Secure Network Foundation 1.1 Design Guide for Single Site Deployments

This document provides a simple vision for a smart and secure business where everyday communications are made easier, faster, and more efficient. Cisco partners and resellers can help small-to-medium size businesses leverage the full value of their data networks by deploying reliable secure routers and switches from Cisco Systems that are easily provisioned and managed via the use of simple graphical user interface (GUI) tools. The validated design guidance provided in this document and the validated implementation guidance covered in the *Secure Network Foundation Implementation Guide for Single Site Deployments* (EDCS-517888) provide a verified reference, ensuring that the individual components that the system is composed of work well together.

Note The design described in this document is based on a simplified and cost-effective approach to establishing a secure network foundation as the initial phase of a network evolution. The redundancy in LAN and WAN design is a mandatory attribute of a resilient network. A resilient network is recommended for any network that transports mission-critical traffic. This aspect of LAN and WAN design will be documented in a subsequent release of the validated design. In the meantime, contact your Cisco representative if you have any questions.

Contents

Overview 1
- Solution Components 2

Secure Network Foundation 3
- Local Area Network Design 3
  - Virtual Local Area Networks (VLANs) 4
  - 802.1Q Trunking 4
  - Spanning Tree 4
  - Smartports Roles 5
- Wide Area Network Design 6

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

Layer 3 Design 7
IP Addressing 7
Network Address Translation (NAT) 8
IP Routing 10
Network Time Protocol 10
Quality of Service 11
LAN QoS 11
WAN QoS 11
Integrated Security Design 12
Infrastructure Protection 13
Policy Enforcement 14
Threat Detection and Mitigation 14
Secure Connectivity 15
Appendix A: Additional References 17
Appendix B: Bill of Materials 18

Overview

This design guide explains how to implement a secure data network that supports up to ninety-six (96) users located within a main office and up to ten teleworker/home offices. The main office supports the majority of the users and provides data networking, integrated security, and application services. The optional home office, which supports a single remote user, provides data networking and integrated security services but leverages the main office for application services.

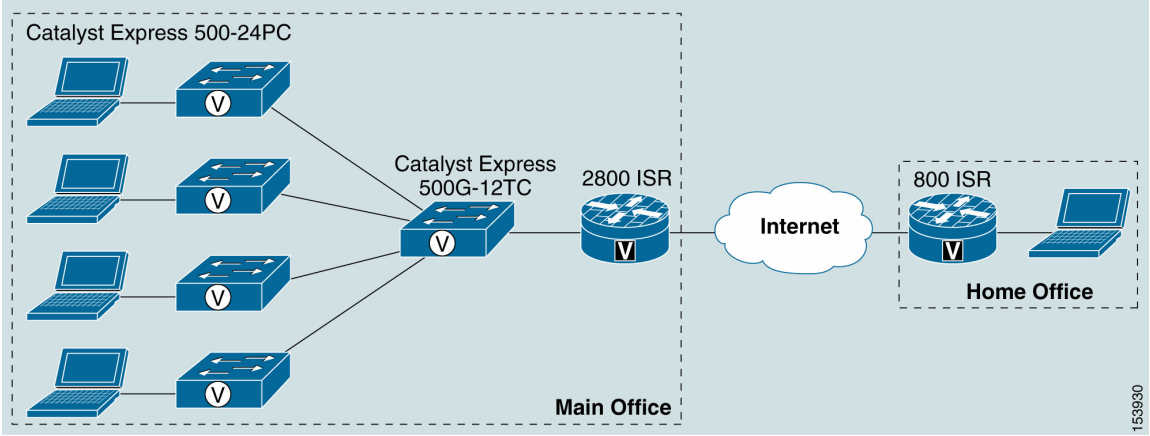
The design provides the following services:

- Wide Area Network (WAN) access
- Local Area Network (LAN) switching
- Integrated security features
- Provisioning and management tools

This design provides a great deal of enhanced functionality. However, it is implemented with the objective of lessening the overall complexity of the system. This enables partners and customers with varying levels of technical knowledge to deploy this design. Additionally, the system is designed with components that support other advanced technologies, such as unified communications and mobility, thereby preserving the customer's initial investment and thus enabling them to evolve their network as needs and new technologies warrant.

Figure 1 shows the network topology of the secure network foundation design for single site deployments.

Figure 1 Secure Network Foundation Design for Single Site Deployments



Solution Components

The main office router platform was selected for this design, based on the number of supported IP phone licenses. This design scales up to 96 users. There are other router platforms that support larger numbers of IP phone licenses and provide the same functionality. Table 1 provides a list of the hardware platforms used to build the validated systems, in addition to the hardware platforms required for larger designs.

Table 1 Hardware Platforms

Number of Users	Router	Aggregation Switch	Access Switch
0-24	Cisco 2801	No	Catalyst Express 500-24PC (1)
25-36	Cisco 2811	Catalyst Express 500G-12TC	Catalyst Express 500-24PC (2)
37-48	Cisco 2821	Catalyst Express 500G-12TC	Catalyst Express 500-24PC (2)
49-96	Cisco 2851	Catalyst Express 500G-12TC	Catalyst Express 500-24PC (3-4)
97-168	Cisco 3825	Catalyst Express 500G-12TC	Catalyst Express 500-24PC (5-7)
169-250	Cisco 3845	Catalyst Express 500G-12TC	Catalyst Express 500-24PC (8-11)

It is important to note that these designs can be built using other hardware components. However, each option has specific considerations. For example, an integrated LAN switch module (which resides within the router) could be used in the larger deployments instead of a separate LAN aggregation switch, but that might require managing two different types of LAN switches. Additionally, a completely different LAN switch, such as the Catalyst 3560 could be used in place of the Catalyst Express 500.

In addition to the hardware platforms listed in Table 1, the Cisco Network Assistant software was used to provision and manage the Catalyst switches used in the design. The Cisco Router and Security Device Manager software was used to provision and manage the Cisco Integrated Services router.

The bill of materials for the validated design described in this document is provided in Appendix B: Bill of Materials, page 18.

Secure Network Foundation

This section describes the secure network foundation design used for the validated single site deployment and explains the features that are implemented to provide the LAN, WAN, and integrated security services.

Local Area Network Design

LAN designs, which can consist of core, distribution, and access layers (core and distribution layers are often collapsed into one layer for smaller deployments), are typically deployed in one of three ways:

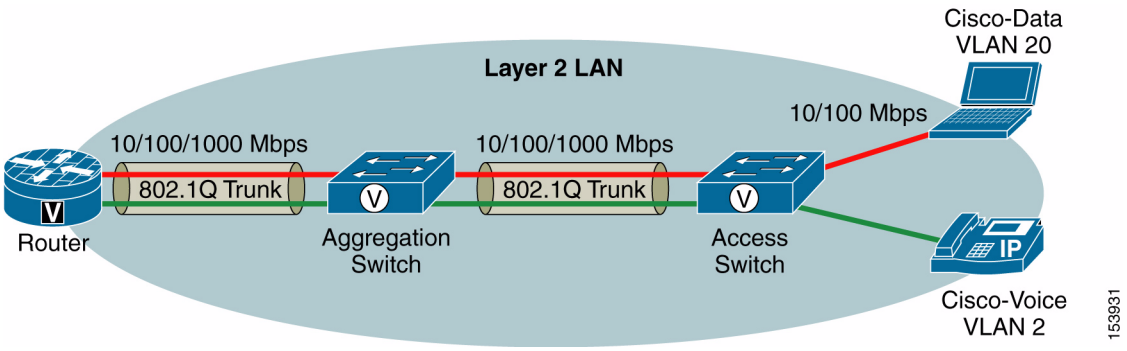
- Layer 2 switching between all layers
- Layer 3 routing between the core and distribution layers, LAN switching between the distribution and access layers
- Layer 3 routing between all layers

Each of these deployment options provides certain benefits. The LAN design used in this system consists only of Layer 2 switching, mainly because of its simplicity. The design has a collapsed core/distribution layer (called aggregation) that does not contain any Spanning Tree Protocol (STP) loops and does not have any redundant LAN components. However. it is important to note that STP is still running on the switches within the system in order to implement some necessary Layer 2 LAN features.

As previously mentioned, the aggregation switch in the design provides the collapsed core and distribution layer functionality. This switch provides 10/100/1000 Mbps connectivity to access layer switches and the router. The aggregation switch is required in this design to aggregate access layer traffic (10/100 Mbps) from PCs, desktops, IP phones, and other devices to the router. For smaller deployments where only one access switch is required, the aggregation switch is unnecessary.

Figure 2 illustrates the Layer 2 characteristics of the LAN design.

Figure 2 Layer 2 LAN Design



Virtual Local Area Networks

Virtual LANs (VLANs) are logical connections that enable groups of devices, such as PCs, desktops, and IP phones, to communicate as if they were connected to the same physical wire even though they might be connected to completely different LAN switches.

In this design, VLANs are used to group voice devices on the Cisco Voice VLAN, which is assigned the value of 2, and data devices on the Cisco Data VLAN, which is assigned the value of 20. This makes it very simple to separate the two types of devices and eases other tasks, such as DHCP server administration and IP addressing. Figure 2 displays the VLAN configuration used in this design.

For more information about VLANs, refer to the VLAN section of the Catalyst Express 500 12.2(25)FY documentation at the following URL:

http://www.cisco.com/en/US/partner/products/ps6545/products_user_guide_chapter09186a0080531ea9.html#wp160367

802.1Q Trunking

In this LAN design, 802.1Q trunking is used between the access and aggregation switches, and between the aggregation switch and router. Trunking enables these physical connections to carry traffic from multiple VLANs. If trunking was not configured, the physical connection could carry traffic from one VLAN only.

When 802.1Q trunks are configured, they require a native VLAN so the devices on both ends of the connection can communicate. In this LAN design, there is an additional VLAN, called the Cisco Control VLAN, which is configured as the native VLAN but it does not carry any data or voice traffic. It is used only for layer 2 control traffic. When deployed in this manner, security risks, such as VLAN hopping and double 802.1Q tagging attacks, are mitigated.

Spanning Tree

Spanning Tree Protocol (STP) is a protocol used by Layer 2 devices that enables them to dynamically discover loops in the network and work around them. As previously mentioned, STP is not an issue in this design because no physical loops exist. However, STP is configured as a precautionary measure to prevent any issues in the event that someone inadvertently connects two switches together with two separate cables.

For more information on STP, refer to the Introduction chapter of the Catalyst Express 500 12.2(25)FY documentation at the following URL:

http://www.cisco.com/en/US/partner/products/ps6545/products_user_guide_chapter09186a0080531d82.html

Smartports Roles

Smartports port roles are Cisco-verified feature templates used to configure LAN switches based on the type of devices, such as desktops, IP phones, servers, routers, switches, and so on that are connected to the switch ports. These templates consistently and reliably configure essential Layer 2, security, power over Ethernet (for IP phones and wireless access points), availability, and Quality of Service (QoS) features with minimal effort and expertise. The templates also streamline the configuration process by reducing redundant command entries and preventing problems caused by switch port misconfiguration.

We recommend port role assignments based on the LAN switch model and port type. These assignments reflect the type of device connections intended for the switch model. Table 2 shows the recommended Smartports roles for the two switch models used in this LAN design.

Table 2 Recommended Smartports Roles

Switch Model	Port Type and Number	Recommended Port Role
WS-CE500-24PC	Fast Ethernet ports 1 to 24	IP phone+desktop
	Gigabit Ethernet or SFP module ports 1 and 2	Switch or router
WS-CE500G-12TC	Gigabit Ethernet ports 1 to 8	Server[1]
	Gigabit Ethernet or SFP module ports 9 to 12	Switch or router

[1] Choose the Router role if one of these ports is connected to a 2800 Series Integrated Services router.

For a complete list of the Smartports roles that are supported on these LAN switch models, refer to the Customization section of the Catalyst Express 500 12.2(25)FY documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/catex500/12225fy/index.htm

Wide Area Network Design

Wide Area Networks (WANs) are built with many technologies and are delivered by different types of service providers. Some WAN access methods provide guaranteed levels of service for bandwidth and quality while others provide best effort services. Table 3 provides a list of both guaranteed and best effort WAN services.

Table 3 WAN Services

Guaranteed Service	Best Effort Service
Asynchronous Transfer Mode (ATM)	Cable
IPSec VPN	Digital Subscriber Line (DSL)
Leased Lines / Frame Relay	Internet
Metro Ethernet	Satellite
Multi-Protocol Label Switching (MPLS)	Wireless

The WAN access method used for this design is based on a DSL or Cable connection. This is a best effort type of service. However, this option is growing in popularity due to the lower monthly price, the ease of installation, and the higher bandwidth available with the service. The 2851 ISR in the main office and the 800 ISR in the home office is connected to a modem device and is provided by a service provider via one of the 10/100/1000 or 10/100 Mbps Ethernet ports. Other WAN access methods, including IPSec, VPN, and Metro Ethernet, are also deployed using one of the router's 10/100/1000 Mbps Ethernet ports.

If a legacy connection, such as a leased line, frame relay, or an ATM connection is used, then a different interface is required on the router.

Layer 3 Design

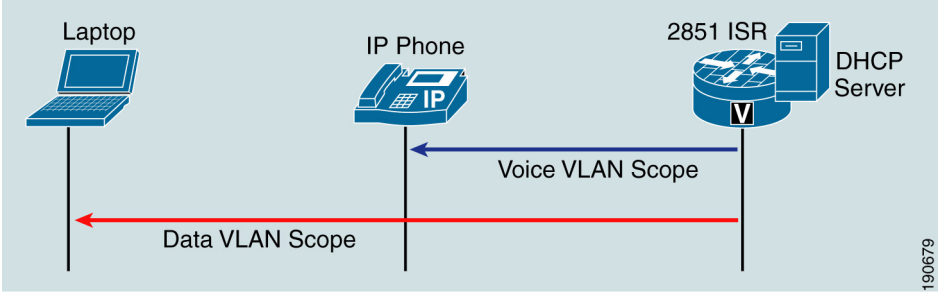
Layer 3 functionality provides the capabilities necessary to forward traffic between Layer 2 switching segments, or VLANs. Layer 3 designs are made up of several components, including IP addressing, network address translation (NAT), and IP routing. This section covers each of these components and describes how they are deployed within the design.

IP Addressing

The IP addressing scheme is integral to the process of routing IP traffic through a network. Each IP address has specific components and follows a basic format. Using IPv4, as in this design, each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts: the network number and the host number. The network number identifies a range of IP addresses and the host number identifies a single device within the network.

IP addressing can be assigned in either a static or dynamic method. If a static method is used, specific addresses are assigned to devices by a network administrator or service provider. This method is recommended for a device that must maintain a consistent address because it is offering services to other devices. An example of this type of device is an e-mail server. If a dynamic method is used, the Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to devices as they are needed. This eases the administration of IP addresses because they do not have to be statically assigned to end points. For example, DHCP enables users to move their devices, such as laptops, to different locations without having to manually change the IP address of the device. DHCP also helps preserve IP addresses because they can be reallocated if an end point no longer needs an IP address. In addition to IP addresses, DHCP can deliver other network information, such as a default gateway, subnet mask, and server addresses. Figure 3 shows the DHCP server running on the router.

Figure 3 DHCP Server Running on the Router



This method is recommended for devices such as PCs and IP phones, where consistent addressing is not required. Often, service providers also use DHCP for DSL and cable services.

This design deploys a combination of static and dynamic IP addressing. It is important to note that the IP addresses are separated into two distinct domains. One domain is managed by the service provider and the other is managed by the customer (or partner). The router's WAN interface resides in the service provider domain and is assigned an IP address, either statically or via DHCP, by the service provider. The router's LAN interfaces, switches, and servers reside in the customer domain and are assigned static IP addresses because other devices rely on them for services such as e-mail, Internet access, and default gateway routing. The remaining end points, including the PCs, desktops, and IP phones, reside in the customer domain are assigned dynamic IP addresses.

The DHCP service is provided by the router in this design. The DHCP server running on the router is configured with the address ranges for the Cisco Data and Cisco Voice VLANs. The DHCP server also provides a default gateway IP address to the end points. For the Cisco Voice VLAN, the DHCP server is configured with option 150 in order to provide the TFTP server address to the voice end points. Finally, the DHCP server is configured with specific addresses that are excluded from the dynamic address range because they are assigned to the router, switches, and servers and must not be assigned to other devices.

If the design includes the optional teleworker/home offices that are connected to the main office via the Internet, an additional DHCP scope is needed for each remote location. This address pool is allocated to the WAN interface of the remote location routers that communicate with the main office via a Virtual Private Network (VPN) connection. The router at the remote location is also configured with a DHCP scope for devices connected to the LAN.

Table 4 provides the IP addressing scheme used in this design.

Table 4 IP Addressing Scheme

Description	IP Addresses	Assignment Method
WAN interface of the main office router	100.100.1.2/24	Dynamic (from SP)
VLAN interface of a home office (optional)	100.100.1.3/24	Dynamic (from SP)
VPN network between main office and home offices (optional)	10.20.51.0/24 - 10.20.51.11/24	Dynamic (from main office router)
Main office Cisco data VLAN	10.20.31.1/24	Static
Main office Cisco voice VLAN	10.20.41.1/24	Static
Main office aggregation switch	10.20.31.2/24	Static
Main office access switches	10.20.31.3/24 - 10.20.31.6/24	Static
Main office servers	10.20.31.7/24 - 10.20.31.15/24	Static
Main office data end points	10.20.31.20/24 - 10.20.31.254/24	Dynamic
Main office voice end points	10.20.41.20/24 - 10.20.41.254/24	Dynamic
Home office end points	10.20.61.2/24-10.20.61.3/24	Dynamic

For more information on IP addressing and DHCP services, refer to the following documents:

- *Cisco IOS 12.4 IP Addressing*:

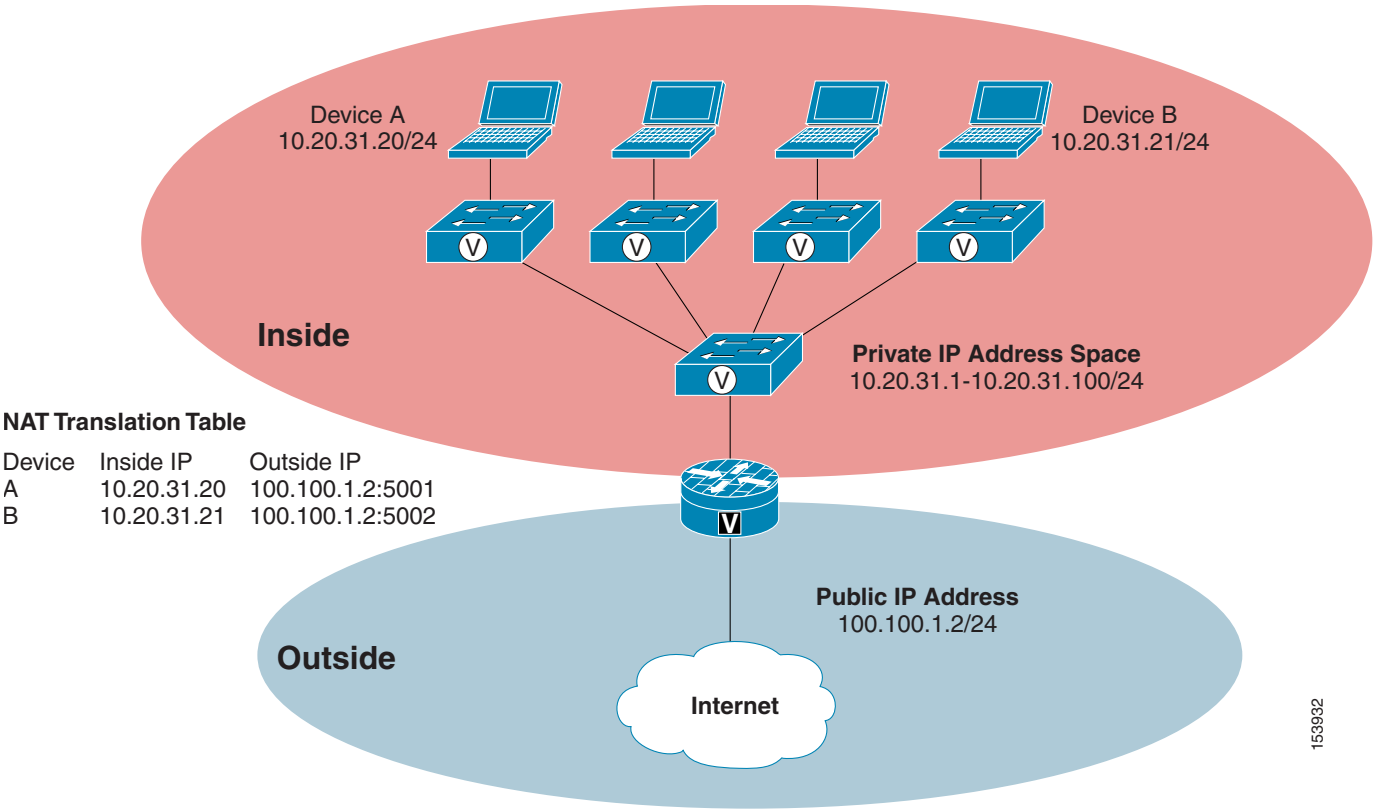
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch05/index.htm
- *Cisco IOS 12.4 DHCP*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch10/index.htm

Network Address Translation

Network Address Translation (NAT) enables devices connected to private (inside) IP networks that use reserved IP addresses (as defined by RFC 1918) to connect to the public (outside) Internet. For example, if a customer uses the IP address range of 10.1.1.0/24 for the devices on their private network, they must use NAT to translate those addresses into an IP address or range of IP addresses that are registered for use on the public Internet so those devices can communicate externally. In essence, NAT simplifies and conserves IP address usage by reducing the customer requirement for a large number of publicly registered IP addresses. Figure 4 provides an example of NAT. NAT typically operates on a router, usually connecting two networks together, and translates the private address space into the public address space.

Figure 4 Network Address Translation



There are three types of NAT:

- Static NAT
- Dynamic NAT
- Overload NAT (often referred to as Port Address Translation, or PAT)

In this design, Overload NAT, or PAT, is used on the main office router because the number of IP addresses provided or purchased from the DSL and cable provider is insufficient to support a one-to-one mapping of inside-to-outside addresses. Typically, the customer is given a single public IP address that is assigned to the WAN interface of the router and is unique on the Internet. When devices on the private network need to access the Internet, the router translates the IP address of the internal device into this external IP address and assign a specific port number to this translation. The port number helps the router identify which translation is mapped to the internal device.

Note If a customer has a Demilitarized Zone (DMZ) where they host servers for external users, then Static NAT is required. There is no DMZ in this design.

If the design includes the optional teleworker/home offices that are connected to the main office via the Internet, NAT does not need to be configured on the home office routers. All traffic sent and received from the teleworker/home office traverses a VPN connection established with the main office router. This includes traffic both internal and external (Internet) traffic.

For more information on NAT, refer to the IOS 12.4 NAT documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hiad_c/ch20/index.htm

IP Routing

IP routing protocols, such as Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) are used in large designs that contain many different networks and multiple entry and exit points to the network from the service providers. These protocols are essential for providing optimum and redundant forwarding paths for IP traffic. However, In smaller deployments, such as the design described in this document, routing protocols are not necessary because they add a layer of provisioning and overhead that is unnecessary.

This design does not have redundant components or paths within the network. There is only one entry and exit point to the service provider. The design has a single Layer 3 device, the router, because the LAN functions completely at Layer 2. In light of these factors, a simple static default route is all that is required on the router to forward traffic to the Internet. For internal traffic, routing protocols are not necessary because the router is directly connected to every Layer 2 VLAN within the design and serves as the default gateway for each VLAN.

If the design includes the optional teleworker/home office, then additional static routes are configured on each router in the network. A static route for each home office is added to the main office router and each home office router contains a single default route to the main office router. The additional static routes ensure that all locations have complete connectivity throughout the entire network.

Network Time Protocol

The Network Time Protocol (NTP) is a standard protocol built on top of TCP/IP that ensures accurate local time synchronization within a network that consists of routers, switches, and other devices. The time is maintained by a master source, which is typically a radio or atomic clock located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NTP is critical in any network because it ensures that all devices contain accurate and synchronized time stamps. This is especially important if the network contains IP communications components, such as Cisco Unified CallManager Express, Cisco Unity Express, and IP phones, all of which require time synchronization to function properly. NTP also ensures that network events and messages, which are captured in error and security logs, traces and system reports, contain accurate time information that helps when troubleshooting and managing any network. Additionally, NTP is important for collecting call detail records and generating billing reports.

The recommendation, if possible, is to reference one of the master clocks located on the Internet as the NTP server within a network. If this is not an option, the router at the main office can be used as the NTP master and the other network devices can reference this router as the NTP server. It is important to note that the router is not the best option for the NTP master because the clock time is not maintained during router reboots and power outages.

Quality of Service

Quality of Service (QoS) is the ability of a network to provide improved service to selected network traffic over various underlying technologies such as Frame Relay, ATM, and Ethernet. QoS delivers improved and more predictable network service by providing the following:

- Dedicated bandwidth support for specific types of traffic
- Improved traffic loss characteristics

- Network congestion avoidance and management techniques
- Traffic shaping to smooth intermittent bursts
- Traffic prioritization across a network

Typically, QoS can be delivered in two areas of a network, the LAN and the WAN.

If voice traffic is sent and received via the WAN connection, then QoS must be configured in order to provide a certain amount of dedicated bandwidth and to prioritize voice over other types of network traffic.

LAN QoS

For this design, QoS in the LAN is dynamically configured via Smartports roles when the templates are assigned to the switch ports. The templates automatically map the Class of Service (CoS) and Differentiated Service Code Point (DSCP) values to specific queues and set the round robin queuing allocations for the switch ports. For example, if the IP Phone + Desktop Smartports role is assigned to a switch port, voice traffic from the IP phone is always prioritized over the data traffic from the connected desktop device. The voice traffic is then sent to one of four available queues within the switch port of the Catalyst Express 500. This queue is provisioned with a specific amount of dedicated bandwidth that is only available to voice traffic. The other three queues share the remaining bandwidth in a round robin fashion for other data traffic.

The other Smartports roles provide QoS based on the type of connected device. For more information, refer to the Customization section of the Catalyst Express 500 12.2(25)FY documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/catex500/12225fy/index.htm

WAN QoS

In most networks, the connection between the aggregation switch and the router is typically 100 or 1000 Mbps while the WAN connection ranges from only 1.5 Mbps to 10 Mbps. This often creates a situation where the router must process more traffic from the LAN than it can send on the WAN. As a result, the WAN interface becomes congested because it cannot handle all of the traffic coming upstream from the LAN. In the absence of QoS on the router, critical traffic, such as routing, VoIP signaling, and real-time voice traffic will suffer. Congestion is not issue with downstream traffic sent from the WAN because the LAN has more than enough bandwidth to handle the incoming traffic.

To prevent congestion on the WAN interface, specific traffic classes must be designed and an adequate amount of bandwidth must be assigned to each class to ensure that all traffic is provided with the necessary quality of service. When VoIP is present in the network, a special Low Latency Queue (LLQ) must also be provisioned. The LLQ is designed not only to provide a certain amount of bandwidth to voice bearer traffic, but also to prioritize voice bearer traffic over other types of traffic using expedited forwarding that helps prevent delay, jitter, and packet retransmissions. Voice signaling traffic requires special treatment as well, but is not as delay-sensitive as the voice bearer traffic. Therefore, voice signaling is allocated to a Class-Based Weighted Fair Queue (CBWFQ) with assured forwarding. Finally, all other data traffic is assigned to the remaining CBWFQ, but is only provided with best effort service. Table 5 lists the traffic classes and bandwidth allocations used on the main office 2851 ISR in this design. If the design includes the optional teleworker/home office, the same parameters are used on 800 ISR.

Table 5 Traffic Classes and Bandwidth Provisioning for the WAN

Traffic Class	Description	IP Precedence	Per Hop Behavior (PHB)	Queueing Type	Bandwidth (BW) Guarantee
Real Time	Voice Bearer	5	EF (Expedited Forwarding)	Priority (PQ)	33-50%
Signaling	Voice Signaling	3	AF (Assured Forwarding)	CBWFQ	10%
Best Effort	Data Traffic	0, 1, 4	Best Effort	CBWFQ	Remaining BW after PQ has been serviced

For more information on QoS, refer to the IOS 12.4 Quality of Service documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hqos_c/index.htm

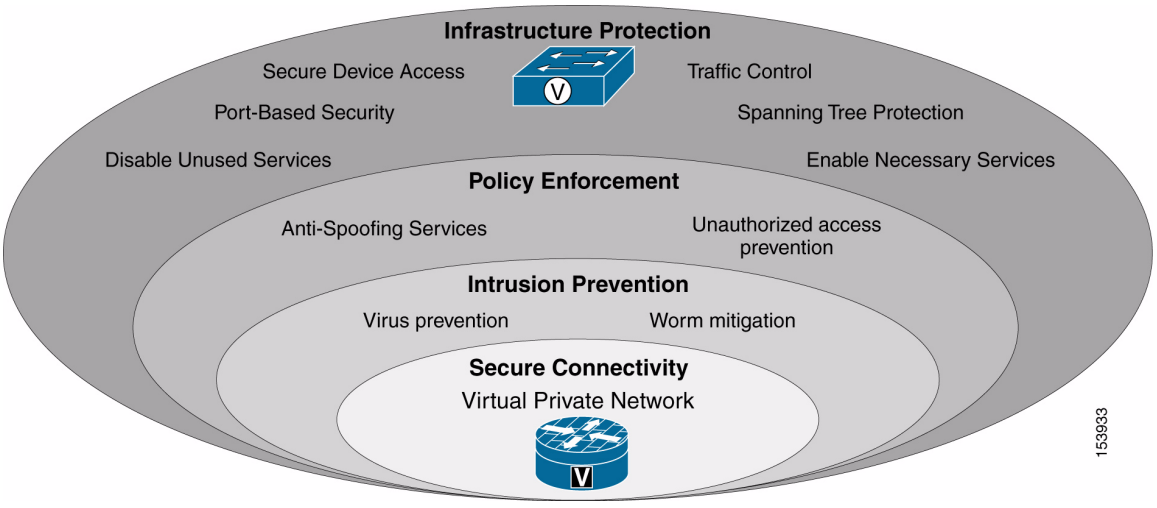
Integrated Security Design

Network security is critical to protecting a business and its resources from various threats, such as viruses, worms, and denial-of-service (DoS) attacks. When a comprehensive security strategy is implemented, protective measures can be implemented to identify, prevent, and mitigate security threats effectively. Integrating these security measures into the network infrastructure components not only helps protect the network but also eliminates the need for standalone security devices. The same functionality can be delivered and managed from existing devices.

This section describes the areas of network security, including infrastructure protection, policy enforcement, threat detection and mitigation, and secure connectivity, all of which have been deployed within this design. Each security function is integrated into the appropriate device within the network. All of the network devices, including the router and switches, provide infrastructure protection services. The router also provides policy enforcement, threat detection and mitigation, and secure connectivity services. Figure 5 shows where the areas of security are deployed in the design.

Note Trust and identity (such as IEEE 802.1X) is not currently implemented in this design.

Figure 5 Areas of Network Security



Infrastructure Protection

The network infrastructure is the foundation on which critical business applications, such as sales tools, voice services, and e-mail access are deployed. As a result, the components of the network infrastructure are often targets of attacks that can directly or indirectly disrupt business operations. In order to ensure the availability of the network, it is critical to implement the security tools and the security best practices that help protect each network component and the infrastructure as a whole.

In this design, the router is configured with infrastructure protection services using the Security Audit feature within the Cisco router and Security Device Manager. The security audit is performed on the router during the initial configuration to ensure that:

- Unused services, such as IP source routing and IP BOOTP server, are disabled.
- Necessary services, such as password encryption and logging, are enabled.
- Secure device access for console, Telnet, SSH, and HTTP connections is enabled.

The switches are configured with infrastructure protection services via Smartports. Each Smartports role configures specific security features based on the connected device. These security features include items such as BPDU guard and filtering, broadcast storm control, and port security.

For more information on the router security audit, refer to the Security Audit chapter of the *Cisco Router and Security Device Manager 2.3 User Guide* at the following URL:

http://www.cisco.com/en/US/partner/products/sw/secursw/ps5318/products_user_guide_chapter09186a0080656061.html

For more information on the Smartports roles, refer to the Customization chapter of the Catalyst Express 500 12.2(25)FY documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/catex500/12225fy/index.htm

Policy Enforcement

Policy enforcement defines the acceptable and unacceptable use of the network resources and other devices attached to the network. For this design, a basic integrated firewall is deployed within the router to uphold policy enforcement. Essentially, the firewall is configured with access and inspection rules on the WAN interface and it does not permit any external traffic into the network unless the traffic arrives via the VPN (optional) or is a reply to a session that was originally sourced from the internal network.

Note There is no DMZ in this design, so an advanced firewall configuration is not required.

For more information on the integrated router firewall, refer to the IOS 12.4 Firewall Overview documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part15/schfirwl.htm

Threat Detection and Mitigation

Threat detection and mitigation refers to the ability of a network device, such as a router or dedicated appliance, to monitor and inspect traffic as it traverses a network, to detect suspicious activity, and respond by mitigating the threat before network security can be compromised. These network devices accomplish this by referring to a signature definition file that is loaded onto the device. This file contains a list of signatures and their definitions that are used to match suspicious traffic.

After the traffic is identified, the network device can perform one of more of the following actions based on its configuration:

- Send an alarm to a Syslog server or a centralized management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

In this design, threat detection and mitigation services are deployed in the router with integrated intrusion prevention services (IPS). IPS is configured on both the WAN and LAN interfaces of the router in order to detect and prevent external and internal attacks. The router performs the default actions as defined by the signature file within the device. The signature file used in this design is the 256MB.sdf, which contains approximately 500 signatures.

Note The pre-built 256MB.sdf signature file from Cisco, which contains approximately 500 signatures, is used in this design for the 2851 ISR main office router. If the router is running other services in addition to those covered in this document, such as CallManager Express and Unity Express for IP communications, it might be necessary to remove signatures from the 256MB.sdf file or use a different (preferably smaller) custom signature file to reduce the impact of IPS on the CPU. Cisco also provides a smaller pre-built signature file, 128MB.sdf, which contains approximately 300 signatures.

It is important to understand that IPS deployments require ongoing management and maintenance. Depending on the customer environment, signature tuning might need to be performed. The signature files within the router need to be updated periodically to ensure that the file contains the latest signatures. Additionally, some form of logging or monitoring is needed to understand if and when attacks are occurring in the network.

For more information on the integrated intrusion prevention system, refer to the IOS 12.4 Configuring Cisco IOS Intrusion Prevention System (IPS) documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part15/sec_ips.htm#wp1110304

For more information on IOS IPS and the signature definition files, refer to the *IOS IPS Deployment Guide* at the following URL:

http://www.cisco.com/en/US/partner/products/ps6634/products_white_paper0900aecd80327257.shtml

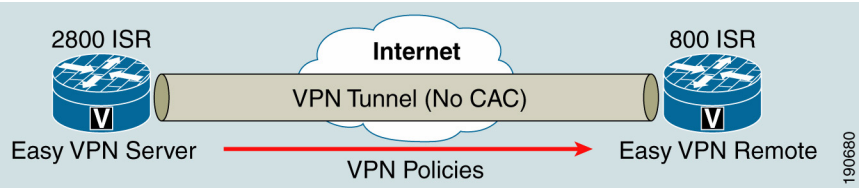
Secure Connectivity

Secure connectivity provides measures to protect against the interception and alteration of information being transported within untrusted environments. The objective is to ensure the confidentiality of the information. VPNs can be used to provide secure connectivity because they help extend the network from a main office to branch offices, home offices, and mobile workers.

VPNs enable IP traffic to travel securely over a public IP network, such as the Internet, by encrypting all of the traffic from one network to another or from one device to another. To encrypt the information, protocols, such as the Digital Encryption Standard or Advanced Encryption Standard, are employed. In addition to encryption, other security features are used to build VPNs. Authentication mechanisms, such as pre-shared keys or RSA signatures, are used to authenticate each side of the VPN tunnel and hash algorithms, such as Message Digest 5 (MD5) and Secure Hash Algorithm (SHA), are used to authenticate the data sent within the tunnel. Together, these security features form secure tunnels that help ensure voice and data privacy and authenticity.

In addition to the protocols that a VPN is comprised of, there are also several different types of VPNs, including site-to-site IPSec VPNs, Dynamic Multi-point IPSec VPNs, Easy VPNs with IPSec, and Secure Socket Layer (SSL) VPNs. Each option provides its own set of benefits for the appropriate deployment. For this design, EasyVPN is used for the optional teleworker/small office because it simplifies the deployment by centralizing the management of all devices to ensure that consistent policies are used and to ease the administration of remote devices. There are two components with Easy VPN, a server and remote. The server runs on the router at the main office and delivers the VPN policies to the remote devices. The remote runs on a router or software-based VPN client and receives the VPN policies from the server which minimizes the configuration requirements in remote home offices and mobile locations. Figure 6 shows the components of the Easy VPN deployment.

Figure 6 Easy VPN



The Easy VPN deployment used in this design is configured with the parameters outlined in Table 6. The recommendations address the Internet Key Exchange (IKE) protocol, which is a key management standard used in conjunction with the IPSec standard, and IPSec, which is a framework of open standards that provides security for transmission of sensitive information over unprotected networks, such as the Internet.

Table 6 IKE & IPSec Protocol Recommendations

Function	IKE	IPSec
Encryption	AES with 128-bit or higher	AES with 128-bit or higher
Hash Algorithm	SHA	SHA
Authentication	Pre-shared keys (strong)	NA
Group	Diffie-Hellman group 5	NA
Lifetime	86,400 seconds	NA
Encapsulation	NA	Encapsulating Security Payload

The recommendations listed in this section provide an ideal scenario. It is important that any partner or customer compare these recommendations to an existing company security policy before implementing them. It is also important to determine whether the routers in the network can support the recommendations. It might be necessary to adjust the recommendations based on the strongest common denominator or supported feature set, which might be dictated by the oldest router in the network. Additionally, it is important to determine whether software clients, such as the Cisco VPN Client, support the recommendations.

For more information on Easy VPN Server and Easy VPN Remote, refer to the IOS 12.4 Configuration documentation at the following URLs:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part17/ch10/hunity.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part17/ch10/hezvpnr.htm

Appendix A: Additional References

For more information, refer to the following documents:

- *Downloading and Installing Cisco Router and Security Device Manager:*

  http://www.cisco.com/en/US/partner/products/sw/secursw/ps5318/prod_installation_guide09186a00803e4727.html

- *Cisco Router and Security Device Manager 2.3 User Guide*:

  http://www.cisco.com/en/US/partner/products/sw/secursw/ps5318/products_user_guide_book09186a0080645da3.html

- *Getting Started Guide for the Catalyst Express 500 Switches:*

  http://www.cisco.com/en/US/partner/products/ps6545/products_getting_started_guide09186a0080524310.html

- *Getting Started with CNA 3.1:*

  http://www.cisco.com/en/US/partner/products/ps5931/products_installation_guide_book09186a008051a512.html

- *Infrastructure Protection on Cisco IOS Software-Based Platforms:*

  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_white_paper0900aecd802b8f21.shtml

- RFC 1918: *Address Allocation for Private Internets:*

  http://www.ietf.org/rfc/rfc1918.txt

Appendix B: Bill of Materials

This section provides the bill of materials used to build the validated system described in this design guide. Table 7 provides the bill of materials to support up to 96 users. Table 7 through Table 10 provide bills of materials for smaller design options.

Table 7 Bill of Materials for the 96 User System

Description	Part Number	Software
Cisco 2851 Integrated Services router	CISCO2851 (Advanced IP Services IOS)	12.4(3b)
Catalyst Express 500G-12TC	WS-CE500-12TC	12.2(25)FY
Catalyst Express 500-24PC	WS-CE500-24PC (4)	12.2(25)FY
Cisco Router and Security Device Manger	ROUTER-SDM	2.3
Cisco Network Assistant		3.1

Table 8 Bill of Materials for the 48 User System

Description	Part Number	Software
Cisco 2821 Integrated Services Router	CISCO2851 (Advanced IP Services IOS)	12.4(9)T
Catalyst Express 500G-12TC	WS-CE500-12TC	12.2(25)FY
Catalyst Express 500-24PC	WS-CE500-24PC (2)	12.2(25)FY
Cisco 871 Integrated Services Router	CISCO871-K9	12.4(9)T
Cisco Router & Security Device Manger	ROUTER-SDM	2.3
Cisco Network Assistant		3.1

Table 9 Bill of Materials for the 36 User System

Description	Part Number	Software
Cisco 2811 Integrated Services Router	CISCO2851 (Advanced IP Services IOS)	12.4(9)T
Catalyst Express 500G-12TC	WS-CE500-12TC	12.2(25)FY
Catalyst Express 500-24PC	WS-CE500-24PC (2)	12.2(25)FY
Cisco 871 Integrated Services Router	CISCO871-K9	12.4(9)T
Cisco Router & Security Device Manger	ROUTER-SDM	2.3
Cisco Network Assistant		3.1

Table 10 Bill of Materials for the 24 User System

Description	Part Number	Software
Cisco 2851 Integrated Services Router	CISCO2851 (Advanced IP Services IOS)	12.4(9)T
Catalyst Express 500-24PC	WS-CE500-24PC	12.2(25)FY
Cisco 871 Integrated Services Router	CISCO871-K9	12.4(9)T
Cisco Router & Security Device Manger	ROUTER-SDM	2.3
Cisco Network Assistant		3.1