Unified Communications: Network Fabric, Connecting People Any Time, Any Where

Introduction

Business communications in today's work culture are having a significant effect on how companies and people operate. People want information right now, want to share complex applications to brainstorm ideas and make decisions quickly. This is driven by a global workforce, rapid travel, and faster business cycles.

Applications such as instant messaging, IP telephony, and video conferencing are becoming a necessity. In fact, businesses not adopting unified communications are being forced by their customers, suppliers, and business partners to do so.

Unified Communications Benefits and Trends

For businesses, deploying unified communications over an IP infrastructure has the following benefits:

- Workforce productivity gains can be realized if people can connect anywhere, any time. This can be because of faster decision time, quick time to market, increased collaboration, and increased employee morale
- Increased business profitability because of better employee customer interaction
- Cutting costs because of reduced travel and efficient utilization of IP resources

Some trends driving unified communications over an IP network are:

- Higher connectivity speeds through devices such as smart phones and laptops. This is because of adoption of wireless LAN technologies (802.11a/b/g/n) and next-generation wired/wireless networks everywhere providing 1-10+ Gigabit and/or 3G connectivity speeds.
- Adoption of interactive applications such as instant messaging, Cisco WebEx™ conferencing, Cisco TelePresence® conferencing, voice-over-IP (VoIP) phones, and PC-based video cameras. These applications enable sharing of voice, video, and data.
- Cost-saving and time-saving measures

Figure 1 shows how people are using unified communications from their desktops with IP phones and video cameras and how teams across the globe can meet using Cisco TelePresence.

Figure 1. Unified Communications in the Workplace

Collaborative applications provide video, voice, and data capabilities. Each capability has unique characteristics. Table 1 shows these characteristics.

Table 1. Collaborative Application Characteristics

Voice	Video	Data
• Smooth • Small packet size (480 bytes or less) • Drop sensitive (up to 1%) • Delay sensitive • UDP Priority • Latency (one-way): 150 ms • Jitter: up to 30 ms	• Bursty • Large packet sizes (800-1500 bytes) • Mostly variable bit rate • Drop sensitive (0.05%-1%) • Somewhat delay sensitive • UDP unicast or multicast • Latency : 150 ms – 400 ms • Jitter: 10 ms-50ms	• Smooth/bursty • IMIX average ~ 300 bytes • Drop insensitive • Delay insensitive • TCP/UDP • Best effort

Challenges and Considerations

While unified communications provides benefits, it poses certain upfront challenges to network architects. The network acts as an enabler for unified communications and should provide:

- **Scalability:** includes bandwidth availability, Power over Ethernet (PoE) and intelligent green capabilities and quality of service (QoS).
- **Nonstop communications:** include high availability features such as hardware redundancy, Stateful Switchover (SSO), Nonstop Forwarding (NSF), In-Service Software Upgrade (ISSU), Virtual Switching System (VSS), and tools such as Generic Online Diagnostics (GOLD), Embedded Event Manager (EEM), and Smart Call Home.
- **Quality of user experience:** includes application and location awareness, auto-QoS, and operational features such as IPSLA and ERSPAN.
- **Security:** includes identity 4.0 and enhancements, IP telephony, and PC integration as well as segmentation.

In order to provide a robust collaborative capability over an IP network, the following design considerations are important:

Network Scalability

This aspect deals with network bandwidth, PoE capabilities to provide a baseline where collaborative devices and applications can be connected and operated successfully. These devices can be IP access points, desktops/laptops, IP phones, video phones, IP surveillance cameras, and video conferencing systems. Green capabilities on access switch platforms help optimize performance.

Network bandwidth considerations require 10/100/1000 Mbps connectivity to end devices in the access layer, 10 Gbps uplink in the distribution, and multiple 10 Gbps bandwidth in the core to enable high-definition video applications. Video can be a big bandwidth consumer; for example, a single Cisco TelePresence session providing 720p-1080p high-definition video requires about 4-15Mbps and video generally is variable bit rate. As Table 1 shows, the network bandwidth requirements should be able to handle video/voice latency of 150 ms, jitter of 10 ms-30ms, and loss of 0.05%.

Cisco® access and core switches such as the Cisco® Catalyst® 4500 and the Cisco Catalyst 6500 provide interfaces ranging from 10Mbps to 10Gbps. The 4500 provides 24 Gbps per slot and the 6500 provides up to 40 Gbps per slot.

PoE provides Power over Ethernet to PoE, Enhanced PoE, and PoEP-ready devices. This capability is critical to power devices facilitating unified communications (for example, IP phones, IP video cameras, wireless access points, and certain video screens). It is recommended to operate power supplies in access switches in redundant mode. This not only provides power but provides power high availability for end devices. The Cisco Catalyst 4500 and Cisco Catalyst 6500 can support up to 289 and 423 PoE (15.4 Watt, Class 3) devices respectively. Cisco Catalyst 4500 can support up to 148 PoEP-ready devices, which is a leading capability. Table 2 shows PoE and PoEP scalability on the Cisco Catalyst 4500 platform with different power supplies.

Table 2. PoE and PoEP Scalability on the Cisco Catalyst 4500

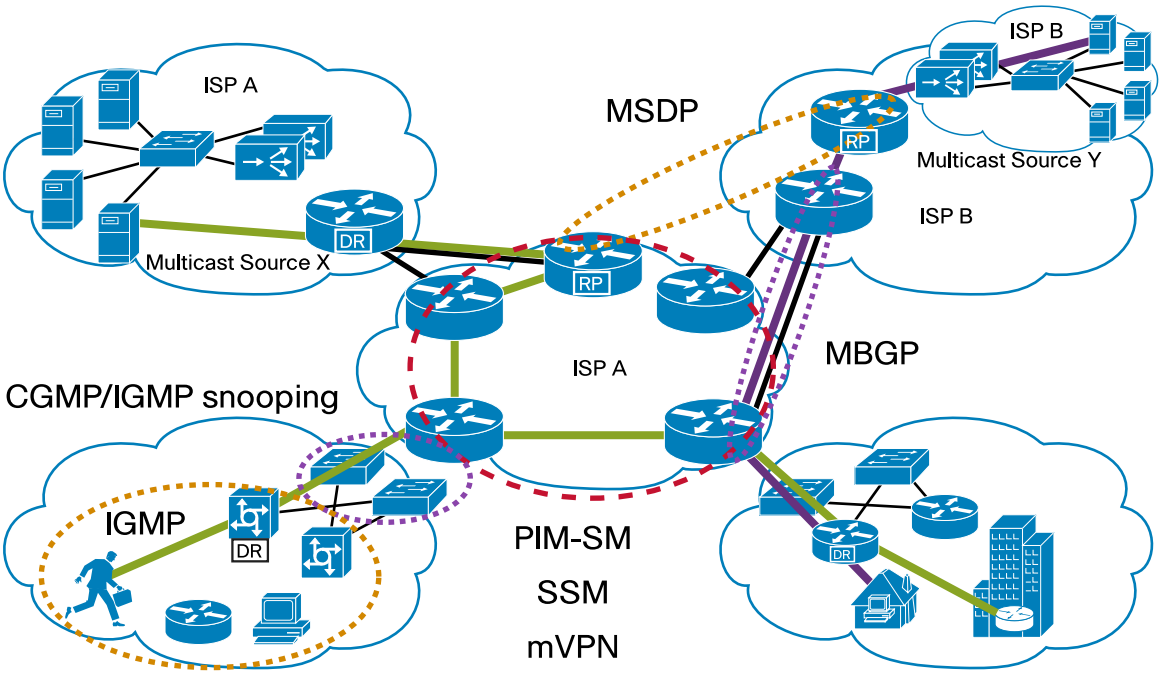
Input Voltage	Lines Connected	Output Power	Max Number PoE 15.4W (Class 3) Powered Device	Max Number PoEP 30W (Class 4) Powered Device
220 VAC	Both	6000 W	289	148
	Single	3000 W	142	76
110 VAC	Both	2100 W	95	49
	Single	1050 W	39	20

Intelligent power management capabilities such as efficient high-capacity power supplies (providing over 90% power efficiency), CDP or Link Layer Discovery Protocol (LLDP) based power negotiation, PoE monitoring (to look at actual power consumption for PoE devices), and PoE policing (to control power to ports and to shut down rogue ports) enable the network access layer to optimally operate the connected collaborative devices. These green capabilities are available on both Cisco Catalyst 4500 and 6500 switches.

QoS capabilities provide the ability to mark and queue the application packets appropriately. VoIP applications can be marked as “Expedited Forwarding” and queued in the “Priority queue.” Video applications can be marked either as “Expedited Forwarding” or as “Assured Forwarding” depending on video volume and delay characteristics. The Cisco Catalyst 6500 and the Cisco Catalyst 4500 use Weighted Random Early Detection (WRED) and Dynamic Link Buffering (DLB) respectively as congestion avoidance mechanisms. The Cisco Catalyst 4500 has differentiated services code point (DSCP) to queue mapping capabilities with 1P3Q1T queue architecture. The Cisco Catalyst 6500 has CoS to queue mapping capabilities with 1P2Q2T or 1P3Q8T queue architecture and has ingress and egress queues per line card. With the QoS architecture on the 4500s and 6500s, the network can differentiate different unified communication applications and provide the service level agreements (SLAs) needed (as shown in Table 1).

Multicast is required for streaming voice/video applications such as music-on-hold and IP surveillance. Multicast support and optimizations are critical to provide optimal unified communication services. Features such as bidirectional PIM help in the distribution and core, while features such as IGMP snooping and IGMP filtering help provide multicast session and bandwidth management optimizations. Figure 2 shows different multicast features required to provide comprehensive unified communications.

Figure 2. Multicast in the Enterprise for Unified Communications



Campus Multicast	Interdomain Multicast
End stations (hosts-to-routers): • IGMP (v2, v3)	**Multicast routing across domains:** • MBGP
Switches (Layer 2 Optimization): • IGMP Snooping, CGMP and RGMP	**Multicast Source Discovery:** • MSDP with PIM-SM
Routers (Multicast Forwarding Protocol): • PIM Sparse Mode or Bi-Dir	• **Source Specific Multicast (SSM)** • **Multicast VPN (mVPN)**

Nonstop Communications

This aspect provides high availability for unified communications. This means that the network needs to keep forwarding voice, video, and data traffic even if there are component level or device level failures. If the switches need to be upgraded with a new release of Cisco IOS® Software (because of PSIRT security alerts, bug fixes, or to support new hardware), traffic still needs to be forwarded. In certain mission critical environments, network services always need to available. The Enterprise Campus 3.0 Architecture at http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html provides high availability requirements for unified communications.

Nonstop communications provide the SLAs needed to help ensure quick network convergence and high availability such that VoIP calls not drop (avoid delays greater than 150ms) and video does not have artifacts/drops (avoid drops of more than 0.05% to 1%, based on applications).

Table 3 shows design consideration features needed for different types of failures.

Table 3. Nonstop Communications Features for Failure Scenarios

Failure/Risk	Feature	Benefit
Component or Linecard Level	GOLD, EEM, Smart Call Home	In case of component failure, detect failure using automatic GOLD scheduling and EEM. Using Smart Call Home, a switch can itself open a TAC case and provide the necessary outputs. This is available on the Cisco Catalyst 4500 (12.2(52)SG) and 6500 (12.2(33)SXI) platforms
Supervisor, Protocol or Uplink Level	Redundant Supervisors, Redundant power supplies, SSO, NSF, VSS, BFD, GLBP, VRRP	If a supervisor fails, SSO with NSF will switch over to the redundant supervisor while no impact to traffic or routing protocol adjacencies. This is available on the Cisco Catalyst 4500 and 6500 platforms. On the 6500 platform VSS provides High Availability. It also provides Multichassis EtherChannel (MEC) allowing the lower layers to connect to 2 different uplink 6500s. The Cisco Catalyst 4500 and the Cisco Catalyst 6500 (with VSS) can recover within 10-250 msecs in an outage scenario.
Redundant uplinks	Shared backplane mode	Allows Cisco Catalyst 4500 in the access layer to always have an uplink to the network distribution/core
In Service Software Upgrade	ISSU, VSS + ISSU, Modular Software	Allows Cisco IOS Software upgrade or subsystem upgrade of a Cisco IOS Software module while the network is still up. This feature is available on the Cisco Catalyst 4500 and the Cisco Catalyst 6500 with VSS. In each case the outage is in the range of 10-250 msecs.

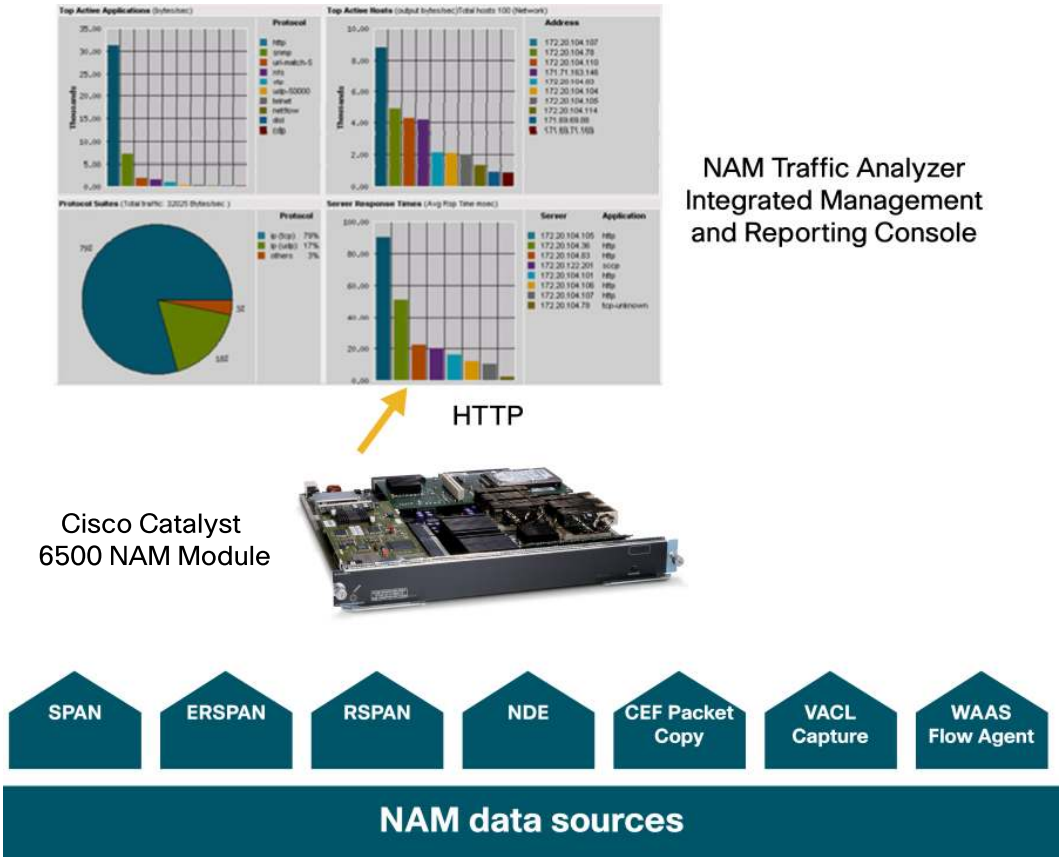
User Quality of Experience

This aspect provides qualitative enhancement to collaborative applications and technologies. In order to achieve this goal, the network has to be application and location aware. It should enable plug and play capabilities for collaboration and provide means to manage and measure application delivery metrics.

Application intelligence can be achieved through technologies such as Network-Based Application Recognition (NBAR) and Netflow. Application awareness provides granular network visibility at an application level. This ability allows correct QoS prioritization of the appropriate applications. While Netflow is available on the Cisco Catalyst 6500 and 4500 platforms, Supervisor32-PISA provides hardware based NBAR capabilities to provide application awareness.

Service modules such as Cisco Network Analysis Module (NAM) on the Cisco Catalyst 6500 platform offer comprehensive VoIP quality monitoring. This provides granular reporting of MOS and other KPIs such as jitter and packet loss to accurately measure how the end user experiences the delivery of voice services. Figure 3 shows how Cisco NAM can take data from different sources and provide it to the NAM Traffic Analyzer.

Figure 3. Integrated Location Services

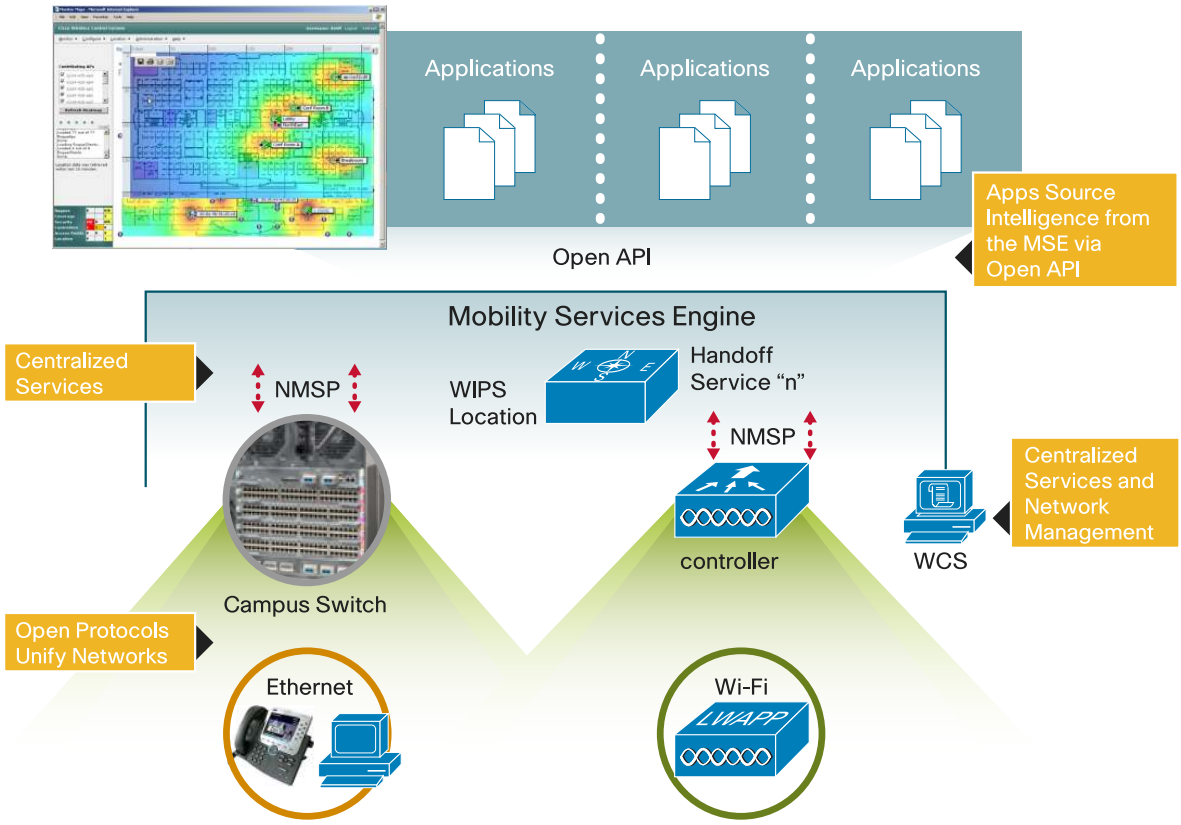


Location awareness provides the ability to collaborate intelligently keeping location in consideration. Some examples of smart unified communications based on location are location awareness for selecting correct language with video screens based in different geographies, or location awareness for IP video surveillance, where it makes sense to verify if a camera is in the correct location, before starting to record video for surveillance.

Location services are made possible using Network Mobility Service Protocol (NMSP). This protocol enables the network administrator to see the location of end devices connected to switch ports or location of entire switches. It ties the location information, configured on switch ports, to device IP address, MAC address. NMSP carries this information to a management interface call Mobility Services Engine (MSE).

NMSP can also carry information from wireless controllers, such as Wireless Service Module (WiSM) on the 6500, to MSE. WiSM can terminate up to 3000 access points on the 6500. NMSP is supported on all Cisco Catalyst 4500 and 4900 switches in Cisco IOS Software Release 12.2(52)SG. Cisco Catalyst 4500 and 6500 also support termination of 802.11n access points with Power over Ethernet. Figure 4 shows the integrated wired and wireless location services architecture.

Figure 4. Integrated Location Services



Plug and play with auto-QoS provides the ability to automatically configure QoS policies (including correct marking and queuing) for ports where a collaboration appliance (for example, a VoIP phone) is attached. Without this feature, the network administrator may have to statically configure ports where IP phones are attached. This feature is available on both the Cisco Catalyst 4500 and the Cisco Catalyst 6500. For more details on auto-QoS, visit http://www.cisco.com/en/US/tech/tk543/tk759/technologies_white_paper09186a00801348bc.shtml.

Operational features such as IPSLA and ERSPAN help to monitor application response times and the ability to replicate actual application sessions, if needed. Using SPAN or ERSPAN, VoIP traffic can be recorded for quality, troubleshooting, or law enforcement purposes.

Features such as smartport macros, which are built-in preconfigured configuration templates, can be added to a port when a laptop/PC, IP phone, WAN router, or switch is connected to this port.

These features are available on both the Cisco Catalyst 4500 and the Cisco Catalyst 6500.

Security

Connecting access devices to enable unified communication also requires providing security and flexible based access to resources. General security features, Identity 4.0 features, IP telephony integration, and unified communications segmentation are some of the features that should be kept in consideration. These features are available on both the Cisco Catalyst 4500 and the Cisco Catalyst 6500. Table 4 shows general security features for different attacks and their value. DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard can be used to prevent man-in-the-middle attacks, keeping VoIP and unified communication services available during the attacks.

Table 4. General Security for Securing Unified Communications

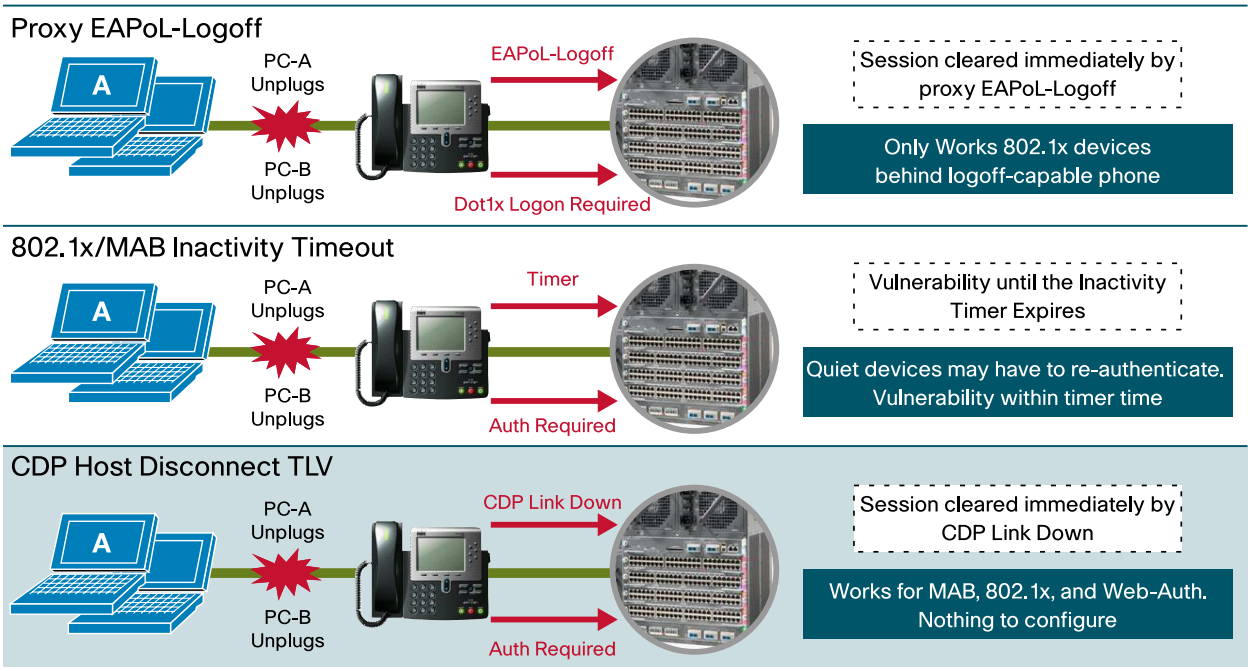
Feature	Security Attack	Value
Port Security	CAM attacks	Limits MAC addresses on interface which may shut down ports. It is recommended not to shut down the ports because of MAC attack (using Restrict and Protect Port Security Violation modes), so that VoIP services stay up
DHCP Snooping	Rogue DHCP attacks	Allows DHCP services only on trusted ports. Switch builds a DHCP Snooping Binding Table which has port MAC, IP address mappings
Dynamic ARP Inspection	ARP attacks	Builds on top of DHCP Snooping. Inspects DHCP Snooping Binding Table to verify IP address and corresponding MAC
IP Source Guard	IP/MAC Spoof Attacks	Builds on top of DHCP Snooping. Inspects DHCP Snooping Binding Table to verify IP address and corresponding MAC for each packet. For MAC spoofing only, DHCP option 82 should be supported on DHCP servers
Unicast Reverse Path Forwarding (uRPF)	IP Spoof Attacks	**uRPF Strict mode** checks to see if the IP packet is reachable by the same interface (in the Routing Table) through which it arrived. **uRPF Loose mode** checks to see if the source IP prefix is reachable via routing table. The interface check is relaxed, since we may have asymmetrical routing.
Control Plane Policing	Various Denial-of-Service Attacks	Prevents abnormally high TCP, MAC and other requests from overwhelming the Switch Control Plane, using CPU rate limiters

Identity 4.0 is a flexible authentication structure, allowing multiple types of devices using diverse authentication mechanisms (802.1x, MAC Authentication Bypass [MAB], and Web based authentication) to connect to the network. Open access mechanisms on the Cisco Catalyst 4500 and 6500 allow unified communication devices to get critical services such as DHCP and DNS before authentication.

Details on Identity 4.0 framework are available at http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/CiscoIBNS-Technical-Review.pdf.

Multidomain Authentication (MDA) allows VoIP devices and a PC/laptop to be connected to the same switchport, as is the case with many businesses. The IP **telephony integration** aspect of identity 4.0 help with CDP Host Disconnect TLV allows PC/laptop supporting either MAB or 802.1x to be moved from one location to another, without ERRDISABLE'ing the switch port or creating a temporary vulnerability, where an attacker can gain access to the switchport. Figure 5 shows different IP telephony-PC move scenarios.

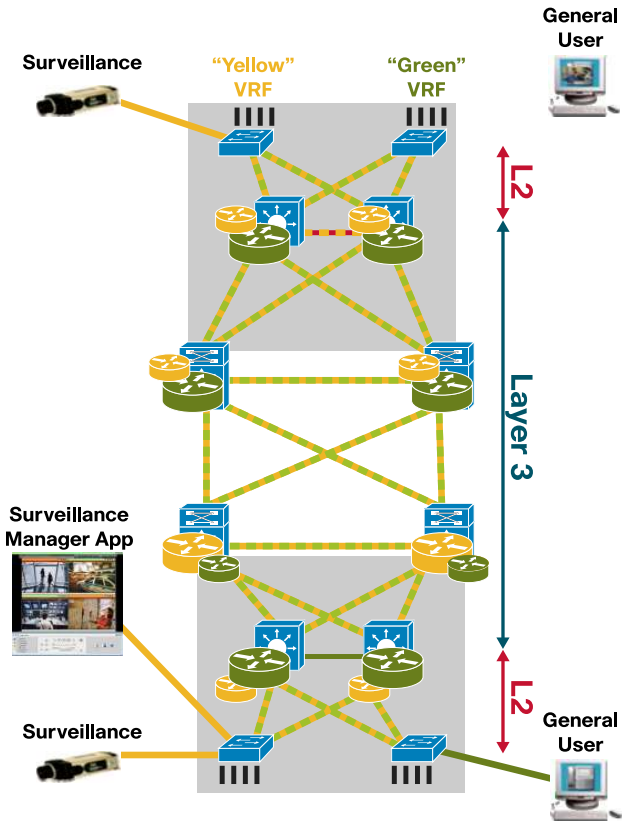
Figure 5. IP-Telephony-PC Integration Move Scenarios



Unified communications segmentation uses segmentation techniques such as VRF-lite to isolate a critical application such as IP surveillance. This could be because of confidentiality requirements. This could also be driven by a need to separate different services, for example, VoIP traffic in a campus could be segmented into a voice VLAN.

Figure 6 shows an example where VRF-lite can be used to isolate IP video surveillance traffic.

Figure 6. Secure Video Segmentation



Conclusion

Businesses are moving toward a collaborative model and using their networks as a platform to enhance unified communications.

In order to achieve this goal, the network should provide end-to-end support for network scalability, nonstop communications, security, and user quality of experience.

For more information, visit http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html and http://www.cisco.com/en/US/products/hw/switches/ps708/index.html.

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.

Printed in USA C11-533069-01 10/11