

Ethernet Switching Configuration Guide

SRX Series (SRX3xx, SRX550M, SRX1500)

RAHUL RAMACHANDRAN

Table of Contents

Introduction.....	3
Scope	3
Hardware Scope	3
Software Scope.....	3
Feature and Capabilities	4
Supported Features	4
Limitations	4
Summary of Changes (CLI)	5
Life of Packet in Ethernet Switching	7
Ethernet Switching Deployment Scenarios	7
Enabling Ethernet Switching on New SRX Branch Series.....	7
Configuring Layer 2 Switching	8
Configuring VLAN	8
Attaching Switch Ports to VLANs.....	8
Extending Broadcast Domains and Configuring Tagged Interfaces.....	9
Native VLAN-ID.....	10
Configuring Integrated Routing and Bridging (IRB) Interface	10
Link Aggregating – LACP.....	11
Configuration Examples	12
Simple Ethernet Switching	12
Troubleshooting	13
Adding VLANs.....	13
Troubleshooting	13
Routing Traffic between VLANs.....	13
Troubleshooting	15
Adding Tagged Interface.....	15
Troubleshooting	16
Native-VLAN-ID Configuration	17
Troubleshooting	17
Link Aggregation with LACP	18
Troubleshooting	19
Configuring DHCP (JDHCPD) Using IRB	20
Troubleshooting	21
Appendix	22
Transparent Mode.....	22
When to User Transparent Mode.....	22

Secure-Wire	22
DHCP Configuration on SRX3XX, SRX550M and SRX1500	22
Table 1 – Physical Interface support on SRX devices	3
Table 2 – Software support scope on SRX devices	4
Table 3 – Summary of CLI Changes on SRX devices	6
Table 4 – Number of VLANs supported on SRX devices	8
Figure 1 - Life of Packet in Ethernet Switching	7
Figure 2 – Simple Ethernet Switching	12
Figure 3 – Adding VLANs - Ethernet Switching	13
Figure 4 – IRB in Ethernet Switching	14
Figure 5 – Life of Packet in Ethernet Switching	16
Figure 6 – Link Aggregation with LACP	18
Figure 7 – Configuring DHCP	20

Introduction

Juniper Networks SRX Series Services Gateways for the branch enables an enterprise to provide services without boundaries. Ethernet Switching feature eliminates the need for L2 switches in branch offices.

Juniper Networks Junos operating system Release 15.1 for SRX Branch Series introduces changes in Ethernet Switching features. Changes are mainly in the CLI configuration of L2 features on SRX Branch Series. This application note is targeted to capture all relevant information regarding these changes. It describes common deployment scenarios with detailed configurations and examples.

Scope

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

Please refer SRX technical documentation for Ethernet Switching features in SRX Chassis Cluster environment.

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
SRX550 (HM)	6	4	2	6*
SRX1500	12	4x1GE + 4x 10GE	2	x

Table 1 – Physical Interface support on SRX devices

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

All interfaces will have support for Ethernet Switching starting 15.1X49-D50 release. [\[Release Notes\]](#)

Software Scope

SRX Branch Series devices, support two modes, Transparent Mode and Switching Mode. Table, describes the matrix of current support on these modes as of Junos release 15.1X49-D50.

Scenarios	Global Mode	
	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 devices

Ethernet switching on the SRX Branch Series is based on Juniper Networks EX Series Ethernet Switches which follows ELS style configuration.

Feature and Capabilities

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 port
- Intra-VLAN and Integrated Routing and Bridging (IRB) for Inter-VLAN traffic
- Link Aggregation using Link Aggregation Control Protocol (LACP)

Limitations

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

- IEEE 802.1x authentication
- Link Layer Discovery Protocol (LLDP), LLDP-MED
- 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)

	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]unit 0 { family ethernet-switching { vlan members <vid-list> port-mode trunk/access; }	[edit interfaces]unit 0 { family bridge { vlan-id <vid> vlan-id-list <vid-list> }	[edit interfaces]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] { ether-options gigheter-options }	[edit interfaces] { ether-options gigheter-options }	[edit interfaces] { ether-options }
	[edit vlans] <name> { I3-interface vlan.x }	[edit bridge-domain] <bd-name> { routing-interface <ifl-name> }	[edit vlans] <name> { 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 devices

Life of Packet in Ethernet Switching

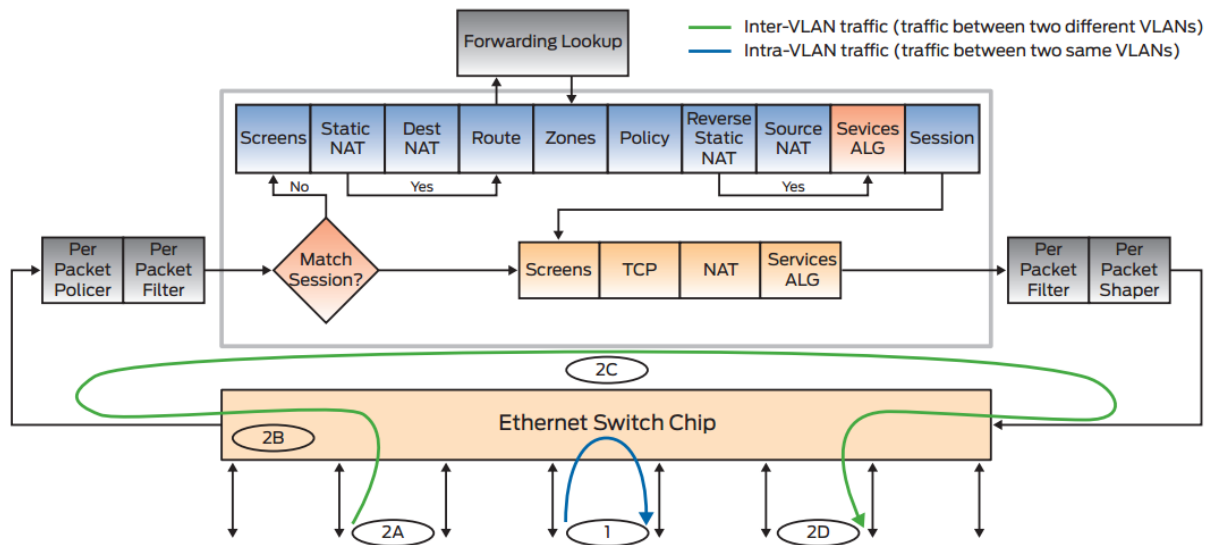


Figure 1 – Life of Packet in Ethernet Switching

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 at the L2 hardware. Packets in the same VLAN are switched internally at the L2 Ethernet switch. Since packets does not traverse through 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 are 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 further sends out the traffic

Changes between Release 12 and 15.1: *Inter-VLAN IRB interfaces on 15.1 would be **irb.x** while legacy 12 or older had **vlan.x**.*

Ethernet Switching Deployment Scenarios

Enabling Ethernet Switching on New SRX Branch Series

From Junos OS Release 15.1X49-D50, SRX Branch series have global switching enabled. The factory default configuration would include the following configuration:

“set protocols l2-learning global-mode switching”

The above configuration can be used to enable and disable Ethernet Switching on the SRX Branch Series. This includes both L2 switching as well as IRB based routing.

The default behavior, when the above configuration is not present is ‘Transparent Mode’. Enabling and disabling ‘switching mode’ requires a system reboot.

Configuring Layer 2 Switching

The following configuration defines an interfaces as a switching port.

```

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

```

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 Release 12 and 15.1: None

Configuring VLAN

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 a 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
SRX550 (HM)	3967
SRX1500	3900

Table 4 – Number of VLANs supported on SRX devices

Note: On SRX3xx, SRX5xx and SRX1500, the VLAN IDs 3968 – 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.

```

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.

```

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

```

Changes from 12.3 to 15.1: None

Extending Broadcast Domains and Configuring Tagged Interfaces

VLAN tagging (IEEE 802.1q) provides this functionality by extending the Ethernet header with a VLAN identifier (a 12-bit value) used to differentiate traffic from different VLANs. To configure a switch port as an access port, following configurations can be used.

```

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 stated below,

```

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

```

```

    }
  }
}

```

Trunk ports can be defined as a part of multiple VLANs which allows a switching port to be associated with more than one VLAN. Traffic forwarded from a trunk port is tagged using the VLAN ID of the originating VLAN, while received traffic is forwarded to the appropriate VLAN for distribution.

Changes from 12 to 15.1: CLI change, **port-mode** (used on 12) is changed to **interface-mode** on 15.1.

Native VLAN-ID

'native-vlan-id' can be added to the interface trunk configuration to classify untagged packets.

```

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, please refer [VLAN-Tagging on SRX](#)

Configuring Integrated Routing and Bridging (IRB) Interface

Integrated Routing and Bridging (IRB) interface can be configured to enable inter-vlan routing. These logical interfaces work similar to any Layer 3 interfaces and should be added to Security Zones. In L2TM, IRB works only for Management access, while in Switching mode, it works for inter-vlan routing.

A logical Layer 3 interface or routed VLAN interface can be created under the [interfaces] hierarchy. After the logical interface is created, it must be associated with a particular VLAN using 'l3-interface' keyword.

```

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 12 to 15.1: [*interfaces vlan unit*] to [*interface irb unit*]

Routed IRB interfaces are no different than any other L3 interfaces in Junos OS and thus requires 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 Aggregating – 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>;
        }
    }
}

```

Next step is to configure the link speed for each aggregated interfaces using the following configuration,

To increase availability of the links, minimum number of links that are required to be fault-free can be configured to label the aggregated interface as UP or DOWN. For example, if an aggregated interface has 4 links and if only 1 link is needed to keep the aggregated interface UP and process traffic, the number of minimum links required to keep the AE UP is 1.

```

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, provides additional functionalities 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 [[Understanding LACP](#)].

Configuration Examples

From 15.1X49-D50, factory default configuration comes with 'Global Switching Mode' enabled. This can be verified from using "show ethernet-switching global-information"

```
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 the Quick Start Guide for SRX default configurations and settings. Modification to the default setting might be required on 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.

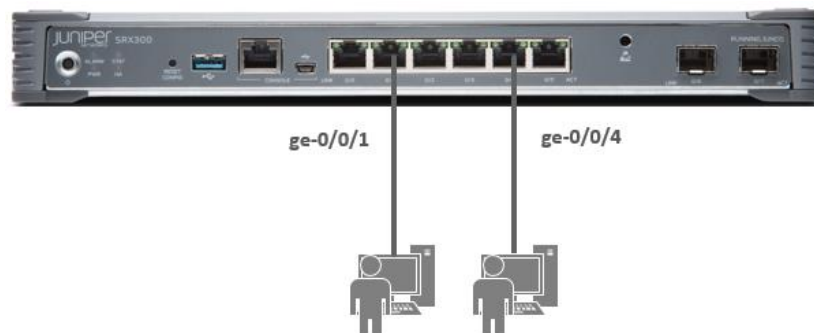


Figure 2 – Simple Ethernet Switching

Troubleshooting

```

root@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, to isolate the departments and prevent traffic from leaking between domains, VLANs are added to the design, resulting in a new topology, as illustrated in Figure 3.

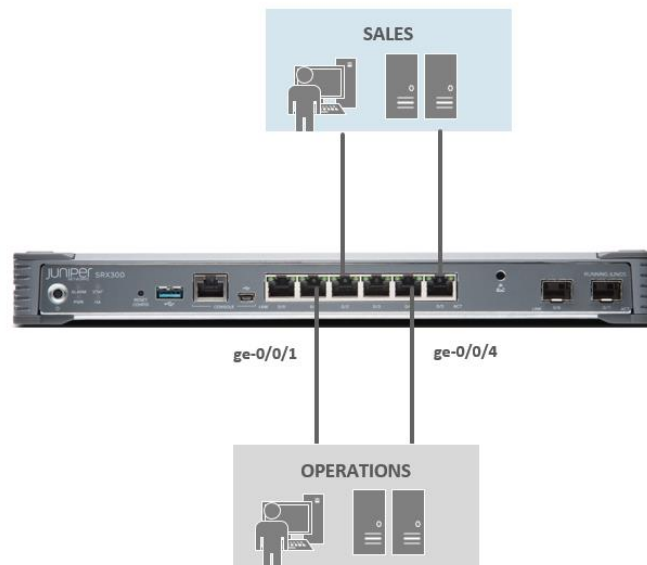


Figure 3 – Adding VLANs - Ethernet Switching

Troubleshooting

The following command shows interfaces and VLAN association:

```

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     ge-0/0/1.0
                                     ge-0/0/4.0
  
```

Routing Traffic between VLANs

In this example, this small branch is assumed to provide connectivity between the different business units controlled 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).

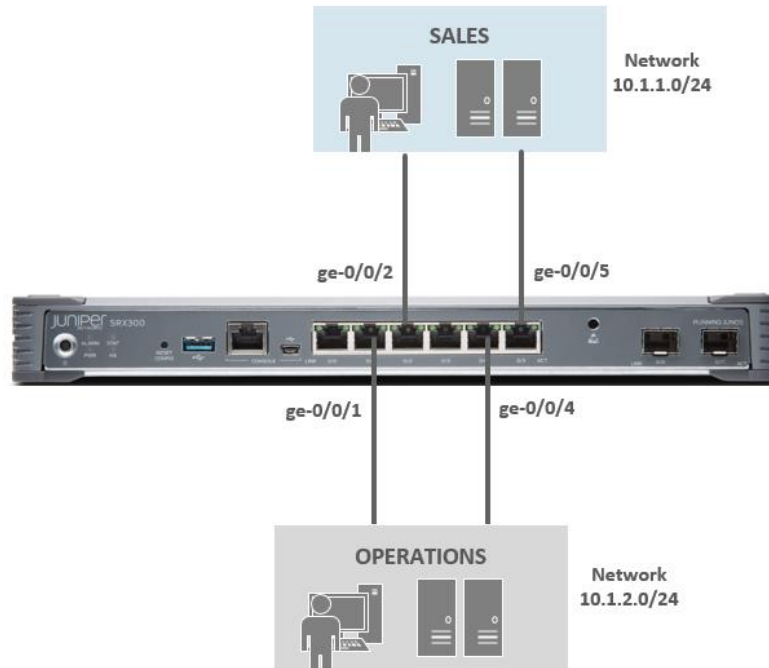


Figure 4 – IRB in Ethernet Switching

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
    
```

Troubleshooting

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 in another switch, keeping their VLAN domain separately as show in the Figure. To enable VLAN communication between the two devices, a 'trunk' link is configured between the two.

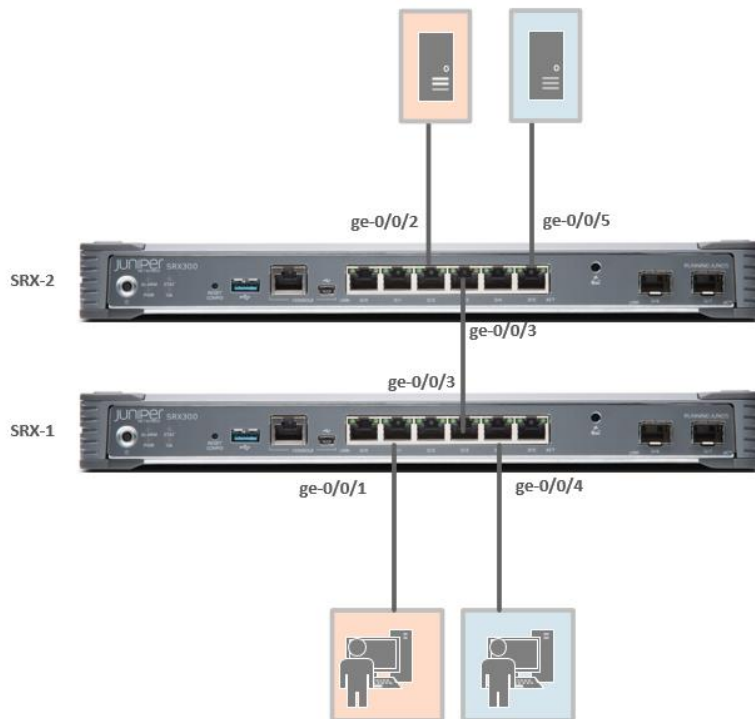


Figure 5 – Life of Packet in Ethernet Switching

SRX1 – Configuration

VLANS:

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

Interface:

```
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
```

SRX2 – Configuration

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
```

Troubleshooting

SRX1: “show ethernet-switching interface brief”

```
user@SRX300# 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 interface	Vlan members	TAG limit	MAC	STP state	Logical interface flags	Tagging
ge-0/0/1.0	OPERATIONS	20	16383	Forwarding		untagged
ge-0/0/4.0	SALES	20	16383	Forwarding		untagged
ge-0/0/3.0			16383			tagged
	OPERATIONS	20	16383	Forwarding		tagged
	SALES	10	16383	Forwarding		tagged

SRX2: “show ethernet-switching interface brief”

```
user@SRX300-2# run show ethernet-switching interface
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 interface	Vlan members	TAG	MAC limit	STP state	Logical interface flags	Tagging
ge-0/0/2.0			16383			untagged
ge-0/0/3.0	OPERATIONS	20	16383	Forwarding		untagged
	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

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

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

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

```
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
```

Troubleshooting

```
user@SRX300# run show ethernet-switching interface
```

Logical interface	Vlan members	TAG	MAC limit	STP state	Logical interface flags	Tagging
ge-0/0/4.0			16383			tagged
	TESTVLAN	40	16383	Forwarding		tagged
	NATIVE	50	16383	Forwarding		untagged

Link Aggregation with LACP

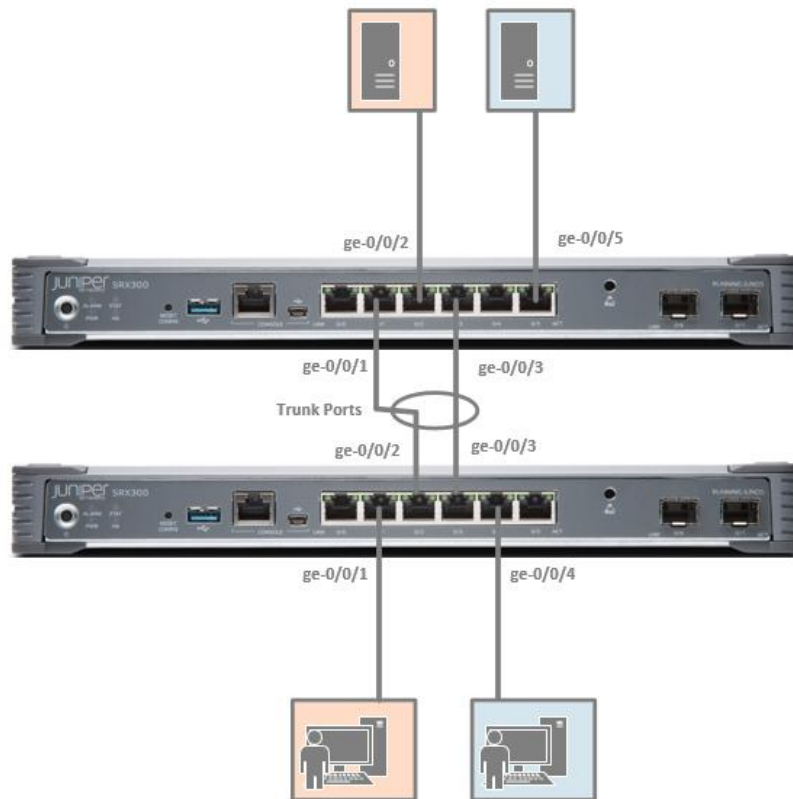


Figure 6 – Link Aggregation with LACP

SRX1 - Configuration

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
```

Aggregate interface

```
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 I3-interface irb.20
set vlans SALES vlan-id 10
set vlans SALES I3-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
```

SRX2 – Configuration**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 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
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 I3-interface irb.20
set vlans SALES vlan-id 10
set vlans SALES I3-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
```

Troubleshooting

```
user@SRX300# 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 (JDHCPD) Using IRB

Assuming a user is connected to a SRX300 on port ge-0/0/1.

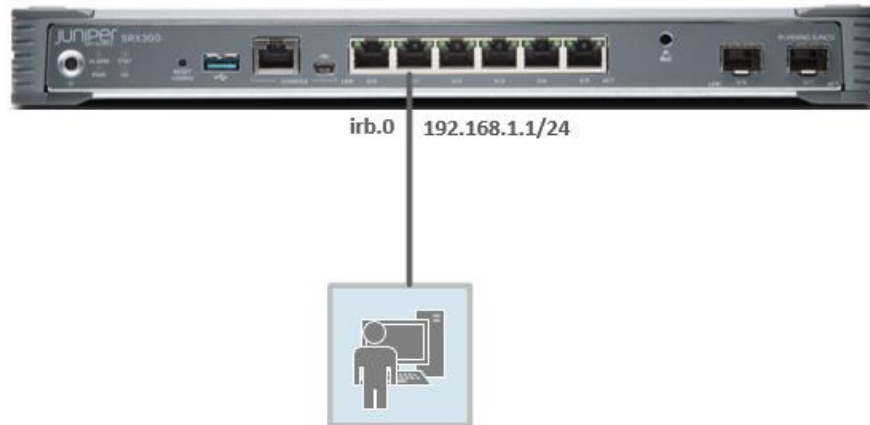


Figure 7 – Configuring DHCP

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.

Configure physical

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

Configure IRB

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

Configure VLAN

```
set vlans vlan-trust vlan-id 3
```

```
set vlans vlan-trust I3-interface irb.0
```

Configure 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
```

Troubleshooting

DHCP Server Binding:

```
user@SRX300# run show dhcp server binding
```

IP address	Session Id	Hardware address	Expires	State	Interface
192.168.1.10	1	0c:86:10:10:83:c1	86390	BOUND	irb.0

DHCP Server Statistics:

```
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 where, SRX acts as a L2 switch providing security functionality of being a Stateful firewall, as well as providing additional services like IPS and AppSecure and UTM. Transparent mode can co-exist with routed mode and is called Mixed Mode. This means SRX branch series can have L2 interfaces and L3 interfaces simultaneously.

In transparent mode, the SRX series devices filters 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 through. Layer 2 interfaces are configured as a part of Security Zones and Security Policies are applied to it. Thus various security features can be applied to the traffic. More details please refer to [L2 Switching and Transparent Mode for security](#).

“set protocols l2-learning global-mode transparent-bridge”

When to User Transparent Mode

Typically, scenarios where Layer 3 implementation of a firewall is not ideal or if needs to be avoided, Transparent Mode can be used. Ideally, when there is a need for security standard compliance such as PCI, HIPAA, etc., and integrating a Layer 3 firewall would involve making IP changes. To prevent this, a SRX device can be deployed in a Transparent mode, where it provides the security functionalities of a firewall without any change to the existing IP infrastructure.

Please refer to [L2 Switching and Transparent Mode for security](#)<http://chimera.labs.oreilly.com/books/1234000001633/ch06.html> for more details.

Secure-Wire

While in Transparent mode, the SRX series devices are deployed on Layer 2, it is also possible to provide security by just using Layer 1 connectivity. Traffic arriving on 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 security zone and security policies are applied. There is no routing or switching decision made on the packet.

Secure-wires is a special case of Transparent mode and is best suited when SRX device deployment need to be transparent to L2 protocol PDUs without compromising security.

Secure-wire can be configured under [edit security forwarding-options] hierarchy. Similar to Transparent mode, security features which uses routing, like NAT, IPsec VPN are not supported in Secure-wire deployment, which features like AppSecure, IPS and UTM are supported.

For more information please refer [L2 Switching and Transparent Mode for security](#).

DHCP Configuration on SRX3XX, SRX550M and SRX1500

Starting from the 15.1X49-D60 the DHCP process (DHCPD) is replaced with a new advance DHCP process known as JDHCP (JDHCPD) as a factory default. The new version has been available on the existing SRX1XX, SRX2XX since Junos 11.4 and is also the default DHCP process in EX, MX platforms.

Please note that the configuration on the CLI have changed. Below listed is the new way of configuring DHCP on a SRX Series device. Starting 15.1X49-D60, legacy DHCP CLI commands will be hidden.

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>;
        }
      }
    }
  }
}
```