# Table of Contents

- Introduction ........................................................................................................ 4
- Scope ..................................................................................................................... 4
- Design Considerations .......................................................................................... 4
  - Control Plane ..................................................................................................... 4
    - Control Link Failure and Recovery ................................................................. 4
  - Data Plane .......................................................................................................... 5
    - Data Link Failure and Recovery .................................................................... 5
- Protocol Operation .................................................................................................. 5
  - Dedicated Node Interfaces ............................................................................... 5
  - Redundant Ethernet Interfaces ......................................................................... 5
  - Redundancy Groups ........................................................................................... 6
  - Interface Monitoring .......................................................................................... 6
  - IP Address Monitoring ....................................................................................... 6
- Implementation ....................................................................................................... 6
  - Implementation Environment .............................................................................. 6
    - Physical Topology .......................................................................................... 7
  - Enabling the Chassis Cluster .............................................................................. 7
    - Physical Connectivity ..................................................................................... 7
    - Configure Cluster and Node ID ..................................................................... 7
    - Configure Node-Specific Settings .................................................................. 8
    - Define Redundancy Groups ............................................................................ 8
    - Configure Redundant Ethernet Interfaces ..................................................... 8
    - Configure Interface Monitoring Thresholds .................................................. 8
  - Security Configuration ......................................................................................... 8
    - IPsec Configuration ....................................................................................... 8
    - Assign Security Zones ..................................................................................... 9
    - Security Policies .............................................................................................. 9
- Implementation Validation ...................................................................................... 10
  - Cluster Monitoring ............................................................................................ 10
  - Cluster Status .................................................................................................... 10
  - Cluster Statistics ................................................................................................ 10
  - Cluster Interfaces ................................................................................................ 10
  - Failure Validation ............................................................................................... 11
    - Monitored Interface Link Failure ................................................................. 11
    - Manual Failover ............................................................................................. 11
    - Power Failure .................................................................................................. 11
- Summary ............................................................................................................... 12
- About Juniper Networks ......................................................................................... 12
Table of Figures
Figure 1: Physical topology implementing SRX Series active/passive HA ................................................. 7

List of Tables
Table 1: Dedicated and Required Ethernet Interfaces for Chassis Clustering ................................................. 5
Table 2: Ethernet Interface Renumbering Per Cluster Node ........................................................................ 5
Table 3: Hardware and Software List for This Implementation ................................................................. 6
Introduction

Juniper Networks® SRX Series Services Gateways for the branch deliver essential enterprise networking security features to branch and remote offices. As network connectivity to both corporate offices and data centers is critical for business applications and operations, high availability (HA) is often a requirement that is achieved with device level redundancy. Device level redundancy for the branch SRX Series can be implemented by enabling the chassis cluster feature that is also known as Juniper Networks Junos® OS Services Redundancy Protocol (JSRP).

The chassis cluster implements an active/backup device pair, where the backup device takes over traffic forwarding if the active device happens to fail. When a chassis cluster failover occurs, traffic continues to be forwarded on the newly active device. While there may be some packet loss during the transition, session states are maintained so that applications can continue to function without interruption.

Scope

This document provides a guide for implementing the branch SRX Series chassis cluster feature, while reviewing design considerations for the solution. Chassis clustering on the high-end SRX Series platforms is outside the scope of this document (details can be found in the Junos OS Security Configuration Guide). While IPsec is implemented as part of the solution, security concepts such as policies, intrusion prevention system (IPS), and unified threat management (UTM) are not covered in this document.

This document is intended for network design and security engineers, as well as implementation partners supporting customers requiring secure branch office connectivity.

Design Considerations

Branch SRX Series chassis clustering supports a grouping of two Juniper Networks SRX Series Services Gateways for the branch of the same model in a cluster. The branch SRX Series platforms consist of Juniper Networks SRX100 Services Gateway, SRX210 Services Gateway, SRX240 Services Gateway, and SRX650 Services Gateway. Chassis clustering for these branch SRX Series platforms is supported in Junos OS 9.6 and later.

The cluster consists of a primary node and a secondary standby node. These nodes back each other up in the event of software or hardware failures. Failover between nodes is stateful to ensure that established sessions are not dropped during the transition. The two nodes synchronize configuration, processes, and services across two Ethernet links—the control link forming the control plane and the fabric link forming the data plane.

Control Plane

The control link connected between the two nodes form a control plane that synchronizes configuration and system processes to ensure high availability of the interfaces and services. The control plane software:

- Runs the Routing Engine on the entire chassis cluster as well as the interfaces on both nodes
- Manages system resources including the Packet Forwarding Engine (PFE) on either node
- Establishes and maintains sessions as well as node management traffic
- Controls Address Resolution Protocol (ARP) processing

Control Link Failure and Recovery

The health of the control plane is monitored by heartbeats sent across the control link. These are sent at configured intervals and a failure is determined when lost heartbeats exceed a configured threshold value.

If the control link fails, the secondary standby node is disabled to prevent it from becoming active. By default, a disabled secondary device must be rebooted to recover the control link. Control link recovery can be configured to automatically reboot a disabled node to restore the control link.
Data Plane

The connection over the fabric ports forms a data plane which manages traffic flow processing and session redundancy between the two nodes. Session or flow redundancy is synchronized between the nodes by special packets called runtime objects (RTOs) across the fabric data link.

Types of RTOs include:
- Session creation RTOs for the first packet
- Session deletion and age out RTOs
- IPsec security associations (SAs)
- Change-related RTOs for timeout synchronization and TCP state changes

Data Link Failure and Recovery

Because the data link maintains session synchronization, it is vital to the chassis cluster. Junos OS sends fabric probes to determine data link failure events. On link failure, the secondary node is disabled and must be rebooted to recover. On completing reboot, the node synchronizes session states with RTOs from the primary node.

Protocol Operation

Dedicated Node Interfaces

Branch SRX Series platforms do not have dedicated ports for node management, control link, or fabric link. Therefore, the onboard Ethernet interfaces are used and renamed after clustering is enabled. Management (FXP0) and control link ports (FXP1) are predefined, but the fabric link port must be configured. The following table identifies the port conventions by model number.

| Table 1: Dedicated and Required Ethernet Interfaces for Chassis Clustering |
|-----------------|-----------------|-----------------|-----------------|
| **SRX SERIES PLATFORM** | **MANAGEMENT (FXP0)** | **CONTROL LINK PORT (FXP1)** | **DATA LINK (FABI)** |
| SRX100 | fe-0/0/6 | fe-0/0/7 | Any other port |
| SRX210 | fe-0/0/6 | fe-0/0/7 | Any other port |
| SRX240 | ge-0/0/0 | ge-0/0/1 | Any other port |
| SRX650 | ge-0/0/0 | ge-0/0/1 | Any other port |

A chassis cluster has a single configuration that encompasses both nodes of the cluster. As a result, the node interfaces are renumbered to allow configuration of specific node interfaces. Renumbering is dependent on the number of expansion slots per model and is determined using the following formula:

\[\text{Cluster slot number} = (\text{node ID} \times \text{maximum slots per node model}) + \text{local slot number}\]

The following table provides examples for each SRX Series platform.

| Table 2: Ethernet Interface Renumbering Per Cluster Node |
|-----------------|-----------------|-----------------|-----------------|-----------------|
| **SRX SERIES PLATFORM** | **ONBOARD PORTS** | **EXPANSION SLOTS** | **NODE 0 INTERFACES** | **NODE 1 INTERFACES** |
| SRX100 | fe-0/0/x | None | fe-0/0/y | fe-1/0/y |
| SRX210 | fe-0/0/x | 1 | fe-0/0/y | fe-2/0/y |
| SRX240 | ge-0/0/x | 4 | ge-0/0/y | ge-5/0/y |
| SRX650 | ge-0/0/x | 8 | ge-0/0/y | ge-9/0/y |

Redundant Ethernet Interfaces

A redundant Ethernet interface (RETh) is a virtual Ethernet interface configured from two Ethernet interfaces in the cluster (one from each node). The RETh interfaces share a common IP address and media access control (MAC) address between the two physical interfaces on either node. RETh interfaces are required to be the same type of physical Ethernet interface (fe-fe or ge-ge).
Redundancy Groups

Redundancy groups are the concept in chassis clusters that defines which nodes are active or passive. A redundancy group is active on one node and backup on the other node. The redundancy group has a priority configured with the higher priority becoming active.

The following factors determine whether a redundancy group is primary:

1. The priority configured for the node
2. The node ID which is a factor in case the priorities are tied
3. The order in which the nodes come up
4. Node preemption configuration

A lower priority node that boots up before a higher priority node claims primary node status. Node preemption can be configured to force one node’s primacy once both nodes are booted up.

A chassis cluster can have multiple redundancy groups configured (from 1 to 128) in addition to the default redundancy group 0. Redundancy group 0 is always defined for the control plane which controls the Routing Engine. For an active/passive chassis cluster, there is a redundancy group 1 defined for the data plane.

Each redundancy group can failover independently and can be primary on only one node at a time. Each redundancy group (besides redundancy group 0) can be assigned one or more RETH interfaces whose state determines which node is primary for that redundancy group.

Interface Monitoring

Redundancy group failover is triggered by monitoring the state of the interfaces that belong to the redundancy group. Each RETH interface is assigned to a redundancy group. Each physical interface is assigned a weight which is monitored by the system. If the physical interface fails, its corresponding weight is deducted from the redundancy group threshold which is set at 255. Failover is triggered when the redundancy group threshold hits 0.

IP Address Monitoring

IP address monitoring (Track IP) is not available in Junos OS 9.6 for the branch SRX Series platforms, although it is available for the high-end SRX Series platforms. A workaround for this limitation is to use Junos OS operational/event scripts to monitor IP address reachability; however, this workaround is outside the scope of this document.

Implementation

Implementation Environment

The table below shows the hardware and software used for this implementation

<table>
<thead>
<tr>
<th>EQUIPMENT</th>
<th>COMPONENTS</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 x SRX Series Services Gateways</td>
<td>SRX240</td>
<td>Junos OS 9.61</td>
</tr>
<tr>
<td>1 x SRX Series Services Gateway</td>
<td>SRX5600</td>
<td>Junos OS 9.61</td>
</tr>
<tr>
<td>4 x Juniper Networks EX Series Ethernet Switches</td>
<td>EX4200</td>
<td>Junos OS 9.6</td>
</tr>
</tbody>
</table>
Physical Topology

![Physical Topology Diagram]

Enabling the Chassis Cluster

Physical Connectivity

Prior to any configuration on the SRX Series devices, cluster nodes must be physically connected to enable the control link and data link. Table 1 details the ports to be used to ensure proper setup of the FXP and Fab interfaces.

Configure Cluster and Node ID

To enable clustering on each of the SRX240 devices, log in and set the following command in management mode, not in config mode:

```
set chassis cluster cluster-id <n> node <m> reboot
```

This command will cause a reboot of each device. If more than one cluster on a single Layer 3 broadcast domain is clustered, make sure that each cluster has a unique cluster-id. Failure to do this will cause a MAC address conflict.

On node SRX240-0:

```
root@SRX240-0> set chassis cluster cluster-id 1 node 0 reboot
```

On node SRX240-1:

```
root@SRX240-1> set chassis cluster cluster-id 1 node 1 reboot
```

**Note**: This command must be entered in management mode, not in config mode.

After reboot, all subsequent configurations are done in config mode on node 0.
Configure Node-Specific Settings

The system host name FXP0 (management) IP settings are node-specific settings.

set groups node0 system host-name SRX240-0
set groups node0 interfaces fxp0 unit 0 family inet address 172.19.59.220/24
set groups node0 system backup-router 172.19.59.1 destination 0.0.0.0/0
set groups node0 system host-name SRX240-1
set groups node1 interfaces fxp0 unit 0 family inet address 172.19.59.221/24
set groups node1 system backup-router 172.19.59.1 destination 0.0.0.0/0

set apply-groups "${node}"

Configure the fabric data link port. As node 1’s interfaces are renumbered, refer to Table 2 for the renumbered interface.

set interfaces fab0 fabric-options member-interfaces ge-0/0/2
set interfaces fab1 fabric-options member-interfaces ge-5/0/2

Define Redundancy Groups

For this solution, define the two RETH interfaces for the cluster. Define redundancy group 1 and give node 0 higher priority. The preempt statement allows for a node with a higher priority to become the primary in a redundancy group.

set chassis cluster reth-count 2
set chassis cluster node 0
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 99
set chassis cluster redundancy-group 1 preempt
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 99

Configure Redundant Ethernet Interfaces

set interfaces ge-0/0/5 gigether-options redundant-parent reth0
set interfaces ge-0/0/6 gigether-options redundant-parent reth1
set interfaces ge-5/0/5 gigether-options redundant-parent reth0
set interfaces ge-5/0/6 gigether-options redundant-parent reth1
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 10.10.1.20/24
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 40.10.1.20/24
set routing-options static route 172.0.0.0/8 next-hop 172.19.59.1

Configure Interface Monitoring Thresholds

set chassis cluster redundancy-group 1 interface-monitor ge-0/0/5 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/6 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-5/0/6 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-5/0/5 weight 255
set chassis cluster control-link-recovery

Security Configuration

IPsec Configuration

set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.30.1.1/30
set security ike policy preshared mode main
set security ike policy preshared proposal-set standard
set security ike policy preshared pre-shared-key ascii-text "$9$w22oZHqfn/tUj/tu0C5wYg"
set security ike gateway SRX5600 ike-policy preshared
set security ike gateway SRX5600 address 10.10.1.40
set security ike gateway SRX5600 external-interface reth0.0
set security ipsec policy std proposal-set standard
set security ipsec vpn SRX5600 bind-interface st0.0
set security ipsec vpn SRX5600 ike gateway SRX5600
set security ipsec vpn SRX5600 ike ipsec-policy std
set security ipsec vpn SRX5600 establish-tunnels immediately

**Assign Security Zones**

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces reth0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces reth1.0
set security zones security-zone vpn host-inbound-traffic system-services all
set security zones security-zone vpn host-inbound-traffic protocols all
set security-zones security-zone vpn interfaces st0.0

**Security Policies**

set security policies from-zone trust to-zone trust policy default-permit match source-address any
set security policies from-zone trust to-zone trust policy default-permit match destination-address any
set security policies from-zone trust to-zone trust policy default-permit match application any
set security policies from-zone trust to-zone untrust policy default-permit match source-address any
set security policies from-zone trust to-zone untrust policy default-permit match destination-address any
set security policies from-zone trust to-zone untrust policy default-permit match application any
set security policies from-zone trust to-zone untrust policy default-permit then permit
set security policies from-zone untrust to-zone trust policy default-deny match source-address any
set security policies from-zone untrust to-zone trust policy default-deny match destination-address any
set security policies from-zone untrust to-zone trust policy default-deny match application any
set security policies from-zone untrust to-zone trust policy default-deny then deny
set security policies from-zone trust to-zone vpn policy any match source-address any
set security policies from-zone trust to-zone vpn policy any match destination-address any
set security policies from-zone trust to-zone vpn policy any match application any
set security policies from-zone trust to-zone vpn policy any then permit
Implementation Validation

Cluster Monitoring

Cluster Status

The chassis cluster status can be validated with the following command:

```
root@SRX240-0> show chassis cluster status
Cluster ID: 1
Node name                  Priority     Status    Preempt  Manual failover
Redundancy group: 0 , Failover count: 1
node0                   100         primary   no       no
node1                   99          secondary no       no
Redundancy group: 1 , Failover count: 1
node0                   100         primary   yes      no
node1                   99          secondary yes      no
```

The heartbeats for the control link and RTO probes for the fabric link can be validated using the “show chassis cluster statistics” command. Statistics are not synchronized between the member nodes, so it can be useful to collect this information from each member.

Cluster Statistics

```
root@SRX240-0> show chassis cluster statistics
Control link statistics:
    Heartbeat packets sent: 442445
    Heartbeat packets received: 439810
Fabric link statistics:
    Probes sent: 442441
    Probes received: 439087
Services Synchronized:
    Service name                              RTOs sent    RTOs received
    Translation context                       0            0
    Incoming NAT                              0            0
    Resource manager                          0            0
    Session create                            2335            105356
    Session close                             2331            102990
    Session change                            0            0
```

Cluster Interfaces

Cluster interfaces can be verified with the “show chassis cluster interfaces” command, which displays the control link between the nodes and information about the RETH interfaces and monitored interfaces.

```
root@SRX240-0> show chassis cluster interfaces
Control link name: fxp1
Redundant-ethernet Information:
    Name         Status      Redundancy-group
    reth0        Up          1
    reth1        Up          1
Interface Monitoring:
    Interface     Weight  Status Redundancy-group
    ge-5/0/5      255       Up    1
    ge-5/0/6      255       Up    1
    ge-0/0/6      255       Up    1
    ge-0/0/5      255       Up    1
```
Failure Validation

Monitored Interface Link Failure

Link failure was simulated on a monitored interface by disconnecting a cable. Interface status shows:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Weight</th>
<th>Status</th>
<th>Redundancy-group</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-5/0/5</td>
<td>255</td>
<td>Up</td>
<td>1</td>
</tr>
<tr>
<td>ge-5/0/6</td>
<td>255</td>
<td>Up</td>
<td>1</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>255</td>
<td>Up</td>
<td>1</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>255</td>
<td>Down</td>
<td>1</td>
</tr>
</tbody>
</table>

Redundancy Group 1 failed over to the standby node within 30 seconds:

```
root@SRX240-0> show chassis cluster status
Cluster ID: 1

Node name                  Priority     Status    Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
    node0                   100         primary   no       no
    node1                   99          secondary no       no

Redundancy group: 1 , Failover count: 2
    node0                   0           secondary no       no
    node1                   99          primary   no       no
```

With preempt off, interface failure on node0 causes failover of redundancy group 1 to node1. If the interface recovers on node0, node1 remains primary as preemption is turned off.

With preempt on, interface failure on node0 causes failover of redundancy group 1 to node1. If the interface recovers on node0, node0 recovers as primary. The preempt setting gives priority to node0.

Manual Failover

If node0 is manually rebooted from the command-line interface (CLI), node1 detects that both control plane and data plane connections have failed and node1 becomes primary. After completing reboot, node0 becomes secondary. If preempt is enabled, node0 subsequently becomes primary.

A failover can be triggered by command to force the standby to become active with the command “Manual reboot of node0 (primary)”:  

```
root@SRX240-0> request chassis cluster failover redundancy-group 0 node 1
```

After issuing a manual failover, the reset failover command must be issued before requesting another failover.

Power Failure

On power outage of the primary node, the secondary node takes over both RG 0 and RG 1. Cluster status shows the former primary as lost. When node1 recovers (former primary), its status is “hold” initially. Once proper RTOs and synchronization occur, it becomes secondary.

```
(node:node1)
root@SRX240-1> show chassis cluster status
Cluster ID: 1

Node name                  Priority    Status    Preempt  Manual failover

Redundancy group: 0 , Failover count: 1
    node0                   0           lost      n/a      n/a
    node1                   100         primary   no       no

Redundancy group: 1 , Failover count: 1
    node0                   0           lost      n/a      n/a
    node1                   100         primary   no       no
```

( primary:node1)
Summary

Juniper Networks SRX Series Services Gateways for the branch provide a cost-effective, network security enabling, remote connectivity solution to corporate offices. The chassis clustering features allow for device level redundancy to protect the network against software and hardware failures.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.