

# Deploy and Monitor IPv6 End to End

## Introduction

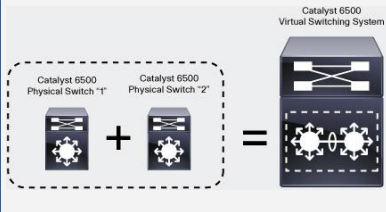
This white paper is a reference guide for designing an IPv6-enabled network. Using Las Vegas InteropNet 2011 as a real-life template, this paper navigates through emerging IPv6 framework, challenges, and design elements, exemplifying an IPv4 and IPv6 dual-stack network.

At Interop 2011, Cisco was a primary sponsor of InteropNet, a high-speed network built in collaborative fashion by innovative vendors and volunteer engineers, creating a completely interoperable network using the industry's most innovative technology.

One of the main focuses at InteropNet 2011 was IPv6, the next-generation IP protocol designed to resolve limitations of IPv4, for example, data security and maximum number of user addresses. Deploying IPv6 over wireless, security, and network management creates many new challenges. However, successful end-to-end IPv6 deployment is achievable. Due to the wide array of IPv6-ready Cisco® technologies, InteropNet experienced zero "severity one" issues, while providing continuous, dual-stack availability over the course of five days.

## IPv6-Ready Technology

In quad VSS mode, the Cisco Catalyst 6500-E switch can ensure stateful switchover (SSO) from an active to standby supervisor in case of a failure; while the "active" supervisor is managing and running control protocols, the "standby" supervisor is actively forwarding information - doubling the amount and speed of data transmission.

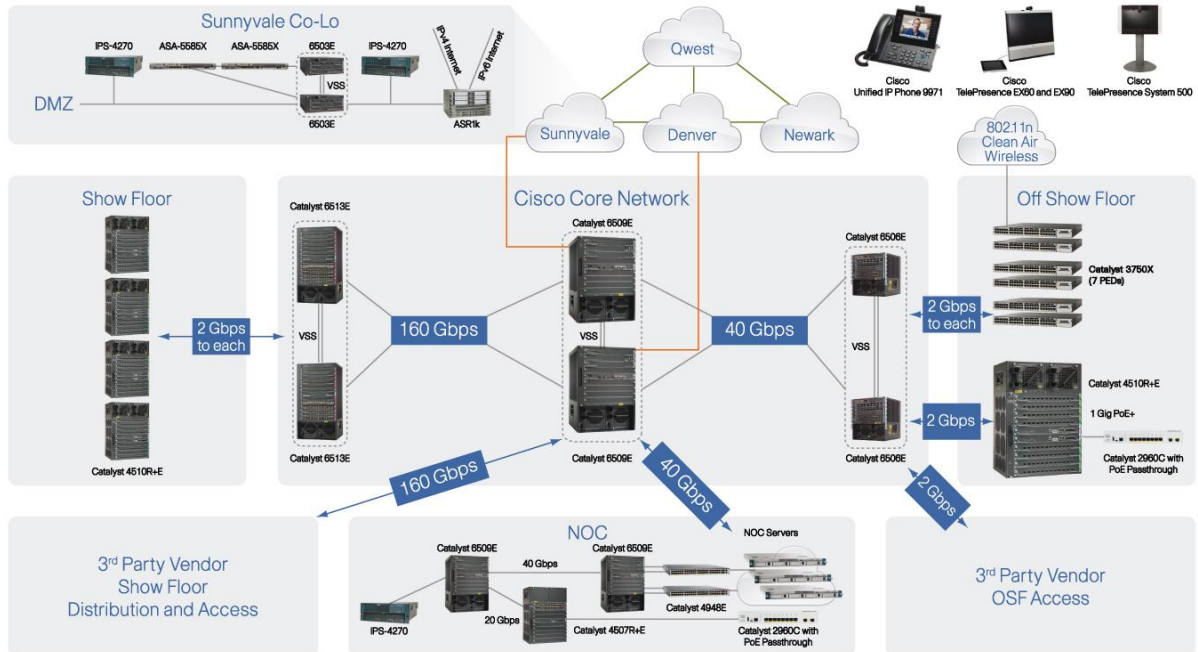


The diagram illustrates the Catalyst 6500 Virtual Switching System (VSS). On the left, two physical switches are shown: 'Catalyst 6500 Physical Switch "1"' and 'Catalyst 6500 Physical Switch "2"'. These are combined (indicated by a plus sign) to form a single 'Catalyst 6500 Virtual Switching System' unit on the right, which is represented by a larger switch icon with a gear and a plus sign inside.

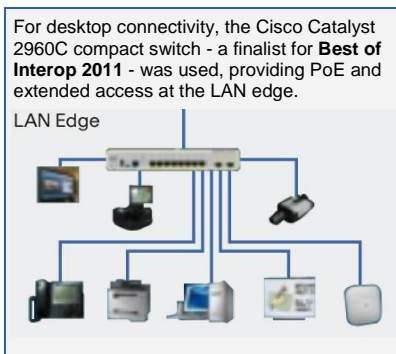
InteropNet's core and distribution networks (see Figure 1) were designed around the Cisco Catalyst® 6500-E Series Switch. Using 80 GigE link aggregation, the Cisco Catalyst 6500-E provides IPv4 and IPv6 multicast forwarding in hardware (with aggregated bandwidth of 2 terabits/second) providing high-quality voice and video enablement.

The Cisco Catalyst 4500-E with Supervisor Engine 7-E was used for access layer connectivity, offering full line-rate IPv6 forwarding performance at 125 million packets per second (pps).

**Figure 1.** InteropNet Topology



Where remote Cisco TelePresence<sup>®</sup> and IP phone deployments were needed, the more mobile and lightweight Cisco Catalyst 3750-X Series Switch provided scalability and convenience through native rapid deployment technologies (discussed later). The Cisco Catalyst switches provide Power over Ethernet Plus (POE+) of 30 watts per port to the IPv6-enabled voice and video endpoints, eliminating the need for a power supply, thus giving more flexibility for device placement.



Cisco's Unified Communications 7975 IP Phone and the Cisco EX90 TelePresence devices offered full IPv6 support and DNS integration while interworking with video-to-phone calling (or vice versa) regardless of protocol.

For IPv6 wireless mobility, a Cisco Catalyst 6500 Series with two Wireless Services Module 2s (WiSM2) offered scalable IPv6 connectivity. The Cisco Aironet<sup>®</sup> 3500 Series Access Point (**Best of Interop in 2010**) was employed for endpoint wireless access providing:

- Ability to scale power and increase/control serviceable range with Wireless LAN Controller (WLC)
- Multiple input and multiple output (MIMO) transmissions simultaneously
- Cisco CleanAir technology to suppress interference from undesired radio frequencies

## Security

InteropNet provided three levels of network security:

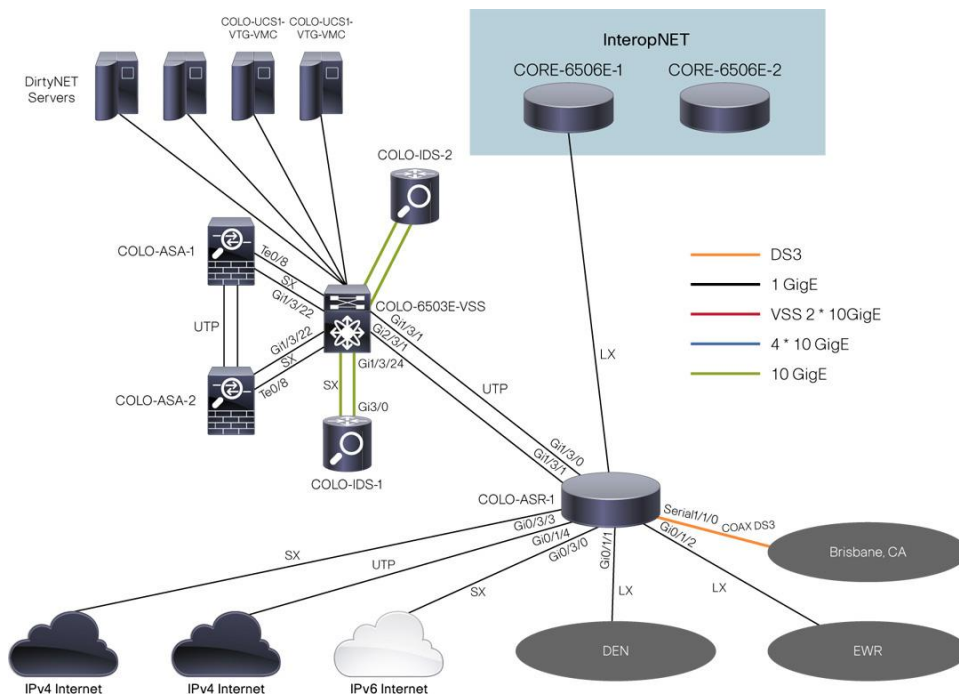
- Security for the colocation (CoLo) facility, located in Sunnyvale, California (see Figure 2)
- Network operations center (NOC) security (see Figure 3)
- Wireless security

Most Cisco products now have IPv6-compatible security features, making securing a dual-stack network with Cisco products a natural process in network deployment. Some examples of security features integrated within Cisco devices include:

- Transparent Cisco IOS® Firewalls
- First Hop Security
- Cisco TrustSec® security
- Port access control lists (PACLs)
- IPv6 Router Advertisement Guard
- IPv6 service level agreements (SLAs)

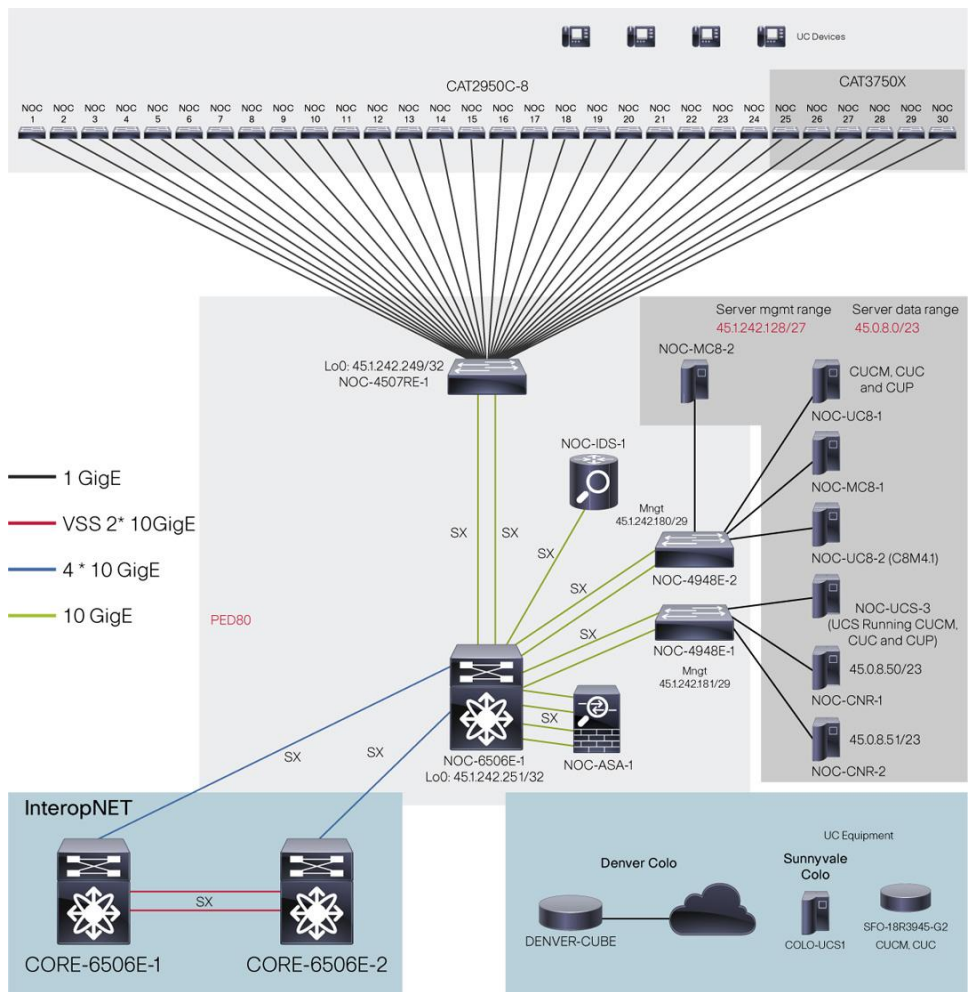
Each of these integrated security features is built into Cisco's routing and switching portfolio of products.

**Figure 2.** InteropNet CoLo Topology



In addition to native security features, the InteropNet CoLo featured redundant Cisco ASA 5585s with Cisco Adaptive Security Device Manager (ASDM), providing a browser-based management and monitoring interface enabling remote management of the colocation facility.

**Figure 3.** InteropNet NOC and Classroom Topology



An additional Cisco ASA 5585 provided security for the NOC. The Cisco ASA appliances combines firewall and content filtering while providing a full dual-stack security solution. Software Release 8.2 provides support of IPv6 addressing to enable quick ASA deployments into existing IPv6 networks without requiring IP readdressing.

In addition, the Cisco Intrusion Detection System (IDS) was included in the NOC, moving security of IP traffic above and beyond a “permissive” firewall screening to an active surveillance of behavior. The IDS proactively seeks and disables maliciously acting traffic before a threat can arise.

### A Rapid Deployment Network

In addition to integrated security technologies, Cisco products also integrate multiple deployment tools to help with switch/router and network rollout. This allowed the Interop volunteers to quickly deploy network devices throughout the Mandalay Bay Convention Center. Cisco technologies enabled the switches to automatically recognize attached devices through Auto Smart Port Configuration, or push Cisco IOS Software images onto several switches instantaneously through LMS configuration templates. Overall, this saved 80 to 90 percent over average manual configuration time.

---

These integrated tools made the setup of the unified communications portfolio of products transparent and easily programmable through inherently designed features within the Cisco network devices. The Cisco IP phones and Cisco TelePresence video stations were very adaptable to volunteer and attendee errors. If they were unplugged and mistakenly plugged back into a different port, the intelligence of the Cisco network recognized the device and automatically reconfigured that port for security and proper management of that endpoint.

## DHCP

Dynamic Host Configuration Protocol (DHCP) is an automatic configuration tool to help assign IP addresses to devices on the network without the need for a network administrator. To perform these services within InteropNet, Cisco Network Registrar was deployed - a software solution for DNS, DHCP and IP address management services. As this DHCP server provides high performance, scalability, and fully functional DHCPv4 and DHCPv6 services, it was an obvious choice to provide these services - as well as dynamically register clients in DNS. Of the 13,530 people attending Interop Las Vegas 2011, the Cisco DHCP server detected 9952 unique clients (based upon MAC address) accessing the InteropNet network. The Mandalay Bay Convention Center had disabled its own network, so InteropNet was the only available network for attendees.

Based on the organizationally unique identifier (OUI) of the extracted MAC addresses of these 9952 clients:

- 4093 were DHCPv4 only
- 756 were multiinterface devices, some perhaps IPv6 only
- 5103 were dual-stack IPv4/IPv6 (of which a majority of these dual-stack clients were Apple devices: 4304, or 84 percent)

## Network Monitoring, Management and Troubleshooting

A state-of-the-art network such as InteropNet is not complete without insight into network devices, management of energy consumption, or remote troubleshooting access. All of these were provided by the new Cisco Prime LAN Management Solution (LMS) 4.0.

Cisco Prime LMS provides step-by-step guidance to help operators quickly provision, monitor, and manage network devices. At InteropNet, Cisco Prime LMS was able to establish alerts based upon custom-configured CPU thresholds. It was also able to monitor memory and device availability, identify internal attacks with monitoring and fault management, and push configurations onto devices using configuration templates (discussed earlier).

The Cisco Prime Network Analysis Module (NAM) with its web-based Interface provided network operators visibility into IPv4 and IPv6 traffic, enterprise applications, and real-time troubleshooting capability. The Cisco Catalyst 6500 Series Network Analysis Module NAM-3, deployed in the NOC, reduced the network footprint, simplified manageability, and reduced total cost of ownership by integrating NAM-3 into preexisting infrastructure.

During prestaging, the Cisco Prime NAM identified an application that was unintentionally consuming nearly the entire WAN link. Having this visibility, network operators disabled the application to prevent a network failure.

The Cisco Prime NAM also allows network operators to quickly identify IPv4 and IPv6 issues by drilling down from monitor to analysis dashboards and troubleshoot with NAM's built-in packet capture. As compared to traditional troubleshooting methods like deploying personnel and equipment to a remote location, the Cisco Prime NAM can reduce the time and effort involved in problem resolution from days to hours.

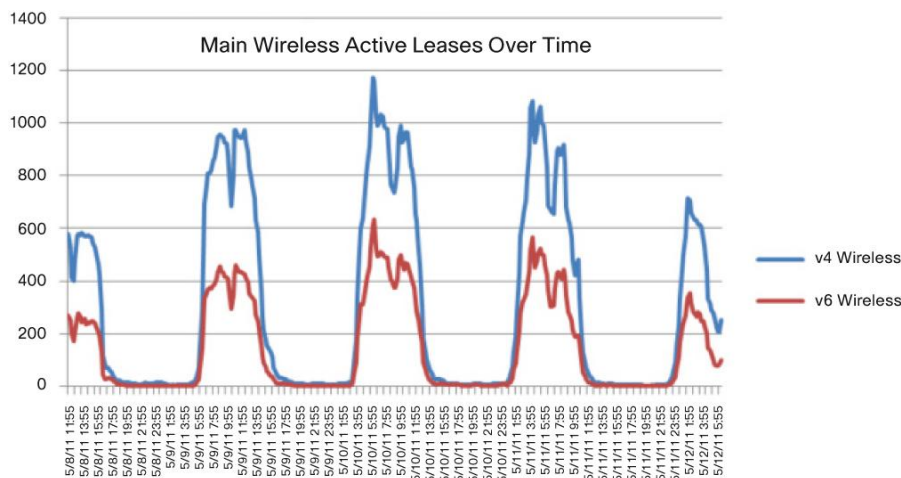
## Wireless

Designing a wireless network for IPv6 has its particular challenges. Subnetting is an established best practice of IPv4 wireless deployment (to protect from broadcast storms), and network designers often attempt to do the same with wireless IPv6.

Currently, assigning a subnet to each wireless access point (APs) results in a loss of network connectivity when roaming between IPv6 APs. Cisco resolved this by implementing a single, flat VLAN. This keeps IPv6 wireless deployment simple and allows for continuous roaming connectivity.

Does this configuration open up the network to broadcast storms? Because broadcast storms have been a concern with flat IPv4 networks for many years, Cisco has developed solutions called “traffic suppression,” preventing a “storm” of incoming nefarious traffic onto the network. Each port has a single traffic threshold that is used for all types of traffic (broadcast, multicast, and unicast). When these tools are incorporated into the design of a flat IPv6 network, the campus can enjoy a reliable, safe, and easily deployable IPv6 wireless experience. As evidence, nearly 50 percent of all Interop wireless users were connecting over IPv6.

**Figure 4.** Wireless v4 and v6 Leases



## Conclusion

InteropNet Las Vegas 2011 was a truly state-of-the-art network, featuring the latest in end-to-end security, management, and communication design from the Cisco Borderless Network portfolio. From the high-bandwidth, fully redundant core to high-definition video endpoints, Cisco at InteropNet provided a real-world model of IPv6 solutions for the enterprise.



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

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](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA

C11-678026-01 08/11