

# JUNOS<sub>e</sub> SOFTWARE SUPPORT FOR DHCP IN-SERVICE VLANS

---

Scaling and Improving Availability with Juniper Networks JUNOS<sub>e</sub> Software  
Enhanced Features

## Table of Contents

|   |    |
|---|----|
| Introduction .....  | 1  |
| Scope.....  | 1  |
| Description and Deployment Scenario .....                       | 1  |
| Subscriber Management in an S-VLAN Environment.....             | 3  |
| Subscriber Management Configuration .....                       | 4  |
| Scaling Subscribers in an S-VLAN network.....                   | 5  |
| Scaling Configuration .....                                     | 6  |
| Packet Trigger for Higher DSI Availability .....                | 7  |
| Packet Trigger Configuration.....                               | 9  |
| Summary .....   | 10 |
| Appendix: IP Subscriber Route Map .....                         | 10 |
| Route-Map .....   | 10 |
| IP Service-Profile .....  | 10 |
| IP Interface-Profile .....                                      | 10 |
| Appendix: RADIUS Communication.....                             | 11 |
| RADIUS Access Request to RADIUS Server .....                    | 11 |
| RADIUS Access Accept from RADIUS Server .....                   | 11 |
| RADIUS Accounting Start Packet sent to Accounting Server .....  | 12 |
| RADIUS Interim Accounting Packet Sent to Accounting Server..... | 12 |
| RADIUS Accounting Stop Packet Sent to Accounting Server .....   | 13 |
| About Juniper Networks.....                                     | 14 |

## Table of Figures

|  |   |
|--|---|
| Figure 1: Conceptual map of broadband network architectures .....                                    | 1 |
| Figure 2: S-VLAN design for multi-edge networks .....  | 2 |
| Figure 3: Dynamic subscriber interface .....   | 3 |
| Figure 4: Dependencies between DHCP client and DHCP external server applications running on BSR..... | 4 |
| Figure 5: Architecture for scaling the S-VLAN model .....  | 6 |
| Figure 6: Implications of loss of DHCP state.....  | 8 |

## Introduction

This application note provides an overview of extended Juniper Networks<sup>®</sup> JUNOS<sup>e</sup><sup>™</sup> Software feature sets to support Dynamic Host Configuration Protocol (DHCP)-based subscriber management in a service VLAN (S-VLAN) environment. JUNOS<sup>e</sup> Software is the operating system for the Juniper Network E Series Broadband Services Routers.

There are two fundamental concepts about provider broadband network architectures that are important to understand (see Figure 1):

- Service management: subscriber-oriented versus service-oriented
- Subscriber termination: customer VLAN versus service VLAN

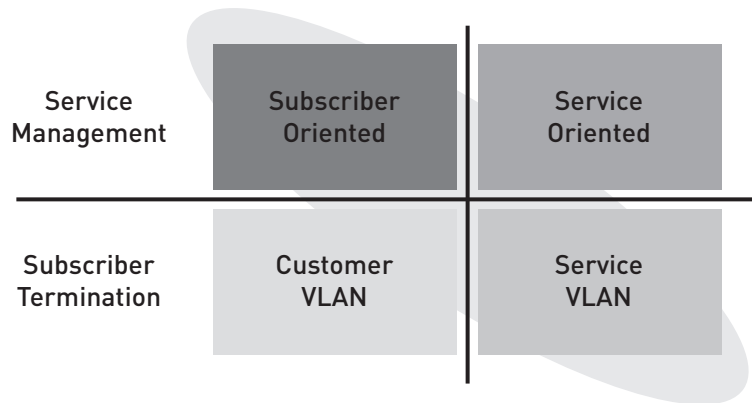


Figure 1: Conceptual map of broadband network architectures

In a customer-VLAN model, each customer site is connected via a specific VLAN or Q-in-Q<sup>1</sup> VLAN to the Broadband Services Router (BSR). In contrast, in the S-VLAN model a number of subscribers share a common VLAN. This is mainly used to support the multi-edge model where different edge systems provide Internet, voice over IP (VoIP), and IPTV services.

Although there is no 1:1 relationship between the VLAN and the subscriber interface, JUNOS<sup>e</sup> Software provides features to support RADIUS-based subscriber management services in the 1: N model.

This application note first discusses the basic concept for Dynamic Subscriber Interface in an S-VLAN environment. Later sections show how this model scales for large deployments. The document also explains how the concept of packet trigger can be used to increase service availability.

## Scope

This application note outlines the use of JUNOS<sup>e</sup> DHCP scalability and high availability (HA) enhancements for S-VLAN environments. To use this document effectively, you should have a good understanding of DHCP concepts. You should also know how to set up the JUNOS<sup>e</sup> DHCP-based subscriber management features.

The information in this document is general. Individual designs can vary based on constraints such as MAC-address translation on the access nodes. Beyond basic features such as DHCP relay and DHCP external server, this application note specifically covers the topics of subscriber scaling in an S-VLAN environment beyond the slot capacity. This document also discusses a fast recovery mechanism, which allows the network to quickly re-establish subscriber interfaces after reloading a Broadband Services Router (BSR), for example, after a software upgrade.

## Description and Deployment Scenario

Multi-edge networks that provide different services via different edge functions to the subscribers often use an S-VLAN design for subscriber termination. This application note is based on a multi-edge design with two different edge functions:

- BSR handles all unicast-based services.
- Video Service Router (VSR) manages all IPTV multicasts and video on demand (VOD) unicast traffic.

<sup>1</sup>The IEEE 802.1Q-in-Q VLAN tag expands the VLAN space by double-tagging packets. The expanded VLAN space allows the service provider to provide certain services, such as Internet access on specific VLANs for specific customers, and yet still allows the service provider to provide other types of services for their other customers on other VLANs.

In this model, the DSLAM is responsible for multicast replication as well as any quality of service (QoS) mechanism on the user access line. Figure 2 shows the basic concept of the S-VLAN design. DHCP clients at consumer locations are connected via the access nodes to the S-VLAN, which is implemented on the aggregation network. The access nodes can serve any access technology such as DSL or active or passive fiber. Each access node is connected to each S-VLAN (only one drawn in the picture) and another to a common multicast-VLAN.

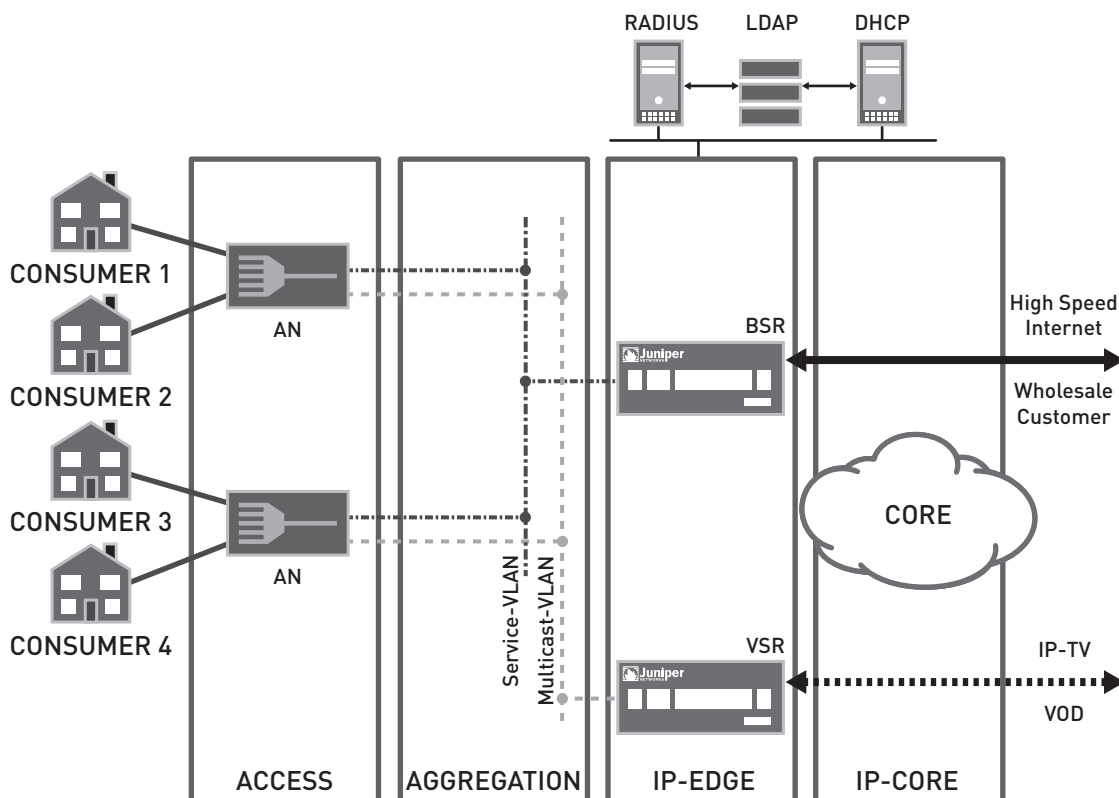


Figure 2: S-VLAN design for multi-edge networks

The access node connects the DHCP client to the S-VLAN for a specific service (or a specific ISP, in case of a wholesale model) controlled by the BSR. The access node is also responsible for multicast replication based on the Internet Group Management Protocol (IGMP) join/leave messages received from subscribers. The access node acts as an IGMP proxy for connected clients and the VSR provides the multicast traffic. The VSR may also provide IPTV unicast traffic (zapping) as well as VOD traffic.

In the multi-edge approach, the BSR uses a static carve-out model to apply QoS policies to unicast traffic. In an improved QoS design, the IGMP states are sent to the BSR by the DHCP client (via IGMP forking) or the access node (via L2C). The BSR can dynamically adjust the unicast bandwidth on a per-subscriber basis depending on the current multicast load on the subscriber's access line.

The DHCP server authenticates the subscriber and provides an IP address. The authentication is based on DHCP option 82 information, which was added by the access node to the DHCP packets sent by the client to the DHCP server. The IP address is either provided by the DHCP server dynamically from an IP address pool on the DHCP server or is statically assigned to a subscriber. Such information is usually stored on an external LDAP server.

The RADIUS server provisions subscriber-specific interface configurations such as input and output policies and QoS profiles. This type of information is also stored on an LDAP server. As discussed later, the DHCP server can update the LDAP database with the IP address dynamically assigned to the DHCP clients. This design allows the RADIUS server to authenticate subscribers based on their IP source address.

<sup>2</sup>DHCP option 82 allows a downstream device such as a DSLAM to insert a unique identifier, called a remote identifier, during DHCP session establishment.

## Subscriber Management in an S-VLAN Environment

In an S-VLAN environment, all subscribers share the same VLAN interface on the BSR. To provide subscriber management functionality, JUNOSe supports the concept of a dynamic subscriber interface (DSI). A DSI is a virtual interface on the access interface of the BSR connected to the S-VLAN. The DSI is identified by the IP address assigned to the DHCP client.

Each DSI can be configured to the individual subscriber by applying QoS-profile and ingress- and egress-policies via RADIUS at the time that the interface is created (see Figure 3). JUNOSe provides different methods to identify the DHCP client when requesting subscriber specific configuration information from RADIUS—for example, DHCP option 82, IP address, or MAC address.

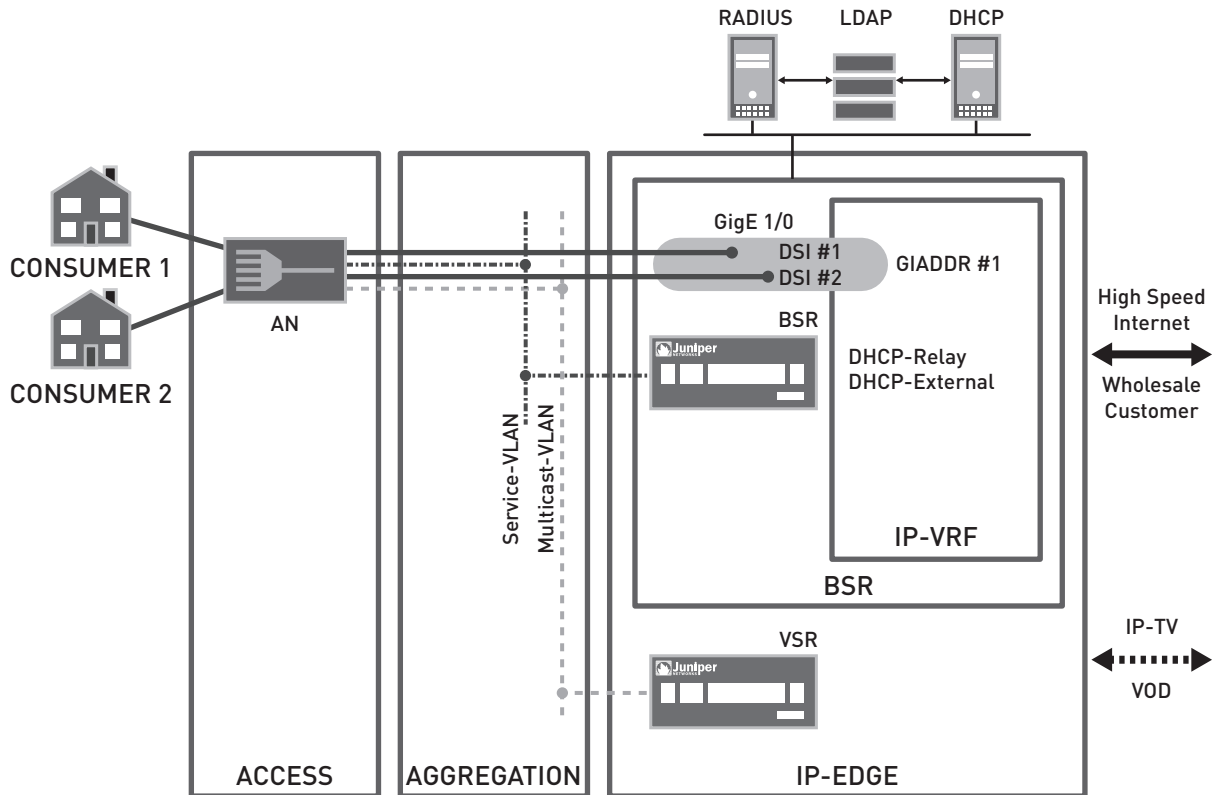


Figure 3: Dynamic subscriber interface

The BSR forwards all packets to and from a particular IP address (subscriber) via the DSI created for that subscriber. All packets are treated by the QoS-profile and the ingress/egress policies, and the interface statistics are updated as well. Because the DSI was authorized via RADIUS, the BSR can generate RADIUS accounting (start, interim, and stop) messages for each DSI. Because DHCP is a decoupled subscriber access protocol, components involved in the DHCP process must know the states for all subscribers. In case of a centralized DHCP server such as in this example, the BSR needs a way to keep the state of all its connected DHCP clients.

To meet this need, JUNOSe includes a DHCP External Server application that mirrors the state of the centralized DHCP server for all locally attached DHCP clients. The JUNOSe Software DHCP External Server application runs on the Juniper Networks E Series Broadband Services Routers that is functioning as the BSR.

Figure 4 shows the dependencies between the DHCP client and DHCP External Server running on the BSR. DHCP External Server stores DHCP state information and DSI state internally. When DHCP External Server detects the ACK sent by the DHCP server, it enters the DHCP client in its internal binding table, logs the assigned IP address, and creates the DSI. DHCP External Server also sets an expire timer for the DHCP lease time. DHCP External-Server updates its binding state with each DHCP renewal sent by the DHCP client after the renew time, which is normally half of the DHCP lease time.

If the DHCP client is not available, DHCP External Server receives neither a DHCP renew nor a DHCP rebind. In this case, the DHCP expire timer eventually times out and the DSI is removed for that DHCP client.

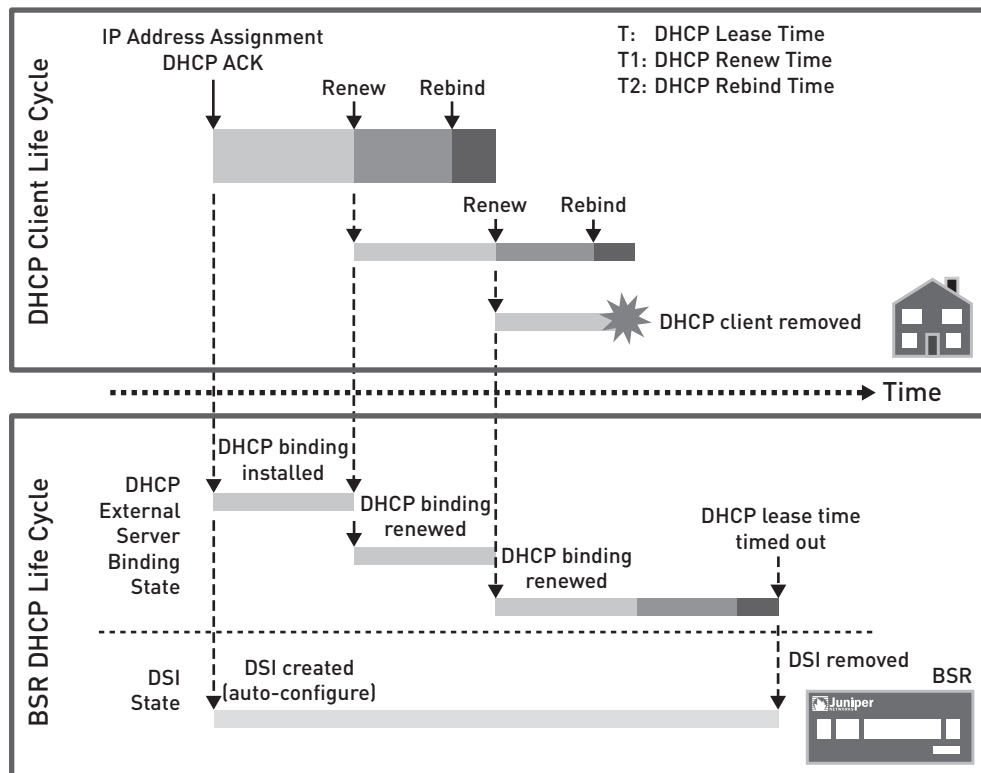


Figure 4: Dependencies between DHCP client and DHCP external server applications running on BSR

## Subscriber Management Configuration

The JUNOS Software configuration to support RADIUS-authorized DSIs consists of three parts:

- DHCP External Server Configuration
- DHCP Relay Configuration
- Access Interface Configuration

The DHCP External Server configuration keeps the DHCP states on the BSR in sync with the external DHCP physical server. DHCP External Server sniffs all DHCP-ACK messages from the DHCP server to the DHCP client and updates its DHCP binding table accordingly.

If a DHCP client is switched off silently, the DHCP state on the DHCP server will eventually time out after the expiration of the lease time and the state is removed in the DHCP server. DHCP-External provides the means to also clear the DHCP states on the BSR as well as remove the DSI, accessinternal routes for the DHCP-client and generate an Accounting-Stop record.

A typical DHCP-External configuration is shown below:

```

.....
! DHCP-External configuration
service dhcp-external
ip dhcp-external auto-configure
ip dhcp-external server-address 172.26.18.100
ip dhcp-external server-address 255.255.255.255
!
.....

```

The "auto-configure" statement instructs DHCP External Server to request interface configuration via RADIUS. The "server-address" statements designate which packets DHCP External Server is to examine.

The DHCP Relay function is used to send the local broadcast packets to a remote DHCP server:

```
.....
! DHCP Relay Configuration
set dhcp relay
set dhcp relay 172.26.18.100
set dhcp relay inhibit-access-route-creation
!
.....
```

The “inhibit-access-route-selection” statement instructs the DHCP Relay to not build or remove access routes, as this function is handled by DHCP External Server together with the DSI.

The access interface is often configured in IP unnumbered mode, with reference to a loopback interface that will be used by DHCP Relay as the DHCP Relay Gateway IP Address (GIADDR).

```
.....
! Interface Configuration
! GIADDR#1
interface loopback 11
ip address 10.103.1.1 255.255.0.0
!
interface GigabitEthernet 1/0
ip auto-configure ip-subscriber exclude-primary
ip route-map ip-subscriber routeMap
ip unnumbered loopback 11
!
.....
```

The “auto-configure ip-subscriber exclude-primary” statement instructs JUNOSe to dynamically build a DSI with the IP address assigned by the DHCP server. To build the DSI, JUNOSe consults the route map in “route-map ip-subscriber routeMap” for the configuration information needed to build the DSI.

In this example, the route map refers to a service profile, which triggers a RADIUS access request to dynamically gather the DSI configuration information from the RADIUS server. The Appendix shows an example of a route map as well as the RADIUS access request and access accept packet.

## Scaling Subscribers in an S-VLAN network

In an S-VLAN model, all subscribers are installed on the physical port or VLAN connected to the S-VLAN. The ASIC infrastructure on the BSR’s line cards—needed to implement the QoS-profile and ingress and egress policies for all subscriber interfaces—limits the maximum number of subscribers to 8,000 for the Juniper Networks ERX1440 Broadband Services Router and 16,000 for the Juniper Networks E320 Broadband Services Router (E320).

However, JUNOSe Software provides a mechanism for extending the S-VLAN model beyond these limits. JUNOSe can control the creation of dynamic subscriber interface based on the GIADDR set by the DHCP server in the DHCP ACK packets. For cases in which an S-VLAN is connected via multiple interfaces to the same routing-domain (VR or VRF), this method can be used to define the local interface that supports the DSI. This technique allows an external resource planning tool running on an LDAP or other directory server to provide the user specific configuration information to the DHCP server.

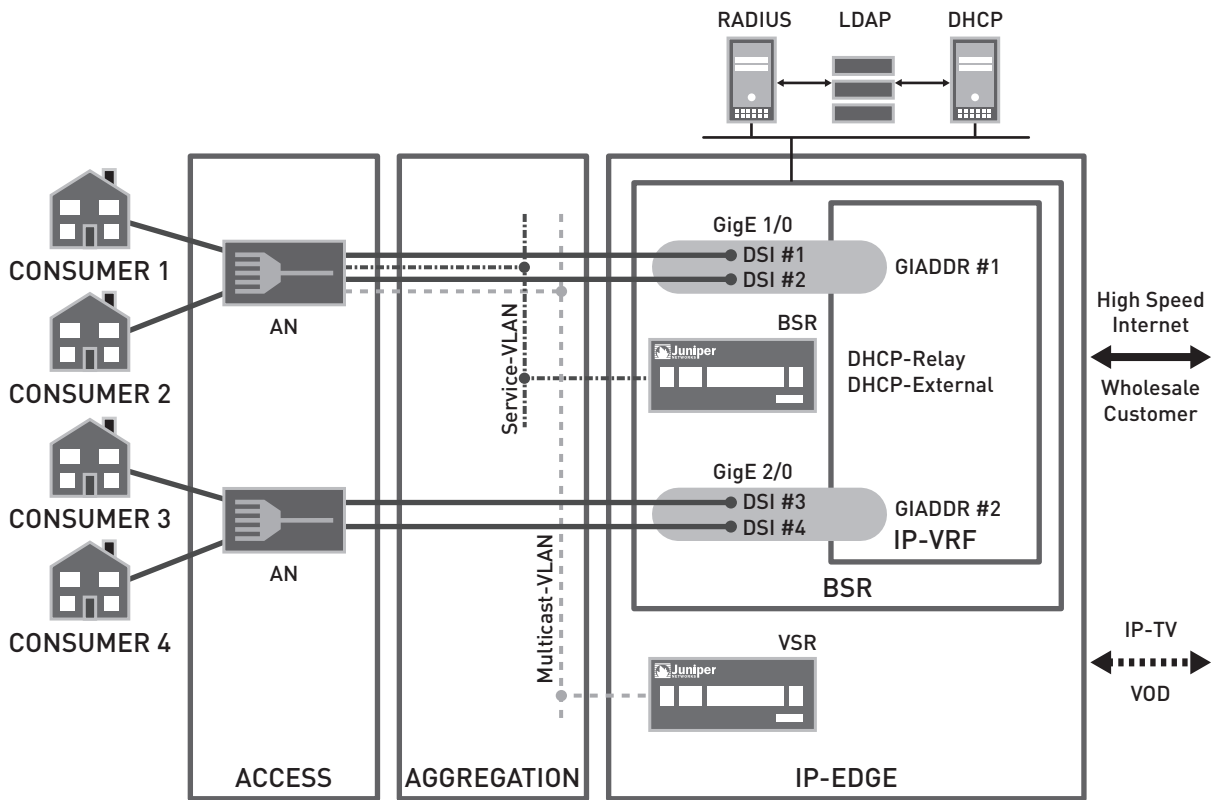


Figure 5: Architecture for scaling the S-VLAN model

Figure 5 shows the architecture that allows scaling of the S-VLAN model beyond the intrinsic limits of 8,000 or 16,000. The basic DSI concept discussed earlier is extended with additional interfaces connected to the same S-VLAN. Because the access node is part of the IP forwarding path, it must know where to send customer up-stream packets. Therefore, AN#1 is configured to send all IP packets from its connected subscribers to GigE 1/0 on the BSR, while AN#2 sends all upstream traffic to GigE 2/0. By setting the GIADDR in the DHCP ACK packets to GIADDR#1, the DHCP server indicates that the DSIs for customer 1 and customer 2 are being built on GigE 1/0. The DHCP server will set GIADDR#2 for customer 3 and 4 to have their DSIs built on GigE 2/0.

## Scaling Configuration

This configuration is essentially the same as the one discussed earlier in "Subscriber Management over S-VLAN." The main differences are the new DHCP Relay option "giaddr-selects-interface" in the DHCP relay configuration.

```

! DHCP relay configuration
set dhcp relay
set dhcp relay 172.26.18.100
set dhcp relay inhibit-access-route-creation
set dhcp relay giaddr-selects-interface
!
    
```

Additionally, another access interface as well as an additional loopback interface must be configured:

```

.....
! Interface Configuration
! GIADDR#1
interface loopback 11
ip address 10.103.1.1 255.255.0.0
!
! GIADDR#2
interface loopback 12
ip address 10.103.1.1 255.255.0.0
!
interface gigabitEthernet 1/0
ip auto-configure ip-subscriber exclude-primary
ip route-map ip-subscriber routeMap
ip unnumbered loopback 11
!
interface gigabitEthernet 2/0
ip auto-configure ip-subscriber exclude-primary
ip route-map ip-subscriber routeMap
ip unnumbered loopback 12
!
.....

```

The DHCP External Server configuration does not change:

```

.....
! DHCP-External configuration
service dhcp-external
ip dhcp-external auto-configure
ip dhcp-external server-address 172.26.18.100
ip dhcp-external server-address 255.255.255.255
!
.....

```

## Packet Trigger for Higher DSI Availability

In addition to the “auto-configure” option, JUNOSe also supports the “auto-detect” option for DSIs. This option is also called Packet Trigger. Packet Trigger analyses all incoming IP packets on the access interface and builds a DSI for every source IP address that does not already have a DSI. There are different use cases for Packet Trigger. In this discussion Packet Trigger is used to increase the availability of the DSIs on the BSR.

A number of devices are involved in processing the DHCP state machine, including the routing gateway at the customer site (DHCP client), the access node, the BSR, and the DHCP server. In contrast to Point-to-Point Protocol over Ethernet (PPPoE), DHCP does not build an end-to-end session with a clear session state between all these devices.

Therefore, each of these components must have the current DHCP state for every DHCP client—or the network can experience problems. To avoid this situation on the BSR, Packet Trigger can be used to re-synchronize the DHCP state. Note that the BSR supports multiple HA mechanisms such as state-full switch route processor (SRP) switchover and line-module redundancy as well as unified in-service system upgrades (ISSU) in the future to prevent such a loss of DHCP states. The concept explained here can handle all issues not covered by those mechanisms. Figure 6 shows the impact of the BSR becoming unavailable.

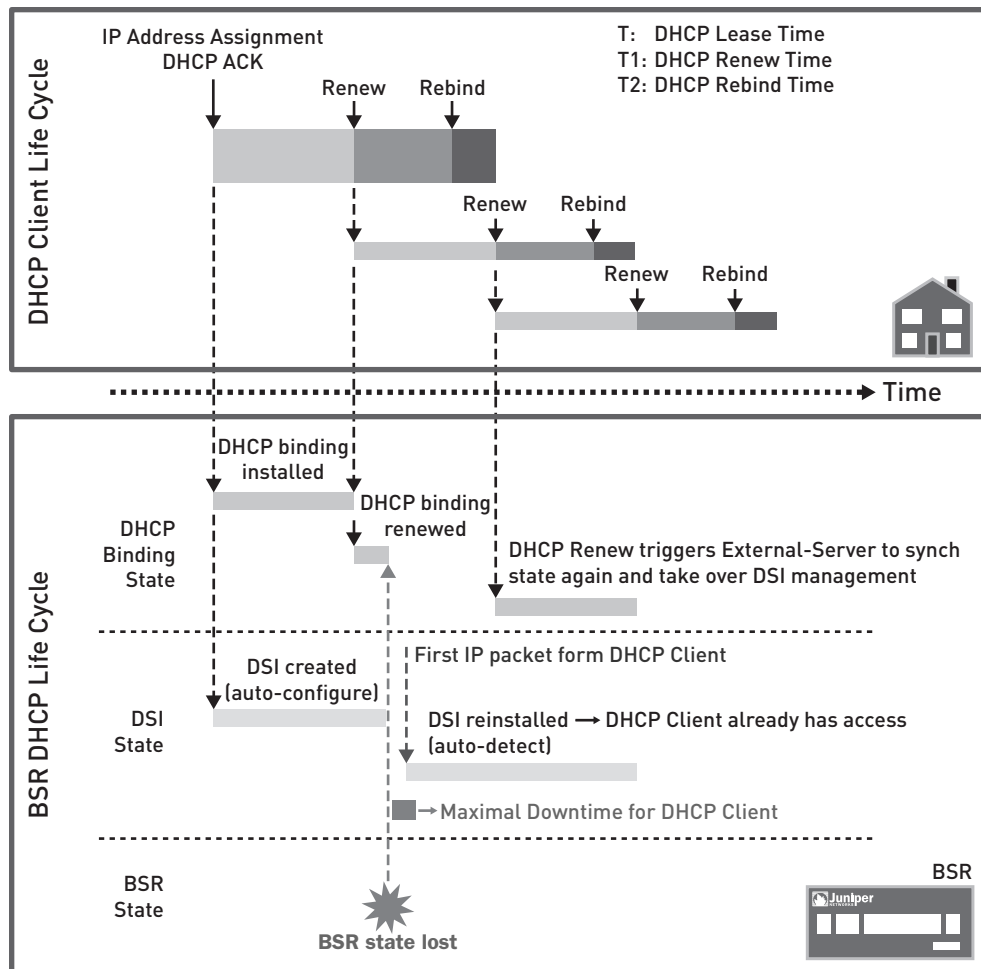


Figure 6: Implications of loss of DHCP state

If any system component loses its DHCP state information, it can be recovered using the DHCP Review and DHCP Rebind mechanisms in the DHCP protocol stack. However, depending on the DHCP timer settings (lease, renew and rebind time), this recovery could take quite a long time.

To eliminate a major service disruption for all subscribers connected to the BSR, Packet Trigger can be used to shorten the overall outage to the time to bring the system back online again. As discussed earlier, the DSI must be installed on the BSR for packets to be successfully forwarded to and from the DHCP clients. The following example shows how Packet Trigger can help short the overall downtime. For this example, assume that the BSR has lost all its DHCP states. All other systems involved in the DHCP process are all still up and have not changed any DHCP state for all subscribers. Refer to Figure 6 to track the sequence of events:

1. The BSR loses all DSI and DHCP state information (for example, through a software upgrade).
2. DHCP clients are still tracking the lease time for their assigned IP addresses and continue to attempt to communicate with the BSR.
3. As it detects each source IP addresses on the access interface to the S-VLAN, the BSR rebuilds a DSI.
4. Using Packet Trigger, the BSR consults the route map and sends a RADIUS access request to gather the interface configurations for the DSI.
5. The BSR builds a DSI for all source IP addresses identifying active subscribers. The DSIs have the correct QoS-profile and policies assigned as well as the access-internal route placed in the routing table for accurate packet forwarding.
6. In this state, BSR packet forwarding is working again for all active DHCP clients. However, the BSR does not yet have the proper DHCP states for all subscribers.

7. The next time a DHCP client attempts to renew its lease time, the DHCP External Server function analyzes the ACK sent by the DHCP server and creates a new entry in the DHCP binding table to reflect DHCP state information such as IP address and expire-timer.
8. Packet Trigger can now be managed by DHCP External Server. If a DHCP client sends a release or the lease-time expires in the DHCP binding table, the DSI and the access-route are removed correctly.

## Packet Trigger Configuration

To enable Packet Trigger on the BSR requires only a single configuration statement on each access interface:

```
!
interface gigabitEthernet 1/0
ip auto-configure ip-subscriber exclude-primary
ip auto-detect ip-subscriber
ip route-map ip-subscriber routeMap
ip unnumbered loopback 11
!
```

The “ip auto-detect ip-subscriber” statement allows a DSI to be built for every source IP address not already installed in the IP demux table of the access interface. Here is an example of the demux table:

```
BSR:PE:VRF#show ip demux interface gigabitEthernet 1/0
Prefix/Length  SA/DA  Subscriber-Intf VR/VRF  Description
23.0.0.0/8     SA     ip10.103.41.3  VRF     *
22.12.0.0/16  SA     ip10.103.41.2  VRF     *
22.13.0.0/16  SA     ip10.103.41.2  VRF     *
21.11.11.0/24 SA     ip10.103.41.1  VRF     *
21.11.12.0/24 SA     ip10.103.41.1  VRF     *
21.11.13.0/24 SA     ip10.103.41.1  VRF     *
10.103.41.1/32 SA     ip10.103.41.1  VRF     *
10.103.41.2/32 SA     ip10.103.41.2  VRF     *
10.103.41.3/32 SA     ip10.103.41.3  VRF     *
10.103.41.4/32 SA     ip10.103.41.4  VRF     *
Note: Entries with * are dynamic (dhcp) entries
```

As discussed above, “ip auto-configure” and “ip auto-detect” can request the interface parameters from the RADIUS server. For DSIs triggered by DHCP, subscriber information such as DHCP option 82 is used in the RADIUS access request to identify the subscriber. In contrast, Packet Trigger only has the IP address of the DHCP client.

To enable Packet Trigger to install the correct interface parameters, the RADIUS server needs the current IP address of the subscriber, whether fixed or dynamically allocated. The RADIUS server needs to be tightly coupled with the DHCP server so that the RADIUS server has access to IP addresses. This coupling is often accomplished via an LDAP database, which is common to both RADIUS and DHCP.

Finally, DHCP External Server must synchronize its DHCP binding state for the new DSI built for the DHCP client via Packet Trigger. This is accomplished by setting the “server-sync” option in the DHCP External configuration.

```
! DHCP-External configuration
service dhcp-external
ip dhcp-external auto-configure
ip dhcp-external server-sync
ip dhcp-external server-address 172.26.18.100
ip dhcp-external server-address 255.255.255.255
!
```

Server-Sync allows DHCP External Server to reset the expire timer in the DHCP binding table back to the lease time captured when the DHCP server sends an ACK to a DHCP renew initiated by the DHCP client.

## Summary

Subscriber management in S-LANs often involves the use of the DHCP protocol. However, DHCP is limited in terms of scalability and availability. JUNOS Software—the operating system that powers E Series routers—includes a number of features to address these limitations. JUNOS supports the concept of a DSI, which provides flexibility and scalability of the DHCP protocol in S-VLAN deployments. Another JUNOS feature, DHCP External Server, helps ensure consistency of state information between the BSR and the external DHCP server.

The maximum number of subscribers that can be supported on the ERX1440 and E320 Broadband Services Router is 8,000 and 16,000, respectively. However, JUNOS Software provides a mechanism for extending the S-VLAN model beyond these limits using the DSI feature. This capability allows service providers to scale their DHCP deployments as demand increases, without massive investments in new hardware. In addition, the JUNOS Software Packet Trigger functionality increases network availability by re-synchronizing the DHCP state in the case of component failure.

## Appendix: IP Subscriber Route Map

### Route-Map

IP subscriber manager uses the route map to build the DSI. The route map can include two components: the Service-Profile used to get the interface configuration from RADIUS and the Interface-Profile that defines the interface properties. Both or only one of the profiles can be present in the route map.

```
.....
!  
route-map routeMap permit 10  
set ip service-profile serviceProfile  
set ip interface-profile interfaceProfile  
!
```

### IP Service-Profile

The Service-Profile is used to retrieve the DSI interface configuration from RADIUS. It can include a static user-name and password that would be the same for all subscribers. In such a case, the NASport- id might be used on the RADIUS to distinguish between the different DHCP clients.

```
.....
!  
ip service-profile serviceProfile  
include dhcp-option 82 agent-circuit-id  
password secret  
!
```

The “include” statement provides a way to add user-specific information to the user-name field of the RADIUS Access Request packet sent to the RADIUS. In this example, the ip-address assigned by the DHCP-Server in the DHCP ACK packet is used (this makes it simpler for Packet Trigger, as shown later). Normally information such as the DHCP option 82 would be copied into the username field of the RADIUS request to uniquely identify the subscriber.

### IP Interface-Profile

In this configuration, the interface-profile is used as the backup configuration in case the RADIUS server does not provide any information, for whatever reason. For such a DHCP client, an input and output policy will be attached, which allows traffic to and from the DHCP server.

```
.....
!  
profile interfaceProfile  
ip policy input "fwd_todhcp_p1" statistics enabled  
ip policy output "fwd_fromdhcp_p1" statistics enabled  
!  
ip policy-list "fwd_todhcp_p1"
```

```

classifier-group "fwd_todhcp" precedence 10
forward
!
ip policy-list "fwd_fromdhcp_pl"
classifier-group "fwd_fromdhcp" precedence 10
forward
!
ip classifier-list "fwd_todhcp" udp any eq 68 any eq 67
!
ip classifier-list "fwd_fromdhcp" udp any eq 67 any eq 68
!

```

## Appendix: RADIUS Communication

### RADIUS Access Request to RADIUS Server

The Access-Request sent to the RADIUS server shows that the username is set to the DHCP option 82:

```

DEBUG radiusSendAttributes: ACCESS-REQUEST attributes (default)
DEBUG radiusSendAttributes: username attr added: Customer1
DEBUG radiusSendAttributes: acct-session-id attr added: erx
GigabitEthernet 1/0:0005242900
DEBUG radiusSendAttributes: user-password attr added: <value withheld>
DEBUG radiusSendAttributes: framed-ip-address attr added: 10.103.41.1
DEBUG radiusSendAttributes: calling-station-id attr added: #lima#E10#0
DEBUG radiusSendAttributes: nas-port-type attr added: 15
DEBUG radiusSendAttributes: nas-port attr added: 603979776
DEBUG radiusSendAttributes: nas-port-id attr added: GigabitEthernet
1/0
DEBUG radiusSendAttributes: nas-ip-address attr added: 172.26.18.240
DEBUG radiusSendAttributes: nas-identifier attr added: lima

```

### RADIUS Access Accept from RADIUS Server

The RADIUS Server provides the framed-routes, ingress- and egress-policy and the qos-profile in the Access Accept packet:

```

DEBUG radiusAttributes: USER ATTRIBUTES: (Customer1)
DEBUG radiusAttributes: acct interval time attr: 600
DEBUG radiusAttributes: class attr: (binary data)
DEBUG radiusAttributes: total eap message attr length = 0
DEBUG radiusAttributes: framed route attr: 21.11.11.0/24
DEBUG radiusAttributes: framed route attr: 21.11.12.0/24
DEBUG radiusAttributes: framed route attr: 21.11.13.0/24
DEBUG radiusAttributes: ingress policy name (vsa) attr: ingressPolicy
DEBUG radiusAttributes: ingress policy stats (vsa) attr: 1
DEBUG radiusAttributes: egress policy name (vsa) attr: egressPolicy
DEBUG radiusAttributes: egress policy stats (vsa) attr: 1
DEBUG radiusAttributes: qos profile name (vsa) attr: qosProfile
DEBUG radiusAttributes: virtual router name (vsa) attr: PE:VRF
DEBUG radiusAttributes: local interface (vsa) attr: loopback0

```

## RADIUS Accounting Start Packet sent to Accounting Server

Based on the information provided, IP-SubscriberManager builds the DSI and a RADIUS Accounting Start Record is sent to the RADIUS accounting server.

```
.....  
DEBUG radiusSendAttributes: ACCOUNTING-REQUEST attributes (default)  
DEBUG radiusSendAttributes: acct-status-type attr added: 1  
DEBUG radiusSendAttributes: username attr added: Customer1  
DEBUG radiusSendAttributes: event-timestamp attr added: 1191507395  
DEBUG radiusSendAttributes: acct-delay-time attr added: 0  
DEBUG radiusSendAttributes: nas-identifier attr added: lima  
DEBUG radiusSendAttributes: acct-session-id attr added: erx  
GigabitEthernet 1/0:0005242900  
DEBUG radiusSendAttributes: nas-ip-address attr added: 172.26.18.240  
DEBUG radiusSendAttributes: class attr added: (binary data)  
DEBUG radiusSendAttributes: framed-compression attr added: 0  
DEBUG radiusSendAttributes: framed-ip-address attr added: 10.103.41.1  
DEBUG radiusSendAttributes: framed-ip-netmask attr added: 0.0.0.0  
DEBUG radiusSendAttributes: ingress-policy-name (vsa) attr added:  
ingressPolicy  
DEBUG radiusSendAttributes: egress-policy-name (vsa) attr added:  
egressPolicy  
DEBUG radiusSendAttributes: calling-station-id attr added: #lima#E10#0  
DEBUG radiusSendAttributes: nas-port-type attr added: 15  
DEBUG radiusSendAttributes: nas-port attr added: 603979776  
DEBUG radiusSendAttributes: nas-port-id attr added: GigabitEthernet 1/0  
DEBUG radiusSendAttributes: acct-authentic attr added: 1  
.....
```

## RADIUS Interim Accounting Packet Sent to Accounting Server

```
.....  
DEBUG radiusSendAttributes: ACCOUNTING-REQUEST attributes (default)  
DEBUG radiusSendAttributes: acct-status-type attr added: 3  
DEBUG radiusSendAttributes: username attr added: Customer1  
DEBUG radiusSendAttributes: event-timestamp attr added: 1189688465  
DEBUG radiusSendAttributes: acct-delay-time attr added: 0  
DEBUG radiusSendAttributes: nas-identifier attr added: lima  
DEBUG radiusSendAttributes: acct-session-id attr added: erx  
GigabitEthernet 1/0:101:0014680104  
DEBUG radiusSendAttributes: nas-ip-address attr added: 172.26.18.240  
DEBUG radiusSendAttributes: class attr added: (binary data)  
DEBUG radiusSendAttributes: framed-compression attr added: 0  
DEBUG radiusSendAttributes: framed-ip-address attr added: 10.103.41.1  
DEBUG radiusSendAttributes: framed-ip-netmask attr added: 0.0.0.0  
DEBUG radiusSendAttributes: ingress-policy-name (vsa) attr added:  
ingressPolicy  
DEBUG radiusSendAttributes: egress-policy-name (vsa) attr added:  
egressPolicy  
DEBUG radiusSendAttributes: calling-station-id attr added:  
#lima#E10#101  
DEBUG radiusSendAttributes: acct-input-gigawords attr added: 0  
DEBUG radiusSendAttributes: acct-input-octets attr added: 2880  
DEBUG radiusSendAttributes: acct-output-gigawords attr added: 0  
DEBUG radiusSendAttributes: acct-output-octets attr added: 0  
DEBUG radiusSendAttributes: acct-input-gigapackets (vsa) attr added: 0  
DEBUG radiusSendAttributes: acct-input-packets attr added: 5  
DEBUG radiusSendAttributes: acct-output-gigapackets (vsa) attr added: 0  
DEBUG radiusSendAttributes: acct-output-packets attr added: 0  
DEBUG radiusSendAttributes: nas-port-type attr added: 15  
DEBUG radiusSendAttributes: nas-port attr added: 603979877  
.....
```

```
DEBUG radiusSendAttributes: nas-port-id attr added: GigabitEthernet
1/0 :101
DEBUG radiusSendAttributes: acct-authentic attr added: 1
DEBUG radiusSendAttributes: acct-session-time attr added: 596
```

---

## RADIUS Accounting Stop Packet Sent to Accounting Server

---

```
DEBUG radiusSendAttributes: ACCOUNTING-REQUEST attributes (default)
DEBUG radiusSendAttributes: acct-status-type attr added: 2
DEBUG radiusSendAttributes: username attr added: Customer1
DEBUG radiusSendAttributes: event-timestamp attr added: 1189687869
DEBUG radiusSendAttributes: acct-delay-time attr added: 0
DEBUG radiusSendAttributes: nas-identifier attr added: lima
DEBUG radiusSendAttributes: acct-session-id attr added: erx
GigabitEthernet 1/0 :101:0014680102
DEBUG radiusSendAttributes: nas-ip-address attr added: 172.26.18.240
DEBUG radiusSendAttributes: class attr added: (binary data)
DEBUG radiusSendAttributes: framed-compression attr added: 0
DEBUG radiusSendAttributes: framed-ip-address attr added: 10.103.41.1
DEBUG radiusSendAttributes: framed-ip-netmask attr added: 0.0.0.0
DEBUG radiusSendAttributes: ingress-policy-name (vsa) attr added:
ingressPolicy
DEBUG radiusSendAttributes: egress-policy-name (vsa) attr added:
egressPolicy
DEBUG radiusSendAttributes: calling-station-id attr added:
#lima#E10#101
DEBUG radiusSendAttributes: acct-input-gigawords attr added: 0
DEBUG radiusSendAttributes: acct-input-octets attr added: 5760
DEBUG radiusSendAttributes: acct-output-gigawords attr added: 0
DEBUG radiusSendAttributes: acct-output-octets attr added: 0
DEBUG radiusSendAttributes: acct-input-gigapackets (vsa) attr added: 0
DEBUG radiusSendAttributes: acct-input-packets attr added: 10
DEBUG radiusSendAttributes: acct-output-gigapackets (vsa) attr added: 0
DEBUG radiusSendAttributes: acct-output-packets attr added: 0
DEBUG radiusSendAttributes: nas-port-type attr added: 15
DEBUG radiusSendAttributes: nas-port attr added: 603979877
DEBUG radiusSendAttributes: nas-port-id attr added: GigabitEthernet
1/0 :101
DEBUG radiusSendAttributes: acct-authentic attr added: 1
DEBUG radiusSendAttributes: acct-session-time attr added: 876
DEBUG radiusSendAttributes: acct-terminate-cause attr added: 10
```

---

## 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](http://www.juniper.net).

---

### Corporate and Sales Headquarters

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

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin,  
Ireland  
Phone: 35.31.8903.600  
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

