Configuring and Deploying Ethernet Switching on SRX3xx, SRX550M, and SRX1500 Services Gateways

Application Note

September 2016

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Contents

List of Tables

List of Figures

Introduction

Juniper Networks SRX Series Services Gateways for the branch enable an enterprise to provide services without boundaries. The Ethernet switching features on these devices can reduce or even eliminate the need for Layer 2 switches in branch offices.

Juniper Networks Junos operating system Release 15.1 for the SRX Series introduces changes in the Ethernet switching features, mainly in the CLI configuration of Layer 2 features. This application note is intended to capture all relevant information regarding these changes. It also describes common deployment scenarios and includes detailed configurations and examples.

Scope

This application note covers details for the hardware platforms listed in Table 1 only.

For information on using Ethernet switching features in an SRX Chassis Cluster environment, see the SRX Series Services Gateway technical documentation.

Hardware Scope

Platform	On-Board Cu GE	On-Board SFP GE	mPIM	gPIM
SRX300	6	2	x	x
SRX320	6	2	2	x
SRX320-POE	6	2	2	x
SRX340	8	8	4	x
SRX345	8	8	4	x
SRX550M	6	4	2	6*
SRX1500	12	4x1GE + 4x 10GE	2	x

*Out of 6 GPIM slots only 2 (slot 3 and slot 5) support Ethernet switching

Table 1 – Physical Interface Support on SRX Series Devices

Starting with Junos OS 15.1X49-D50, all interfaces have support for Ethernet switching. [Release Notes]

Software Scope

SRX Series devices for the branch support two modes: *transparent* mode and *switching* mode. Table 2 shows a matrix of current support for these modes as of Junos OS Release 15.1X49-D50.

	Global Mode	
Scenarios	**L2 - Transparent Mode (L2TM)**	**Switching**
L3 Routing	Yes	Yes
Stateful Firewall for L2 traffic	Yes	No
L1 Secure-Wire	Yes	No
Management over IRB	Yes	Yes
Routing over IRB	No	Yes

Packet Switched	at flowd (SRXPFE)	Broadcom (L2) Chip
Mixed Mode	L1 | L2TM | L3	L2 Switch | L3
Platforms Supported	All (Including High-End)	SRX300, SRX320, SRX340, SRX345, SRX550M SRX1500 Only
Link Aggregation - LACP	No	Yes
HA Support	Yes	No (Roadmap)
IPv6 Support	Yes	Yes
L2 interfaces and Zones	Physical Interfaces must be added to Zones	IRB interfaces (not physical) must be added to zones

Table 2 – Software Support Scope on SRX Series Devices

The Ethernet switching features on SRX Series branch devices are based on Juniper Networks EX Series Ethernet switches, which follow the Enhanced Layer 2 Switching (ELS) configuration method.

Feature and Capabilities

This section describes the Ethernet switching feature and capabilities on SRX Series Services gateways.

Supported Features

As of Junos OS Release 15.1X49-D50, the following features are supported:

- Layer 2 switching of traffic, including support for both trunk and access ports
- Intra-VLAN and Integrated Routing and Bridging (IRB) for Inter-VLAN traffic
- Link Aggregation using the Link Aggregation Control Protocol (LACP)

Limitations

As of Junos OS Release 15.1X49-D50, the following features are not supported. Please check the release notes for more details.

- IEEE 802.1x authentication
- Link Layer Discovery Protocol (LLDP), LLDP-MED (available in Junos OS 15.1X49-D60)
- Ethernet switching in HA (Chassis Cluster)
- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RTSP)
- Multiple Spanning Tree Protocol (MSTP)
- IGMP snooping
- IEEE 802.1Q (dot1q) tunneling (Q-in-Q)
- IRB support in Packet mode (available in 15.1X49-D60 release)
- Port Security features (MAC limiting, allowed MAC address)
- GVRP / MVRP
- Ethernet OAM, CFM, and LFM

Summary of Changes (CLI)

Table 3 provides a summary of the CLI changes made for Ethernet switching features on SRX SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Services Gateways.

	Old CLI - Switching	Old CLI - L2TM	New Common CLI
VLANs	[edit **vlans**] <vlan-name> vlan-id <vlan-id>	[edit **bridge-domain**] <bd-name> vlan-id <vlan-id>	[edit **vlans**] <vlan-name> vlan-id <vlan-id>
	[edit **vlans**] <vlan-name> **vlan-range** <start>-<end>	[edit **bridge-domain**] <bd-name> **vlan-id-list** [values	[edit **vlans**] <vlan-name> **vlan-id-list** [values]
	[edit **vlans**] <vlan-name> interface <ifl-name>	[edit **bridge-domain**] <bd-name> interface <ifl-name>	[edit **vlans**] <vlan-name> interface <ifl-name>

		[edit **bridge-domains**]
		<bd-name> {
		bridge-options
		}
			[edit **vlans**]
			<vlan-name> **switch-options**

Interfaces	[edit **interfaces**]
	<ifd>
	unit 0 {
	family **ethernet-switching** {
	vlan members <vid-list>;
	port-mode trunk/access;
	}
	}
	}
		[edit **interfaces**]
		<ifd>
		unit 0 {
		family bridge {
		vlan-id <vid>;
		vlan-id-list <vid-list>;
		}
		}
		}
			[edit **interfaces**]
			<ifd>
			unit 0 {
			family ethernet-switching {
			vlan members <vid-list>;
			interface-mode trunk/access;
			}
			}
			}

	[edit **interfaces**]
	<ifd> {
	unit 0 {
	family **ethernet-switching** {
	native-vlan-id <vid>;
	port-mode trunk;
	}
	}
	}
		[edit **interfaces**]
		<ifd> {
		native-vlan-id <vid>;
		unit 0 {
		family bridge {
		interface-mode trunk;
		}
		}
		}
			[edit **interfaces**]
			<ifd> {
			native-vlan-id <vid>;
			unit 0 {
			family ethernet- switching {
			interface-mode trunk;
			}
			}
			}

	[edit **interfaces**]
	<ifd> {
	ether-options | gigether-options;
	}
		[edit **interfaces**]
		<ifd> {
		ether-options | gigether-options;
		}
			[edit **interfaces**]
			<ifd> {
			ether-options;
			}

	[edit vlans]
	<name> {
	l3-interface vlan.x;
	}
		[edit bridge-domain]
		<bd-name> {
		routing-interface <ifl-name>;
		}
			[edit vlans]
			<name> {
			l3-interface irb.x;
			}

Show	show vlans	show bridge-domain	show vlans
	show ethernet-switching interface	show l2-learning interface	show ethernet-switching interface
	show ethernet-switching table	show bridge mac-table	show ethernet-switching table
	show route forwarding-table family ethernet-switching	show route forwarding-table family bridge	show route forwarding-table family ethernet-switching

Table 3 – Summary of CLI Changes on SRX Series Devices

Life of a Packet in Ethernet Switching

Figure 1 illustrates the life of a packet processed by Ethernet switching features.

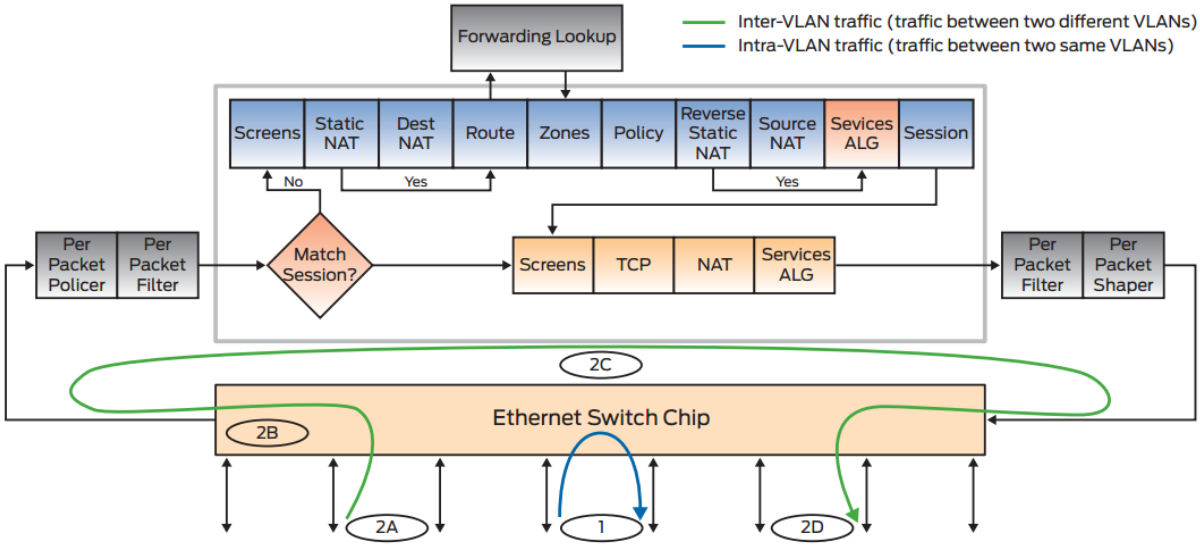

Figure 1 – Life of Packet in Ethernet Switching

1. Intra-VLAN traffic – Once interfaces are configured in the same VLAN, the "Ethernet switch chip" is programmed accordingly; MAC learning and VLAN states are maintained in the Layer 2 hardware. Packets in the same VLAN are switched internally by the Layer 2 Ethernet switch. Since packets do not traverse the flow architecture, security features are not applied to this traffic.
2. Inter-VLAN traffic – Packets for different VLANs are routed/forwarded through the flow architecture.
    a. Incoming traffic is classified according to the port-based VLAN.
    b. The destination MAC address of inter-VLAN traffic is matched with the IRB interface at the Ethernet switch and is sent to the flow module for further processing.
    c. In the flow module, inter-VLAN traffic goes through all security checks and is routed to a different VLAN.
    d. Routed traffic is sent back to the Ethernet switch chip, which then sends out the traffic.

Changes between Junos OS Release 12.3 and Release 15.1: *Inter-VLAN IRB interfaces in Junos OS Release 12.3 or older were named* ***vlan.x****; in Junos OS Release 15.1 they are named* ***irb.x***

Ethernet Switching Deployment Scenarios

Enabling Ethernet Switching on SRX3xx, SRX550M, and SRX1500 Services Gateways

Starting with Junos OS Release 15.1X49-D50, SRX Series branch devices have global switching enabled by default. The factory default configuration includes the following configuration:

```
set protocols l2-learning global-mode switching
```

This configuration can be used to enable and disable Ethernet switching on the SRX Series devices, including both Layer 2 switching and IRB-based routing.

When the SRX Series device does not have the default configuration shown above, its default configuration is transparent mode. Enabling and disabling switching mode requires a system reboot.

Configuring Layer 2 Switching

The following configuration defines an interface as a switching port:

```
interfaces {
          ge-<slot number>/0/<port number> {
                unit 0 {
                      family ethernet-switching;
                }
          }
}
```

The Layer 2 configuration is limited to **unit 0** of an interface. Additionally, Ethernet switching needs to be enabled globally, as described in the previous section.

Changes between Junos OS Release 12.3 and Release 15.1: None

Configuring VLANs

By default, all switching-enabled interfaces form part of the same broadcast domain. If an interface is enabled for Layer 2 switching but not associated with any VLAN, it becomes part of the default VLAN (VLAN ID 1). To configure a new domain, a VLAN has to be defined under the **[vlans]** hierarchy and given a unique identifier (VLAN ID).

```
vlans {
          <vlan name> {
                vlan-id <id>;
          }
}
```

Supported VLAN Range (Table)

Platform	No. of VLANs
SRX300	1000
SRX320	1000
SRX320-POE	1000
SRX340	2000
SRX345	3000
SRX550M	3967
SRX1500	3900

Table 4 – Number of VLANs Supported on SRX Series Devices

Note: On SRX3xx and SRX5xx devices, the VLAN IDs 3968 through 4096 are reserved and cannot be configured.

Attaching Switch Ports to VLANs

There are two ways to attach an interface to a VLAN.

The first way, under the **[interfaces]** hierarchy, is to declare the VLAN as a part of an interface configuration, as follows:

```
interfaces {
          ge-<slot number>/0/<port number> {
                unit 0 {
                      family ethernet-switching {
                             vlan {
                                  members <vlan name>;
                            }
                      }
                }
          }
}
```

The second way, under the **[vlan]** hierarchy, is to define the VLAN member interfaces, as follows:

```
vlans {
          <name> {
                vlan-id <id>;
                interface <interface name>;
                interface <interface name>;
          }
}
```

Changes from Junos OS 12.3 to Release 15.1: None

Configuring the Port Mode

VLAN tagging (IEEE 802.1q) extends the Ethernet header by adding a VLAN identifier (a 12-bit value) that is used to differentiate traffic from different VLANs. To configure a switch port as an access port, use following configuration:

```
interfaces {
          ge-<slot number>/0/<port number> {
                unit 0 {
                      family ethernet-switching {
                            interface-mode access;
                      }
                }
          }
}
```

By default, all switching interfaces are access ports. An interface can be configured as a trunk port by changing the configuration, as shown below:

```
interfaces {
          ge-<slot number>/0/<port number> {
                unit 0 {
                      family ethernet-switching {
                            interface-mode trunk;
                            vlan {
                                  members [<vlan name>, <vlan name> ..];
                            }
                      }
                }
          }
}
```

Changes from Junos OS Release 12.3 to Release 15.1: *CLI change**, port-mode** (used in Junos OS Release 12.3) is changed to **interface-mode** in Release 15.1.*

Native VLAN ID

Typically, trunk ports accept VLAN-tagged packets but do not accept untagged packets. You can enable a trunk port to accept untagged data packets by configuring a native VLAN ID on the receiving interface, as follows:

```
interfaces {
          ge-<slot number>/0/<port number> {
                native-vlan-id <NativeVLAN-ID>;
                unit 0 {
                      family ethernet-switching {
                            interface-mode trunk;
                            vlan {
                                  members [NativeVLAN-ID, <vlan name> ..];
                            }
                      }
                }
```

```
            }
}
```

For more information, see Configuring the Native VLAN Identifier.

Configuring Integrated Routing and Bridging (IRB) Interfaces

Integrated Routing and Bridging (IRB) interfaces (also known as routed VLAN interfaces, or RVIs) are used to enable inter-VLAN routing. These logical interfaces work similarly to Layer 3 interfaces and should be added to security zones. In Layer 2 transparent mode, an IRB works only for management access, while in switching mode, it works for inter-VLAN routing.

An IRB can be created under the **[interfaces]** hierarchy. After the logical interface is created, it must be associated with a particular VLAN using the **l3-interface** statement, as follows:

```
interfaces {
            irb {
                  unit <unit number> {
                        family inet {
                              address <ip address>/<netmask>;
                        }
                  }
            }
}

vlans {
            <vlan name> {
                  vlan-id <id>;
                  l3-interface irb.<unit of newly created irb interface>;
            }
 }
```

Changes from Junos OS Release 12.3 to Release 15.1: [***interfaces vlan unit***] changed to [***interfaces irb unit***]

Routed IRB interfaces are no different than any other Layer 3 interface in Junos OS and therefore require the same configuration. In particular, these interfaces have to be assigned to a security zone, and security policies have to explicitly allow traffic to be forwarded between these interfaces and any other configured Layer 3 interfaces.

Link Aggregation – LACP

Multiple links can be aggregated to form a virtual link or link aggregation group (LAG). The MAC client can treat this virtual link as a single link to increase bandwidth and availability while providing graceful degradation as failure occurs.

Specify the number of aggregated interfaces to be configured on the device using the following configuration:


```
chassis {
          aggregated-devices {
                ethernet {
                      device-count <number of AEs to be configured>;
                }
          }
}
```

Associate physical interfaces to the respective aggregated interfaces using the following configuration:

```
interfaces {
          ge-<slot number>/0/<port number> {
                ether-options {
                      802.3ad ae<0..n>;
                }
          }
          ge-<slot number>/0/<port number> {
                ether-options {
                      802.3ad ae<0..n>;
                }
          }
}
```

For aggregated Ethernet interfaces, you can configure the minimum number of links that must be up for the bundle as a whole before labeling it as down. By default, only one link needs to be up for the bundle to be labeled up.

```
interfaces {
          ae<0..n> {
                aggregated-ether-options {
                      minimum-links <number of minimum links required>;
                }
          }
}
```

Junos OS supports the Link Aggregation Control Protocol (LACP), a sub-component of 802.3ad that provides additional functionality for LAGs. LACP provides a standard mechanism for exchanging information between partner systems on a link. This exchange allows their link aggregation control instances to reach agreement on the identity of the LAG to which the link belongs, and then to move the link to that LAG. This exchange also enables the transmission and reception processes for the link to function in an orderly manner [see Understanding LACP on Standalone Devices].

Configuration Examples

Starting with Junos OS Release 15.1X49-D50, the factory default configuration comes with *global switching mode* enabled. This can be verified from using **show ethernet-switching global-information** operational command, as follows:

```
user@SRX300# run show ethernet-switching global-information
Global Configuration:
MAC aging interval      : 300
MAC learning            : Enabled
MAC statistics          : Disabled
MAC limit Count         : 16383
MAC limit hit           : Disabled
MAC packet action drop  : Disabled
LE  aging time          : 1200
LE  VLAN aging time     : 1200
Global Mode             : Switching
```

Note: Please check your product's Quick Start (How to Set Up) Guide for SRX default configurations and settings. Modification to the default settings might be required in certain scenarios.

Simple Ethernet Switching

This example details the configuration needed to use a branch SRX device as simple Layer 2 switch. The topology is illustrated in Figure 2.

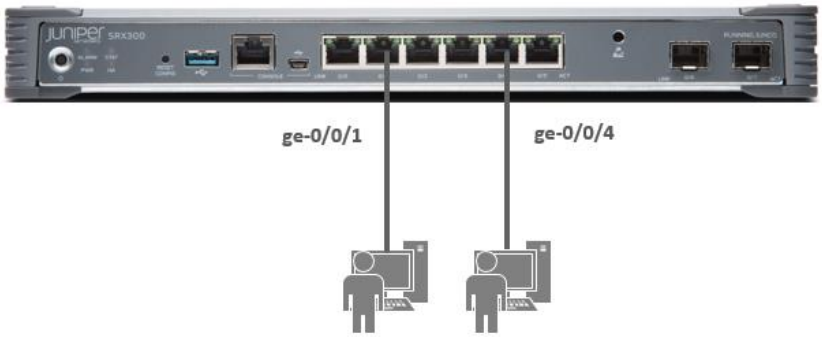

Figure 2 – Simple Ethernet Switching

Configuration

This example is enabled using the following configuration:

Interfaces:

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching
set interfaces ge-0/0/4 unit 0 family ethernet-switching
```

Verification

The following command shows the interfaces as part of the default VLAN:

```
user@SRX300# run show vlans
Routing instance        VLAN name    Tag      Interfaces
default-switch          default      1
                        ge-0/0/1.0
                        ge-0/0/4.0
```

Adding VLANs

Assuming this small branch office has two departments, SALES and OPERATIONS, add VLANs to the design in order to isolate the departments and prevent traffic from leaking between domains. This change results in a new topology, as illustrated in Figure 3.

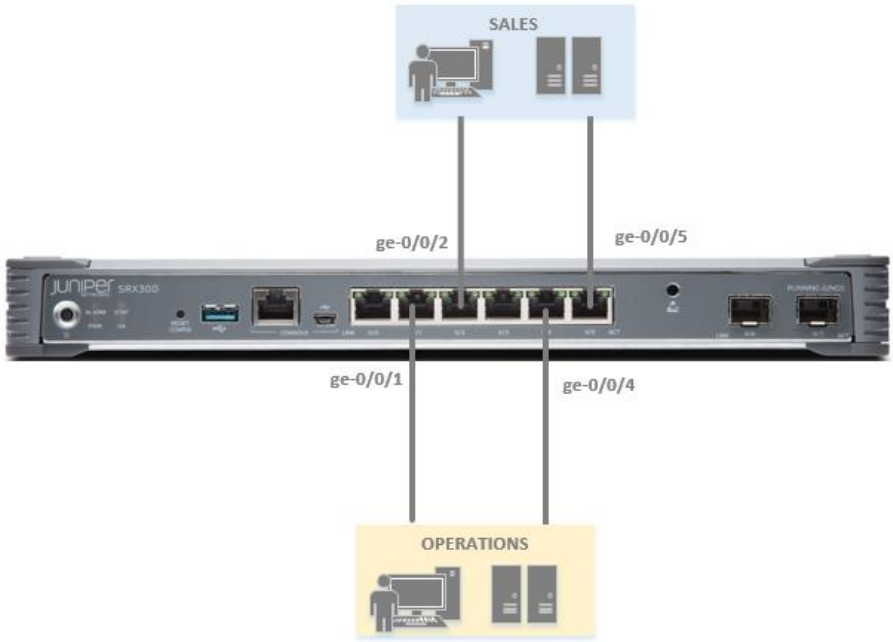

Figure 3 – Adding VLANs - Ethernet Switching

Configuration

This example is enabled using the following configuration:

VLANs

```
set vlans OPERATIONS vlan-id 20
set vlans SALES vlan-id 10
```

Interfaces

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members SALES
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members
OPERATIONS
```



```
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members SALES
```

Verification

The following command shows interface-to-VLAN associations:

```
user@SRX300# run show vlans
Routing instance      VLAN name   Tag      Interfaces
default-switch        OPERATIONS  20
                      ge-0/0/1.0
                      ge-0/0/4.0
default-switch        SALES       10
                      ge-0/0/2.0
                      ge-0/0/5.0
default-switch        default     1
```

Routing Traffic between VLANs

In this example, this small branch provides connectivity between the different business units by assigning each business unit its own Layer 3 segment. The traffic between different business units can be routed and inspected by the firewall module, where security policies can be enforced. The following configuration adds two Layer 3 interfaces, one for each VLAN, which serve as default gateways for the respective network segment. These new IRB interfaces are then added to security zones, and security policies are defined to allow traffic between the zones. In this example, two security zones – SALES and OPERATIONS – are created and HTTP traffic is allowed between them (bidirectional).

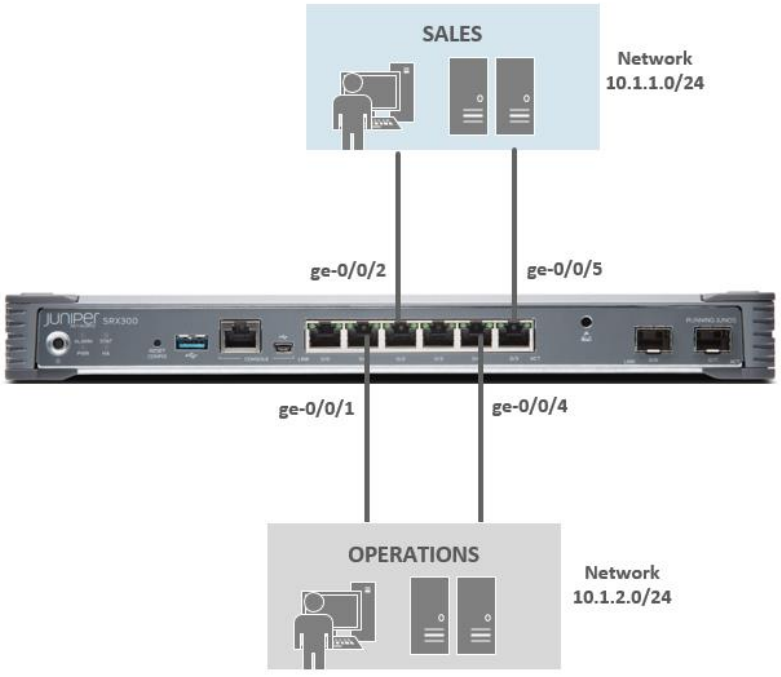

Figure 4 – IRB in Ethernet Switching

Configuration

This example is enabled using the following configuration:

VLANs

```
set vlans OPERATIONS vlan-id 20
set vlans OPERATIONS l3-interface irb.20
set vlans SALES vlan-id 10
set vlans SALES l3-interface irb.10
```

Interfaces

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members SALES
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members SALES
set interfaces irb unit 10 family inet address 10.1.1.1/24
set interfaces irb unit 20 family inet address 10.1.2.1/24
```

Security Zones

```
set security zones security-zone OPERATIONS interfaces irb.20
set security zones security-zone SALES interfaces irb.10
```

Security Policies

```
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match source-address any
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match destination-address any
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match application junos-http
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
then permit
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match source-address any
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match destination-address any
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match application junos-http
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
then permit
```

Verification

The following commands show the interface-to-VLAN associations and IRB configuration:

```
user@SRX300# run show vlans
Routing instance      VLAN name   Tag     Interfaces
default-switch        OPERATIONS  20
                      ge-0/0/1.0*
                      ge-0/0/4.0*
```



```
default-switch        SALES       10
                      ge-0/0/2.0
                      ge-0/0/5.0
default-switch        default     1

user@SRX300# run show interfaces terse irb
Interface Admin Link Proto  Local    Remote
irb       up    up
irb.10    up    up   inet   10.1.1.1/24
irb.20    up    up   inet   10.1.2.1/24
```

Adding Tagged Interface

In this example, two SRX Series devices are connected together, where SALES and OPERATIONS users belonging to one switch want to access their respective servers on another switch while keeping their VLAN domains separate. You enable VLAN communication between the two devices by configuring a trunk link, as shown in Figure 5:

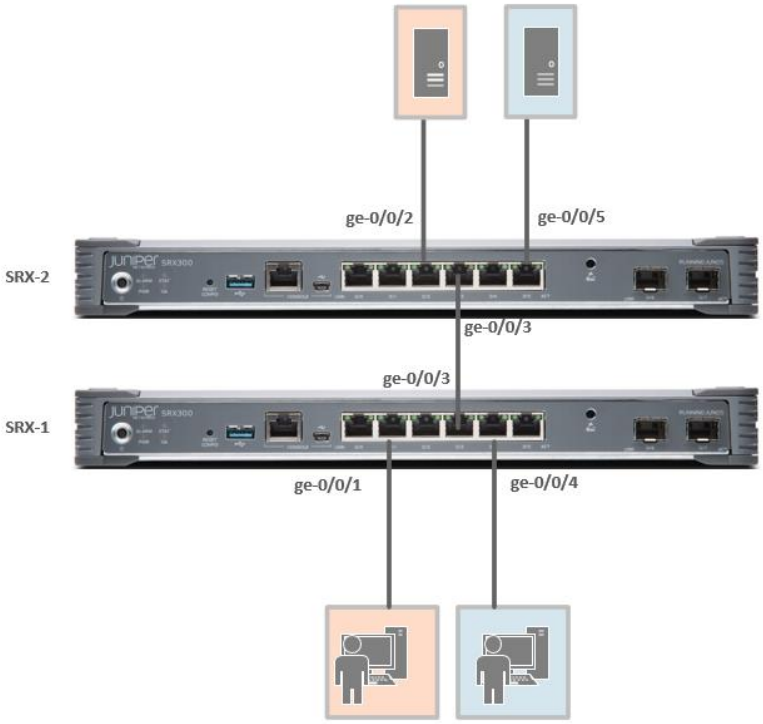

Figure 5 – Enabling VLAN Communication Between Two Devices Using a Trunk Link

Configuration – SRX1

VLANs

```
set vlans OPERATIONS vlan-id 20
set vlans SALES vlan-id 10
```

Interfaces

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/3 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members SALES
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members SALES
```

Configuration – SRX2

VLANs

```
set vlans OPERATIONS vlan-id 20
set vlans SALES vlan-id 10
```

Interfaces

```
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/3 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members SALES
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members SALES
```

Verification

The following commands show the VLAN tagging state of the interfaces:

```
user@SRX300-1# run show ethernet-switching interface brief
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown,
                         SCTL - shutdown by Storm-control )

Logical   Vlan        TAG   MAC      STP       Logical            Tagging
interface members           limit    state       interface flags
ge-0/0/1.0                  16383                                 untagged
          OPERATIONS  20    16383    Forwarding                   untagged
ge-0/0/4.0                  16383                                 untagged
          SALES       20    16383    Forwarding                   untagged
ge-0/0/3.0                  16383                                 tagged
          OPERATIONS        20 16383 Forwarding                   tagged
          SALES       10    16383    Forwarding                   tagged



user@SRX300-2# run show ethernet-switching interface brief
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown,
                         SCTL - shutdown by Storm-control )
```

```
Logical   Vlan         TAG   MAC    STP           Logical           Tagging
interface members            limit  state         interface flags
ge-0/0/2.0                   16383                                  untagged
          OPERATIONS   20    16383  Forwarding                      untagged
ge-0/0/3.0                   16383                                  tagged
          OPERATIONS   20    16383  Forwarding                      tagged
          SALES        10    16383  Forwarding                      tagged
ge-0/0/5.0                   16383                                  untagged
          SALES        10    16383  Forwarding                      untagged
```

Native VLAN ID Configuration

The **native-vlan-id** option can be added to an interface to help classify untagged packets on trunk ports.

Configuration

This example is enabled using the following configuration:

VLANs

```
set vlans TESTVLAN vlan-id 40
set vlans NATIVE vlan-id 50
```

Interfaces

```
set interfaces ge-0/0/4 native-vlan-id 50
set interfaces ge-0/0/4 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members
TESTVLAN
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members NATIVE
```

Verification

```
user@SRX300# run show ethernet-switching interface
Logical   Vlan     TAG MAC    STP      Logical    Tagging
interface members      limit  state interface flags
ge-0/0/4.0             16383                     tagged
          TESTVLAN 40  16383  Forwarding         tagged
          NATIVE   50  16383  Forwarding         untagged
```

Link Aggregation with LACP

The following example shows how to configure link aggregation using LACP.

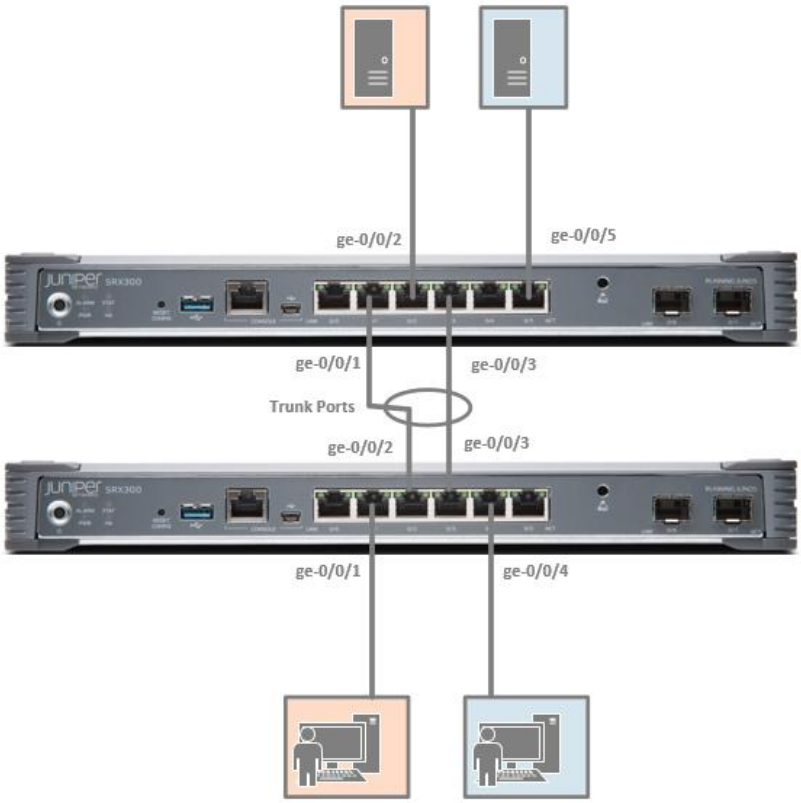

Figure 6 – Link Aggregation with LACP

Configuration – SRX1

Physical interfaces

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/2 ether-options 802.3ad ae0
set interfaces ge-0/0/3 ether-options 802.3ad ae0
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members SALES
```

Aggregated interfaces

```
set chassis aggregated-devices ethernet device-count 1
set interfaces ae0 aggregated-ether-options minimum-links 1
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members OPERATIONS
set interfaces ae0 unit 0 family ethernet-switching vlan members SALES
```

IRB Interfaces

```
set interfaces irb unit 10 family inet address 10.1.1.1/24
set interfaces irb unit 20 family inet address 10.1.2.1/24
```

VLANs

```
set vlans OPERATIONS vlan-id 20
set vlans OPERATIONS l3-interface irb.20
```



```
set vlans SALES vlan-id 10
set vlans SALES l3-interface irb.10
```

Security Zones:

```
set security zones security-zone OPERATIONS interfaces irb.20
set security zones security-zone SALES interfaces irb.10
```

Security Policies:

```
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match source-address any
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match destination-address any
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match application junos-http
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
then permit
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match source-address any
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match destination-address any
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match application junos-http
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
then permit
```

Configuration – SRX2

Physical Interfaces

```
set interfaces ge-0/0/1 ether-options 802.3ad ae0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members
OPERATIONS
set interfaces ge-0/0/3 ether-options 802.3ad ae0
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members SALES
```

Aggregated Interfaces

set chassis aggregated-devices ethernet device-count 1

```
set interfaces ae0 aggregated-ether-options minimum-links 1
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ae0 unit 0 family ethernet-switching vlan members OPERATIONS
set interfaces ae0 unit 0 family ethernet-switching vlan members SALES
```

IRB Interfaces

```
set interfaces irb unit 10 family inet address 10.1.1.1/24
set interfaces irb unit 20 family inet address 10.1.2.1/24
```

VLANs

```
set vlans OPERATIONS vlan-id 20
set vlans OPERATIONS l3-interface irb.20
set vlans SALES vlan-id 10
set vlans SALES l3-interface irb.10
```


Security Zones:

```
set security zones security-zone OPERATIONS interfaces irb.20
set security zones security-zone SALES interfaces irb.10
```

Security Policies:

```
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match source-address any
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match destination-address any
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
match application junos-http
set security policies from-zone SALES to-zone OPERATIONS policy Allow_HTTP
then permit
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match source-address any
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match destination-address any
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
match application junos-http
set security policies from-zone OPERATIONS to-zone SALES policy Allow_HTTP
then permit
```

Verification

```
user@SRX300-1# run show lacp interfaces
Aggregated interface: ae0
  LACP state:   Role  Exp   Def   Dist   Col   Syn   Aggr  Timeout
  Activity
   ge-0/0/2     Actor No    No    Yes    Yes   Yes   Yes   Fast    Active
   ge-0/0/2   Partner No    No    Yes    Yes   Yes   Yes   Fast    Active
   ge-0/0/3     Actor No    No    Yes    Yes   Yes   Yes   Fast    Active
   ge-0/0/3   Partner No    No    Yes    Yes   Yes   Yes   Fast    Active
  LACP protocol:           Receive State      Transmit State  Mux State
   ge-0/0/2    Current     Fast periodic      Collecting    distributing
   ge-0/0/3    Current     Fast periodic      Collecting    distributing

user@SRX300-2# run show lacp interfaces
Aggregated interface: ae0
  LACP state:   Role  Exp   Def   Dist   Col   Syn   Aggr  Timeout
  Activity
   ge-0/0/1     Actor No    No    Yes    Yes   Yes   Yes   Fast    Active
   ge-0/0/1   Partner No    No    Yes    Yes   Yes   Yes   Fast    Active
   ge-0/0/3     Actor No    No    Yes    Yes   Yes   Yes   Fast    Active
   ge-0/0/3   Partner No    No    Yes    Yes   Yes   Yes   Fast    Active
  LACP protocol:           Receive State      Transmit State  Mux State
   ge-0/0/1    Current     Fast periodic      Collecting    distributing
   ge-0/0/3    Current     Fast periodic      Collecting    distributing
```


Configuring DHCP Server

The following example shows how to configure DHCP Server (JDHCP) using an IRB interface, and assumes a user is connected to an SRX300 device on port ge-0/0/1.

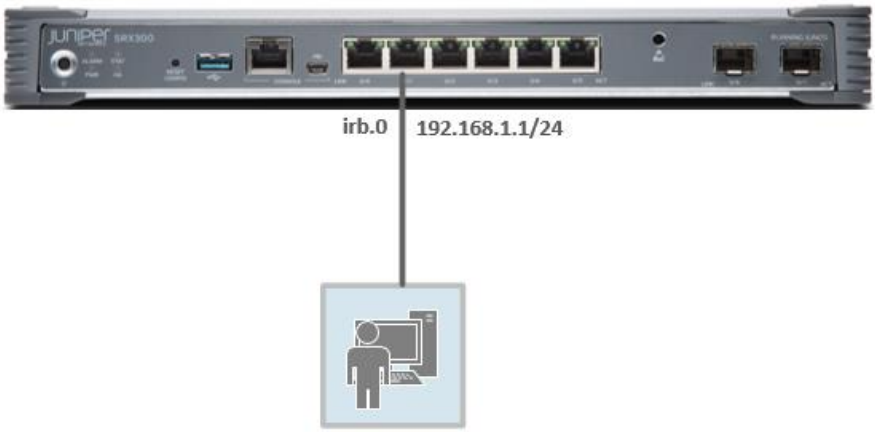

Figure 7 – Configuring DHCP

A DHCP server group has to be configured and the interface should be assigned to a DHCP group. In addition, Security zones and interfaces should be configured.

Configuration

This example is enabled using the following configuration:

Physical

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members vlan-trust
```

IRB

```
set interfaces irb unit 0 family inet address 192.168.1.1/24
```

VLAN

```
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface irb.0
```

DHCP Server

```
set system services dhcp-local-server group DHCP-Group interface irb.0
```

DHCP address pool has to be configured with IP range and network information.

```
set access address-assignment pool DHCP_Pool family inet network
192.168.1.0/24
set access address-assignment pool DHCP_Pool family inet range DCHP_Range low
192.168.1.10
set access address-assignment pool DHCP_Pool family inet range DCHP_Range
high 192.168.1.100
set access address-assignment pool DHCP_Pool family inet dhcp-attributes
router 192.168.1.1
```

```
set access address-assignment pool DHCP_Pool family inet dhcp-attributes
name-server 8.8.8.8
```

Verification

```
user@SRX300# run show dhcp server binding
IP address     Session Id  Hardware address  Expires      State  Interface
192.168.1.10      1        00:00:5e:00:53:c1 86390          BOUND   irb.0

user@SRX300# run show dhcp server statistics
Packets dropped:
    Total 0

Messages received:
    BOOTREQUEST   2
    DHCPDECLINE   0
    DHCPDISCOVER      1
    DHCPINFORM    0
    DHCPRELEASE   0
    DHCPREQUEST   1
    DHCPLEASEQUERY          0
    DHCPBULKLEASEQUERY      0

Messages sent:
    BOOTREPLY         2
    DHCPOFFER         1
    DHCPACK       1
    DHCPNAK       0
    DHCPFORCERENEW          0
    DHCPLEASEUNASSIGNED     0
    DHCPLEASEUNKNOWN  0
    DHCPLEASEACTIVE         0
    DHCPLEASEQUERYDONE      0
```

Appendix

Transparent Mode

Transparent mode is a bump-in-wire firewall deployment in which an SRX device acts as a Layer 2 switch providing the security functionality of a stateful firewall, as well as providing additional services, such as IPS, AppSecure, and UTM. Transparent mode can co-exist with routed mode and is called *mixed* mode. This means that SRX Series branch devices can have Layer 2 interfaces and Layer 3 interfaces simultaneously.

In transparent mode, the SRX series devices filter packets that traverse the device without modifying any of the source or destination information in the IP packet header. Under transparent mode, the device does not route Layer 3 traffic. Layer 2 interfaces are configured to be a part of security zones and security policies are applied to it. In this way, various security features can be applied to the traffic. For more details, see L2 Switching and Transparent Mode for Security.

To enable transparent mode, use the following command:

```
set protocols l2-learning global-mode transparent-bridge
```

When to Use Transparent Mode

Typically, scenarios in which Layer 3 implementation of a firewall is not ideal or needs to be avoided entirely, transparent mode can be used. Ideally, you would use transparent mode when there is a need to comply with security standards, such as PCI, HIPAA, etc., and integrating a Layer 3 firewall would involve making IP changes. To prevent this, an SRX device can be deployed in transparent mode, where it provides the security functionality of a firewall without any change to the existing IP infrastructure.

Secure-Wire

While in transparent mode, with the SRX Series devices deployed in Layer 2, you can also provide security by just using Layer 1 connectivity. Traffic arriving on a specific interface can be forwarded unchanged through another interface. These two interfaces can be mapped to form a *secure-wire* deployment. When the traffic passes through the device, it does not require any change in the routing tables or reconfiguration of neighboring devices. Interfaces are added to a security zone and security policies are applied. No routing or switching decision needs to be made on the packet.

Secure-wire is a special case of transparent mode and is best suited when SRX device deployment needs to be transparent to Layer 2 protocol PDUs without compromising security.

Secure-wire is configured under the **[edit security forwarding-options]** hierarchy. Similar to transparent mode, security features that use routing, such as NAT and IPsec VPN, are not supported in Secure-wire deployments, in which features such as AppSecure, IPS, and UTM are supported.

For more information, refer L2 Switching and Transparent Mode for Security.

DHCP Configuration on SRX3XX, SRX550M and SRX1500

Starting with Junos OS Release 15.1X49-D60, the DHCP process (**dhcpd**) is replaced with a new advanced DHCP process known as JDHCP (**jdhcpd**) as the factory default. The new version has been available on the existing SRX1xx and SRX2xx devices since Junos OS Release 11.4 and is also the default DHCP process in EX Series and MX Series platforms.

Please note that the CLI configuration has changed. The examples below show the new way of configuring DHCP on SRX Series devices. Starting with Junos OS Release 15.1X49-D60, legacy DHCP CLI commands will be hidden. (Please refer D60 release notes for details).

Define the DHCP server group and assign the interface to it:

```
services {
          dhcp-local-server {
                group <group name> {
                interface <interface>;
          }
}
```

Define the DHCP pool with network and the IP list:

```
access {
          address-assignment {
                pool <pool name> {
                      family inet {
                            network <network>/<mask>;
                            range <name of the range> {
                                  low <start IP>;
                                  high <end IP>;
                            }
                            dhcp-attributes {
                                  router {
                                    <router IP>;
                                  }
                                  propagate-settings <interface>;
                            }
                      }
                }
          }
}
```