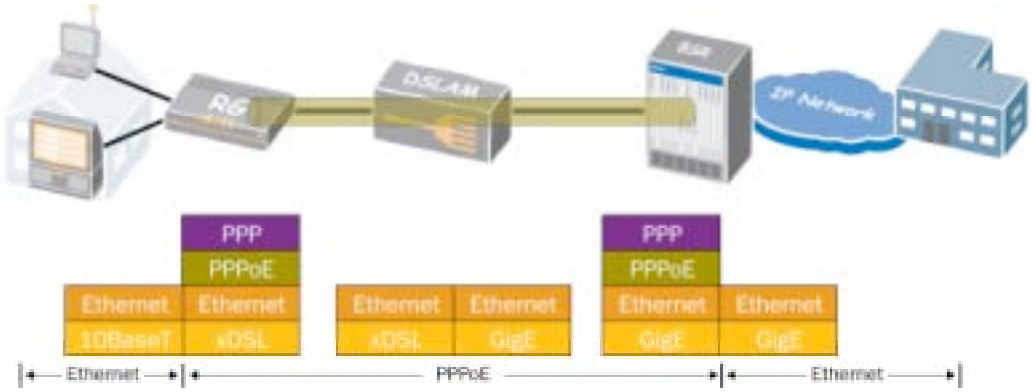

Figure 2: PPPoE Overview

Since PPP was designed to support switched connections such as dial-in users, it is well-suited to support individual subscribers. First, the link connection is established using Link Control Protocol (LCP). Second, the subscriber is authenticated as part of the connection establishment. Third, a Network Control Protocol (NCP) establishes the protocol parameters used for communications. Internet Protocol Control Protocol (IPCP) is the NCP used to establish an IP connection over the established link, including assigning an IP address to the client. At this point the subscriber can access the network, and PPP includes a means of monitoring link quality and availability.

Figure 3 provides an overview of PPPoE session establishment. Although the entire lifecycle is depicted, the "always-on" broadband connections are rarely (if ever) terminated normally.

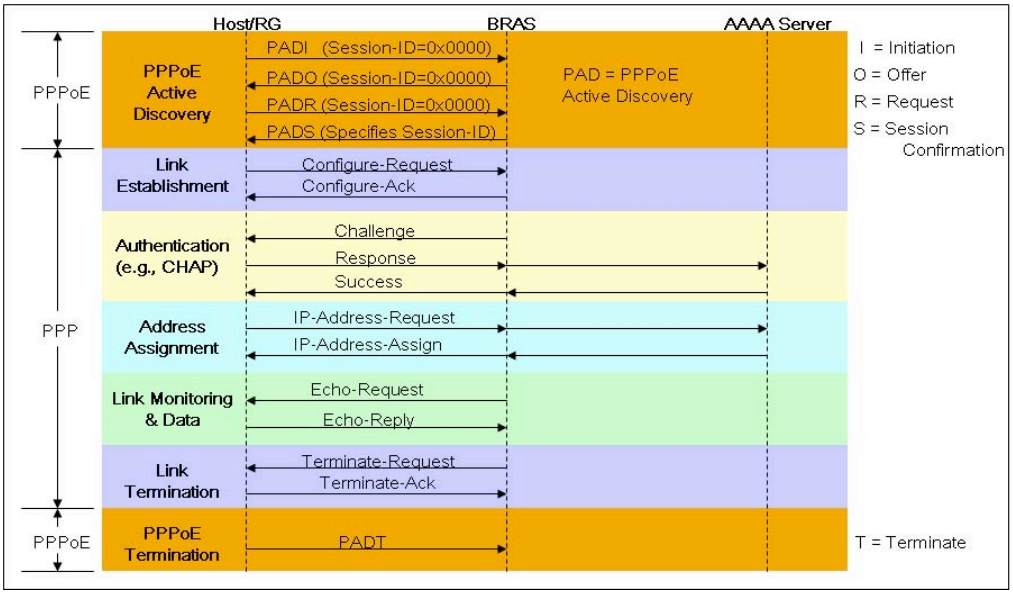

Figure 3: PPPoE Session Flows

PPP maps quite well to the subscriber management requirements required for DSL and other broadband access networks.

PPPoE Session Establishment

PPPoE includes a straightforward mechanism for the host to find a PPPoE server/BRAS to communicate with. The host broadcasts a request to establish a connection (PADI); all potential BRAS devices respond (PADO) with an "offer" to be the termination point; the host selects one (PADR); and the BRAS responds by assigning a session identifier (*session-id*).

PPPoE flows also typically include the PPP link establishment phase. Originally used to establish the dial-up connection, this phase negotiates line characteristics such as the maximum MTU size, the authentication protocol to be used, and the link quality monitoring 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 userid and password[4].

PPP authentication is tightly integrated with RADIUS. 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 allows the BRAS to determine what to do with the session (filters, multicast enable/disable, bandwidth control, QoS control, policy routing rules, L2TP LNS destination, etc.). Once the session gets successfully established, RADIUS accounting will start which allows to provider to do either time-based or volume-based billing. When the session gets disconnected, either explicitly or by means of missing keepalives, RADIUS accounting for the session will be closed by means of RADIUS accounting stop messages.

Offloading the session establishment, control, and accounting to RADIUS simplifies subscriber management. Subscriber-specific data is kept offline in the RADIUS system and the subscriber sessions are created dynamically during PPP LCP and IPCP transactions. The BRAS acts as an intelligent mediation device between the client, AAA, and policy system while acting as the IP control point at the network edge.

These aspects of PPP enable subscriber control in an automated and centralized fashion. The session concept with its short keepalive interval allows the service provider to have accurate accounting data for each subscriber and maintain an accurate view on when subscribers are actually online which could be important for legal purposes. The tight integration with RADIUS allows for centralized policy and QoS control plus detailed accounting information on a per subscriber basis, so whenever services change there is no need to touch any access equipment or to reprovision any subscriber's connection. Enabling lawful interception on a per subscriber basis can now also completely enabled via RADIUS making the RADIUS integration even more complete.

[4] 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 additional, 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.

PPPoE Address Assignment

PPP includes a process for assigning Layer 3 attributes using network control protocols (NCPs). The NCP used to assign IP addresses within a PPP connection is IP Control Protocol (IPCP). IPCP is described in RFC 1332.

The separation between link establishment and IP address allocation makes it possible to figure out who the subscriber is before deciding how to treat his session: Either terminate the session locally or tunnel the session to a wholesaler. The domain name provided in the user's credentials enables automated service or ISP selection. This powerful aspect of PPP is a key reason dictating why PPP will remain the predominant session protocol for providers that are offering wholesale services to third party ISPs.

PPPoE Session Monitoring

Another important aspect of PPP is that it is a session-based protocol which monitors line quality. Using PPP keepalives, both endpoints can monitor whether the session is still up and running. Typical keepalive times are in the order of 30 seconds. Upon missing a few consecutive keepalives, the BRAS will terminate the session and clean up all state information. The client will typically try to re-establish the session automatically. In case of redundant BRAS setups (more typical for Ethernet-DSL than for ATM-DSL), the redundant BRAS could now start to accept incoming PPP sessions.

More advanced line monitoring can also be done using PPP Link Quality Monitoring (LQM), which is defined in RFC 1989.

PPPoE Strengths

Support for Retail and Wholesale

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

Retail Service: PPP Terminated Aggregation (PTA)

When using PTA, the PPP connection is controlled by the network operator. Each PPP session is terminated at the edge router. Forwarding from the edge router to the head-end is done using IP routing.

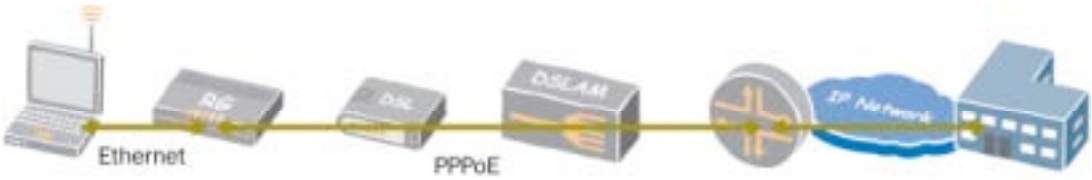

Figure 4: PPP Terminated Aggregation (PTA)

Wholesale Service: L2TP Access Aggregation (LAA)

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/head-end using L2TP.

Figure 5: L2TP Access Aggregation (LAA)

Combining Wholesale and Retail

Equally important, PPPoE allows the telco to easily offer both retail and wholesale services over a single logical connection (VLAN or VC) as depicted in Figure 6.

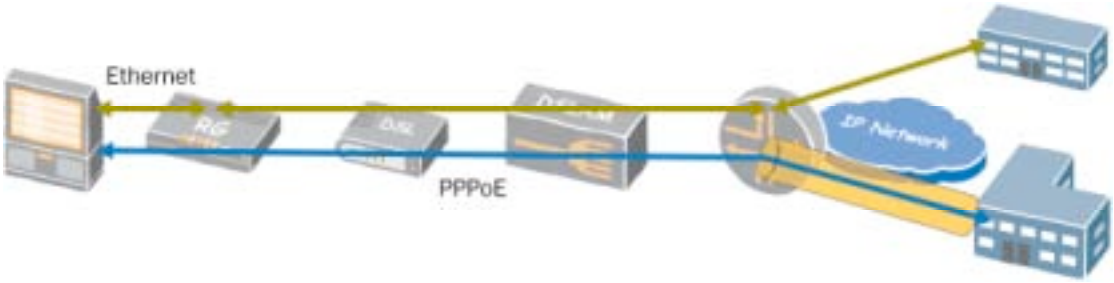

Figure 6: Delivering Retail and Wholesale Services

PPPoE Scalability

The circuit identifier is a key strength of PPPoE. It enables the operator to use a single IP address for each subscriber, as depicted in Figure 7. This conserves IP addresses and VLAN ids while easily tracking network usage by application.

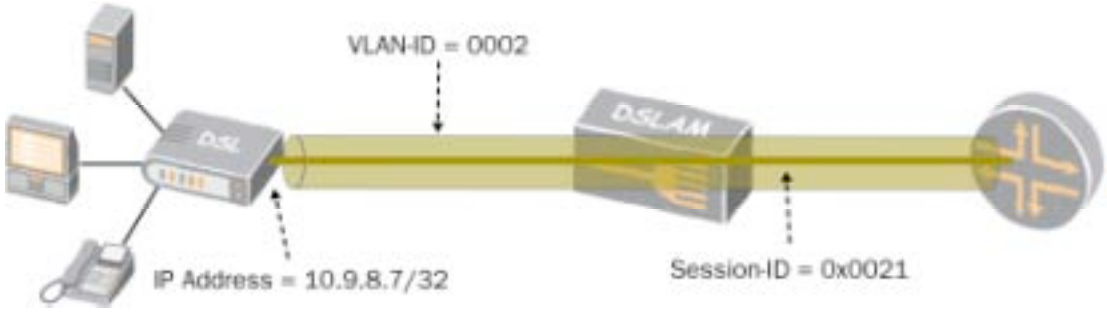

Figure 7: Single Connection per Subscriber

PPPoE Challenges

PPP has two drawbacks.

First, PPP essentially uses two levels of L2 encapsulation. This adds 10 bytes to every packet. This requires more processing to create, inspect and terminate each PPP packet than is required by the simpler IP over Ethernet (IPoE) method. Figure 8 illustrates this overhead by comparing PPPoE (left) with IPoE.

This is a minor issue since PPPoE provides virtually all the necessary capabilities to support broadband users and applications.

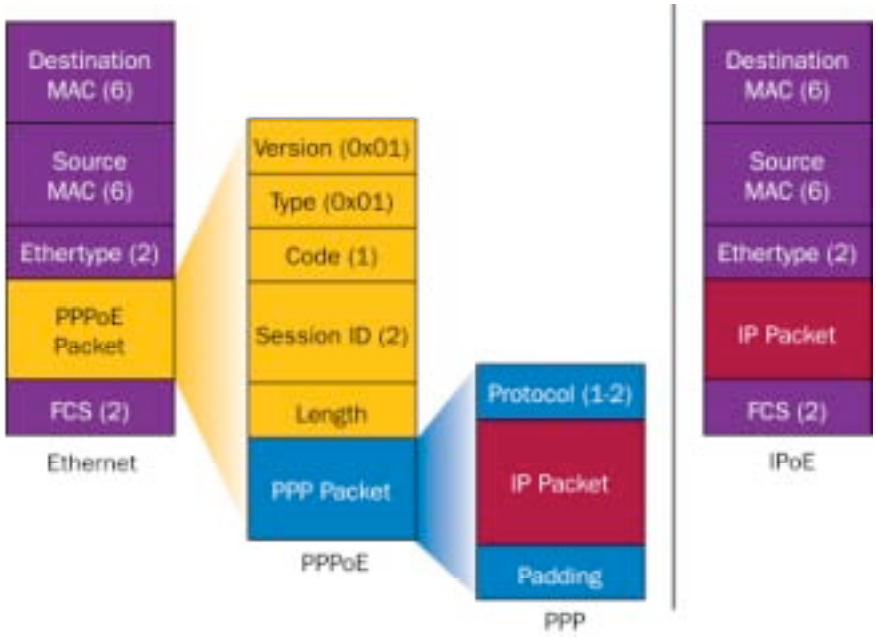

Figure 8: PPPoE and IPoE Packet Format

The other challenge is that PPP is designed to support unicast (point-to-point) connections. 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 9. This prevents PPPoE from efficiently supporting IP multicast between the edge router and the DSLAM/OLT.

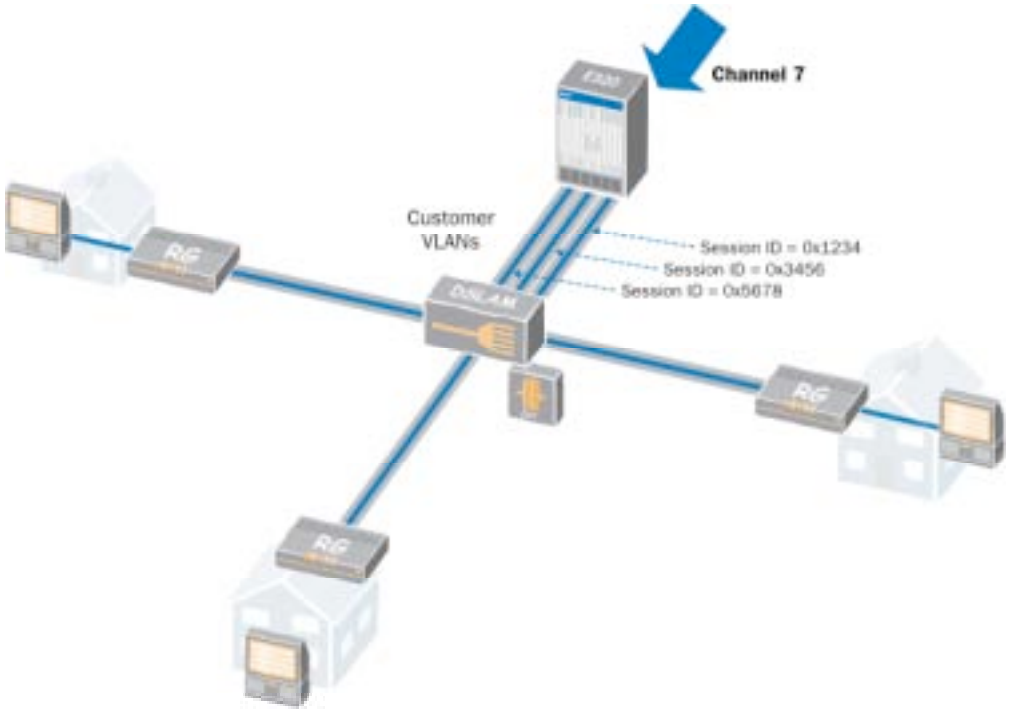

Figure 9: Broadcast Television Distribution Using PPPoE

It is this issue that has led to the recent interest in using IPoE on broadband networks.

IP over Ethernet (IPoE)

IP over Ethernet (IPoE) is a more recent alternative to the PPP-based models. Essentially this is a shorthand way of saying that the IP payload is being delivered across an Ethernet network, without using PPP encapsulation. IPoE does not have all of the capabilities of PPP but is an appropriate substitute in some cases.

IPoE relies on DHCP to provide the IP address. DHCP was designed to assign an IP address to a LAN-attached device. As such, it did not originally include support for establishing links, authenticating users, or link monitoring. DHCP extensions and other protocols (such as Extensible Authentication Protocol) are combined with DHCP to provide similar capabilities as PPPoE.

IPoE Address Assignment

Basic 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. Multiple DHCP servers may respond by sending "DHCP Offers" the host then responds to the offer it wishes to accept, and the DHCP server assigns the IP address. Figure 10 illustrates the basic DHCP assignment process[5].

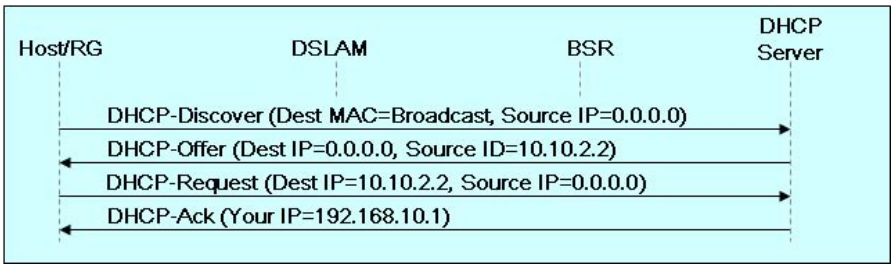

Figure 10: DHCP Address Assignment

IPoE Authentication

A major drawback to DHCP is that authentication can only occur after an IP address has been assigned and the subscriber has been authorized to use the network.

The ideal solution is to use IEEE 802.1x Extensible Authentication Protocol over LANs (EAPoL). This allows EAP, originally developed for PPP, to support LAN-based networks including broadband networks using DHCP. The key capability introduced is that the subscriber is authenticated before being assigned an IP address and gaining network access. However, many clients and DSLAMs do not yet support IEEE 802.1x.

IPoE Monitoring

IPoE does not incorporate link monitoring. Any link monitoring techniques which operate at IP, Ethernet or lower layers can be used with IPoE. For example, Bidirectional Forwarding Detection (BFD) operates at the Layer 2 level to monitor connection availability. However, these techniques typically do not operate on the link from the subscriber to the DSLAM.

IPoE Strengths and Weaknesses

The strength of IPoE is in its simplicity. Because there is no separate connection layer like PPP, DHCP is potentially more scalable. Deep packet inspection is not required to understand what is going on in the packet, allowing the network to more easily understand the packet flows and provide the appropriate bandwidth and queuing to each packet. However, there are several weaknesses with many current DHCP implementations:

- Access before Authorization: As noted previously, authentication can only occur after an IP address has been assigned and the subscriber has been authorized to use the network. This is a potential security exposure since the user has access to the network before having been authorized.

[5] This is an overview of the DHCP address assignment process. Some details unrelated to this discussion are not included.

- Subscriber Management: DHCP servers lack the advanced subscriber management features provided by RADIUS. Lack of tight RADIUS integration therefore limits the amount of subscriber management capabilities.
- Wholesale Support: For wholesale networks, the lack of a PPP session identifier makes it impossible to track which wholesaler each packet belongs to within the same VLAN. Each wholesaler therefore requires a VLAN (or VC) to each subscriber. This is less important in North America where the incumbent telcos are providing the DSL service, but is an issue in many countries.
- 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.
- Monitoring: Finally, IPoE lacks any integrated "last mile" monitoring technique. DSLAM and RG vendors are working to resolve this issue, including reporting information upstream using DSL Forum's Layer 2 Control (L2C) mechanism and Ethernet OAM standards. However, no implementations currently exist which proactively monitor and report this information.

Juniper Networks Enhancements for IPoE

Juniper Networks JUNOSe software resolves two of the critical DHCP shortfalls:

- Access before Authorization: When a new broadband subscriber connects to the network and requests an IP address using DHCP, a *temporary* IP address is assigned to the subscriber. The only thing that can be done with this address is to authenticate the user. After receiving the temporary IP address, the device attempts to authenticate using EAP. EAP is a framework which supports multiple authentication methods. While the details differ, they work similarly to the authentication method described in the PPP section. The DHCP Relay subsystem in the edge router forwards the authentication request to the appropriate AAA server, which authenticates the user and responds. The router passes this response to the requester.
- Once the user is authenticated, the DHCP server revokes the temporary address and assigns a different IP address which can access additional network services. Figure 11 depicts the establishment of the IPoE connection when using Juniper Networks JUNOSe:

Figure 11: IPoE Authentication Using Temporary IP Address Assignment

- RADIUS integration: Another important enhancement which Juniper provides for IPoE is RADIUS integration. After the DHCP server provides the permanent IP address, the JUNOSe router automatically generates an authorization request to the RADIUS server. This server responds with a typical RADIUS authorization response which informs the JUNOSe router which resources the subscriber has access to.

Summary

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 which can adequately support a wholesale environment. In addition, it simplifies the migration to IPv6 and supports integrated link quality monitoring.

IPoE is useful in specific circumstances, particularly for supporting broadcast television and when using service VLANs. In addition, Juniper Networks JUNOSe solves the most critical issues by tightly integrating DHCP and RADIUS.

The following table summarizes the alternatives:

	PPP	IPoE	Juniper IPoE
Business Model	Retail, Wholesale	Retail	Retail
Connectivity	P2P	P2P, P2MP	P2P, P2MP
Subscriber Management	Strong	Weak	Strong
Monitoring	Integrated	Future	Future

Table 1: Comparison of PPPoE and IPoE

To leverage the strengths of each, the two technologies are often combined in a network. PPP carries unicast traffic such as Internet Access and VoIP, while IPoE carries broadcast television. In retail networks, IGMP and Video on Demand traffic are carried using the PPP connection. In wholesale networks, pragmatic realities sometimes force these to be carried with the broadcast television traffic.

Contact

Marc Bernstein
mbernstein@juniper.net
978-392-4996

Glossary

AAA	Authentication, Authorization, and Accounting
BRAS	Broadband Remote Access Server
BSR	Broadband Services Router
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
IPCP	Internet Protocol Control Protocol (part of PPP)
IPoE	IP over Ethernet
LCP	Link Control Protocol (part of PPP)
LQM	Link Quality Monitoring (part of PPP)
NCP	Network Control Protocol (part of PPP)
PPP	Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
RADIUS	Remote Authentication Dial-In User Service

References

Extensible Authentication Protocol (EAP)	
EAP	http://www.faqs.org/rfcs/rfc2284.html
EAPoL (IEEE 802.1x)	http://standards.ieee.org/getieee802/download/802.1X-2001.pdf
RADIUS	
RADIUS	http://www.faqs.org/rfcs/rfc2865.html
Point-to-Point Protocol (PPP)	
PPP	http://www.faqs.org/rfcs/rfc1661.html
PPP over ATM AAL5 (PPPoA)	http://www.faqs.org/rfcs/rfc2364.html
PPP over Ethernet (PPPoE)	http://www.faqs.org/rfcs/rfc2516.html
PPP Link Quality Monitoring (LQM)	http://www.faqs.org/rfcs/rfc1333.html
Dynamic Host Control Protocol (DHCP)	
DHCP	http://www.faqs.org/rfcs/rfc2131.html