

Cisco StackWise Virtual



Q What is StackWise Virtual technology?

A Cisco® StackWise® Virtual technology is next-generation and evolutionary StackWise technology. It enables unified system virtualization by expanding highly proven and industry-leading Cisco StackWise technology for mission-critical enterprise networks.

Q What is the difference between StackWise-480 and StackWise Virtual?

A The existing StackWise technology greatly simplifies the access or distribution layer using high-speed back-panel StackWise ports and cables. The new StackWise Virtual extends switch stack function over the network ports and cables. This solution offers new design potential to virtualize networking devices much beyond a single rack unit space.

Q What are the benefits of new StackWise Virtual technology?

A The next-generation distributed stacking mode delivers common benefits of stacking at the network level instead of the individual system level:

- Simple: Virtualize two redundant Cisco Catalyst® switches as single logical entity in network topologies and from an operation perspective.
- Reliable: Builds a unified control plane with Stateful Switchover (SSO) technology for nonstop business communication.
- Scalable: Fully distributed forwarding architecture increases overall network bandwidth, resulting in improved user experience.
- Manageable: Single management plane to operate as a single entity and integrated with Cisco APIC-EM and Cisco Prime® Infrastructure management applications.

Q How does StackWise Virtual support high availability mechanisms?

A StackWise Virtual supports a 1+1 HA redundancy model using Cisco SSO and Nonstop Forwarding (NSF) technologies.

Q Which StackWise Virtual node handles all control and management plane protocols?

A The stack member with SSO active in the current role centrally manages all network control and management plane protocols. The Layer 2 and Layer 3 protocol states are synchronized with the HOT_STANDBY stack member switch.

Q How does StackWise Virtual synchronize the forwarding plane between both stack members in a domain?

A The SSO active switch builds Layer 2 and Layer 3 forwarding topologies based on various protocols. The SSO active programs local and peer stack member switch hardware to enable the distributed forwarding plane in the StackWise Virtual domain.

Q Can I directly connect one pair of a StackWise Virtual domain to another domain?

A Yes. Each domain is a separate logical entity, and each domain represents one logical Layer 2 or Layer 3 system in the network.

Q How does new StackWise Virtual technology compare to Cisco 6K/4K VSS technology?

A The initial phase of StackWise Virtual capabilities offers consistent capabilities as a Cisco Catalyst 6K/4K VSS solution. However, the StackWise Virtual technology is a new innovation that is extended based on traditional stacking technology. It enables several new network design potentials, and with a combination of Cisco UADP ASIC technology and the next-generation Cisco IOS-XE Software operating system, it enables several new advanced technologies such as programmability, application visibility, Multiprotocol Label Switching (MPLS), and much more.

Q Does StackWise Virtual support the SSO role preemption feature?

A No. The SSO role selection is determined during the initial bootup process of both switches. If the SSO active switch is already in an operational state, then the other stack member will boot up in the HOT_STANDBY switch independent of its switch ID, priority, or MAC address parameters.

Q What are Cisco recommended best practices in building StackWise Virtual domain configuration?

A Following are recommended Cisco StackWise Virtual best practices:

- StackWise Virtual domain ID: Use any range from 1 through 255. No conflict in network.
- Switch ID: Supported range is 1 through 9. Renumber if needed to start in ascending number.
- Switch priority: Default is 1. Recommended to increase priority for specific stack member if prefer to boot up in ACTIVE role.
- Stack MAC address: Default is infinite. Recommended to keep default settings.

Q What is the StackWise Virtual Link (SVL)?

A The SVL is a special interchassis system link between two stack members in a StackWise Virtual domain. It enables extending stack fabric communication over network ports to virtualize the system. The SVL connections do not run any network protocol and remain transparent in Layer 2 and Layer 3 network topologies.

Q What interface types are supported to build SVL connections?

A The SVL connections between two stack members can be built with 40G or 10G interfaces.

Q Do I need to configure SVL EtherChannel?

A No. SVL EtherChannel configuration is automatic when the user configures the interface. The port channel 128 ID is reserved for SVL configurations.

Q Does SVL EtherChannel support Cisco PAgP or LACP?

A No. Each SVL link will be statically bundled into system generated EtherChannel.

Q What is the SVL communication mechanism for both stack member switches?

A All interchassis system control communication between stack members is encapsulated over a special 64-byte StackWise Virtual Header (SVH). This communication is carried over reserved VLAN ID 4094 from the global range.

Q Can I build SVL connections using a 1G interface?

A No.

Q What maximum interface counts are supported in SVL connections?

A Cisco IOS-XE Software Release 16.3.3 supports up to four SVL interfaces.

Q How do I identify the maximum number of SVL connections I need?

A The SVL capacity planning must include the following factors:

- Total uplink bandwidth per stack member switch to handle data reroute during uplink failures without network congestion.
- Handling egress data to single-homed devices (non recommended design).
- Remote network services such as SPAN.

Q What happens when a single or all member links of an SVL connection fail?

A During individual SVL link failure, the system virtualization and network topologies remain intact. When all SVL links between stack members fail, that failure induces a dual active condition in the network that might disrupt network communication.

Q How does the dual active detection and recovery mechanism work?

A The dual active fast hello is a lightweight protocol that operates on a dedicated interface between two stack member switches of a StackWise Virtual domain. If the SSO active switch receives a fast hello message after losing all SVL connections, it detects dual active failure and enters recovery-mode by disabling all network connection ports to minimize disruption.

Q What interface types are supported for fast hello configurations?

A Any 1G/10G/40G interface can be used to configure fast hello.

Q How many maximum fast hello links are supported by StackWise Virtual?

A Cisco StackWise Virtual supports up to four directly connected fast hello links.

Q What are the current feature restrictions on SVL interfaces?

A Following are the SVL interface restrictions for Cisco IOS-XE Software Release 16.3.3:

- Maximum SVL interface is restricted to four. Up to eight interfaces will be supported in future software releases.
- The 10G SVL interfaces must be in port range 45 to 48. In future software releases, any 10G/40G port can be selected for SVL connections.

- Enhanced PAgP for dual active detection will be supported in future software releases.
- In dual active condition, after the SVL connections are fully restored, the user must manually reload the recovery mode stack member switch to join back to the StackWise Virtual domain.
- After StackWise Virtual conversion, any addition to or removal from SVL or fast hello connection will require both stack members to reload to make the configuration effective.

Q Can an SVL connection be bridged or routed across L2/L3 networks?

A No. The SVL connection is encapsulated over a special SVH that cannot be bridged or routed by any intermediate switch or router.

Q What are SVL best practices and recommendations?

A Following are recommended Cisco SVL best practices:

- Make sure SVL connections are built based on recommended capacity planning.
- Minimum of two SVL connections are recommended for better redundancy and load sharing.
- Diversify 10G SVL connections across different port ASICs to protect against any internal soft failure conditions.

Q What hardware and software matrix is required to deploy StackWise Virtual?

A Cisco StackWise Virtual is supported on the hardware and software version shown in Table 1.

Table 1. Cisco StackWise Virtual Support Matrix

Hardware	Software
Cisco Catalyst 3850-48-XS Series	16.3.3

Q What Cisco IOS Software license is required to deploy StackWise Virtual?

A StackWise Virtual requires an IP Base or IP Services Cisco IOS Software license.

Q Does StackWise Virtual support mixed Cisco Catalyst products in a single domain?

A No. Both the stack members in a StackWise Virtual domain must be the same model.

Q Where can I deploy Cisco StackWise Virtual technology?

A StackWise Virtual can be deployed in the distribution or core layer. Deploying it in the access layer is not recommended unless all connecting devices are dual homed to both stack members in the StackWise Virtual domain.

Q What optics are supported to build SVL connections?

A The Cisco Catalyst 3850 deployed in StackWise Virtual supports the same optics as in standalone or StackWise-480 mode. For an up-to-date supported optics matrix, visit http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html.

Q Does StackWise Virtual support IPv6 and its relevant technology?

A Yes.

Q How does StackWise Virtual derive its unique MAC address between two stack members?

A The stack MAC is derived from the base MAC address pool of the SSO active switch. This MAC address is used on all the interfaces.

Q Does the MAC address change if the SSO active switch fails?

A No. By default, the stack MAC timer is set to infinite. Hence, the original MAC address pool is retained even if the original SSO active switch fails.

Q What is the recommended StackWise Virtual deployment model in a campus or branch office network?

A StackWise Virtual can be deployed as a distribution layer system or a collapsed core/distribution layer in enterprise campus and branch networks.

Q What L2/L3 network connection design does StackWise Virtual support?

A StackWise Virtual supports Layer 2 trunk or host mode configurations. The Layer 3 networks can have an equal cost multipath (ECMP) or multichassis EtherChannel (MEC) design to the core.

Q What is MEC?

A MEC shares the same fundamentals as industry-standard EtherChannel technology. The primary difference is that the member links of MEC are physically distributed across multiple physical chassis. By using system virtualization technology such as StackWise Virtual, the distributed physical interfaces can be bundled up into single logical connections to simplify network topologies and operations.

Q What is the maximum number of MECs supported by StackWise Virtual?

A Cisco StackWise Virtual supports a maximum of 128 MECs combined Layer 2 or Layer 3 modes. EtherChannel 128 is reserved for SVL connections. Hence, the maximum available MEC count is 127.

Q How many MEC modes and maximum member links are supported by StackWise Virtual?

A Cisco StackWise Virtual supports the modes with maximum counts shown in Table 2.

Table 2. Cisco StackWise Virtual MEC Support

Mode	Maximum Member Links	Standby Support
Cisco PAgP	8	No
IEEE LACP	16 (8 active and 8 standby)	Yes
Static (on)	8	No

Q What is the recommended EtherChannel mode in Cisco StackWise Virtual?

A Cisco recommends implementing the link bundling protocol using PAgP (desirable/desirable) or LACP (active/active) modes. Use static mode as a last resort if peering devices do not support.

Q How many methods of EtherChannel load sharing are supported?

A StackWise Virtual supports up to 13 different load-sharing permutations. Each permutation ranges from Layer 2 to Layer 4, providing a granular data-forwarding algorithm across each available member link of the L2/L3 MEC.

Q How can I optimally load share egress traffic in an ECMP network design?

A In a Layer 3 ECMP network topology, the egress data load sharing can be optimized with advanced Cisco Express Forwarding configuration that includes source and destination Layer 4 ports across each stack member in a StackWise Virtual domain.

- Q** Does Cisco Express Forwarding automatically optimize the load share IPv6 egress traffic in ECMP network design?
- A** No. IPv4 and IPv6 Cisco Express Forwarding load sharing must be explicitly defined to load share the ECMP traffic across each stack member switch in a StackWise Virtual domain.
- Q** Does StackWise Virtual supports connecting single-homed network devices to one of the stack members in a StackWise Virtual domain?
- A** Yes, but this is not a recommended design.
- Q** Does StackWise Virtual support interoperability with Cisco Nexus switches?
- A** Yes.
- Q** Can a StackWise Virtual L2 MEC interoperate with Cisco Nexus vPC?
- A** Yes. Using LACP (active/active) on each end is recommended.
- Q** How does StackWise Virtual interoperate by connecting with Cisco WLC products?
- A** Cisco WLCs can be directly dual homed to each stack member in a StackWise Virtual domain. The LAG on a WLC does not support PAgP or LACP. Hence, as a fallback, static mode on can be configured on StackWise Virtual domain switches.
- Q** How does network QoS work in a StackWise Virtual deployment model?
- A** The Cisco Catalyst 3850 deployed in StackWise Virtual mode supports the same eight-class QoS (2P6Q3T) model across any available network ports.

- Q** What unicast and multicast routing protocols are supported in StackWise Virtual?
- A** Cisco StackWise Virtual supports consistent routing protocols as standalone units, as shown in Table 3.

Table 3. Cisco StackWise Virtual Routing Protocol Support

Routing	Protocols	IPv4/v6 Support
Unicast	EIGRP OSPF ISIS BGP	Yes
Multicast	PIM: DM, SM PIM: SSM MSDP	Yes

- Q** How many maximum MAC addresses are supported by StackWise Virtual?
- A** Up to 32,000 MAC address are supported by the Cisco Catalyst 3850 in a StackWise Virtual domain.
- Q** What is the maximum number of supported STP instances?
- A** StackWise Virtual can support up to 128 STP instances using the R-PSVT protocol. For increased scale, IEEE 802.1s Multiple Spanning Tree (MST) is the recommended protocol.
- Q** Which VPN technologies are supported by StackWise Virtual?
- A** StackWise Virtual supports multiple VPN technologies, as shown in Table 4.

Table 4. Cisco StackWise Virtual VPN Support

Protocols	IPv4/v6 Support
Multi-VRF GRE MPLS L3 VPN	Yes

Q What is the Cisco IOS Software license requirement to use supported VPN technologies?

A The IP Services software license is required to use supported VPN technologies.

Q Is multicast VPN supported on StackWise Virtual?

A Yes.

Q How many VRFs are supported on StackWise Virtual?

A Up to 27 VRFs can be configured in a Cisco Catalyst 3850 running in StackWise Virtual mode.

Q Does StackWise Virtual support NSF capabilities for all Layer 3 unicast and multicast protocols?

A Yes. By default, the routing protocols are in NSF helper mode, and the capable function must be manually enabled for each protocol.

Q What is the recommended NSF mode when an L3 neighbor is a Cisco Nexus switch?

A It is recommended to configure NSF in StackWise Virtual using IETF mode if an L3 neighbor is a Cisco Nexus switch to gracefully recover the system during switchover conditions.

Q Can I fine-tune routing protocol timers aggressively in a StackWise Virtual deployment?

A Yes, but it is not a recommended configuration. Any aggressive timer tuning for a Layer 2 or Layer 3 protocol might create a false positive in the network during SSO in StackWise Virtual.

Q Does StackWise Virtual support application visibility and NBAR2?

A Yes. Application visibility and NBAR2 can be deployed on a Layer 2 or Layer 3 interface for enabling deep packet inspection of application traffic switched through both stack member switches in a StackWise Virtual domain.

Q How many application types can be detected?

A StackWise Virtual can provide deep packet inspection for 1500+ application signatures.

Q Can the Cisco Catalyst 3850 provide visibility for encrypted data?

A Yes. The Cisco Catalyst 3850 supports industry unique heuristic algorithms to provide visibility in 150+ encrypted applications.

Q What version of the NBAR2 protocol library is supported by StackWise Virtual?

A Cisco IOS-XE Software Release 16.3.3 will support NBAR protocol engine version 27.

Q Can I implement QoS policy based on application protocols in StackWise Virtual?

A Yes. Cisco modular QoS (MQC) policy supports classifying individual or groups of applications to implement various QoS policies.

Q How many flexible NetFlow entries does Cisco StackWise Virtual support?

A The Cisco Catalyst 3850-48-XS series supports a maximum of 96,000 flexible NetFlow entries. In StackWise Virtual mode, the flexible NetFlow function is based on a distributed architecture. Hence, a maximum of 192,000 FNF entries are supported with a pair of 3850-48-XS series platforms in a StackWise Virtual domain.

Q What Cisco IOS Software upgrade mechanisms are available?

A The stack members in a StackWise Virtual domain can be upgraded using the following method:

- Command line: The manual process to download the software to local flash and initiate the upgrade process that automatically installs new software files on both stack members. User must plan downtime to reload both stack members to make the new software effective.
- Cisco Prime Infrastructure: The software image management (SWIM) feature in Cisco Prime can be used to automate the installation process from the remote management server.

Q How do I configure Cisco Prime Infrastructure SWIM to deploy new software in a StackWise Virtual domain?

A Refer to the following step-by-step process in the Cisco Prime Infrastructure documentation to upgrade StackWise Virtual switches: http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-1/user/guide/pi_ug/maint_images.html.

Q What happens if stack members have different Cisco IOS Software versions?

A The Cisco IOS Software mismatch will result in SSO failure. Hence, one of the switches will not join the stack ring and will result in a down state.

Q How do I automatically upgrade software for a new stack member switch to minimize SSO failure?

A Configure the new command line in global configuration mode “software auto-upgrade enable” to automatically download the operating software version to the new switch joining the StackWise Virtual domain.

Q Can I get console access to a StackWise Virtual HOT_STANDBY switch?

A Yes. The standby console access must be manually enabled under the redundancy->main-cpu configuration mode. By using the “session standby ios” command, the user can get console access to the standby stack member switch.

Q Which events cause a StackWise Virtual SSO active stack member switchover?

A The following events can cause an SSO active stack member switchover:

- Active stack member software crash.
- Active stack member hardware error.
- Interchassis stack member poll timer expiration.
- SVL failure and dual active condition detection.
- CLI initiated: reset active sup, or “redundancy force switchover”; EFSU upgrade.
- EEM: action defined and initiated by EEM script.
- Power loss of active stack member switch.

Q How do reload commands work in StackWise Virtual mode?

A The following commands can reload individual or both stack members:

- reload: This command will reboot both stack member switches.
- reload slot <id>: This command will reload individual stack members independent of their SSO role.
- reload standby-cpu: This command will reload HOT_STANDBY stack member switches.

- redundancy force-switchover: This command will reload current ACTIVE stack member switches.
- redundancy reload peer: This command will reload HOT_STANDBY stack member switches.
- redundancy reload shelf: This command will reload both stack members of a StackWise Virtual domain.

Q What is the recommended method to remove the stackwise virtual configuration in 16.3.3 Release?

A Please follow the below order exactly as shown:

- Remove the stackwise virtual configuration from all the SVL Links
- Save the Configuration
- Remove the Stackwise Virtual Dual Active Detection configuration from all the links
- Save the Configuration
- Remove the Global Stackwise Virtual configuration from the switch
- Save the Configuration
- Reload the Switch

Q How does Cisco IOS Software license management work in StackWise Virtual?

A The Cisco IOS Software license between both stack member switches must match. The software license can be modified to match all the stack members using the license CLI in EXEC mode. Both the stack member switches will need to be reloaded to make the new software licenses effective.

Q What SNMP MIBs are supported by StackWise Virtual?

A The SNMP MIB support matrix remains consistent on the Cisco Catalyst 3850 platform independent of deployment modes between StackWise Virtual and StackWise-480.

Q What SNMP MIBs can be used to manage and monitor StackWise Virtual switches?

A The CISCO-STACKWISE-MIB can be used collect information about each stack member switch, including generating a trap when the stack member is added to or removed from the StackWise Virtual domain.

Q What SNMP MIBs can be used to manage and monitor for SVL connections?

A The ifMIB can be used to track the status of SVL connections between both stack member switches of a StackWise Virtual system.

Q Does Cisco Prime Infrastructure support upgrading Cisco IOS Software on both StackWise Virtual systems?

A Yes. The two stack members in a StackWise Virtual domain can be logically represented as a single unit to the Cisco Prime Infrastructure device inventory management.

Q Does Cisco StackWise Virtual support the APIC-EM PnP app?

A Yes. The new 3850-48-XS series platform with factory default configuration can download a configuration that includes StackWise Virtual from the APIC-EM PnP server to automate a StackWise Virtual deployment.

Q Can I monitor all system environments from a single console?

A Yes. With the “show environment” command line, the user can verify status of airflow direction, fan, power supply unit, and system temperature of both stack member switches of a StackWise Virtual domain.

Q Does StackWise Virtual support SPAN?

A Yes. Traffic can be sourced, and destination to the same stack member is supported. Remote stack member SPAN will be supported in future software releases.

Q What are the key software feature differences between Stackwise-Virtual and Stackwise-480?

A Majority of the software feature support is consistent between Stackwise-Virtual and Stackwise-480 deployment model. Certain features like REP and Remote SPAN is not supported today but will be supported in the future releases.