SBC SWe Cloud Port Redundancy and Link Detection

In this section:

Related articles:

- SBC Core Redundancy
- Link Detection Group - Link Monitor - EMA
- Link Detection Group - CLI
- Admin - CLI
- Enabling Geographical Redundancy HA Mode

Feature Overview

The SBC SWe Cloud currently supports a maximum of two packet (PKT) ports such as PKT0 and PKT1. If these PKT ports are virtual interfaces (ports from a virtual Standard Switch (vSS) or virtual Distributed Switch (vDS) on VMware ESXi or ports from OVS on a KVM platform), port redundancy is supported through the NIC teaming or bonding feature, which exists on the respective hypervisor vSwitches.

However, if these PKT ports are SR-IOV interfaces, port redundancy cannot be managed the same way for the PKT interfaces since the hypervisor is by-passed in such a NIC configuration. To support port redundancy on SR-IOV interfaces on the SBC SWe cloud platform, the process works based on an ICMP/ARP probing mechanism. This mechanism requires four PKT ports (SR-IOV VFs) configured on a SWe instance, where each of these SR-IOV VFs may come from different physical NICs for better handling of connectivity failures due to physical NIC or physical link connected towards different physical switches.

The PKT ports are automatically configured in active-standby mode to provide port redundancy on an active SWe instance. The PKT ports connected on a standby SWe instance remain in standby mode. The ICMPv4/v6 probing mechanism is used on active PKT ports, while ARP ACD/ICMPv6 NUD mechanism is used on standby ports.

Note
The port redundancy feature applies to the following SBC platforms only:

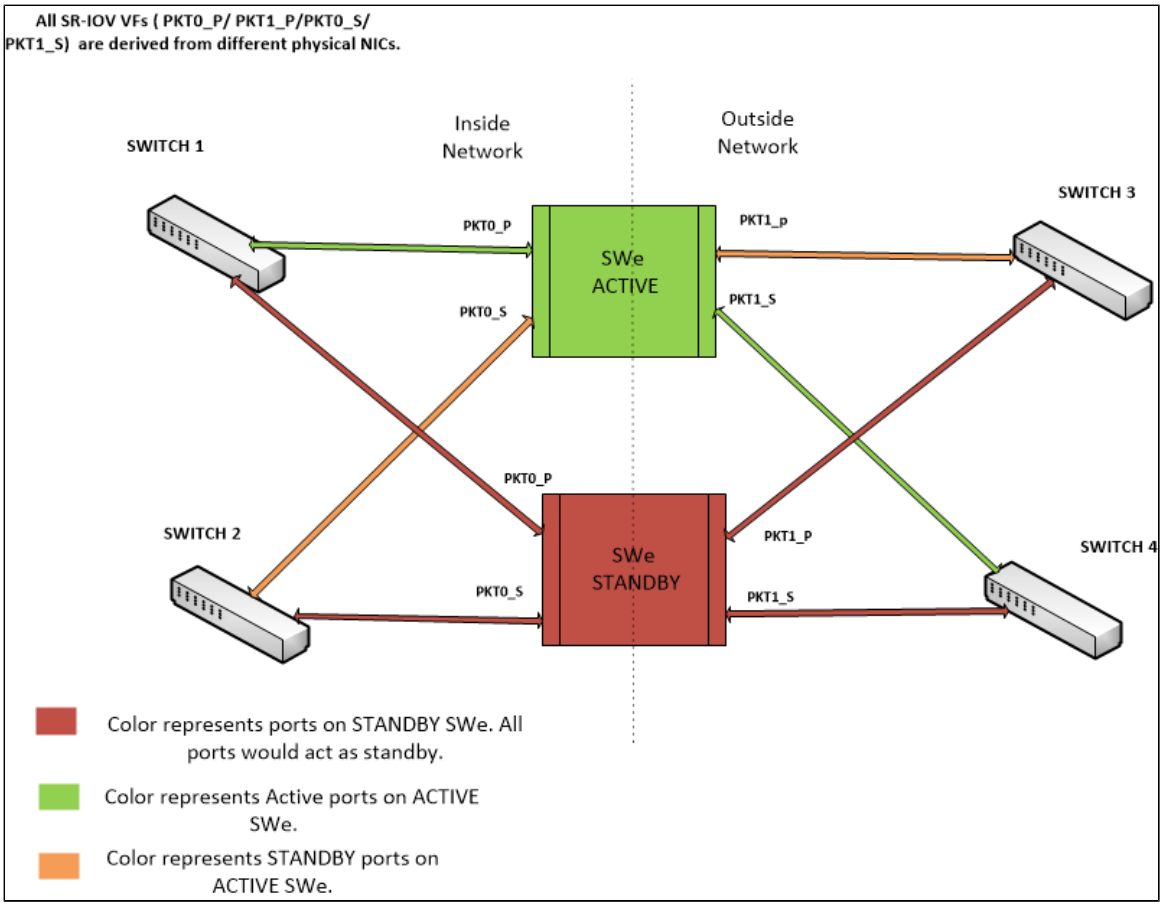
- Distributed SBCs on an OpenStack platform
- SBC 7000 models (Refer to SBC Core Redundancy)

Architecture

If an SBC SWe deployment includes four packet ports, it can be configured for port redundancy in which each active port is backed up by a standby port. To enable packet port redundancy, four packet ports must be attached to the SBC SWe instance when it is instantiated. Within the Link Monitor object that is configured for each port (part of Link Detection Group (LDG) configuration), ensure that the Physical Port (`physicalPort <portname>`) configuration is completed and that the Probe On Standby (`probeOnStandby enabled`) option is enabled. This configuration enables port redundancy through regular monitoring of the link state of standby ports using the ARP/ICMPv6 NUD probing mechanism.

The following figure shows the SBC SWe Cloud redundancy model from a port-centric view using a secondary packet port for each primary packet port. A standby SWe with its own primary and secondary packet ports is also depicted in this figure. On the standby SWe, all packet ports remain as standby. For example, in this diagram, the active SWe ports are PKT0_P and PKT1_S ports.

Figure 1: Port Redundancy Architecture



- **Primary port:** The PKT port that attempts to become active on an active SWe node. The packet ports on the SBC SWe (PKT0_P, PKT1_P) are considered as primary ports.
- **Secondary port:** The PKT port is designated as an alternative for a specific on-board primary port. The SBC SWe contains one secondary port for each primary port.
- **Active port:** The PKT port that is currently selected for use (For example, signaling, media); either a primary or a secondary port on an active SWe node.

> **Note**
> A PKT port's role (primary/secondary) is independent of the port's state (active/standby). A port in the active state does not necessarily imply it is "up".

- **Local standby port:** A standby PKT port on an active SWe node provides redundancy protection to the currently active port.
- **Standby port:** A collective term for a local standby PKT port on an active SWe node or any packet port on an standby SWe node. Standby ports provides protection for active PKT ports.
- **Enabled or Disabled ports:** The PKT port may be administratively enabled or disabled. A PKT port that is disabled cannot be an active port.

> **Note**
> For the SBC SWe Cloud platform, the Out of Service (OOS) `sonusSbxNrsIpInterfaceOOSNotification` alarm for an Interface Group is generated only for logical ports pkt0 and pkt1. This alarm is not generated when physical ports (pkt0P, pkt0S, pkt1P and pkt1S) are down.

Link Detection Support

The SBC SWe Cloud supports two levels of link detection for both standby and active ethernet ports to monitor the health of the ports and to ensure the health of a standby port before initiating a switchover to it. By default, physical link detection is enabled on all ports configured in Link Monitor. This mechanism checks for the presence of the cable and that the adjacent device is powered on. If hardware failures are detected they are reported to the SBC processes that monitor ports and a switchover can be triggered if the standby port is available.

A second level of link detection can be enabled that checks connectivity between a port and and a configured destination. The specific mechanism used to check the port depends on the whether the port is in an active or standby state. These probing mechanisms for link detection are available regardless of the number of ports attached to the SWe instance and are summarized in the following table.

The following probing mechanisms are available on the SBC platforms:

Table 1: SBC Probing Mechanism Types

Probing Mechanism	SBC Platforms	Affected Ports	Purpose
Physical link detection	SBC SWe Cloud Platform	All ports (active and standby CEs)	Detects the presence of the port cable and that the adjacent device is powered on (enabled by default on all physical ports configured by Link Monitor except for any ports administratively disabled or set to out-of-service).
ICMP ping	SBC SWe	Active ports only	Checks two-way connectivity between SBC port and the configured destination (adjacent router) by sending ICMP Ping messages at configured intervals to the destination. **NOTE**: When destination IP address is configured in a Link Monitor, ICMP ping is enabled. By setting the destination IP address to NULL (0.0.0.0), the ICMP ping is disabled.
ARP ACD/ICMPv6 NUD*	SBC SWe Cloud Platform	Standby ports only	Performs active checking of two-way traffic through at least the local Ethernet interface, the cable, and the adjacent layer 2 switching function. Checks are accomplished using ARP (for IPv4) or Neighbor Discovery (for IPv6) mechanisms to probe an arbitrary, operator-specified target IP address on a local IP subnet, typically an address of a router (Gateway IP address). Depending on the address family (IPv4/IPv6) of the gateway IP address configured, either ARP ACD or ICMPv6 NUD probing messages are sent in such a way that explicit assignments of IP addresses to the standby ports are not required. Checks the link state between SBC port and the adjacent router. For SWe cloud deployments with 4 packet ports, the flag "ProbeOnStandby" is provided and enabled by default. ARP probe monitoring of the standby ports is enabled when "ProbeOnStandby" is enabled. For SWe deployments with 2 packet ports, the flag "ProbeOnStandbySWe" is provided and disabled by default. ARP probe monitoring of the standby port is enabled when "ProbeOnStandbySWe" is enabled.

* Address Resolution Protocol - Address Conflict Detection / Internet Control Message Protocol Version 6 – Neighbor Unreachability Detection

ARP ACD/ICMPv6 NUD Methods for Standby Ports

IPv4 ARP ACD

If the destination address configured is an IPv4 address, then IPv4 probing is initiated by sending an ARP Probe requests and listening for the responses.

ARP request probes are sent with:

- **Sender IP address** of 0.0.0.0. The use of 0.0.0.0 is compatible with rfc 5227 on IPv4 Address Conflict Detection. This is convenient to use on standby ports since IP addresses are not assigned for standby ports.
- **Sender hardware address** containing the current local MAC address assigned to the sending port.

- **Target IP address** containing the configured target IP address to be probed.
- **Target hardware address** containing all zeros. The ARP request is sent on the LAN using L2 broadcast.

The target can be expected to respond with an ARP Response using L2 unicast.

IPv6 ICMPv6 NUD

If the destination address configured is an IPv6 address, then IPv6 probing would be initiated using Neighbor Unreachability Detection mechanism (RFC 4861 section 7). This is based on Neighbor Solicitation and Neighbor Advertisement ICMPv6 messages.

Because these are IP packets, the SBC needs IP addresses to send/receive them. The SBC uses auto-generated link local IPv6 address from the current local MAC address.

Neighbor Solicitation messages are sent with:

- **IP source address** containing auto-generated link local IP address
- **IP destination address** containing configured target IP address
- **ICMP layer target address** containing configured target IP address
- **ICMP layer source link layer address** containing PKT port MAC address

The Neighbor Solicitation message is sent on the LAN via L2 unicast to the system with the target IP address.

The target can be expected to respond with a Neighbor Advertisement using L2 unicast. Received messages are validated per RFC 4861 section 7.1.2: Check that the S bit = 1 (solicited) and that the target address = our configured target IP address.

> **Note**
> The SBC SWe Cloud may reduce the call accept rate when it syncs from the active to the standby CE under full load causing some calls to get rejected with a 503 message even though the applied load is below the specified maximum call rate. This condition clears once the synchronization to the standby completes. Additionally, some calls may get rejected with a 503 message when synchronization occurs while the applied load is near the maximum specified.