MX Series Subscriber Management for Customer VLANs

Although Juniper Networks has attempted to provide accurate information in this guide, Juniper Networks does not warrant or guarantee the accuracy of the information provided herein. Third party product descriptions and related technical details provided in this document are for information purposes only and such products are not supported by Juniper Networks. All information provided in this guide is provided "as is", with all faults, and without warranty of any kind, either expressed or implied or statutory. Juniper Networks and its suppliers hereby disclaim all warranties related to this guide and the information contained herein, whether expressed or implied of statutory including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement, or arising from a course of dealing, usage, or trade practice.

Table of Contents

Introduction

This implementation guide describes how to configure subscriber management on Juniper Networks® MX Series 3D Universal Edge Routers when they are used as Broadband Network Gateways and support customer VLANs. Subscriber management is performed by the Broadband Network Gateway (BNG) router, which is a key component of the overall Juniper multiplay architecture depicted in Figure 1. Subscriber management is also called AAA (authentication, authorization, and accounting), or AAAA (which adds address assignment). This includes the following:

- **Authentication:** The first step is to verify that the person attempting to use the network is who they claim to be. Dial-up users must provide a user-id and password, while a mobile phone will quietly send an electronic identifier. In a modern wireline "always on" broadband network (such as xDSL, FTTx, or cable), only authorized users should have network access, but this is typically still validated by the network operator.
- **Authorization:** This step determines which network resources the subscriber is allowed to use. For example, is the subscriber allowed to access at 512 Kbps, 1 Mbps, or 5 Mbps? Has the subscriber signed up for VoIP service? Whether or not Point-to-Point Protocol over X (PPPoX) is used, subscriber information is commonly in a RADIUS server. When a subscriber enters the network, the edge router sends a message to the RADIUS server asking what services the subscriber has access to, and the server responds with this information.
- **Address assignment:** As new devices enter the network, they request an IP address using Dynamic Host Configuration Protocol (DHCP). Different types of clients, such as set-top boxes (STBs), PCs, and VoIP phones, often receive their addresses from different DHCP servers. In fact, set-top boxes often must receive their IP addresses from the middleware server system. Even when devices (such as PCs and VoIP phones) receive their addresses from the same server, the addresses may come from different address pools.
- **Accounting:** This is the tracking of network and resource usage by the subscriber.

The AAA functions are tightly intertwined. In theory, the subscriber cannot access the network until an IP address is assigned; however, it is unwise to assign an address until the subscriber is authenticated.

This document is based on testing performed at Juniper Networks using a network supporting broadcast IPTV, video on demand, VoIP, and Internet traffic concurrently.

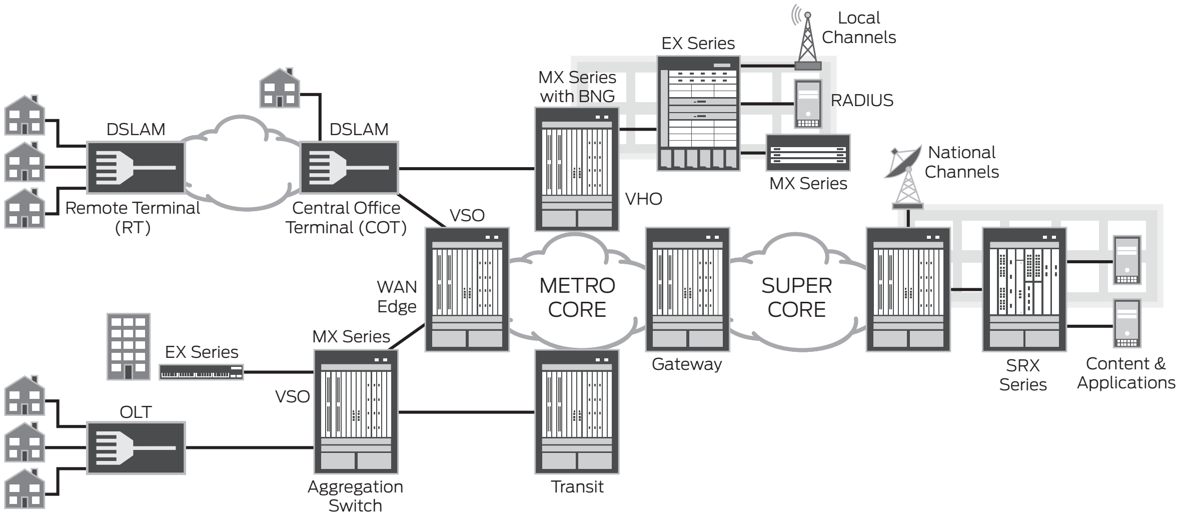

Figure 1: Juniper multiplay reference architecture

Scope

This Implementation guide describes the configuration on an MX Series router as a Broadband Network Gateway to provide subscriber access, authentication, and service creation, activation, and deactivation using customer VLANs. Figure 2 highlights the key network elements covered in this document. Subscriber management support is configured on the MX Series device closest to the multiservice access node (MSAN).

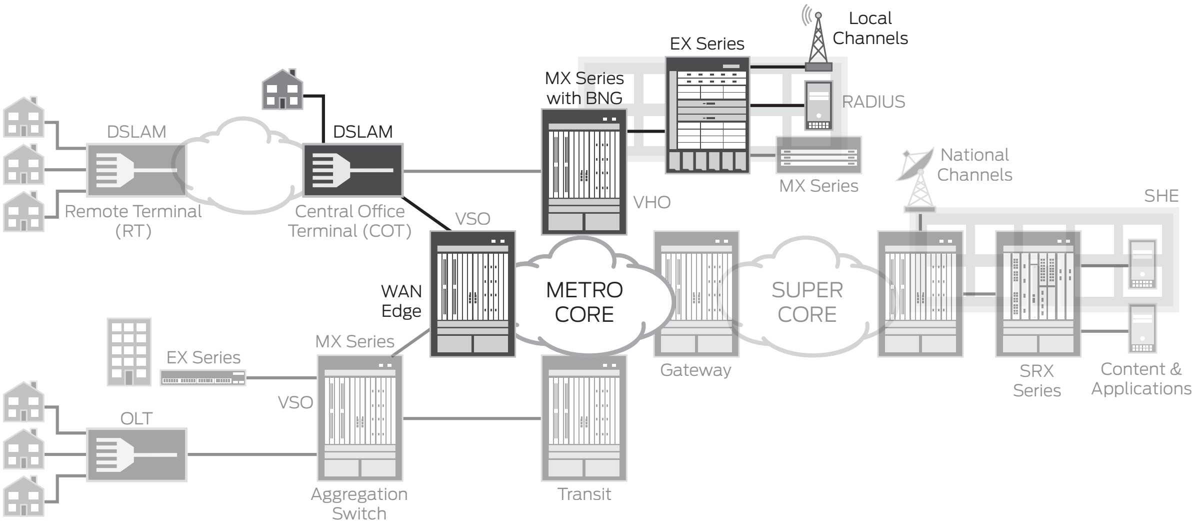

Figure 2: Network topology

Specifically, this document covers two implementations. First, it describes the configuration of static customer VLANs and multicast VLANs on a single physical interface. Second, it describes the configuration of dynamic customer VLANs on a physical interface.

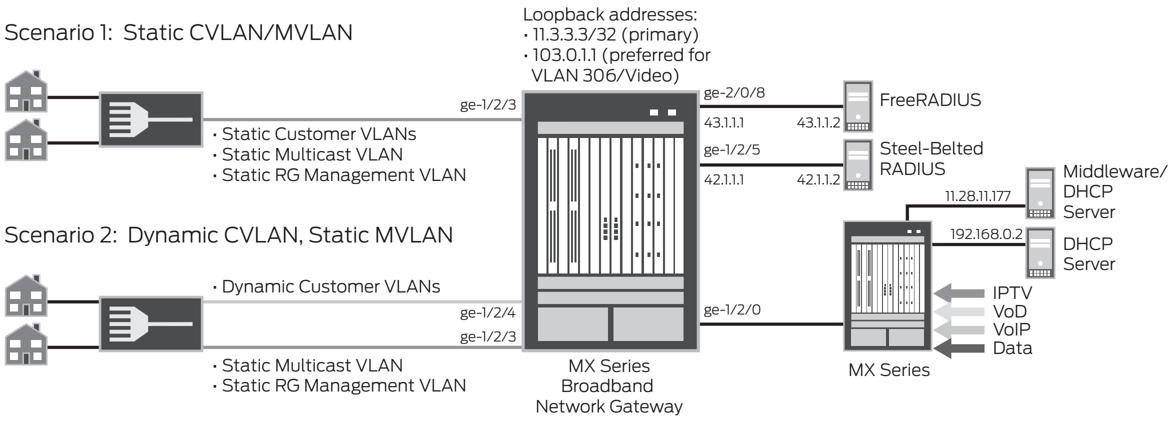

Figure 3: Subscriber management focus details

Design Considerations

Juniper supports a wide range of methods for supporting residential subscribers.

VLAN Models

The most fundamental decision is how VLANs should be configured to carry subscriber traffic across the access network. There are two methods, which for completeness are summarized below. This document covers the customer VLAN implementation.

- Service VLAN (S-VLAN). As depicted in Figure 4, a given VLAN carries one service to all subscribers. There are separate VLANs for voice, Internet access, and IPTV.
- Customer VLAN (C-VLAN). In this model, a given VLAN carries all services to one subscriber. This requires many more VLANs but simplifies network operations since each subscriber is mapped to a VLAN. However, not all MSANs support this model.

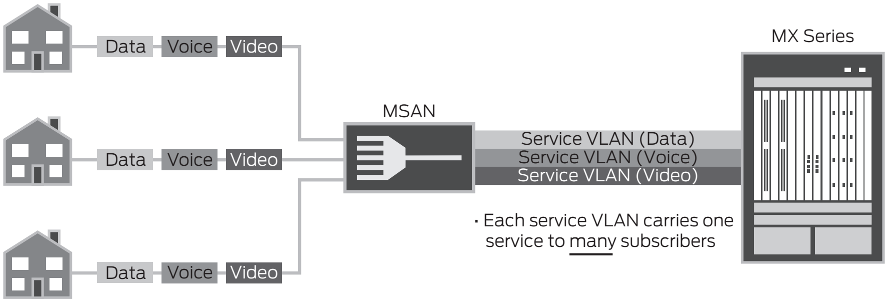

Figure 4: Service VLAN model

A common variation adds a single shared multicast VLAN (M-VLAN) which carries multicast traffic (broadcast IPTV) to all subscribers. This eliminates the need to send a channel multiple times across the network, once to each subscriber viewing the content. In addition, a C-VLAN model always requires service VLANs for managing network equipment such as routers, MSANs, Residential Gateways (RGs), and STBs.

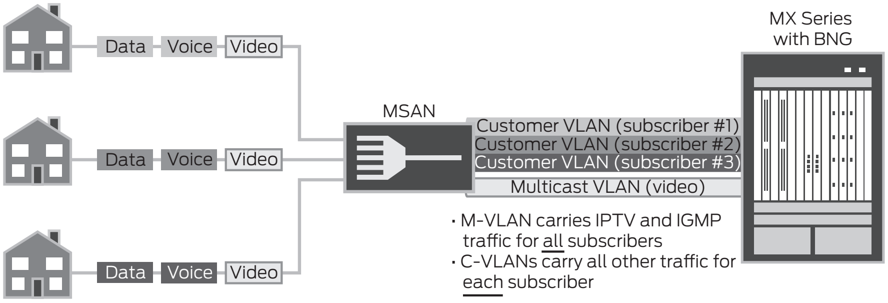
Data
Voice
Video
Data
Voice
Video
Data
Voice
Video
MSAN
MX Series with BNG
Customer VLAN (subscriber #1)
Customer VLAN (subscriber #2)
Customer VLAN (subscriber #3)
Multicast VLAN (video)
• M-VLAN carries IPTV and IGMP traffic for all subscribers
• C-VLANs carry all other traffic for each subscriber

Figure 5: Customer VLAN (with optional multicast VLAN) model

Adding IP Clients

Client connections may be defined statically or dynamically. Using static definitions quickly becomes cumbersome and inefficient to provision new subscribers, so dynamic definitions are more commonly deployed. There are two different dynamic models available within Junos OS, which differ according to whether the VLANs are also created dynamically. For C-VLANs, autosensing creates both VLAN and subscriber definitions dynamically. For S-VLANs, demultiplexing (demuxing) creates client definitions dynamically but uses predefined VLANs.

Stacking Customer VLANs

If there are less than 4,095 subscribers connected to a BNG interface, then a single VLAN tag can be used to uniquely identify each subscriber. However, there can easily be tens of thousands of subscribers on the network. In this case, VLAN stacking is used to bypass the VLAN scaling limit as illustrated in Figure 6. The process is as follows:

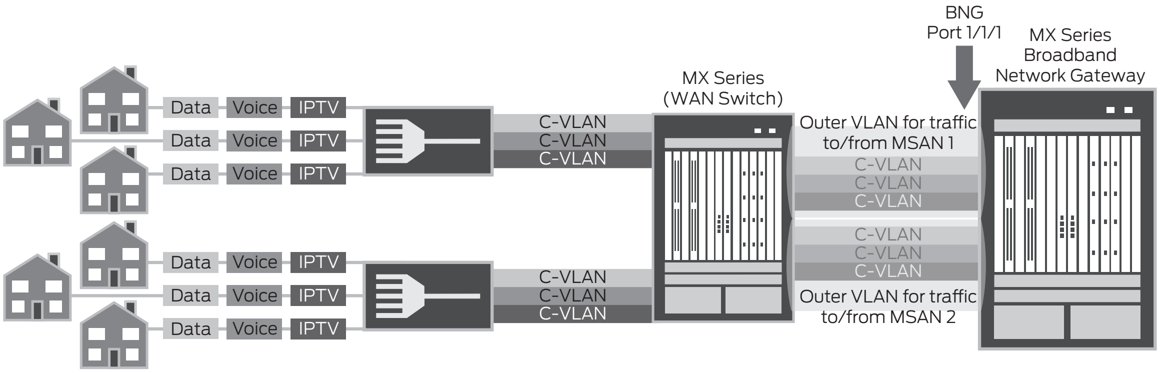

Figure 6: VLAN stacking for C-VLAN/M-VLAN

- The BNG adds the appropriate VLAN tags. For the C-VLANs, the outer tag identifies the destination MSAN, while the inner tag identifies the specific subscriber on that MSAN. IPTV content is also being delivered to two subscribers via the M-VLAN, which does not require stacking since it is shared by all subscribers on the BSE port.
- The Layer 2 switch uses the outer tag to determine where to forward the packet. It removes the outer tag on the C-VLANs (only) before forwarding the packets to the MSAN.
- The MSAN adjusts VLAN tags and forwards the information to each subscriber. There are several variations to this:
  - All traffic to a given subscriber is merged onto the C-VLAN for that subscriber.
  - All VLAN tags may be swapped to a common value or removed. This allows the operator to deploy a single configuration for all connected home gateway routers. Keeping the VLAN tags allows specifying the traffic priority using Ethernet's 802.1p bits carried in the VLAN tag.

Note that when using stacking, the "inner" C-VLAN values may be repeated within each stack.

Additional VLANs

Additional VLANs are often required for MSAN management, RG management, and booting of set-top boxes. These are configured similarly to the M-VLAN.

IP Address Assignment

IP addresses can be assigned to network devices in several ways:

- The IP address can be preconfigured. This is done for the MSAN.
- The IP address can be assigned by a DHCP server embedded within the router. This is the role of Junos OS' "local DHCP server" subsystem, and is used for the residential gateways. All PCs and VoIP equipment sit behind the RG, which hides the other devices by implementing Network Address Translation (NAT).
- The IP address can be assigned by a standalone ("external") DHCP server. This is done for the STBs.

This document uses a combination of these techniques to illustrate the options.

Subscriber Database

Information about subscribers/clients may be defined in various ways:

- The information can be statically configured in the router. In a service VLAN network using dynamic address assignment, this results in having the same services for all subscribers.
- This information can be stored in a DHCP server, and sent as a DHCP option during the address assignment process. Some smaller, newer deployments use this technique. However, DHCP supports a limited set of capabilities.
- The information can be stored in a RADIUS server and sent as RADIUS attributes when the client enters the network. This is the original method supported by the DSL Forum, so it has been implemented by virtually all Tier 1 vendors and early entrants. It is the most mature implementation, with the widest range of supported information which can be pushed down to the router to specify the client's authorizations.

This document uses a RADIUS server as the subscriber repository. Table 1 summarizes the VLAN and IP address allocations used in this setup.

Table 1: VLAN Allocations and Associated Loopback IP Addresses

	VLAN		Preferred (Loopback) Source IP Address	IP Addresses	
	Allowed Range	Configured		DHCP Server	Subnet
Management					
DSLAM Mgt	900-999	901	None	Static	109.1.0.1/30
Services					
Subscribers	1000-4094 (Outer)	1001	None	Junos OS	Unnumbered
Video/IPTV	301-399	306	None	192.168.0.2	100.1.1.x/24

Protocol Operation

Providing AAA service may involve RADIUS authentication and DHCP address assignment. The DHCP server assigning the addresses may be integrated into an MX Series router (local server) or may be a standalone device (external server).

Figure 7 overviews the AAAA process when using an external DHCP server.

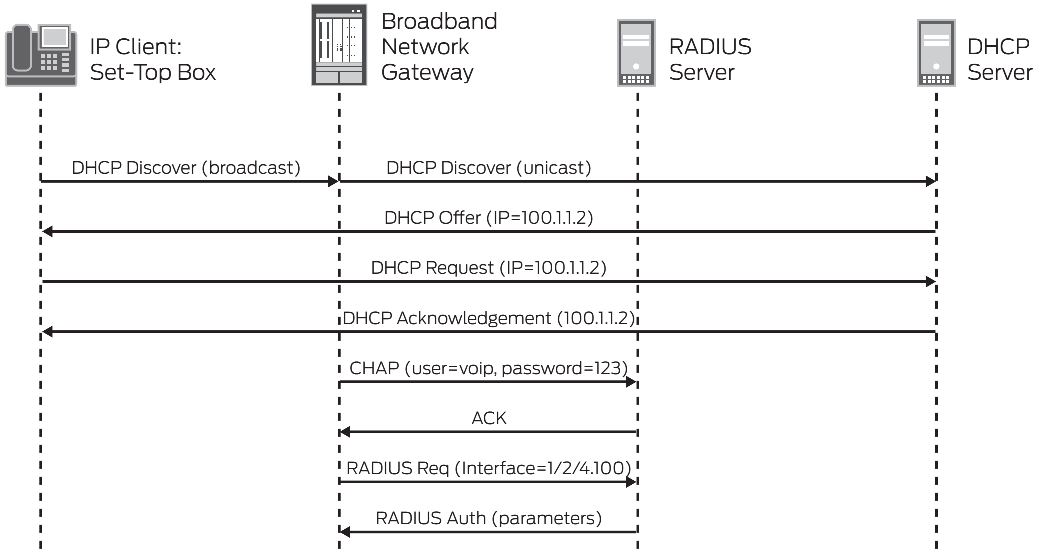
IP Client:
Set-Top Box
Broadband
Network
Gateway
RADIUS
Server
DHCP
Server
DHCP Discover (broadcast)
DHCP Discover (unicast)
DHCP Offer (IP=100.1.1.2)
DHCP Request (IP=100.1.1.2)
DHCP Acknowledgement (100.1.1.2)
CHAP (user=voip, password=123)
ACK
RADIUS Req (Interface=1/2/4.100)
RADIUS Auth (parameters)

Figure 7: Adding new client using DHCP external server

The following general sequence occurs during access configuration for a DHCP client:

1. The client uses a standard DHCP process to get an IP address.

   a. Client issues a DHCP DISCOVER to request an IP address. The MX Series intercepts this request, substituting the destination address to that of defined DHCP servers, and forwards the message. The MX Series will forward the request to each defined DHCP address. The router DHCP component recognizes the DHCP message and adds the client (without an assigned IP address) to the router session database.

   b. The DHCP server issues a DHCP OFFER, proposing an IP address for the client. The client may receive multiple offers.

   c. The client responds with a DHCP REQUEST, indicating the preferred address to use. The request is forwarded to all DHCP servers.

   d. Finally, the DHCP server responds with a DHCP ACKNOWLEDGEMENT, to confirm that the address has been accepted.

2. If RADIUS is configured:

   a. The router "logs into" the RADIUS server by sending a user-id and password. Typically, Challenge Handshake Authentication Protocol (CHAP) is used.

   b. The login request is acknowledged.

   c. The router sends a RADIUS REQUEST message, essentially asking for information about this subscriber's permissions.

   d. The RADIUS server responds by sending a RADIUS RESPONSE with the information, which is sent using IETF standard and Juniper-specific RADIUS attributes.

3. At this point, the router sets the capabilities for this subscriber.

   a. The router adds RADIUS authorization information to the router session database.

   b. The router combines the dynamic profile with the RADIUS authorization information.

   c. The router alerts all internal applications involved with the subscriber access (for example, routing protocols, dynamic firewall, and dynamic class of service).

Figure 8 depicts the AAAA process using the integrated DHCP server.

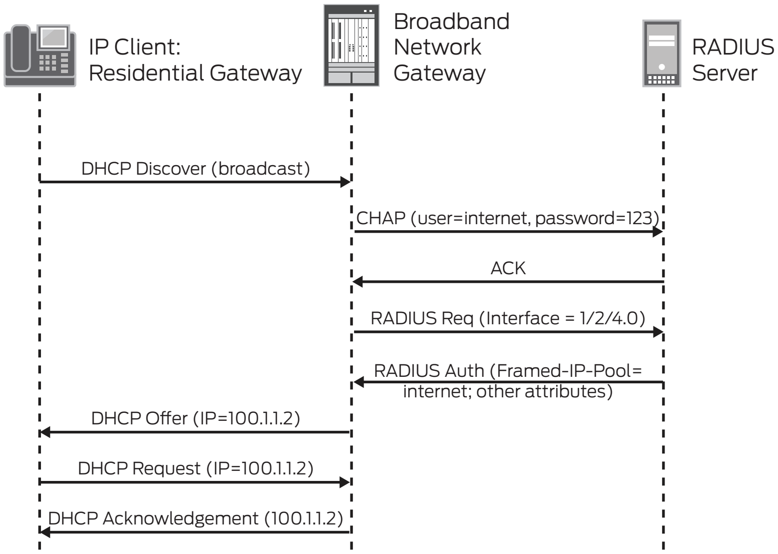
IP Client:
Residential Gateway
Broadband
Network
Gateway
RADIUS
Server
DHCP Discover (broadcast)
CHAP (user=internet, password=123)
ACK
RADIUS Req (Interface = 1/2/4.0)
RADIUS Auth (Framed-IP-Pool=
internet; other attributes)
DHCP Offer (IP=100.1.1.2)
DHCP Request (IP=100.1.1.2)
DHCP Acknowledgement (100.1.1.2)

Figure 8: Adding new client using DHCP local server

When using local server, the IP address is assigned by the router instead of by an external server. The IP address may be assigned in one of three ways:

- The RADIUS server tells the MX Series router the name of the address pool to use (shown), or
- The RADIUS server tells the MX Series router what specific IP address to use, or
- The RADIUS server provides no information, allowing the MX Series router to follow whatever procedure has been defined within the MX Series.

Implementation

A subscriber service is based on the combination of a defined dynamic profile and attributes configured through authentication. Dynamic profiles can include dynamic firewall filters, class-of-service (CoS) settings, and Internet Group Management Protocol (IGMP) settings that define access limits for subscribers and the scope of a service granted to the subscriber once access is obtained.

The remainder of this document walks through how the broadband services edge router is configured to support this. It is organized as follows:

- Loopback addresses
- Defining RADIUS servers and profiles
- Defining DHCP servers
- Interfaces (ports and VLANs)
- Quality of Service (QoS)

Loopback Address

Loopback addresses are not tied to a physical interface. There is one box-wide loopback address, plus one for each *function* that uses an external DHCP server. In our case, there is one function using an external DHCP server—the set-top box. When communicating to the external DHCP server to get an address for an STB, the router specifies 103.1.0.1 as the source address.

```
lo0 {
    unit 0 {
        family inet {
            address 11.3.3.3/32 {
                primary;
            }
        }
    }
}
```

Defining RADIUS Servers and Profiles

There are three steps to defining and configuring RADIUS servers:

1. Specify the available RADIUS servers

2. Configure profile(s) that specify which RADIUS server(s) to contact (multiple profiles can be created)

3. Specify which profile(s) will be used

Specifying RADIUS Servers

The ability to operate with two different RADIUS servers was validated in Juniper testing. 42.1.1.2 is the address used for Juniper's Steel-Belted Radius server, while 43.1.1.2 is FreeRADIUS.

```
access {
    radius-server {
        42.1.1.2 {
            port 1812;
            secret “$9$6Tgs/tO1IcrlMOBxNbwg4”; ## SECRET-DATA
        }
        43.1.1.2 {
            port 1812;
            secret “$9$DwjqfTQn9Cuf5IEyrvM”; ## SECRET-DATA
        }
    }
}
```

Defining RADIUS Profiles

The access profile specifies which RADIUS servers should be checked. This example includes a single profile named "ISE" which checks two RADIUS servers. One server (42.1.1.2) is Juniper's SBR Carrier RADIUS server, while the other is FreeRADIUS. Note that only one server was active at a time during our testing.

The nas-identifier is the address with which the RADIUS server communicates. This configuration uses a loopback address as the nas-identifier.

```
    profile ISE {
        authentication-order radius;
        radius {
            authentication-server [42.1.1.2 43.1.1.2];
            options {
                nas-identifier 11.3.3.3;
            }
        }
        radius-server {
            42.1.1.2 {
                port 1812;
                secret “$9$q.5Fn6Au0IF3SrvMXx”; ## SECRET-DATA
            }
            43.1.1.2 {
                port 1812;
                secret “$9$cytSeWLX-bwgW8ZUHkPf”; ## SECRET-DATA
            }
     }
```

Access Profile

Finally, the access-profile command specifies which profile will be used.

```
access-profile ISE;
```

Defining DHCP Servers

IP addresses can be assigned by the router (local server) or by an external DHCP server. In addition, an IP address may be sent by the RADIUS server. If different IP addresses are returned by the various servers, the following is the priority order:

- External DHCP server: This takes precedence over the address (or pool) from the RADIUS server.
- RADIUS server: If an address (or pool) is sent by the RADIUS server, this takes precedence over the IP address which would otherwise be assigned by a router's local (integrated) DHCP server.
- Local DHCP server: This address pool will be used when no other servers specify an address to use.

Table 1 shows which device assigns the IP addresses. Additional pools can easily be created to support additional devices. For example, if this port supports OLTs as well as digital subscriber line access multiplexers (DSLAMs), different address pools could be created that support clients attached to the OLT (if desired).

Configuring Local DHCP Server

Configuring the local server includes two pieces:

- Configuring the address pools which will be used when assigning IP addresses
- Configuring RADIUS access

Configuring Address Pools

This first portion defines the IP address pools used by the DHCP local server (local server = addresses that are assigned by the MX Series) to assign addresses. Only an "Internet" pool is defined, since only VLAN 101 (PCs) get their IP addresses assigned by the local DHCP server.

```
    address-assignment {
        pool cvlan {
            family inet {
                network 197.20.0.0/16;
                range ip {
                    low 197.20.0.1;
                    high 197.20.255.254;
                }
                dhcp-attributes {
                    maximum-lease-time 10000;
                    grace-period 100;
            }
        }
    }
```

Configuring RADIUS Access

The next piece is to define parameters for communicating with the RADIUS server. As noted in the configuration, this pool only applies to traffic coming from ge-1/2/4.0—that is, all traffic (VLANs) on the specified physical interface.

Pool-match-order specifies that the pool name to use will be sent by the RADIUS server (IETF attribute 88). If this parameter is absent, then the local server will use the IP address specified by the RADIUS server (IETF attribute 8). If RADIUS does not send an IP address, then the local server will assign an IP address from its own pool.

Note that the configuration also specifies that an external dynamic profile called "subscriber" will be used. This is the template which will be used to create subscriber connections as new clients enter the network.

```
system {
    services {
        dhcp-local-server {
            traceoptions {
                file dhcp size 10m;
                flag all;
            }
            pool-match-order {
                external-authority;
            }
            group cvlan {
                authentication {
                    password lab123;
                    username-include {
                        user-prefix cvlan;
                    }
                }
                dynamic-profile dhcp-profile;
                interface ge-1/2/4.0;
            }
```

Configuring DHCP Relay

This section shows the DHCP definition for clients using external servers. When doing this, the router must convert the broadcasted DHCP request into a directed unicast request. This function is one piece of the DHCP Relay function. In addition, this is where the IP addresses of external DHCP servers are specified.

How do these servers know what type of device the requesting client is, so that the appropriate IP address can be assigned? That information typically is provided in one of two ways. First, DHCP flows include a CHADDR field, which is the media access control (MAC) address of the device that initiated the DHCP request. The first half of this field is a vendor identifier field. For example, CHADDR=242337xxxxxx is manufactured by Avaya, and in our network, this is always a VoIP phone. The other alternative is that the equipment may add a DHCP Option 60 field. This option allows the client to send information identifying what type of device it is or what pool to use. In either case, the router does not modify these fields or influence the address assignment process.

In addition to forwarding the request to the external DHCP server, the requests trigger an authentication call to the RADIUS server. For DHCP requests received on interface ge-1/2/4.0 (that is, any VLAN on the specified physical interface), the user-prefix “cvlan” is included in the RADIUS login request to identify the type of client. In our case, “cvlan” is the entire login name. In other cases, this prefix may be added to other information such as the MAC address, to more tightly identify the client.

Note that the middleware group (for IPTV set-top boxes) specifies that an external dynamic profile called “dhcp-profile” will be used. This is the template used to create subscriber connections as new clients enter the network.

DHCP relay converts a broadcasted DHCP request into a unicast request and forwards it to all of the specified servers. Only DHCP servers with pools matching the request will respond by offering an IP address.

While RADIUS can also be used to authenticate RGs, this is not done in this setup.

```
forwarding-options {
    dhcp-relay {
        server-group {
            middleware {
                192.168.0.2;
            }
        }
        group middleware {
            active-server-group middleware;
            authentication {
                password lab123;
                username-include {
                    user-prefix video;
                }
            }
            dynamic-profile dhcp-profile;
            interface ge-1/2/4.0;
        }
    }
}
```

Scenario 1: Interface Definitions for Statically Defined VLANs

The snippet below shows a configuration for an interface supporting statically defined C-VLANs and M-VLAN on the same physical port. The following VLANs are defined:

- One shared multicast VLAN (306)
- Management VLANs for the home gateways (801) and MSANs (901). Additional service VLANs could also be defined to support multiple brands or equipment types. For example, there could be separate VLANs for managing Adtran DSLAMs, Allied Telesis DSLAMs, and Motorola OLTs.
- Four customer VLANs—two connected to each of two different MSANs. Figure 9 depicts the VLANs used in this configuration.

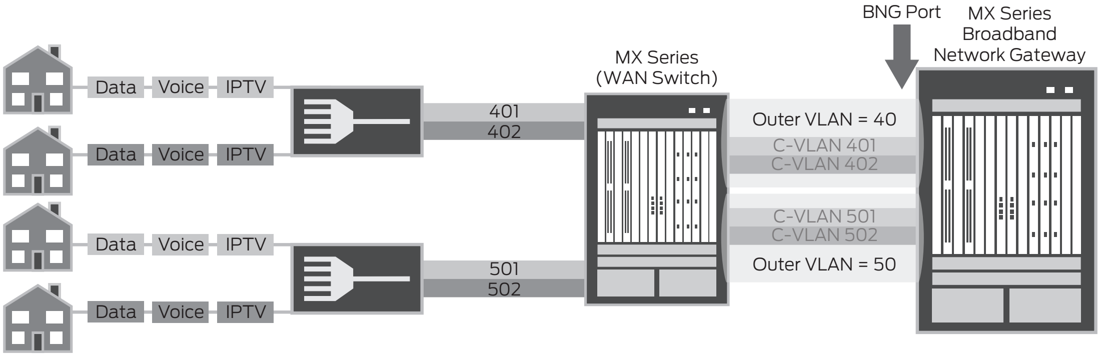

Figure 9: Statically configured customer VLANs

```
ge-1/2/3 {
    description “MSAN using static C-VLANs and M-VLAN”;
    flexible-vlan-tagging;
    gigether-options {
        ethernet-switch-profile {
            tag-protocol-id [ 0x8100 0x9100 ];
        }
    }
    unit 306 {
        description MVLAN;
        vlan-id 306;
        family inet {
            address 100.1.1.1/24;
        }
    }
    unit 901 {
    description “ MSAN management VLAN”;
    vlan-id 901;
    family inet {
        address 109.1.0.1/30;
        }
    }
    unit 4401 {
    description CVLAN;
    vlan-tags outer 0x8100.40 inner 0x9100.401;
    family inet {
        address 110.1.1.1/24;
    }
}
unit 4402 {
    description CVLAN;
    vlan-tags outer 0x8100.40 inner 0x9100.402;
    family inet {
        address 110.1.2.1/24;
    }
}
unit 5501 {
    description CVLAN;
    vlan-tags outer 0x8100.50 inner 0x9100.501;
    family inet {
        address 111.1.1.1/24;
    }
}
unit 5502 {
    description CVLAN;
    vlan-tags outer 0x8100.50 inner 0x9100.502;
    family inet {
        address 111.1.2.1/24;
    }
}
```

Dynamic Bandwidth Adjustment

The MX Series router can dynamically adjust the amount of bandwidth available for use by unicast applications for each subscriber based on the amount of multicast traffic being sent to the subscriber. The key requirement is that the MSAN transparently pass all channel change requests upstream to the MX Series. Reverse OIF (outgoing interface) mapping is used to associate traffic to each subscriber on the M-VLAN and C-VLAN.

By default, the router enables QoS adjustment by building this mapping automatically. QoS adjustment can be disabled using the configuration shown below.

```
multicast {
    interface ge-1/2/3.306 {
        reverse-oif-mapping {
            no-qos-adjust;
        }
    }
}
```

Link Aggregation

As a periphery test, the ability to support cross-Dense Port Concentrator (DPC) aggregated Ethernet interfaces was also verified. This test aggregated ge-1/1/9 and 2/1/9 together into the ae0 aggregated interface. The capability worked as expected.

Scenario 2: Dynamically Defined Customer VLANs

This section shows how to define dynamically created customer VLANs. Since there are few M-VLANs in the network, these are typically statically defined.

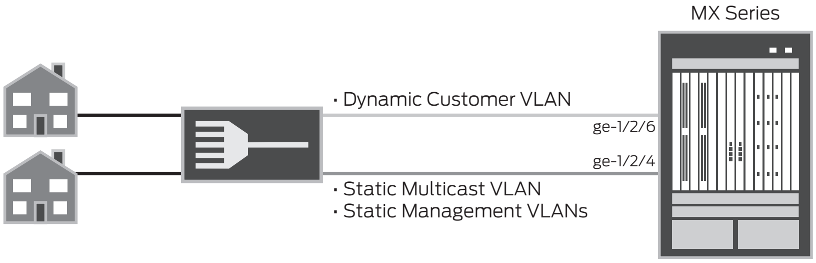

Figure 10: Dynamic C-VLAN with static M-VLAN

Dynamic definition consists of two pieces—the interface definition and the dynamic profile (C-VLAN) which is applied to that interface. A dynamic DHCP profile (described earlier) is also required.

Interface Definition

The key point of this interface definition is that it supports any outer/inner VLAN combination (ranges {any, any}) using IPv4 (accept inet).

```
ge-1/2/4 {
      description “Dynamic C-VLAN”;
      traceoptions {
          flag all;
      }
      hierarchical-scheduler;
      flexible-vlan-tagging;
      auto-configure {
          stacked-vlan-ranges {
              dynamic-profile CVLAN {
                  accept inet;
                  ranges {
                      any,any;
                  }
              }
          }
      }
  }
```

C-VLAN Template

Below is the dynamic profile (C-VLAN) specified in the interface definition shown above. When a DHCP request is received, the router builds a subscriber interface record using this template.

- $junos-interface-ifd-name: The physical interface on which the request was received (e.g., ge-1/2/4)
- $junos-interface-unit: The unique 10-digit session identifier assigned by the router (e.g., 1073766100)
- $junos-stacked-vlan-id: The VLAN-identifier for the outer tag (e.g., 40)
- $junos-vlan-id: The VLAN-identifier for the inner tag (e.g., 401)
- $junos-interface-unit: The unit number (e.g., 4401)

```
 CVLAN {
     interfaces {
         “$junos-interface-ifd-name” {
             unit “$junos-interface-unit” {
                 proxy-arp;
                 vlan-tags outer “$junos-stacked-vlan-id” inner “$junos-vlan-
id”;
                 family inet {
                     mac-validate strict;
                     unnumbered-address lo0.0 preferred-source-address 11.3.3.3;
                 }
             }
         }
     }
 }
```

Dynamic QoS Profile

The final piece is the dynamic QoS profile, or template, which will be used. Templates are built using Junos OS variables, which are replaced by the actual values when bringing up new connections. Junos OS variables start with the $ symbol. Some variables are assigned by the MX Series when a DHCP request is received based upon the received port. These are forwarded to the RADIUS server for determining other parameters applicable to this client. The sample includes a handful of Junos OS variables to illustrate their usage.

Some variables are assigned by Junos OS based upon the interface that received the triggering packet (typically a DHCP DISCOVER). For example:

- 10-digit sequence is randomly assigned by the router to $junos-interface-ifd-name = ge-1/2/4
- $junos-underlying-interface-unit = 1073766100
- $junos-interface-name = ge-1/2/4.1073766100. (The identify a client. It is also called a logical interface.)

RADIUS can also return an IP address to be assigned to the client. This value may be overridden by the value sent by an external DHCP server.

- $junos-subscriber-ip-address = 103.1.0.2   (IETF 8)

This snippet also shows the scheduler supporting dynamically configured traffic. Since QoS is not the focal point of this document, a simple QoS mechanism is used. Traffic is assigned into four forwarding classes: VoIP, video, gaming, and Internet.

```
dhcp-profile {
       interfaces {
           “$junos-interface-ifd-name” {
               unit “$junos-underlying-interface-unit” {
                   family inet;
               }
           }
      }
        class-of-service {
            traffic-control-profiles {
                Subscriber_CoS {
                    scheduler-map “Multiplay”;
                    shaping-rate 25m;
                }
            }
            interfaces {
                “$junos-interface-ifd-name” {
                    unit “$junos-underlying-interface-unit” {
                        output-traffic-control-profile Subscriber_CoS;
                    }
                }
            }
            scheduler-maps {
                Multiplay {
                    forwarding-class VoIP scheduler VoIP-SCHED;
                    forwarding-class VIDEO scheduler VIDEO-SCHED;
                    forwarding-class GAMING scheduler GAMING-SCHED;
                    forwarding-class INTERNET scheduler INTERNET-SCHED;
                }
            }
            schedulers {
                VoIP-SCHED {
                    transmit-rate 1m rate-limit;
                    priority high;
                    drop-profile-map loss-priority any protocol any drop-profile
VoIP-DROP;
                }
                GAMING-SCHED {
                    drop-profile-map loss-priority any protocol any drop-profile
GAMING-DROP;
                }
                VIDEO-SCHED {
                    transmit-rate 18m rate-limit;
                    priority medium-low;
                    drop-profile-map loss-priority any protocol any drop-profile
VIDEO-DROP;
                }
                INTERNET-SCHED {
                    transmit-rate remainder;
                    priority low;
                    drop-profile-map loss-priority any protocol any drop-profile
INTERNET-DROP;
                }
            }
        }
```

Summary

Juniper testing confirms that Junos OS subscriber management provides the functionality required to support customer VLAN implementations. The configuration pieces provided in this document have been implemented and tested at Juniper using a variety of MSANs. For additional information on configuring the MX Series 3D Universal Edge router, refer to the Junos OS software guides at **www.juniper.net/techpubs/software/junos/index.html**

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701