CHAPTER 1

Virtual Switching Systems Design Introduction

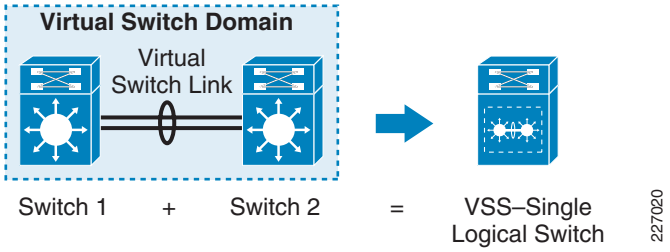
Executive Summary

VSS enables unprecedented functionality and availability of campus network by integrating network and systems redundancy into a single node. The end-to-end campus network enabled with VSS capability allows flexibility and availability described in this design guide.

The single logical node extends the integration of services in a campus network beyond what has been previously possible, without significant compromise. Integration of wireless, Firewall Services Module (FWSM), Intrusion Prevention System (IPS), and other service blades within the VSS allows for the adoption of an array of Service Ready Campus design capabilities. For example, VSS implementation allows for the applications of Internet-edge design (symmetric forwarding), data center interconnection (loop-less disaster recovery), and much more. Though this document only discusses the application of VSS in campus at the distribution layer, it is up to network designer to adapt the principles illustrated in this document to create new applications—and not just limit the use of VSS to the campus environment.

The key underlying capability of VSS is that it allows the clustering of two physical chassis together into a single logical entity. See Figure 1-1.

Figure 1-1 Conceptual Diagram of VSS



This *virtualization* of the two physical chassis into single logical switch fundamentally alters the design of campus topology. One of the most significant changes is that VSS enables the creation of a *loop-free* topology. In addition, VSS also incorporates many other Cisco innovations—such as Stateful Switch Over (SSO) and Multi-chassis EtherChannel (MEC)—that enable non-stop communication with increased bandwidth to substantially enhance application response time. Key business benefits of the VSS include the following:

- Reduced risk associated with a looped topology
- Non-stop business communication through the use of a redundant chassis with SSO-enabled supervisors
- Better return on existing investments via increased bandwidth form access layer

- Reduced operational expenses (OPEX) through increased flexibility in deploying and managing new services with a single logical node, such as network virtualization, Network Admission Control (NAC), firewall, and wireless service in the campus network
- Reduced configuration errors and elimination of First Hop Redundancy Protocols (FHRP), such as Hot Standby Routing Protocol (HSRP), GLBP and VRRP
- Simplified management of a single configuration and fewer operational failure points

In addition, the ability of the VSS to integrate services modules, bring the full realization of the Cisco campus fabric as central to the services-oriented campus architecture.

Virtual Switching System (VSS) Design

To better understand the application of the VSS to the campus network, it is important to adhere to existing Cisco architecture and design alternatives. The following section illustrates the scope and framework of Cisco campus design options and describes how these solve the problems of high availability, scalability, resiliency and flexibly. It also describes the inefficiency inherent in some design models.

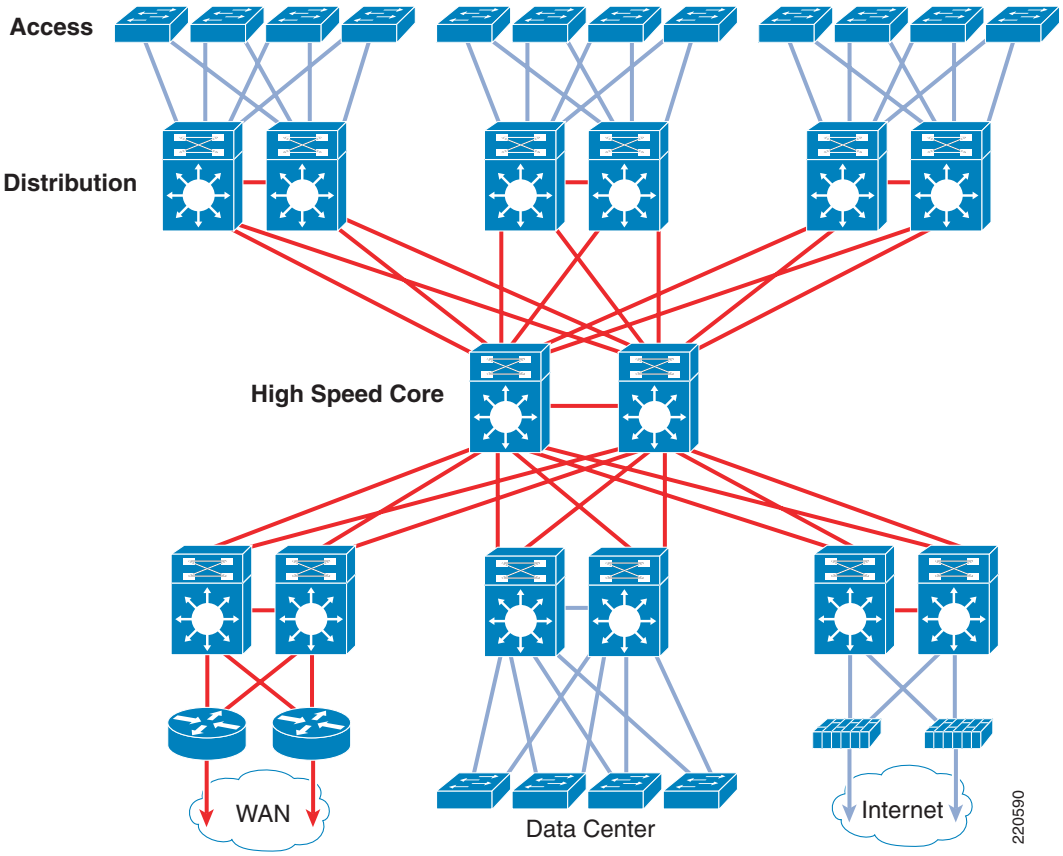
Campus Architecture and Design

The process of designing a campus architecture is challenged by new business requirements. The need for non-stop communication is becoming a basic starting point for most campus networks. The business case and factors influencing modern campus design are discussed in following design framework:

Enterprise Campus 3.0 Architecture: Overview and Framework
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html

The use of hierarchical design principles provides the foundation for implementing campus networks that meet these requirements. The hierarchical design uses a building block approach that uses a high-speed routed core network layer to which multiple independent distribution blocks are attached. The distribution blocks comprise two layers of switches: the actual distribution nodes that act as aggregators for building/floors/section and the wiring closet access switches. See Figure 1-2.

Figure 1-2 Hierarchical Campus Building Blocks



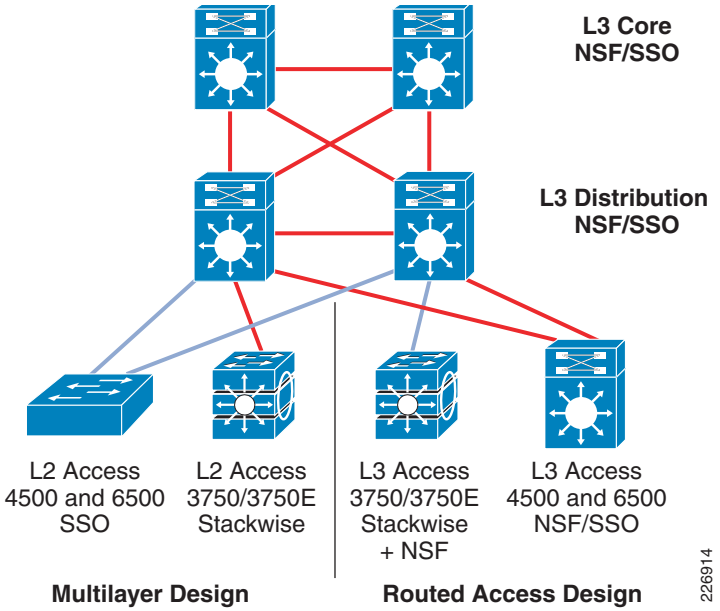
VSS at the Distribution Block

The Campus 3.0-design framework covers the functional use of a hierarchy in the network in which the distribution block architecture (also referred as access-distribution block) governs a significant portion of campus design focus and functionality. The access-distribution block comprises two of the three hierarchical tiers within the multi-tier campus architecture: the access and distribution layers. While each of these two layers has specific services and feature requirements, it is the network topology control plane design choices (the routing and spanning tree protocols) that are central to how the distribution block is glued together and how it fits within the overall architecture. There are two basic design options for how to configure the access-distribution block and the associated control plane:

- Multilayer or multi-tier (Layer 2 in the access block)
- Routed access (Layer 3 in the access block)

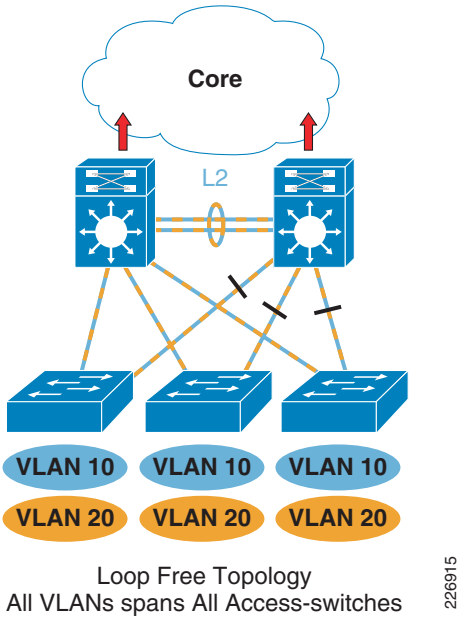
While these designs use the same basic physical topology and cabling plant, there are differences in where the Layer-2 and Layer-3 boundaries exist, how the network topology redundancy is implemented, and how load balancing works—along with a number of other key differences between each of the design options. Figure 1-3 depicts the existing design choices available.

Figure 1-3 Traditional Design Choices



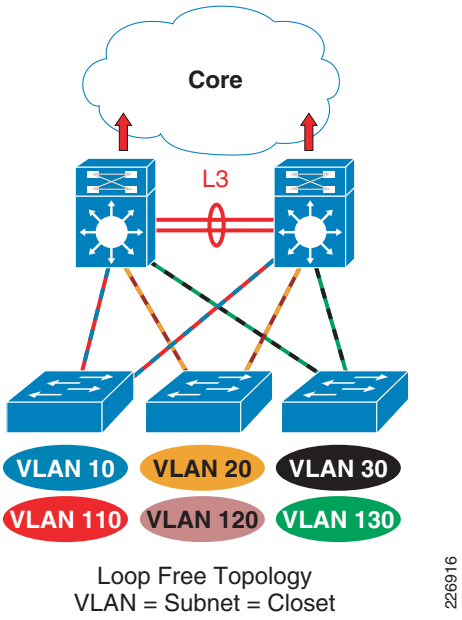
The multilayer design is the oldest and most prevalent design in customer networks while routed access is relatively new. The most common multilayer design consists of VLANs spanning multiple access-layer switches to provide flexibility for applications requiring Layer-2 adjacency (bridging non-routable protocols) and routing of common protocol, such as IPX and IP. This form of design suffers from a variety of problems, such as instability, inefficient resources usage, slow response time, and difficulty in managing end host behavior. See Figure 1-4.

Figure 1-4 Multilayer Design—Looped Topology



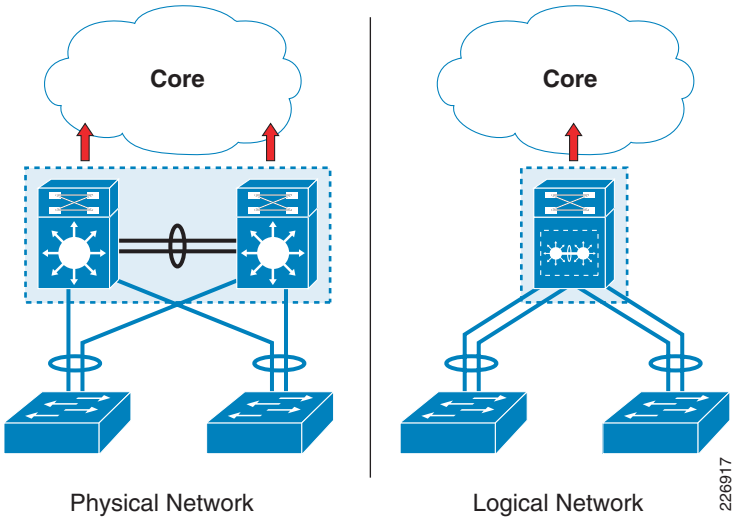
In the second type of multilayer design, VLANs do not span multiple closets. In other words VLAN = Subnet = Closet. This design forms the basis of the best-practice multilayer design in which confining VLANs to the closet eliminate any potential spanning tree loops. See Figure 1-5. However, this design does not allow for the spanning of VLANs. As an indirect consequence, most legacy networks have retained a looped spanning tree protocol (STP)-based topology—unless a network topology adoption was imposed by technology or business events that required more stability, such as implementation of voice over IP (VoIP).

Figure 1-5 Multilayer Design—Loop Free Topology



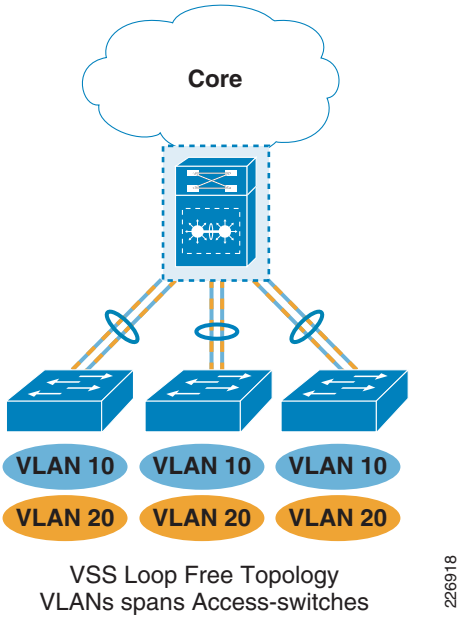
When VSS is used at the distribution block in a multilayer design, it brings the capability of spanning VLANs across multiple closets, but it does so without introducing loops. Figure 1-6 illustrates the physical and logical connectivity to the VSS pair.

Figure 1-6 Virtual Switch at the Distribution layer



With VSS at the distribution block, both multilayer designs transform into one design option as shown in Figure 1-7 where the access layer is connected to single logical box through single logical connection. This topology allows the unprecedented option of allowing VLANs to span multiple closets in loop-free topology.

Figure 1-7 VSS-Enabled Loop-Free Topology



The application of VSS is wide ranging. VSS application is possible in all three tiers of the hierarchical campus—core, distribution, and access—as well as the services block in both multilayer and routed-access designs. However, the scope of this design guide is intended as an application of VSS at the distribution layer in the multilayer design. It also explores the interaction with the core in that capability. Many of the design choices and observations are applicable in using VSS in routed-access design because it is a Layer-3 end-to-end design, but the impact of VSS in multilayer is the most significant because VSS enables a loop-free topology along with the simplification of the control plane and high availability.

Application of VSS

Application of VSS in a multilayer design can be used wherever the need of Layer-2 adjacency is necessary, not just for application but for flexibility and practical use of network resources. Some of the use cases are as follows:

- Application requiring Layer -2 adjacency—Data VLANs spanning multiple access-layer switches
- Simplifying user connectivity by spanning VLANs per building or location
- Network virtualization (guest VLAN supporting transient connectivity, intra-company connectivity, merger of companies, and so on)
- Conference, media room and public access VLANs spanning multiple facilities
- Network Admission Control (NAC) VLAN (quarantine, pasteurization, and patching)
- Outsource group and inter-agency resources requiring spanned VLANs
- Wireless VLANS without centralized controller
- Network management and monitoring (SNMP, SPAN)

Virtual Switching Systems (VSS) Recommended Best Practices—Summary

Throughout this design guide, Cisco recommended best practices have been provided. The key ones are flagged as "Tips" in the sections that discuss the relevant topics. The following table lists all the key Cisco recommended best practices to make it easier for users to see them at-a-glance.

VSS Best Practice Recommendations	Topic
The recommendation is to use a unique domain ID as a best practice, even when you are not connecting multiple VSS domains together.	See "Virtual Domain" for details.
Cisco strongly recommends that you do not modify the default LMP (VSLP) timers.	See "Why Timer Should Not be Modified" for details.
It is recommended to keep the VSL link load-sharing hash method to default (adaptive) as that method is more effective in recovering flows from failed links.	See "Hashing Methods—Fixed versus Adaptive" for details.
Always bundle the numbers of links in the VSL port-channels in the power of 2 (2, 4, and 8) to optimize the traffic flow for load-sharing.	See "Hashing Methods—Fixed versus Adaptive" for details.
Cisco recommends that you do *not* configure switch preemption for the following reasons: • It causes multiple switch resets, leading to reduced forwarding capacity and unplanned network outages. • The VSS is a single logical switch/router. Both switch members are equally capable of assuming the active role because it does not matter which is active—unless required by enterprise policy.	See "Switch Preemption" for details.
The best practice is to keep the PAgP timer settings to default values and to use the normal UDLD to monitor link integrity.	See "Why You Should Keep the PAgP Hello Value Set to Default" for details.
The best practice is to keep the LACP timer settings to the default values and to use the normal UDLD to monitor link integrity.	See "Why You Should Keep the LACP Hello Value Set to Default" for details.
Cisco recommends the configuration of a virtual MAC address for VSS domain using the *switch virtual domain* command.	See "MAC Addresses" for details.
Cisco recommends that you enable and keep the default MAC OOB synchronization activity interval of 160 seconds (lowest configurable value) and idle MAC aging-timer of three times the default MAC OOB synchronization activity interval (480 seconds).	See "Out-Of-Band Synchronization Configuration Recommendation" for detail.
Cisco recommends that trunks at both end of the interfaces be configured using the desirable-desirable or auto-desirable option in a VSS-enabled design.	See "Trunking Configuration Best Practices" for details.
Cisco recommends explicit configuration of required VLANs to be forwarded over the trunk.	See "VLAN Configuration Over the Trunk" for details.
The aggressive UDLD should not be used as link-integrity check, instead use normal mode of UDLD to detect cabling faults and also for the link integrity.	See "Unidirectional Link Detection (UDLD)" for details.

VSS Best Practice Recommendations	Topic
Cisco recommends that you always use a star-shaped topology with MEC (Layer-2 and Layer-3) from each device connected to the VSS to avoid loops and have the best convergence with either link or node failures.	See Topology Considerations with VSS for details.
Cisco recommends that you do *not* enable Loop Guard in a VSS-enabled campus network.	See "Loop Guard" for details.
In the VSS-enabled network, it is critically important to keep the edge port from participating in the STP. Cisco strongly recommends enabling PortFast and BPDU Guard at the edge port.	See "PortFast and BPDU Guard" for details.
Cisco strongly recommends *not* tuning below the values listed in Table 3-5. All other NSF-related route timers should be kept at the default values and should not be changed.	See "NSF Recovery and IGP Interaction" for details.
Cisco recommends using a Layer-3, MEC-based topology to prevent multicast traffic replication over the VSL bundle and avoids delay associated with reroute of traffic over VSL link.	See "Traffic Flow with ECMP versus MEC" for details.
In Layer-2 environment, single logical link between two VSS (option 5) is the *only* topology that is recommended; any other connectivity scenario will create looped topology.	See "VSS in the Core" for details.
Cisco strongly recommends enabling dual-active detection in VSS-enabled environment.	See "Campus Recovery with VSS Dual-Active Supervisors" for details.
The best practice recommendation is to *avoid* entering into configuration mode while the VSS environment is experiencing a dual-active event; however, you cannot avoid configuration changes required for accidental shutdowns of the VSL link or the required configuration changes needed to have a proper VSL restoration.	See "VSL-Link Related Configuration Changes" for details.
The routing-protocols are recommended to run default hello and hold timers.	See "Effects of Dual-Active Condition on Convergence and User Data Traffic" for details.