Delivering High Availability in the Wiring Closet with Cisco Catalyst Switches

Why Now? High Availability at the Network Edge

The enterprise network is no longer just a means for PCs to access data on servers. It is a critical part of business communications. Although the claim has been made for years that the network is mission critical, this statement is true now more than ever as enterprises, both small and large, are transitioning to Unified Communications such as IP telephony and collaboration. As part of this transition, enterprises are taking a new look at the role of the wiring closet in providing the high availability expected from their network investments. Traditionally, this emphasis has been limited to the network core, where potentially thousands of desktops converge. The wiring closet was relegated to an area of the network where corners were cut, since at worst a group of users would lose connectivity to a file server.

This is now a path to instability with real-time applications such as IP telephony or desktop videoconferencing. This same group of users might be the enterprise's inside sales force in the midst of a critical transaction or be on the receiving end of its Web-based customer support calls.

Traditional network design criteria leave the network open to severe disruption of the users' applications in the event of a failure. Therefore, the same design criteria that defined the core are now applicable to the last mile within the campus. These criteria include designing the overall network for high availability.

High availability is a percentage that expresses how available a network is. Figure 1 shows the downtime experienced by a network and how it translates to a high-availability metric. To achieve 99.999 percent ("five nines") availability, the network needs to be designed for less than 5 minutes of downtime per year. This includes planned and unplanned outages. To achieve high availability, a network design must look at device-level, protocol-level and network-level reliability, including hardware redundancy, software modularity, and quick recovery from failures. The Cisco® Catalyst® product line offers a complete and widely deployed line of LAN switching solutions for these requirements.

Figure 1. High Availability and Downtime

Availability	DPM	Downtime Per Year (24x365)		
99.000%	10000	3 Days	15 Hours	36 Minutes
99.500%	5000	1 Day	19 Hours	48 Minutes
99.900%	1000		8 Hours	46 Minutes
99.950%	500		4 Hours	23 Minutes
99.990%	100			53 Minutes
99.999%	**10**			**5 Minutes**
99.9999%	**1**			**30 Seconds**

"High Availability"

DMP—Defects per Million

Device-Level High Availability

The device (Ethernet switch) is the first point of contact into the network. This is where the Ethernet cable connects to a port on a wiring closet switch. Hence, the type of switch deployed in the wiring closet becomes the first critical point of consideration for a highly available network design. Multiple types of redundancy can exist and should be considered to deliver a highly available design. These include processor redundancy, power supply redundancy, and low mean time between failure (MTBF) for the cards and components used in the device. Cisco has many device-level high-availability features based on years of customer feedback. Depending upon whether a modular platform or stackable platforms are deployed, hardware redundancy is enabled through intelligent replication of common elements or StackWise technology.

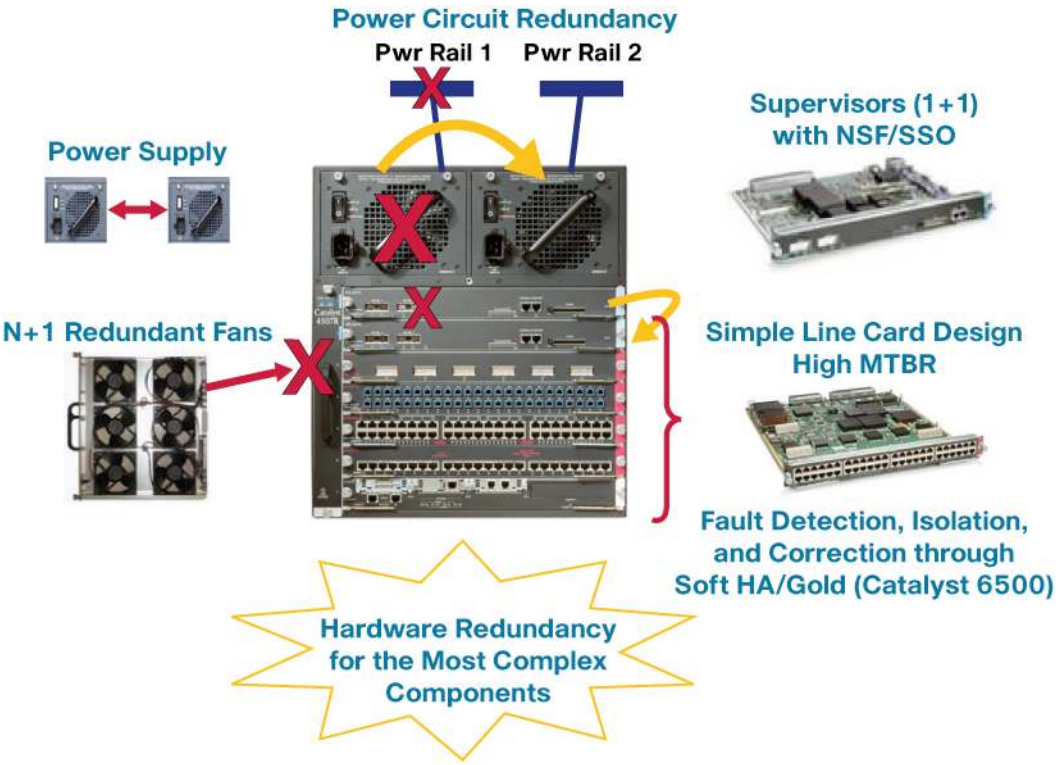
Chassis-Based Devices

Where the enterprise has opted for a chassis-based system such as the Cisco Catalyst 6500 Series or the Cisco Catalyst 4500 Series, hardware redundancy is important. Line cards, which are typically deployed in the wiring closet, have a high MTBF because they do not contain many complex electronics. Most intelligence and processing occur in the supervisor for chassis-based platforms, where most of the electronics exist instead of on a line card. Redundant supervisor engines provide the first level of device reliability, preventing session loss under hardware failure conditions. With features such as Stateful Switchover (SSO) and Nonstop Forwarding (NSF), session state is maintained, and forwarding continues in case of a supervisor failure.

In addition to supervisor redundancy, it is important to deploy redundant hardware system architectures as the basis for a highly available system. Figure 2 shows a typical modular Cisco Catalyst switch designed for device-level high availability. The following device-level elements should be considered in the wiring closet switch to help ensure chassis-based hardware redundancy:

- **Supervisor engine**—Wiring closet switches should support redundant supervisors to provide for system high availability. Supervisors operate in active and standby modes and support a variety of redundancy mechanisms for failover.
- **Power supplies**—Every chassis can support redundant power supplies so that a power supply failure does not affect operations.
- **Fan trays**—Each fan tray has multiple fans.
- **Line-card online insertion and removal (OIR)**—New modules can be added without affecting the system, and line cards can be exchanged without losing the configuration. This allows changes to the switch without having to take it out of service.

Figure 2. Device-Level High Availability



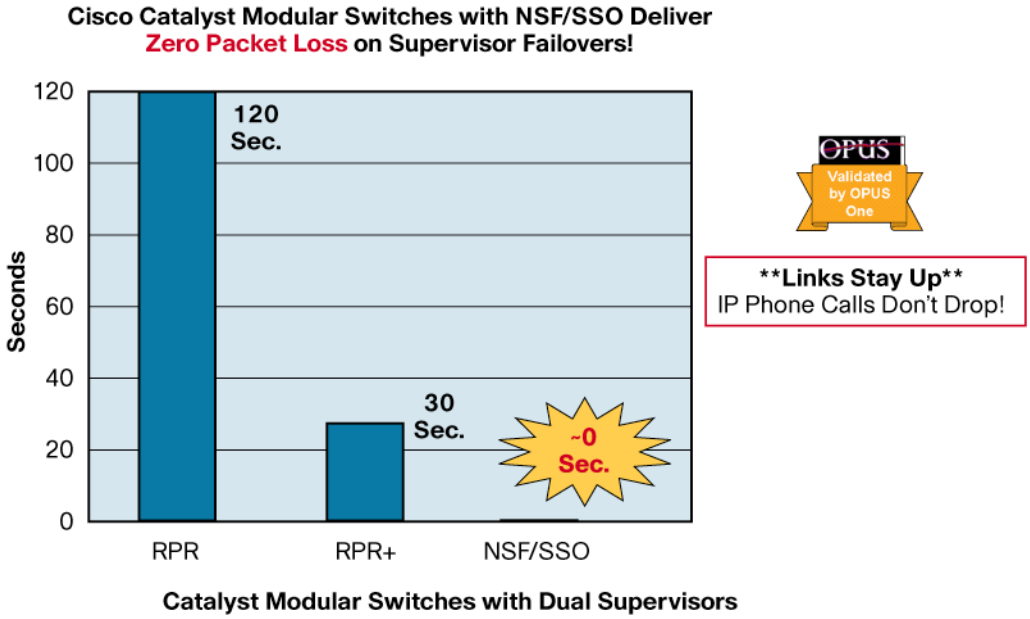
Nonstop Forwarding with Stateful Switchover

Nonstop Forwarding with Stateful Switchover (NSF with SSO) is a supervisor redundancy mechanism to provide intrachassis supervisor failover at Layers 2 through 4. NSF with SSO Supervisor redundancy on Cisco Catalyst switches requires two supervisors in a chassis. NSF with SSO reduces the mean time to recovery (MTTR) by allowing extremely fast supervisor switchover. It is an essential feature for single points of termination in the network, and it minimizes downtime when voice over IP (VoIP), video, and other packet loss–sensitive applications are involved.

In normal processes, the active supervisor is responsible for forwarding decisions. The second supervisor is in standby mode and does not participate in the forwarding decisions. The active supervisor synchronizes configuration and protocol state information to the standby supervisor. As a result, the standby supervisor is ready to take over the active supervisor's responsibilities immediately if the active supervisor fails. This takeover process from the active supervisor to the standby supervisor is referred to as *switchover* and happens almost instantaneously. Figure 3 shows the results of an independent test conducted by OPUS. The test shows supervisor failover times with and without NSF/SSO. This test indicated that Cisco Catalyst modular switches with

NSF/SSO deliver zero packet loss on supervisor failure, meaning that IP phone calls are not likely to be dropped.

Figure 3. Supervisor Switchover Test Results with and Without NSF/SSO



Even though only one supervisor is active at a time, the interfaces on a standby supervisor engine are active when the supervisor is up and thus can be used to forward traffic in a redundant configuration.

Control Plane Policing

In addition to supervisor redundancy, it is important to prevent malicious traffic from impeding a switch by flooding the CPU to the point that the switch can no longer forward packets or perform its function. One way to achieve this is by using control plane policing. This technique helps ensure that the control plane is not flooded by unnecessary or malicious traffic. It allows users to configure a quality-of-service (QoS) filter that manages the traffic flow of control plane packets. This in turn protects the control plane of Cisco switches against reconnaissance and denial-of-service (DoS) attacks. By enabling control plan policing, the switch can maintain packet forwarding and protocol states despite an attack on the switch.

Supervisor Fault Detection with Generic Online Diagnostics

Supervisor redundancy is just one part of system high availability. Detecting hardware and software faults is a primary requirement for providing resilient supervisor switchover mechanisms. Generic Online Diagnostics (GOLD) and platform-dependent diagnostics provide the framework for this fault detection.

GOLD defines a common architecture for diagnostic operation on Cisco Systems® platforms. GOLD works together with platform-specific online diagnostics to help ensure that a system booting up and a live system are healthy.

Fault-detection diagnostics mechanisms are enabled on most modules in Cisco Catalyst switches, including the active and standby supervisors. Diagnostics test results can be used to make switchover decisions. Switchover triggers are not limited to software crashes or keepalive mechanisms. Instead, switchovers can be triggered when the supervisor control and data paths are inconsistent or faulty or when runtime diagnostics detect a malfunctioning piece of hardware.

In addition to helping trigger switchover decisions, GOLD regularly monitors the standby supervisor to make sure that it is ready to take over if the need to switch over occurs.

GOLD detects the following problems to make supervisor switchover decisions:

- Faulty hardware components
- Faulty connectors
- Failed interfaces
- Memory errors
- Inconsistencies between the data plane and the control plane

Stackable Devices

In some environments, an enterprise can choose to deploy a fixed platform instead of a chassis-based platform. To help ensure high availability, the enterprise can deploy what is in effect a virtual chassis-based system using Cisco StackWise technology, which uses stack interconnect cables to create virtual switch fabric for stacks of the Cisco Catalyst 3750 Series. This technology brings to stackables a level of resiliency, manageability, intelligence, and performance previously not found in stackables. Up to nine Cisco Catalyst 3750 Series chassis can be connected into a single logical unit with a 32-Gbps switching stack interconnect, with management under the control of a single “master” switch automatically elected. This master is responsible for loading Cisco IOS® Software across the stack as well as global configuration control, maintenance of switching and routing tables, and acceptance of new switches to the stack.

Software Modularity

A new emphasis is on software high availability, enabled by modular operating systems. In the past, switch operating systems were monolithic, with protocols interdependence. If one failed, the entire device might fail. Cisco provides Cisco IOS Software modularity on the Cisco Catalyst 6500 Series Supervisor Engine 720 on the Cisco Catalyst 6500 Series. With a modular OS, disruption of a single protocol or process caused by internal or external influences will no longer affect the system. An added benefit is that individual protocols and processes can be upgraded without bringing down the entire device, critical for in-service maintenance.

As important as actual redundancy is, now switches can monitor failures and alert the network operator or automatically take a prescribed action to improve overall reliability. This is the role of the Cisco IOS Embedded Event Manager (EEM), which lets the network operator customize network behavior based on events as they happen with the goal of automating many network management tasks and increasing network availability.

Protocol-Level High Availability

A new design recommendation that is proving to deliver increased high availability in the wiring closet is the use of routing or Layer 3 for access switches. This is commonly called Routed Access. Routed Access reduces network recovery times and simplifies configuration and troubleshooting. It uses simple and efficient IP load balancing and tightens broadcast domains.

In the past, Layer 2 protocols were the dominant wiring closet protocols. Recovery times provided by Spanning Tree Protocol were sufficient. Today, more and more enterprises are dependent on peer-to-peer models and distribution of computing everywhere. In addition, real-time applications (for example, IP telephony) require a recovery time of less than 200 ms. A protocol such as Spanning Tree Protocol is not deterministic and cannot guarantee such results. Although many

network operators have optimized Spanning Tree Protocol, nonetheless, a new network design is required if deterministic recovery is needed.

By utilizing the intelligence and resiliency capabilities of Cisco routed protocols such as Enhanced Internet Gateway Routing Protocol (EIGRP) or Open Shortest Path First (OSPF) in the wiring closet, a network can recover from failure in a deterministic way without having to fine tune multiple protocols or devices. Not only that, but the network is better able to utilize existing network links versus than with Spanning Tree Protocol. EIGRP delivers convergence times of less than 200 ms by using Layer 3 recovery mechanisms instead of Layer 2 link updates. The inherent deterministic recovery from failure helps ensure that your network remains available for your critical communication applications. An additional benefit of deploying Layer 3 in the wiring closet is the time saved in network troubleshooting. Layer 3 troubleshooting tools are easier to use than Layer 2 tools in that they clearly identify the IP address of a potential problem. This helps network administrators isolate and repair problems more quickly, resulting in lower network downtime.

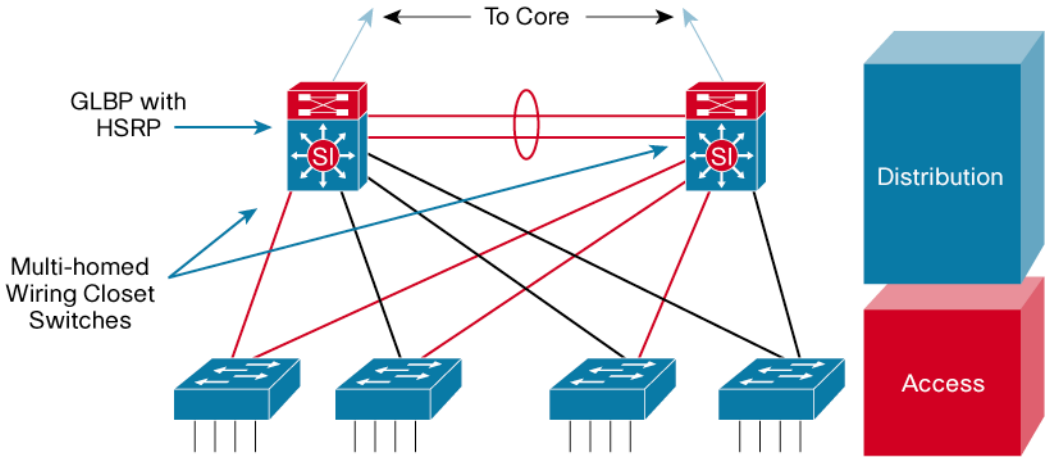
Network-Level High Availability

At the network level, high availability is achieved through multihoming an end device and helping ensure that the wiring closet switches are also multihomed at the distribution or core layer. Because typical end devices do not currently support a dual homing strategy (for example, an IP phone has only one Ethernet cable), it becomes very important that the wiring closet switch does not become the point of failure. By helping ensure that the switch selected has the appropriate device-level high availability and that the protocols used are Layer 3 in the wiring closet, the next step is to try to ensure that links from the wiring closet switch terminate on two different switches at the distribution layer.

At the distribution layer, verified protocols such as Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) come into use, helping ensure that end-user connectivity is not disrupted if a single node fails. Under HSRP, user application sessions are no longer dropped if the default distribution switch fails. With HSRP, a virtual router is created with state shared among two physical switches. If one fails, the end system transparently fails over to the alternate. VRRP, also available within Cisco IOS Software, is a standardized version of HSRP.

Enhancing on the capabilities of HSRP, Cisco developed Gateway Load Balancing Protocol (GLPB). GLBP provides automatic, first-hop gateway load balancing, which allows for more efficient resource usage and reduced administrative costs. It is an extension of HSRP and specifies a protocol that dynamically assigns responsibility for a virtual IP address and distributes multiple virtual MAC addresses to members of a GLBP group. Figure 4 shows a network design deploying both protocol-level and network-level high availability.

Figure 4. Network-Level and Protocol-Level High Availability



Like HSRP, GLBP supplies a method of providing nonstop path redundancy for IP by sharing protocol and Media Access Control (MAC) addresses between redundant gateways. Additionally, GLBP allows a group L3 switches to share the load of the default gateway on a LAN. It therefore improves performance by facilitating better use of network resources when multiple upstream paths are available and increases reliability and network availability by removing the single point of failure (the first-hop router). GLBP enables a router to automatically assume the forwarding function of another router in the group if there is a failure in any other gateway router. By combining the redundancy of HSRP with the load-balancing capabilities of GLBP, you can design your gateway redundancy with the maximum amount of uptime with the best utilization of network resources. For customers who cannot implement a full Routed Access network, the combination of HSRP and GLBP provides the first step in helping ensure availability at the network edge.

High-Availability Deployment Choices

High availability in the network becomes more critical as real-time applications running on the network become more prevalent. As end devices such as PCs or IP phones become business communication devices, the wiring closet and the high availability it delivers are important design considerations for network operators. In the past core and distribution resiliency was important; today this needs to extend to the wiring closet.

Cisco Catalyst switches provide extensive resiliency and help network managers build highly available networks. In the wiring closet, the network manager has many choices of which switch to use. Table 1 shows the various Cisco Catalyst switches and which high-availability features they support. Depending on the level of high availability desired, the network manager can select the appropriate switch.

Table 1. High-Availability Features on Cisco Catalyst Switches

Feature	Cisco Catalyst 6500 Series	Cisco Catalyst 4500 Series	Cisco Catalyst 3750 Series	Cisco Catalyst 3560 Series
Device Level				
Redundant Power Supplies	Yes—Internal	Yes—Internal	Yes—External	Yes—External
Redundant Supervisors	Yes	Yes	Virtual with StackWise	No
Redundant Fans	Yes	Yes	No	No
Cisco IOS Software Modularity	Yes	No	No	No
Control Plane Policing	Yes	Yes	No	no

Feature	Cisco Catalyst 6500 Series	Cisco Catalyst 4500 Series	Cisco Catalyst 3750 Series	Cisco Catalyst 3560 Series
GOLD	Yes	Subset	Subset	Subset
StackWise	NA	NA	Yes	NA
Protocol Level				
Routed Access	Yes	Yes	Yes	Yes
Network Level				
HSRP	Yes	Yes	Yes	Yes
VRRP	Yes	Yes	No	No
GLBP	Yes	Yes	No	No

Designing a highly available network can no longer be relegated to the core or distribution. Network managers who want to prepare their networks for the future will try to ensure that the same core and distribution design considerations are now extended to the access layer or wiring closet. Only careful end-to-end design will help ensure that employees or customers will have their IP-based business communications always available for use.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-340384-01 01/07