Branch-WAN Solution Overview

January 27, 2009

Executive Summary

The enterprise business is changing as new types of applications as well as real-time voice and video are being deployed. The communication paradigm is shifting; Web 2.0 collaborative applications are on the rise. Shared workspace, TelePresence, Voice over IP (VoIP), and IPTV create requirements for consistent and enhanced end user experience and guaranteed service levels. As the number of branches continues to increase, the reliable and secure delivery of these evolving services demands a network that can similarly evolve to meet these demands and enable business success.

According to IDC WAN Survey (January 2008), CIO's main objectives are service levels, business relevance, and IT operational expenses. IT professionals require higher network performance, scalability, availability, security, and service capabilities. The Cisco Branch-WAN solution is developed to address these key areas of customer concerns. To meet these requirements, the Branch-WAN solution features scalable and resilient network infrastructure, integrated security, wireless, and application intelligence to provide seamless service capabilities that include Unified Communication, media collaboration, and data/Web 2.0.

Cisco delivers integrated Branch-WAN solution to support a broad set of applications with different requirements from unified communications to transaction-oriented applications. Cisco continues to add best-in-breed functionalities and delivers the *network as the platform*.

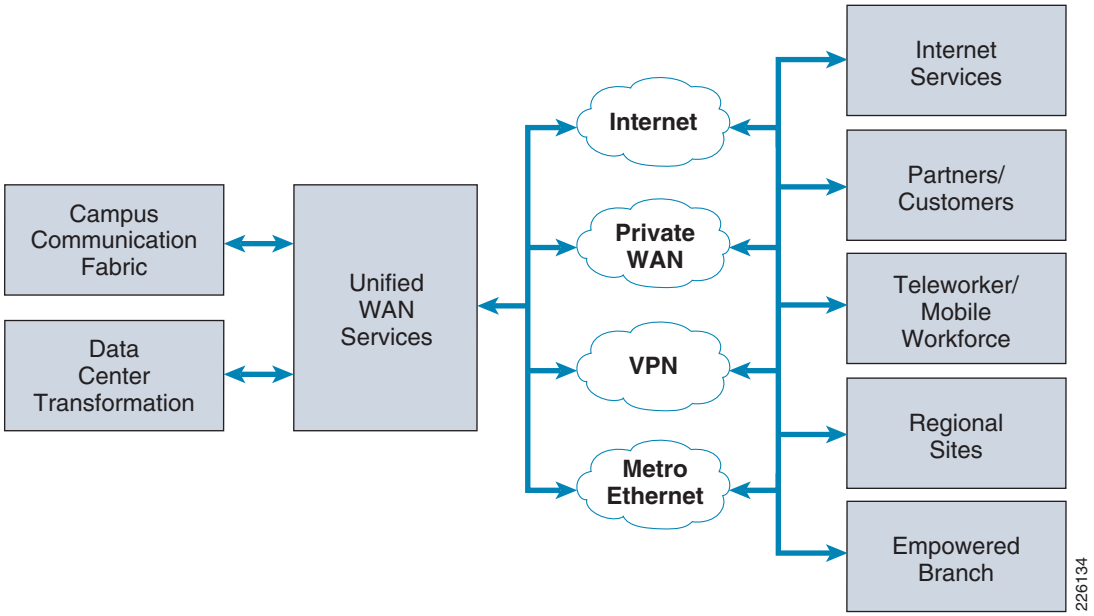
System Overview

Cisco is dedicated to delivering solutions that meet and exceed customers' business and technology requirements by integrating best-of-breed technologies, services, and platforms. The Cisco Branch-WAN Solution is part of a comprehensive approach to providing an end-to-end enterprise network architecture. The Branch-WAN Solution is based on the concept that different portions of the network play different roles in an overall end-to-end architecture. This model is known as *Cisco Places in the Network (PIN)* architecture.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The Cisco PIN architecture addresses the differing requirements for systems design and deployment in the three principal network areas: the campus, the data center, Internet edge, and the Branch-WAN. See Figure 1.

Figure 1 Cisco PIN Architecture

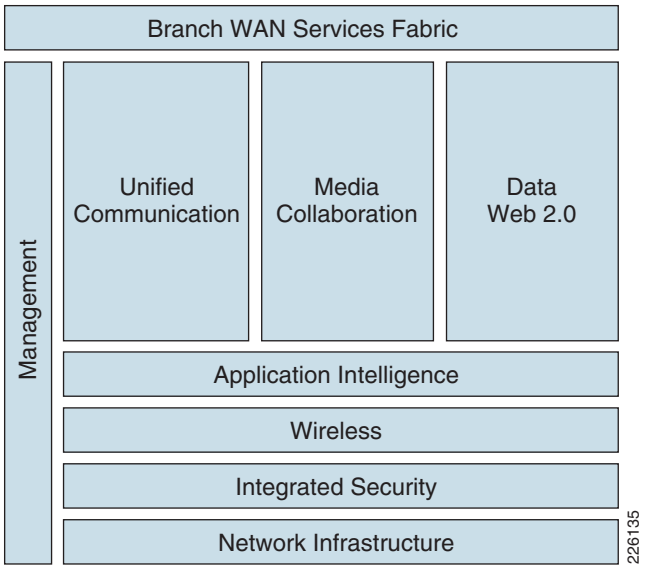


When discussing an enterprise network, it is important to consider that most networks are built from a discreet set of interconnected, architectural elements—each of which has its own requirements. A branch office, for example, may not have the same scalability requirements as a data center, but has a greater need for reduced form-factor devices with high-value integrated services.

The typical corporate campus network offers users high speed and secure network connectivity, Unified Communication services, wireless services, and access to corporate applications and databases. A well engineered network must offer workers at branch sites the same network services as campus workers, to maximize productivity and ensure business objectives are met. The Branch-WAN solution offers an end-to- end system design that delivers a flexible, scalable, and secure network that supports advanced network services for branch office workers.

Figure 2 highlights the framework for the Branch-WAN solution.

Figure 2 Branch-WAN Solution Framework



The Branch-WAN solution shown in Figure 2 has the following layers:

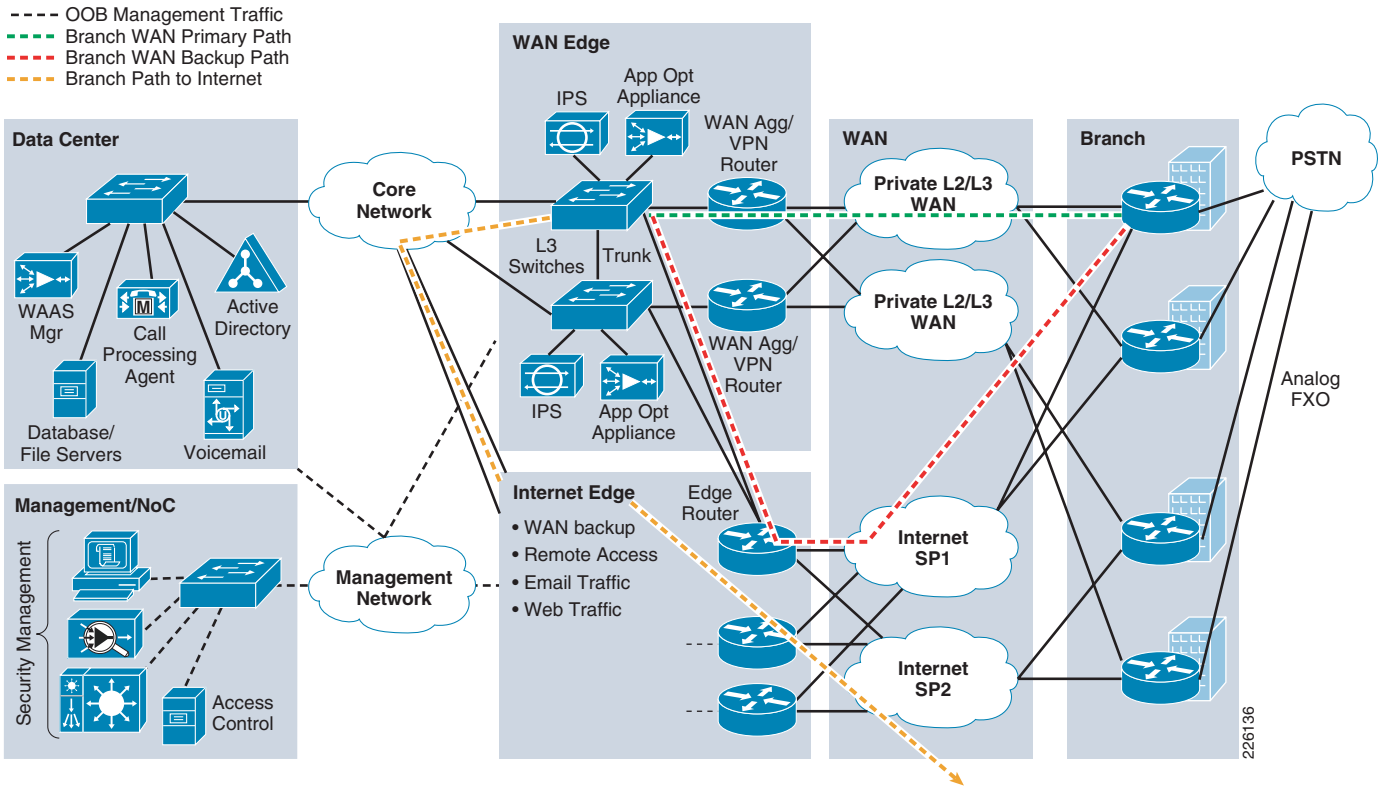
- **Network Infrastructure**—The foundation that provides routing, switching, quality-of-service (QoS), high availability, and other functionalities to ensure that the network is scalable, flexible, and resilient.
- **Integrated Security**—This layer extends the corporate security policy to the branch, providing network infrastructure protection, secure communication, threat mitigation, and network monitoring across both the Branch and WAN PINs.
- **Wireless**—This layer provides user network connectivity anywhere within the enterprise, giving employees greater flexibility, and increased productivity.
- **Application Intelligence**—This layer provides various application optimization techniques using optimization (i.e., TCP flow optimization, data redundancy elimination) and control for application classification and prioritization using QoS. This optimizes use of the WAN bandwidth and, enables branch users to access the same applications as campus users, with similar user experience.
- **Management**—This layer provides the ability to easily provision and monitor the network.

With these layers, it is imperative that unified communication (i.e., Cisco Unified Communication Manager), Media Collaboration (i.e., Cisco Telepresence, IP Video Surveillance, Desktop Video, and Digital Media Systems), and Data Web 2.0 (i.e., collaboration applications) work seamlessly across the Branch-WAN solution.

Branch-WAN Network Architecture

The Branch-WAN is a well designed network architecture (see Figure 3) that provides a flexible, scalable, reliable, and secure network infrastructure that integrates security, unified communications, application intelligence, and wireless.

Figure 3 Branch-WAN Network Architecture



The Branch-WAN network architecture shown in Figure 3 is divided into the following areas:

- WAN Edge
- Branch (the WAN is either Layer 2 or Layer 3 VPN from a service provider)
- Internet Edge
- Data Center
- Management Network Operation Center (NOC)

Each element is designed to work within the end-to-end network as an integrated system.

Network Infrastructure

The network infrastructure layer provides network connectivity and basic network services. The network connectivity defines routing and switching in both the Branch and Campus, as well as managing the Wide Area Network (WAN) links and Virtual Private Networks (VPNs). Basic network services include the following:

- Quality-of-service (QoS)
- Platform, WAN, and VPN redundancy for the WAN Edge
- WAN and VPN redundancy for the branch
- Secure VPN authentication using PKI
- Scalable DMVPN design using SLB

The network infrastructure is the foundation upon which the rest of the network and advanced services are built. Flexibility and scalability are the two key design requirements for network infrastructure. It is important to design a flexible network infrastructure such that advanced network services can be efficiently and seamlessly integrated. It is also very important to design a scalable network infrastructure so that one may easily add more capacity or more branch sites without disrupting the existing network operations.

Branch

The Branch-WAN solution includes two branch topologies. One is a typical small branch with modest WAN connection speed and services integrated into the router for 50 users. The other is a higher performance branch with larger bandwidth WAN connection for 100 users.

Typical Branch Design

The typical small branch design includes a 1.5 Mbps Ethernet private WAN connection. The router terminates the VPN and routing from the central site and implements QoS policy. The router also hosts the following integrated services:

- Security (Firewall, IPS)
- Unified Communications (SRST, FXO / FXS ports)
- Application intelligence

The branch also includes a Layer-2 access switch with the following key features:

- Power-over-Ethernet (PoE)
- DHCP snooping
- Spanning tree
- Class-of-Service (CoS) on access ports
- QoS
- Port security
- Dynamic Address Resolution Protocol (ARP) Inspection

Wireless LAN may be implemented with a router module or standalone controller/switch.

High Performance Branch Design

The high performance branch design includes a 40 Mbps Ethernet private WAN connection. The router terminates the VPN and routing from the central site, and implements the QoS policy. The router hosts the following integrated services:

- Unified Communications services, including local call control, and FXO / FXS ports for direct PSTN connectivity (emergency 911, and backup connectivity)
- Application intelligence
- Security services (Firewall, IPS) are implemented in a separate appliance. This satisfies some customer's needs to separate Network Operations and Security Operations, in addition to delivering enhanced performance.

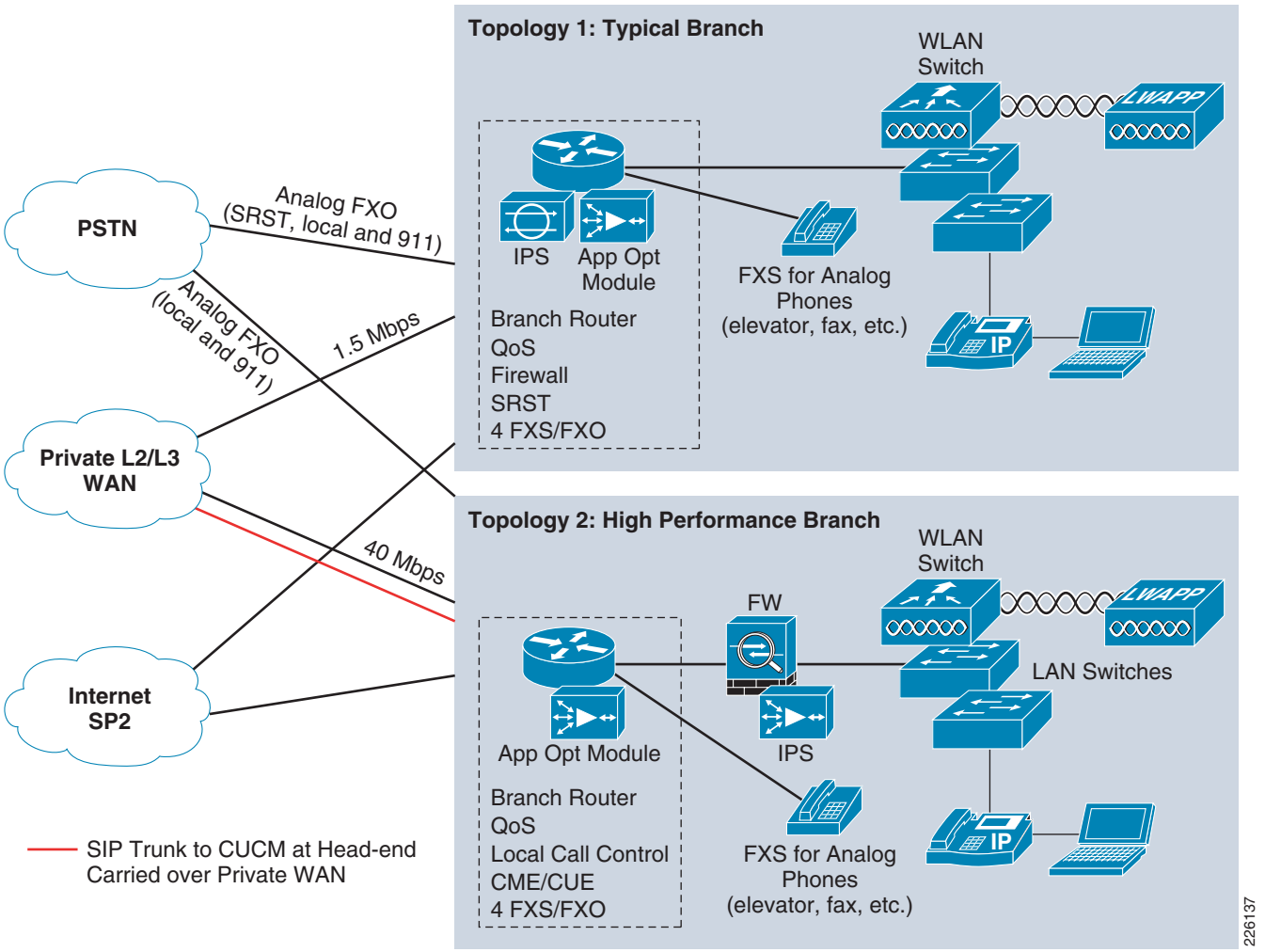
The branch also includes a Layer-2 access switch with the following key features:

- PoE
- DHCP snooping
- Spanning tree
- CoS on access ports
- QoS
- Port security
- Dynamic ARP Inspection

Wireless LAN may be implemented with a router module or standalone controller/switch.

Both branch designs include a backup WAN link over the Internet. The purpose of this link is to provide branch connectivity back to the central campus, if failure occurs in the private WAN connection. All Internet traffic goes through the Internet Edge. All branch traffic goes back to the central site; there is no direct connection from the branch to the Internet (i.e., no split-tunnel). See Figure 4.

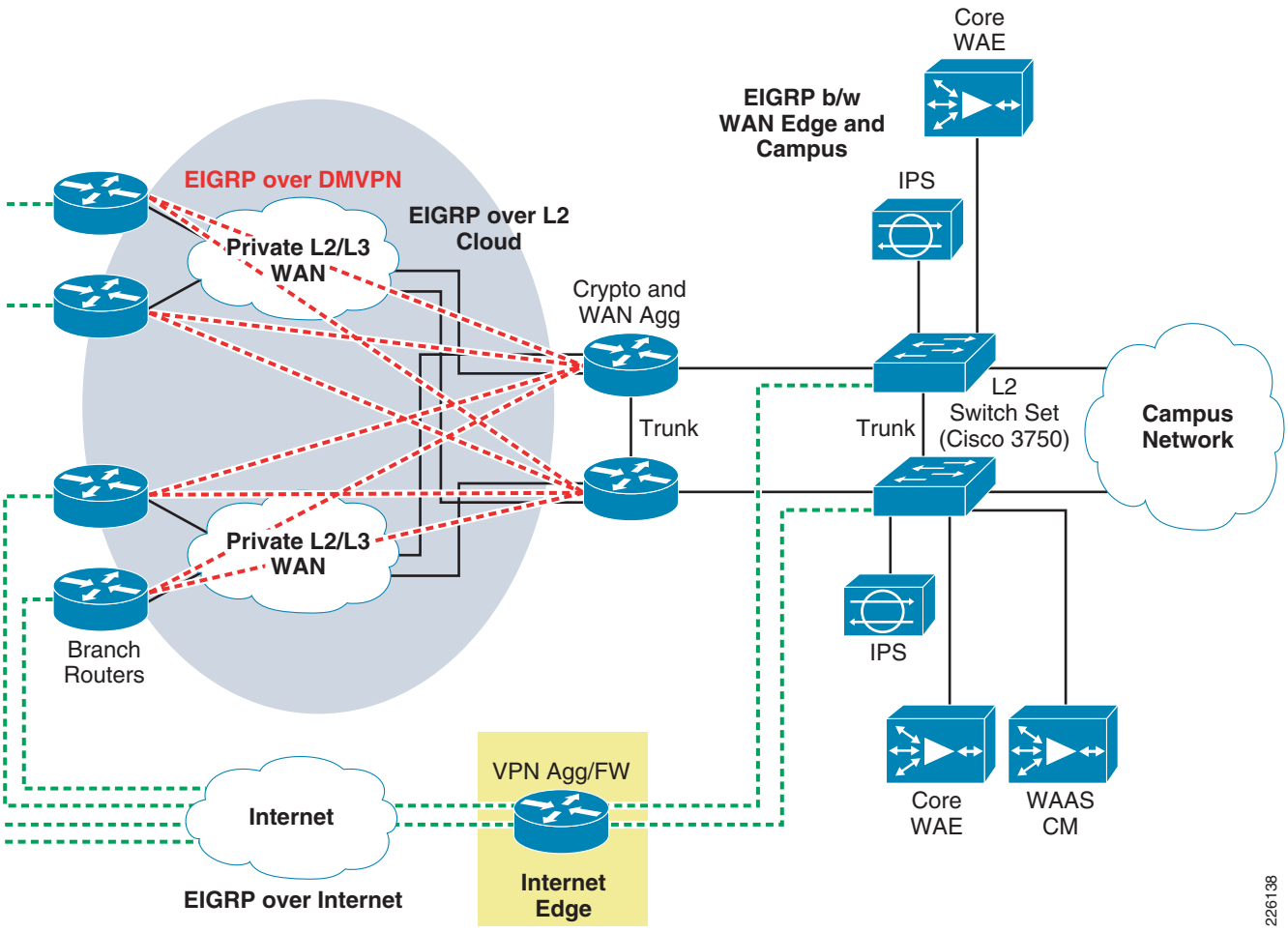
Figure 4 Branch Deployment Designs



WAN Edge

The Branch-WAN solution features Layer 2 or Layer 3 VPNs as the private WAN service. The architecture includes two different service provider (SP) WANs to address cases where an enterprise may need multiple SPs to provide branch connectivity across a large geographic region. The reference architecture (see Figure 5) is designed to support up to 700 branches and it is scalable to more as needed. The headend design includes two WAN routers, each with two-Gigabit Ethernet connections; one to each SP's WAN. It is assumed that half of the branches connect to one SP WAN and the other half connect to the other SP WAN.

Figure 5 WAN Edge Architecture



Dynamic Multipoint Virtual Private Network (DMVPN) dynamically manages the tunnels over the WAN and PKI is used to provide secure establishment as well as revocation. EIGRP routing protocol is run over DMVPN to provide routing between the WAN edge and branches. The WAN aggregation router implements the QoS policies to ensure the WAN edge interfaces, and individual branches do not receive more traffic than they can handle and to prioritize traffic correctly. The WAN edge design uses both platform and link redundancy to provide a high performance, high availability design.

If the private WAN connection fails, the branch connects to the WAN edge via the backup connection through the Internet. The backup WAN connection also runs EIGRP over DMVPN and terminates on the backup VPN/Firewall router in the Internet edge. The Internet edge backup WAN router terminates the WAN, applies QoS policies, and terminates DMVPN.

Services Architecture

Security

Security is critical to businesses being able to collaborate with confidence, whilst using the rich services that have become a fundamental part of business operations. The complex security challenges being faced in this environment demand an integrated, defense-in-depth approach to security that is embedded in an end-to-end solution architecture.

The security services integrated in this phase of the Branch-WAN solution represent the first layers of an integrated, defense-in-depth approach to security, focused on ensuring the availability of network services, as well as the protection of hosts, clients, and their data across the end-to-end architecture. These first layers are fundamental to effective network security, creating a strong foundation on which more advanced methods and techniques can subsequently be built. Knowing where to start and how to implement these first layers is thus critical, but can also be challenging due to the vast range of products and features available.

The security component of the Branch-WAN solution is designed to assist in this endeavor by providing guidelines on the key security objectives to target and the Cisco products and features available to address them, along with implementation guidelines to assist in their design and deployment in production networks.

The key security objectives addressed in this phase of the solution are as follows:

- Harden the network infrastructure.
- Harden each network infrastructure device, secure the routing and switching services, and enforce baseline network security policies.
- Secure communication.
- Encrypt traffic over the WAN and enforce baseline firewall policies at the branch.
- Detect and mitigate threats.
- Deploy endpoint protection on the branch clients and integrate Intrusion Prevention Systems (IPS) into the branch or the corporate headend.
- Monitor the network.
- Enable baseline security operations through the implementation of network telemetry and anomaly detection and correlation tools.

In this phase of the Branch-WAN solution, the branch profile does not offer split-tunneling to permit local Internet access, thus all branch traffic is directed through the corporate headquarters. Consequently, application, content, email, and web security is enforced at the Internet edge. Subsequent phases will address different branch topologies and profiles, along with appropriately modified security guidelines as well as details about how to implement additional layers of security.

The security component of the Branch-WAN solution provides guidance on implementing the first layers of an integrated, defense-in-depth approach to security. The primary focus is on ensuring the availability of network services and the protection of hosts, clients, and their data across the end-to-end architecture.

The tasks being implemented to meet the key security objectives in this phase are shown in Table 1.

Table 1 Primary Security Objectives

Primary Security Objective	Security Focus Area
Harden the Network Infrastructure	• Secure Infrastructure Device Access • Device Resiliency and Survivability • Secure Routing • Baseline Policy Enforcement • Baseline Switching Security
Secure Communication	• Traffic Isolation • Encrypt Data In Motion
Detect and Mitigate Threats	• Endpoint Security • Intrusion Prevention Systems (IPS)
Monitor the network	• Baseline Telemetry • Anomaly Detection and Correlation

These security areas will be addressed and integrated across the baseline network infrastructure and services, as well as for Unified Communications and Wireless LAN (WLAN).

Harden the Network Infrastructure

Hardening the network infrastructure is a fundamental element of network security. The network infrastructure and its services are vulnerable to attack, be it malicious or unintentional, including unauthorized access and a variety of denial-of-service (DoS) attacks. Unless the network infrastructure and its services are secured and resilient, additional security technologies and features are typically ineffective. For example, if a default account and password are active on a network infrastructure device, it is not necessary to mount a sophisticated attack since attackers can simply login to the device and perform whatever actions they choose.

The implementation of this objective requires each network infrastructure device in the end-to-end architecture to be hardened. The key areas to address in order to harden these network infrastructure devices and the critical services they offer are outlined in Table 2, along with the tasks that will be implemented in this phase.

Table 2 Harden Primary Security Objective

Primary Security Objective	Security Focus Area	Implementation Task
Harden the Network Infrastructure	Secure Infrastructure Device Access	• Restrict Device Accessibility • Restrict Login Vulnerability to Dictionary and DoS Attacks • Present Legal Notification • Authenticate Access • Authorize Actions • Enforce session management • Protect Data in Motion and in Transit • Log and Account for all Access
	Device Resiliency and Survivability	• Disable unnecessary services • Restrict Access to the Infrastructure Address Space (ACLs) • Protect Control Plane • Control Switch Content Addressable Memory (CAM) Usage • Redundancy
	Secure Routing	• Restrict Routing Protocol Membership • Control Route Propagation • Log Status Changes
	Baseline Policy Enforcement	• IP Spoofing Protection • Baseline Firewall Policy at Branch Edge
	Baseline Switching Security	• Broadcast domain restriction • ARP and DHCP Spoofing Protection • Spanning Tree Protocol (STP) Security (if needed) • VLAN BCPs

More information on the focus areas outlined above, including detailed information on features available and implementation details, is available in the *Network Security Baseline* guide at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html

Secure Communications

Data in transit on a network is subject to threats such as snooping and data manipulation. When data transits a non-corporate network, such as an SP-owned WAN, the corporate security policy may identify this threat as a security risk to be addressed.

To ensure the confidentiality and integrity of data in transit across the branch WAN, a VPN is implemented, offering both tunneling and encryption. The secure creation and management of this VPN is based on a PKI, discussed in "WAN Edge" section on page 7. Table 3 lists the primary security objective for secured communications.

Table 3 Primary Security Objective for Secure Communications

Primary Security Objective	Security Focus Area	Implementation Task
Secure Communication	• Traffic Isolation • Encrypt Data in Motion	PKI-based VPN over WAN

Detect and Mitigate Threats

The threat environment continues to evolve and, with greater collaboration and eroding network perimeters, a systems approach to threat detection and mitigation is critical. Threat detection and mitigation in this phase of the Branch-WAN solution starts by addressing the two key areas shown in Table 4.

Table 4 Primary Security Objective for Detection and Mitigation Threats

Primary Security Objective	Security Focus Area	Implementation Task
Detect and Mitigate Threats	Endpoint Security	• Host-based signature and behavioral-based anomaly detection and mitigation on branch clients • Host-based IPS on branch clients
	Intrusion Prevention Systems (IPS)	• Network-based IPS either in the branch or at the corporate headend

Monitor the Network

In order to operate and ensure availability of a network, it is critical to have visibility into and awareness of the status of the network and events occurring on it. Without proper monitoring, operational staff are blind to incidents, be they malicious or unintentional.

Monitoring in this phase of the solution starts by addressing the two key areas shown in Table 5.

Table 5 Primary Security Objective for Monitoring the Network

Primary Security Objective	Security Focus Area	Implementation Task
Monitor the network	Baseline Telemetry	• Time Synchronization • System Status Information • CDP Best Common Practices • Syslog • SNMP • ACL Logging • Accounting • Archive Configuration Change Logger
	Anomaly Detection and Correlation	• Centralized end-to-end anomaly detection and correlation tool

Baseline network telemetry is both inexpensive and relatively simple to implement. Coupled with anomaly detection and correlation tools, it provides an effective base for security operations.

Unified Communication Security

Security of the Unified Communications (UC) service involves extending and applying general network security policies, principles and techniques to UC and its related infrastructure and endpoints. The primary security objectives and focus areas for this phase, as outlined in the previous sections, will be extended and applied to the UC service and its related infrastructure and endpoints. The areas that are applicable to UC are shown in Table 6. More advanced UC security features will be integrated in subsequent phases of the solution.

Table 6 Primary UC Security Objective

Primary UC Security Objective	UC Security Focus Area	UC Implementation Task
Harden the Network Infrastructure	• Secure Infrastructure Device Access • Device Resiliency and Survivability • Baseline Policy Enforcement • Baseline Switching Security	• Secure Access to UC Infrastructure • Disable unnecessary services on UC Infrastructure • ACLs for UC Infrastructure Ports • Branch firewall policy updates for UC survivability • Port Security for UC Infrastructure
Secure Communication	• Traffic Isolation	• VLANs for UC service
Detect and Mitigate Threats	• Endpoint Security	• Host-based security on CUCM
Monitor the network	• Baseline Telemetry • Anomaly Detection and Correlation	• Baseline Telemetry for UC Infrastructure

Wireless LAN (WLAN) Security

Security of the WLAN service involves extending and applying general network security policies, principles and techniques to the WLAN and its related infrastructure and endpoints.

The primary security objectives and focus areas for this phase, as outlined in the previous sections, will be extended and applied to the WLAN service and its related infrastructure and endpoints. The areas that are applicable to WLAN are listed in Table 7.

Table 7 WLAN Security Objectives

Primary WLAN Security Objective	WLAN Security Focus Area	WLAN Implementation Task
Harden the Network Infrastructure	• Secure Infrastructure Device Access • Device Resiliency and Survivability • Baseline Policy Enforcement • Baseline Switching Security	• Secure Access to WLAN Infrastructure • Disable unnecessary services on WLAN Infrastructure • ACLs for WLAN Infrastructure Ports • Port Security for WLAN Infrastructure

Table 7 WLAN Security Objectives (continued)

Secure Communication	• Traffic Isolation	• VLANs for WLAN service • LWAPP Access Points • WPA2 with AES for WLAN access
Detect and Mitigate Threats	• Endpoint Security	• Host-based security on WLAN client
	• Intrusion Prevention Systems (IPS)	• Wireless IDS/IPS • Wireless and Network IDS/IPS integration
Monitor the network	• Baseline Telemetry • Anomaly Detection and Correlation	• Baseline Telemetry for WLAN Infrastructure • Integration with end-to-end anomaly detection and correlation tool

Application Intelligence Security

Security of the application enablement service involves extending and applying general network security policies, principles and techniques to application enablement and its related infrastructure. The primary security objectives and focus areas for this phase, as outlined in the previous sections, will be extended and applied to the application enablement service and its related infrastructure. The areas that are applicable to application enablement are identified in Table 8.

Table 8 Application Intelligence Security

Primary Application Enablement Security Objective	Application Enablement Security Focus Area	Application Enablement Implementation Task
Harden the Network Infrastructure	• Secure Infrastructure Device Access • Device Resiliency and Survivability • Baseline Policy Enforcement • Baseline Switching Security	• Secure Access to Application Enablement Infrastructure • Disable unnecessary services on Application Enablement Infrastructure • ACLs for Application Enablement Infrastructure Ports • Port Security for Application Enablement Infrastructure
Monitor the network	• Baseline Telemetry • Anomaly Detection and Correlation	• Baseline Telemetry for Application Enablement Infrastructure

Unified Communications

The Cisco Unified Communications Manager is a scalable, distributed, and highly available enterprise-class IP telephony call-processing system that delivers voice, video, mobility, and presence services to IP phones, media processing devices, VoIP gateways, mobile devices, and multimedia applications. It enhances business productivity and facilitates agility by creating a unified workspace encompassing every combination of applications, devices, networks, and operating systems for up to 30,000 unsecured phones or a maximum of 27,000 secured phones.

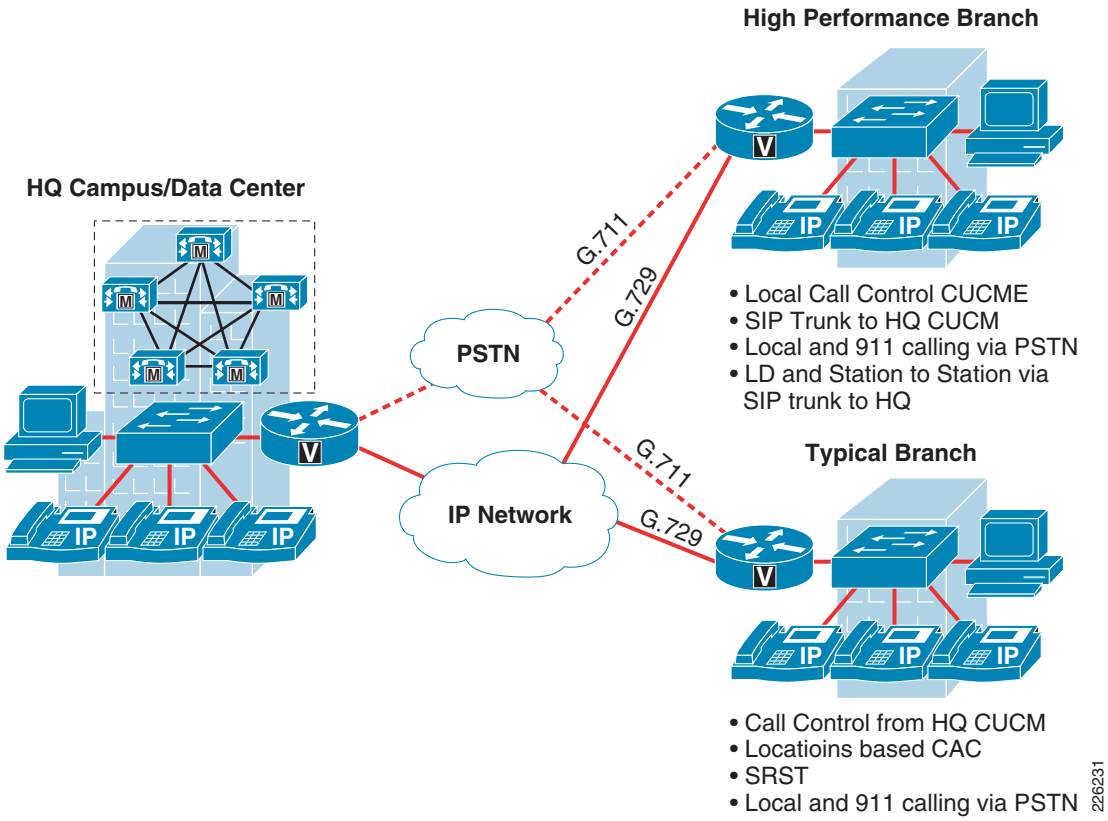
The Unified Communications layer of the Branch-WAN solution provides flexible and scalable unified communications services to branch offices. This is done within two branch models as shown in Table 9.

Table 9 Unified Communications Deployments

Model 1 (Typical Branch)	**Model 2 (High Performance Branch)**
Up to 50 Users	**Up to 100 Users**
1.5 Mbps	40 Mbps
Centralized Call Control with Cisco Unified Communications Manager (CUCM) within the data center of an enterprise campus.	Local call control in the branch using Cisco Unified Communications Manager Express (CUCME).
The branch phones receive all call control over the private WAN and use the local router for Survivable Remote Site Telephony (SRST) when the WAN is unavailable.	SIP trunk over the private WAN to route calls back to the campus (station to station and long distance).

The typical branch communicates with the centralized Unified Communications Manager over the private WAN (see Figure 6). In the event of a WAN failure, call control traffic is *not* sent over the backup Internet WAN due to the inability to guarantee QoS. During WAN failure, the branch router becomes the call control agent using Survivable Remote Site Telephony (SRST). The branch has FXO (analog PSTN) trunks available for emergency 911 phone services and to support limited inbound and outbound traffic while in SRST mode.

Figure 6 UC Deployments



This topology employs location-based Call Admission Control (CAC). Each device (phone) within a branch will be assigned to a location within CUCM. Each location has a finite amount of bandwidth that will be allocated for calls to or from that location. CUCM allows calls in and out of that location as long as the aggregate bandwidth used by all active calls is less than or equal to the configured values. In order to preserve WAN bandwidth, all calls that traverse the WAN will be compressed using the G.729 codec. Calls within the branch and entering or leaving the branch FXO ports will remain at G.711.

The higher performance branch has local call control and voice services integrated into the router. This router will have a SIP trunk to route station to station calls to the head quarter (HQ) campus. Typically, long distance calls would also be aggregated to leave the campus to take advantage of volume long distance agreements. In the event of a WAN failure the SIP trunk will *not* be sent over the back Internet WAN due to the inability to guarantee QoS. The branch has FXO (PSTN) links available for emergency 911 phone services and any calls local to the branch geography. These local trunks would also support limited inbound and outbound traffic in the event of WAN failure. In order to preserve WAN bandwidth, all calls that traverse the WAN will be compressed using the G.729 codec. Calls within the branch and entering or leaving the branch FXO ports will remain at G.711.

Application Intelligence

One of the key design objectives for the Branch-WAN solution is to provide branch network users with the same network capabilities and service levels as corporate users. This can be challenging due to the limited bandwidth, and inherent delay in WAN links. The typical small branch, which has limited WAN bandwidth, can benefit greatly from application intelligence services, such as the following:

- Data Compression
- Transport optimization
- Data redundancy elimination (DRE)

Application intelligence is primarily a branch support service, and covers several PINs. Branch WAN solution focuses on application optimization (see Figure 7). Components for application optimization are:

- WAN optimization/application acceleration using the Cisco Wide Area Application Services (WAAS).
- TCP performance tuning

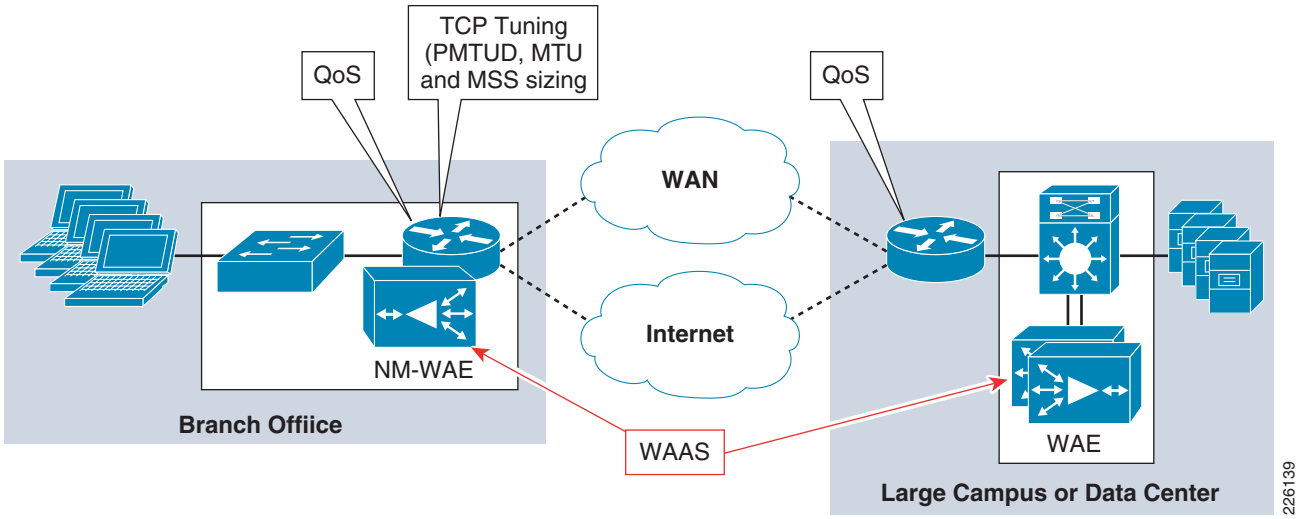
The Application intelligence solution consists of three basic components:

- WAN optimization/application acceleration using WAAS
- application classification and prioritization using QoS
- Best practices in TCP performance tuning along the transmission path between the branch and the WAN

WAAS typically resides at the branch and WAN edge. WAAS is a symmetric solution and cannot be configured solely in one PIN. WAEs must be deployed at both the branch and WAN edge (or data center) PINs in order to function. The Branch-WAN solution focuses on the topology with WAAS Module in branch router and WAE appliance at WAN edge, along with WCCP on WAN edge services routers.

Both branches contain the WAAS network module with WAN interface redundancy to a private WAN as a primary, and an Internet connection as the backup. WAE appliance resides at WAN edge. QoS provides a means of classifying and prioritizing traffic so that the most critical applications receive the highest response. Client performance tuning are additional enhancements to avoid fragmentation and buffer overflows which may slow application response time. Additional classification methods, such as Network-Based Application Recognition (NBAR), will be addressed in subsequent phases, along with monitoring.

Figure 7 Application Intelligence Design



Wireless

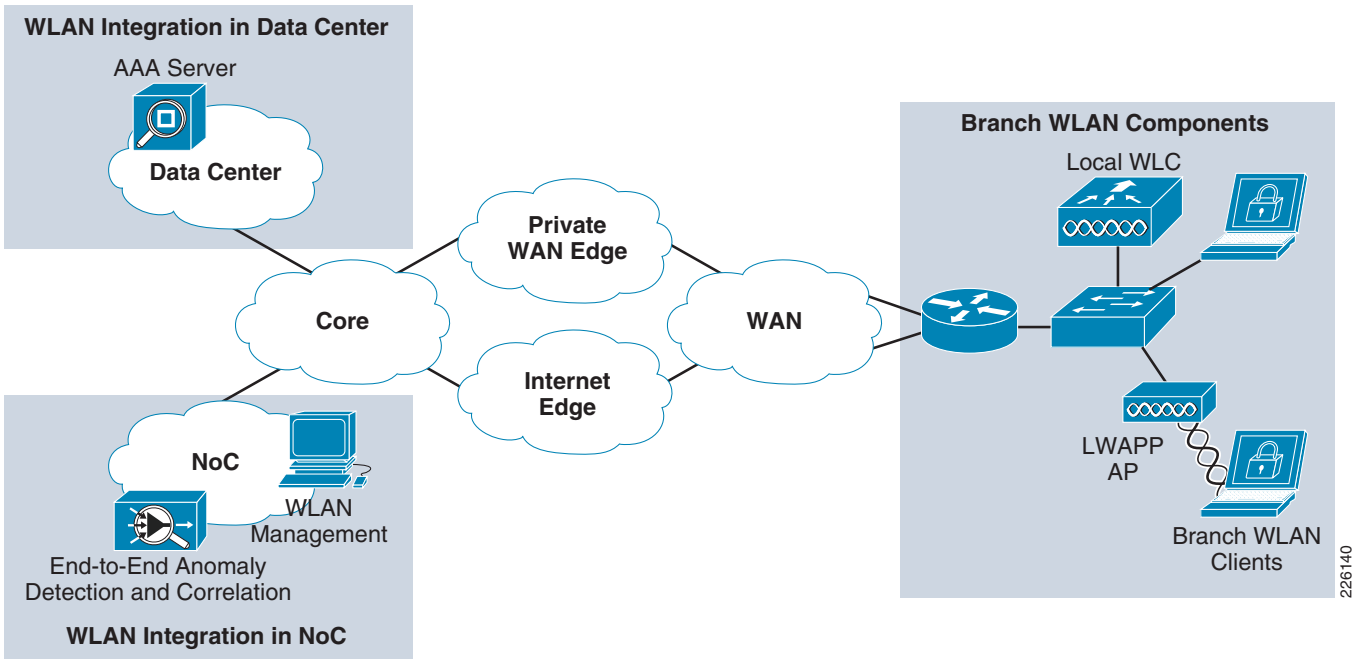
A WLAN provides users with mobility that extends the enterprise network beyond the traditional desk environment, giving employees greater flexibility and increased productivity through pervasive access to network resources and applications.

Integration of the Cisco Unified Wireless Network (UWN) provides branches with these mobility benefits through a cost-effective, scalable, and manageable solution that includes industry-leading security features, as well as unified wired and wireless access.

The WLAN component of the Branch WAN solution presents how to integrate the Cisco UWN into a branch, along with implementation guidelines to assist in its design and deployment in production networks.

The WLAN service of the Branch-WAN solution integrates the Cisco UWN into the end-to-end architecture, as shown in Figure 8.

Figure 8 WLAN Integration for the Branch



The baseline branch WLAN components and the centralized elements with which they are integrated are listed in Table 10.

Table 10 Branch WLAN Components

PIN	WLAN Components
Branch	• Local WLAN Controller (WLC) • LWAPP APs (LAP) • CSSC as 802.1x/EAP supplicant on branch clients
Data Center (DC)	• ACS as AAA server
NoC	• WCS for WLAN management • CS-MARS integration for end-to-end anomaly detection and correlation

For some customers, WLAN security remains a concern and a barrier to deployment for mobility services. Consequently, the Branch-WAN solution will also show how to extend end-to-end network security to the WLAN, using the same defense-in-depth techniques to prevent, detect, and mitigate anomalies. The areas that are addressed are shown in Table 11. See "Security" section on page 9 for more details.

Table 11 WLAN Security Integration

Primary WLAN Security Objective	WLAN Security Focus Area	WLAN Implementation Task
Harden the Network Infrastructure	• Secure Infrastructure Device Access • Device Resiliency and Survivability • Baseline Policy Enforcement • Baseline Switching Security	• Secure Access to WLAN Infrastructure • Disable unnecessary services on WLAN Infrastructure • ACLs for WLAN Infrastructure Ports • Port Security for WLAN Infrastructure
Secure Communication	• Traffic Isolation	• VLANs for WLAN service • LWAPP Access Points • WPA2 with AES for WLAN access
Detect and Mitigate Threats	• Endpoint Security	• Host-based security on WLAN client
	• Intrusion Prevention Systems (IPS)	• Wireless IDS/IPS • Wireless and Network IDS/IPS integration
Monitor the network	• Baseline Telemetry • Anomaly Detection and Correlation	• Baseline Telemetry for WLAN Infrastructure • Integration with end-to-end anomaly detection and correlation tool

Terms and Acronyms

Table 12 lists and defines the terms used throughout this document.

Table 12 Terms and Acronyms used on this Document

Term	Description
AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AF	Assured Forwarding class of service
ASR	Advanced Services Router
CBWFQ	Class-Based Weighted Fair Queue
CDP	Cisco Discovery Protocol
CE	Customer Edge - MPLS Customer Edge Router

Table 12 Terms and Acronyms used on this Document

CoS	Class of Service
CS	Class Selector class of service
DPI	Deep Packet Inspection
DSCP	Differentiated Services Code Point
EF	Expedited Forwarding class of service
GE	Gigabit Ethernet
GLBP	Gateway Load Balancing Protocol
H.323	Call Signaling Standard
HA	High Availability
HSRP	Hot-Standby Routing Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISR	Integrated Services Router
ISSU	In-Service Software Upgrade
LAN	Local Area Network
MAN	Metropolitan Area Network
MPLS	Multi Protocol Label Switching
NSF	Non-Stop Forwarding
OAM	Operations, Administration, and Maintenance
PC	Personal Computer
PfR	Performance Routing
PHB	Per-Hop Behavior
PIN	Places-in-the-Network
PQ	Priority Queue
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RSVP	Resource Reservation Protocol
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SRST	Survivable Remote Site Telephony
SSO	Stateful-Switchover
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UDLD	Uni-Directional Link Detection
VLAN	Virtual Local Area Network

Table 12 Terms and Acronyms used on this Document

WAN	Wide Area Network
XML	Extensible Markup Language

References

- Design Zone

http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html