Secure Network Foundation Implementation 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 use this guide to help small to medium size businesses (SMBs) leverage the full value of their data networks by deploying reliable secure routers and switches from Cisco Systems, which are easily provisioned and managed via the use of simple graphical user interface (GUI) tools. The validated implementation guidance provided in this document and the validated design guidance contained in the *Secure Network Foundation Design Guide for Single Site Deployments* provide verification that the individual components that the system is comprised of work together as designed.

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, targeted for Q1FY07. In the meantime, contact your Cisco representative if you have any questions.

Contents

CISCO SYSTEMS

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

Introduction

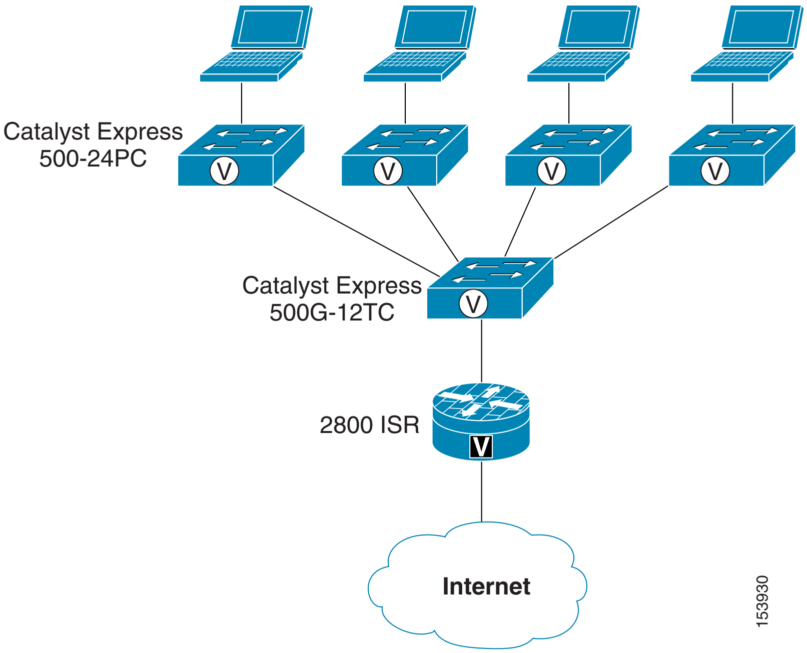
This document describes how to deploy a secure network foundation that supports up to 96 users in a single location. The system provides the following services:

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

The system provides a great deal of enhanced functionality for small and medium businesses (SMBs). However, this functionality is implemented in a very simplistic manner in order to lessen the overall complexity. Additionally, the system is implemented with components that can 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 provides a topology diagram of the secure network foundation system for single site deployments.

Figure 1 Secure Network Foundation System for Single Site Deployments



Solution Components

The validated system described in this document supports up to 96 users. Table 1 provides a list of the hardware platforms used to build this system and also lists the required components for other systems that support a smaller number of users.

Table 1 Hardware Platforms

Number of Users[1]	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)

[1] The Maximum User information is based on the number of IP phones that each router platform supports; this guideline helps partners, resellers and customers plan accordingly for the future.

It is important to note that these systems can be built with other hardware components. However, each option has specific considerations. For example, an integrated LAN switch module (which resides in the router) could be used in the 0-24 user deployment instead of a separate LAN access switch, but that might require a different 2800 series router. As another example, an integrated LAN switch module (which resides in the router) could be used in the 25-36, 37-48, or 49-96 user deployments instead of a separate LAN aggregation switch, but that would require managing two different types of LAN switches.

Refer to Bill of Materials, page 25 for the bill of materials used for the validated design described in this document.

Secure Network Foundation

This section describes the process used to implement the secure network foundation system for single site deployments. For a detailed explanation of the technologies and features deployed in the system, refer to the *Secure Network Foundation Design Guide for Single Site Deployments*.

Cisco 2851 Integrated Services Router

The Cisco 2851 Integrated Services router (ISR) deployed in this system provides several services, including:

- WAN access
- LAN connectivity
- IP routing and addressing
- Integrated security

All of these services are configured using the Cisco Router and Security Device Manager (SDM) web interface tool. This tool reduces the need for extensive Cisco command line interface (CLI) knowledge and expedites the overall implementation process. The following sections provide the steps used to configure the Cisco 2851 ISR.

Note When configuring the router for the first time, it is important to connect to the router from the LAN interface and not the WAN interface because the firewall configuration will block access on the WAN interface when complete.

Refer to the following documents for instructions on how to use the Cisco Router and Security Device Manager,

Downloading and Installing the Cisco Router and Security Device Manager at the following URL:

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

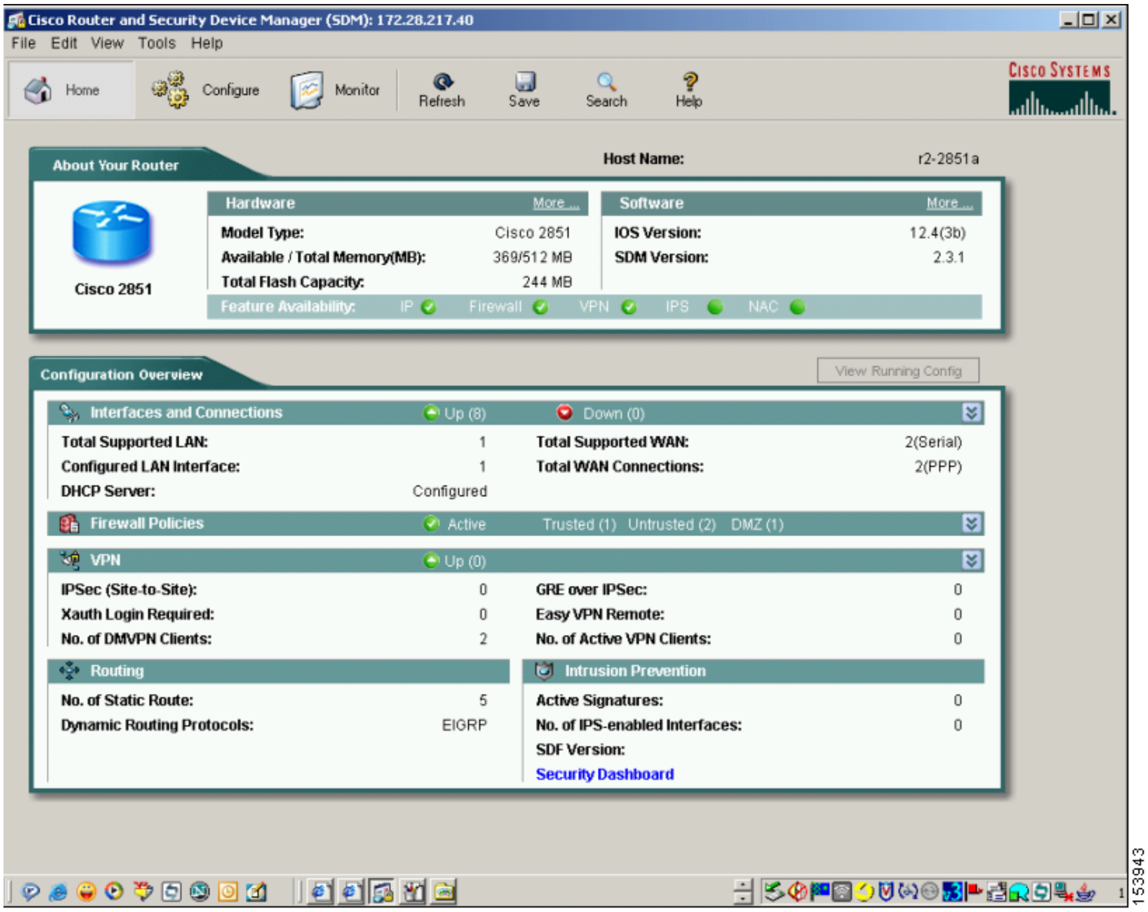
Cisco Router and Security Device Manager 2.3 User Guide at the following URL:

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

Note Quality of Service (QoS) is not explicitly configured on the router because no delay-sensitive traffic, such as voice or video, is sent over the WAN connection.

Figure 2 shows the Security Device Manager (SDM) web interface that you use to configure the router.

Figure 2 SDM Web Interface Window



About Your Router

Host Name: r2-2851a

Hardware (More ...)

Model Type: Cisco 2851
Available / Total Memory(MB): 369/512 MB
Total Flash Capacity: 244 MB

Software (More ...)

IOS Version: 12.4(3b)
SDM Version: 2.3.1

Feature Availability: IP ✓ Firewall ✓ VPN ✓ IPS ● NAC ●

Configuration Overview

Interfaces and Connections — Up (8) — Down (0)

Total Supported LAN:	1	Total Supported WAN:	2(Serial)
Configured LAN Interface:	1	Total WAN Connections:	2(PPP)
DHCP Server:	Configured		

Firewall Policies — Active — Trusted (1) Untrusted (2) DMZ (1)

VPN — Up (0)

IPSec (Site-to-Site):	0	GRE over IPSec:	0
Xauth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	2	No. of Active VPN Clients:	0

Routing

No. of Static Route:	5
Dynamic Routing Protocols:	EIGRP

Intrusion Prevention

Active Signatures:	0
No. of IPS-enabled Interfaces:	0
SDF Version:	

Security Dashboard

Configuring Local Area Networking

Perform the following steps to configure Local Area Networking.

Step 1 From the Main menu, click **Configure** and choose **Interfaces & Connections** from the Task pane.

Step 2 Choose **Ethernet LAN** and click **Create New Connection**.

The Layer 3 Ethernet Interface Configuration Wizard opens.

Step 3 Click **Next**.

Step 4 For an Ethernet configuration, choose **Configure this interface for 802.1Q trunking**. For an 802.1Q configuration, enter the VLAN ID for the Cisco-Data VLAN and place a check mark in the **Native VLAN** check box.

Step 5 Click **Next**.

Step 6 Enter the IP address and subnet mask designated for this interface. For example, the LAN interface should be configured with a private, or reserved, IP address, such as 10.20.31.1/24. Click **Next**.

Step 7 For DHCP Server, choose **Yes** to enable the DHCP server on the LAN interface and click **Next**.

Configuring DHCP Options

Step 1 For DHCP options, enter the following:

- **a.** DHCP pool name.
- **b.** Starting and ending IP addresses for the DHCP pool and the subnet mask; the IP address range is part of the same network configured on the LAN interface (remember to exclude statically assigned IP addresses used for switches, servers, and so on, from the DHCP pool).
- **c.** Default router IP address.
- **d.** Items, such as addresses for the DNS and WINS servers and the domain name, are optional (this information may be assigned by the service provider).

Step 2 In the summary window, review the options and click **Finish**.

Step 3 After the configuration is delivered to the router, click **OK**.

Configuring Additional Logical Interfaces

Perform the following steps to add additional logical interfaces, such as the Cisco-Voice VLAN.

Step 1 Choose the LAN interface that you configured in the previous procedure and click **Add**.

Step 2 Choose **New Logical Interface** and choose **Subinterface**.

Step 3 For Connection, enter the VLAN ID, IP address, and subnet mask for the interface. For example, the LAN interface should be configured with a private, or reserved, IP address, such as 10.20.41.1/24.

Step 4 Click **OK**.

Step 5 In the summary window, review the options and click **Finish**.

Step 6 After the configuration is delivered to the router, click **OK**.

Configuring a DHCP Server for the Additional Logical Interface

Perform the following steps to configure a DHCP server for this additional logical interface.

Step 1 Click **Additional Tasks** in the Tasks pane.

Step 2 Open the DHCP folder, choose the **DHCP Pools** option and click **Add**.

Step 3 Enter the following:

- **a.** DHCP pool name.
- **b.** Starting and ending IP addresses for the DHCP pool and the subnet mask; the IP address range is part of the same network configured on the LAN interface (remember to exclude statically assigned IP addresses used for switches, servers, and so on, from the DHCP pool).
- **c.** Default router IP address.
- **d.** Items, such as addresses for the DNS and WINS servers and the domain name, are optional (this information might be assigned by the service provider).

Step 4 After the configuration is delivered to the router, click **OK**.

Configuring Wide Area Networking

Perform the following steps to configure Wide Area Networking.

Step 1 From the Main menu, click **Configure** and choose **Interfaces & Connections** from the Task pane.

Step 2 Choose **Ethernet (PPoE or unencapsulated routing)** and click **Create New Connection**.

The Ethernet WAN Configuration Wizard opens. Click **Next**.

Step 3 For Encapsulation, click **Next** (if the connection was DSL instead of cable, choose to enable PPoE).

Step 4 For the IP Address, choose the **Dynamic** option (choose **Static** if service provide assigns a specific IP address). Click **Next**.

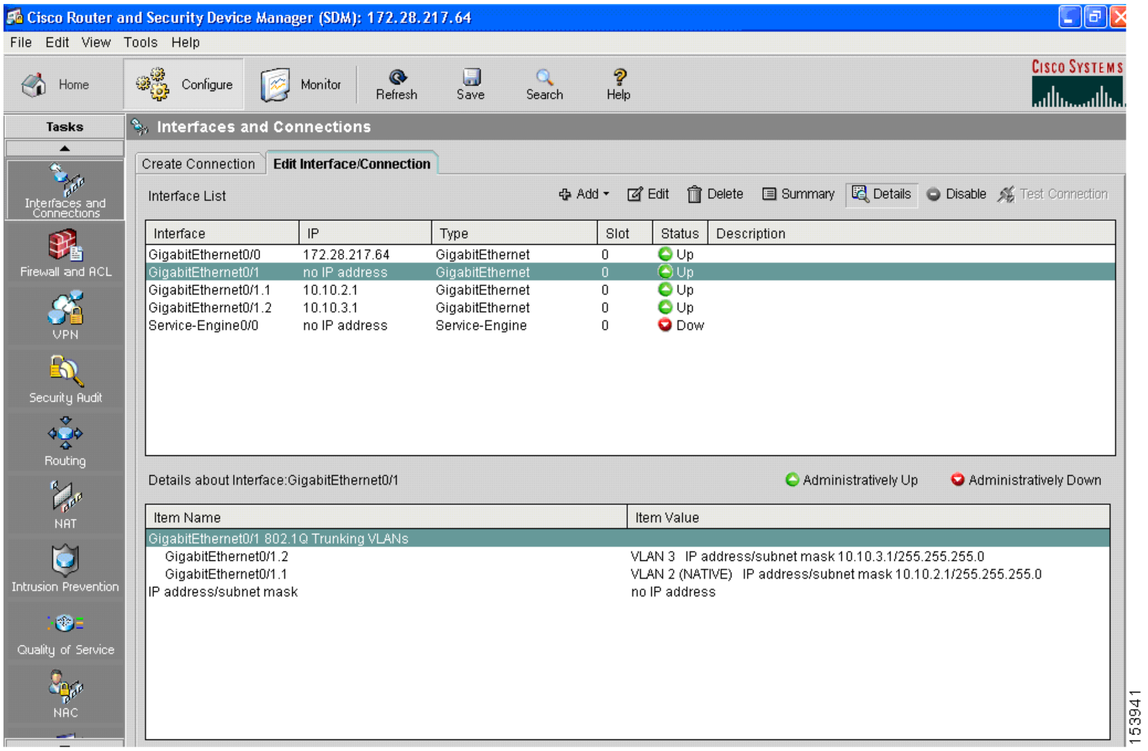
Step 5 For Advanced Options, do not place a check mark in the PAT check box at this time; this will be done later. Click **Next**.

Step 6 In the summary window, review the options and click **Finish**.

Step 7 After the configuration is delivered to the router, click **OK**.

Figure 3 shows the Interfaces and Connections configuration after you have configured the LAN and WAN interfaces.

Figure 3 Interfaces and Connections Configuration Window



Cisco Router and Security Device Manager (SDM): 172.28.217.64

Interfaces and Connections

Interface List

Interface	IP	Type	Slot	Status	Description
GigabitEthernet0/0	172.28.217.64	GigabitEthernet	0	Up	
GigabitEthernet0/1	no IP address	GigabitEthernet	0	Up	
GigabitEthernet0/1.1	10.10.2.1	GigabitEthernet	0	Up	
GigabitEthernet0/1.2	10.10.3.1	GigabitEthernet	0	Up	
Service-Engine0/0	no IP address	Service-Engine	0	Dow	

Details about Interface:GigabitEthernet0/1

Item Name	Item Value
GigabitEthernet0/1 802.1Q Trunking VLANs	
GigabitEthernet0/1.2	VLAN 3 IP address/subnet mask 10.10.3.1/255.255.255.0
GigabitEthernet0/1.1	VLAN 2 (NATIVE) IP address/subnet mask 10.10.2.1/255.255.255.0
IP address/subnet mask	no IP address

Configuring IP Routing

Perform the following steps to configure IP routing.

Note This information needs to be configured only if the service provider assigns static IP information including IP addresses, default router, and so on.

Step 1 From the Main menu, click **Configure** and choose **Routing** from the Task pane.

Step 2 In the Static Routing section, click **Add**.

Step 3 For the Destination Network, place a check mark in the **Make this the default route** check box.

Step 4 Under Forwarding (Next Hop), choose the **IP Address** option and enter the IP address of the default router on the WAN. (The service provider will provide this IP address.)

Step 5 Place a check mark in the **Permanent Route** option check box to ensure that the route stays in the routing table.

Step 6 Click **OK**.

Step 7 After the configuration is delivered to the router, click **OK**.

Configuring Network Address Translation (NAT)

Perform the following steps to configure NAT.

Step 1 From the Main menu, click **Configure** and choose **NAT** from the Task pane.

Step 2 Choose **Basic NAT** and click **Launch Selected Task**.

Step 3 In the Welcome to the Basic NAT Wizard window, click **Next**.

Step 4 For Sharing the Internet Connection, choose the interface (configured as the WAN interface) that connects to the Internet from the drop-down list options.

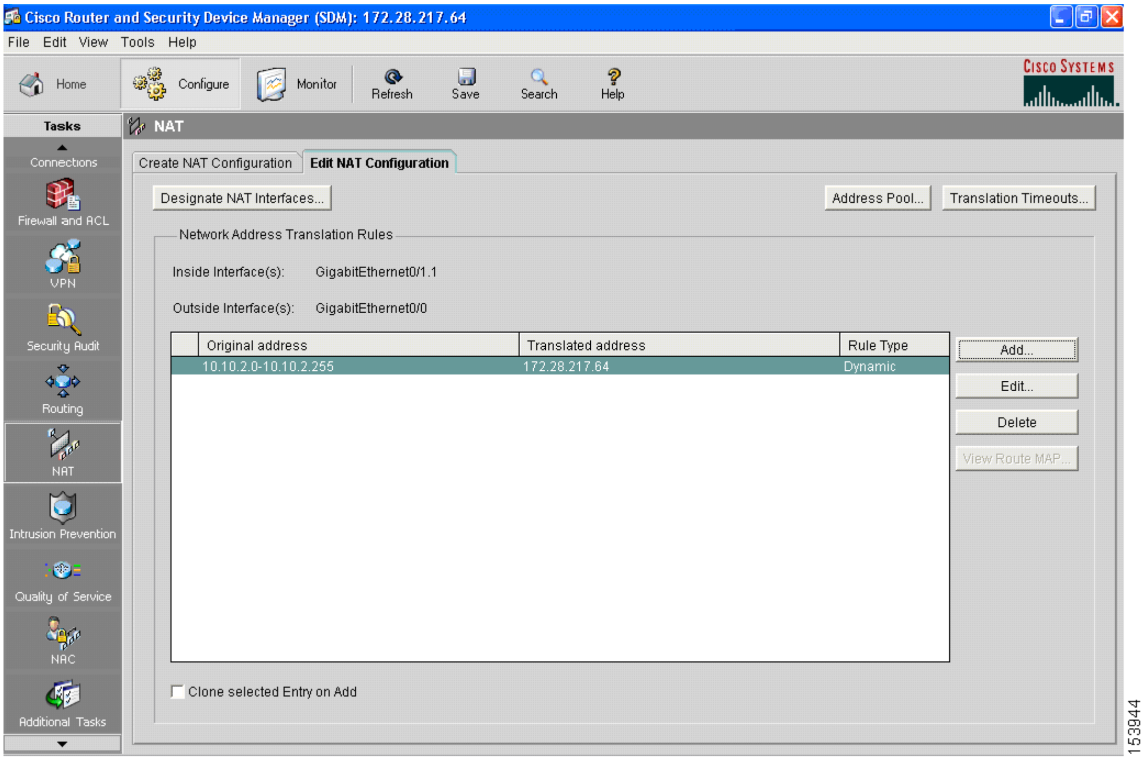
Step 5 Choose the internal network (configured as the Cisco data VLAN) that will share the Internet connection. The Cisco-VLAN should not be selected because traffic never exits the LAN to the Internet. Click **Next**.

Step 6 In the summary window, review the options and click **Finish**.

Step 7 After the configuration is delivered to the router, click **OK**.

Figure 4 displays the NAT configuration that you created in the previous procedure.

Figure 4 Network Address Translation Configuration Window



Inside Interface(s): GigabitEthernet0/1.1

Outside Interface(s): GigabitEthernet0/0

Original address	Translated address	Rule Type
10.10.2.0-10.10.2.255	172.28.217.64	Dynamic

☐ Clone selected Entry on Add

Performing a Security Audit

Perform the following steps to run the security audit, which configures infrastructure protection services on the router.

Note Before running the security audit, use the CLI to configure a password that is more than six characters in length to prevent users from being locked out when the router is reloaded.

Step 1 From the Main menu, click **Configure** and choose **Security Audit** from the Task pane.

Step 2 Click **Perform Security Audit** and then click **Next**.

Step 3 Choose the outside (untrusted) and inside (trusted) interfaces and click **Next**.

After the security audit is complete, a list of passed and failed items is displayed. Click **Close**.

Step 4 Leave the default setting of Select an option: Fix the security problems.

Step 5 Click the **Fix all** button to fix all of the security issues that have been identified and then clear the **Cisco Discovery Protocol (CDP)** check box. This is necessary on the LAN, but not on the WAN; CDP must manually be disabled on the WAN interface using the **no cdp enable** command. Click **Next**.

Note Figure 5 displays the output of the security audit and the items that must be fixed.

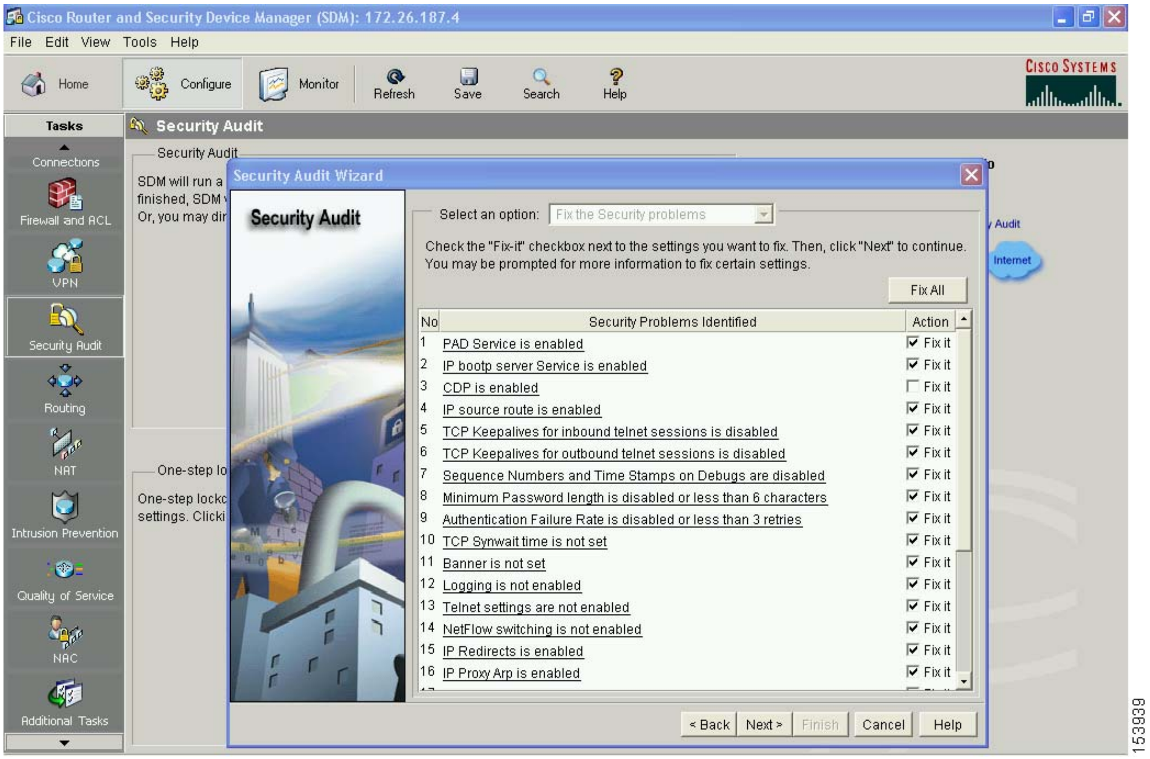
Step 6 Follow the instructions, as prompted, to repair all of the security issues. When prompted to configure the Advanced Firewall, click **Cancel** and then click **Yes**. (The basic firewall option will be configured in a separate step.)

Step 7 In the summary window, review the options and click **Finish**.

Step 8 After the configuration is delivered to the router, click **OK**.

Note We recommend consulting with legal counsel for the wording of the banner so that all local laws are represented appropriately.

Figure 5 Security Audit Window



SDM will run a
finished, SDM
Or, you may dir

One-step lockc
settings. Clicki

Select an option: Fix the Security problems

Check the "Fix-it" checkbox next to the settings you want to fix. Then, click "Next" to continue. You may be prompted for more information to fix certain settings.

No	Security Problems Identified	Action
1	PAD Service is enabled	☑ Fix it
2	IP bootp server Service is enabled	☑ Fix it
3	CDP is enabled	□ Fix it
4	IP source route is enabled	☑ Fix it
5	TCP Keepalives for inbound telnet sessions is disabled	☑ Fix it
6	TCP Keepalives for outbound telnet sessions is disabled	☑ Fix it
7	Sequence Numbers and Time Stamps on Debugs are disabled	☑ Fix it
8	Minimum Password length is disabled or less than 6 characters	☑ Fix it
9	Authentication Failure Rate is disabled or less than 3 retries	☑ Fix it
10	TCP Synwait time is not set	☑ Fix it
11	Banner is not set	☑ Fix it
12	Logging is not enabled	☑ Fix it
13	Telnet settings are not enabled	☑ Fix it
14	NetFlow switching is not enabled	☑ Fix it
15	IP Redirects is enabled	☑ Fix it
16	IP Proxy Arp is enabled	☑ Fix it

Configuring Firewall and Access Control Lists

Perform the following steps to configure the firewall and the Access Control Lists (ACLs).

Step 1 From the Main menu, click **Configure** and choose **Firewall** and **ACL** from the Task pane.

Step 2 From from the Create Firewall tab, choose the **Basic Firewall** option. Click **Launch the selected task**.

Step 3 From the Basic Firewall Configuration Wizard window, click **Next**.

Step 4 For the Basic Firewall Interface Configuration, choose the outside (untrusted) interface, which is the WAN interface, and clear the **Allow secure SDM access from outside interfaces unless absolutely needed** check box. Choose the inside (trusted) interface, which includes only the Cisco-Data VLAN (devices on the Cisco-Voice VLAN never have access to the Internet).

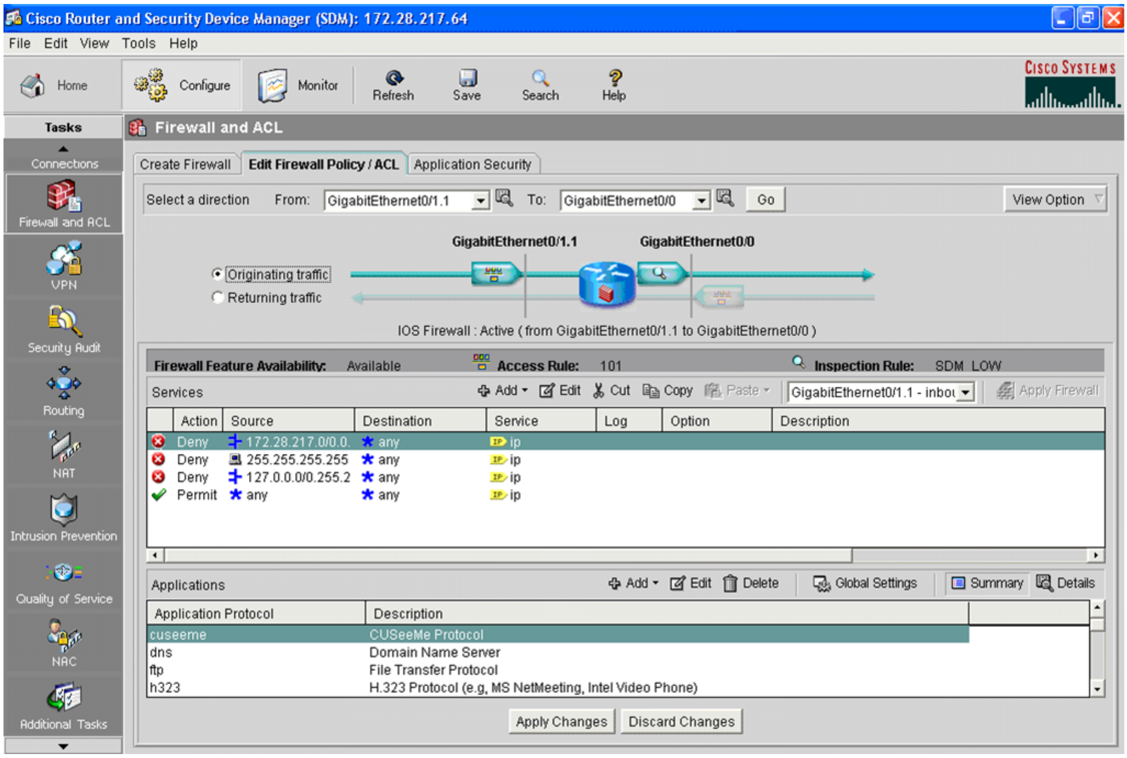
Step 5 Click **Next**.

Step 6 In the summary window, review the options and click **Finish**.

Step 7 After the configuration is delivered to the router, click **OK**.

Figure 6 displays the firewall configuration that you created in the previous procedure.

Figure 6 Firewall and ACL Configuration Window



Select a direction From: GigabitEthernet0/1.1 To: GigabitEthernet0/0

● Originating traffic
○ Returning traffic

IOS Firewall : Active (from GigabitEthernet0/1.1 to GigabitEthernet0/0)

Firewall Feature Availability: Available Access Rule: 101 Inspection Rule: SDM LOW

Services GigabitEthernet0/1.1 - inbou

Action	Source	Destination	Service	Log	Option	Description
Deny	172.28.217.0/0.0.	any	ip			
Deny	255.255.255.255	any	ip			
Deny	127.0.0.0/0.255.2	any	ip			
Permit	any	any	ip			

Applications

Application Protocol	Description
cuseeme	CUSeeMe Protocol
dns	Domain Name Server
ftp	File Transfer Protocol
h323	H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)

Configuring the Intrusion Prevention System

Perform the following steps to configure the Intrusion Prevention System.

Step 1 From the Main menu, click **Configure** and choose **IPS** from the Task pane.

Step 2 From the Create IPS window, click **Launch IPS Rule Wizard** and then click **OK** in the SDEE notification window.

Step 3 Click **OK** on the SDM subscription window, then click **Next** on the Welcome to the IPS Policies Wizard window.

Step 4 Choose both the inbound and outbound inspection rules for the WAN and LAN interfaces from the Select interfaces window and click **Next**.

Step 5 Click **Add** for the SDF Location, using the default setting of Specify SDF on flash and choose the signature file from the drop-down list (the 256MB.sdf file is the default for the 2851). Click **OK** and then click **Next**.

Note If an information box regarding the order of SDF file locations is displayed, click **OK**.

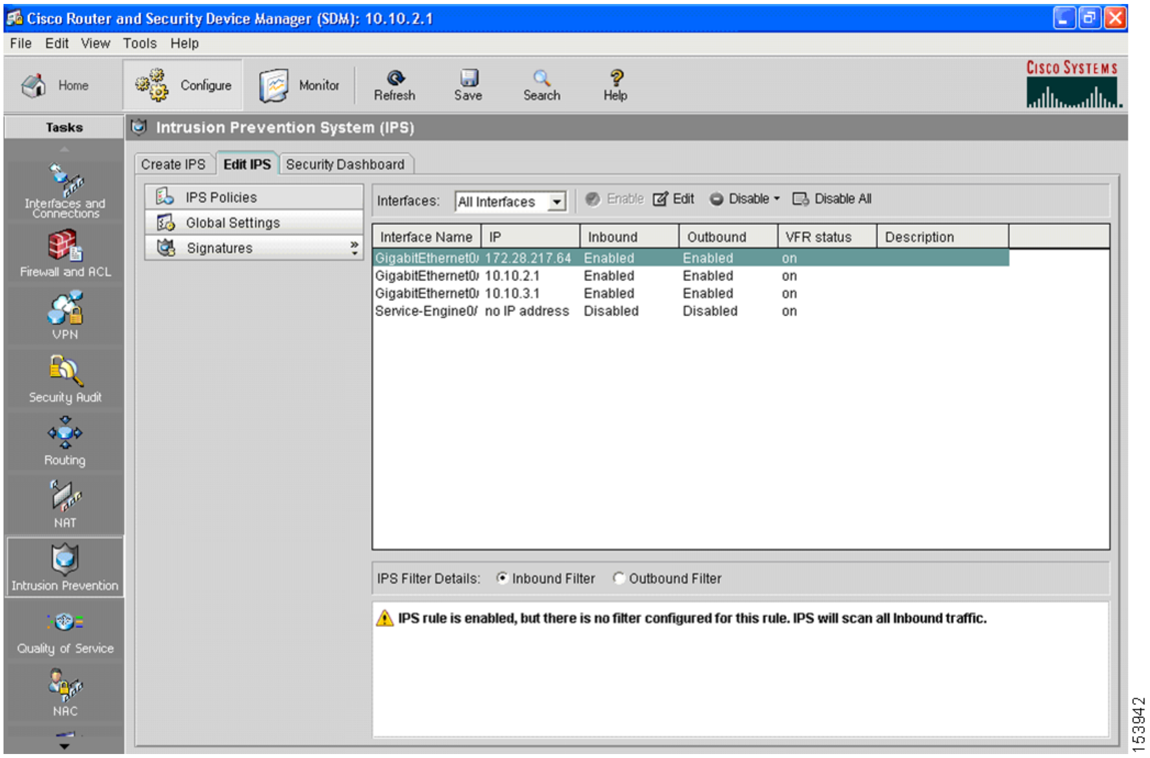
Step 6 In the summary window, review the options and click **Finish**.

Step 7 After the configuration is delivered to the router, click **OK**.

Note Actions, such as reset, deny, and alarm are pre-configured, based on the type of signature in the SDF file loaded on the router.

Figure 7 displays the IPS configuration that you created in the previous procedure.

Figure 7 IPS Configuration Window



Interfaces: All Interfaces

Interface Name	IP	Inbound	Outbound	VFR status	Description
GigabitEthernet0/	172.28.217.64	Enabled	Enabled	on	
GigabitEthernet0/	10.10.2.1	Enabled	Enabled	on	
GigabitEthernet0/	10.10.3.1	Enabled	Enabled	on	
Service-Engine0/	no IP address	Disabled	Disabled	on	

IPS Filter Details: ● Inbound Filter ○ Outbound Filter

⚠ IPS rule is enabled, but there is no filter configured for this rule. IPS will scan all Inbound traffic.

Setting the Date and Time

Perform the following steps to configure the date and time on the router.

Step 1 From the Main menu, click **Configure** and choose **Additional Tasks** from the Task pane.

Step 2 Open Router Properties and choose **Date/Time**.

Step 3 Click the **Change Settings** button.

Step 4 In the Date and Time Properties window, edit the date and time.

Step 5 Click **Apply**.

Step 6 In the Router clock configured window, click **OK**.

Step 7 In the Date and Time Properties window, click **Close**.

Catalyst Express 500 Switches

The Catalyst Express 500 LAN switches deployed within this system provide several services including:

- Layer 2 LAN access connectivity
- Layer 2 LAN aggregation connectivity
- Power over Ethernet for IP phones, wireless access points and other devices
- Integrated security and quality of service via Smartports macros

All of these services are configured using the Cisco Network Assistant (CNA) graphical user interface (GUI) tool. This tool centralizes the administration of all the switches within the system and speeds the overall implementation process. The following sections outline the simple steps used to configure the Catalyst Express 500 access and aggregation LAN switches.

When installing and configuring the switches for the first time it is important to follow the steps outlined in the document, *Getting Started Guide for the Catalyst Express 500 Switches* at the following URL:

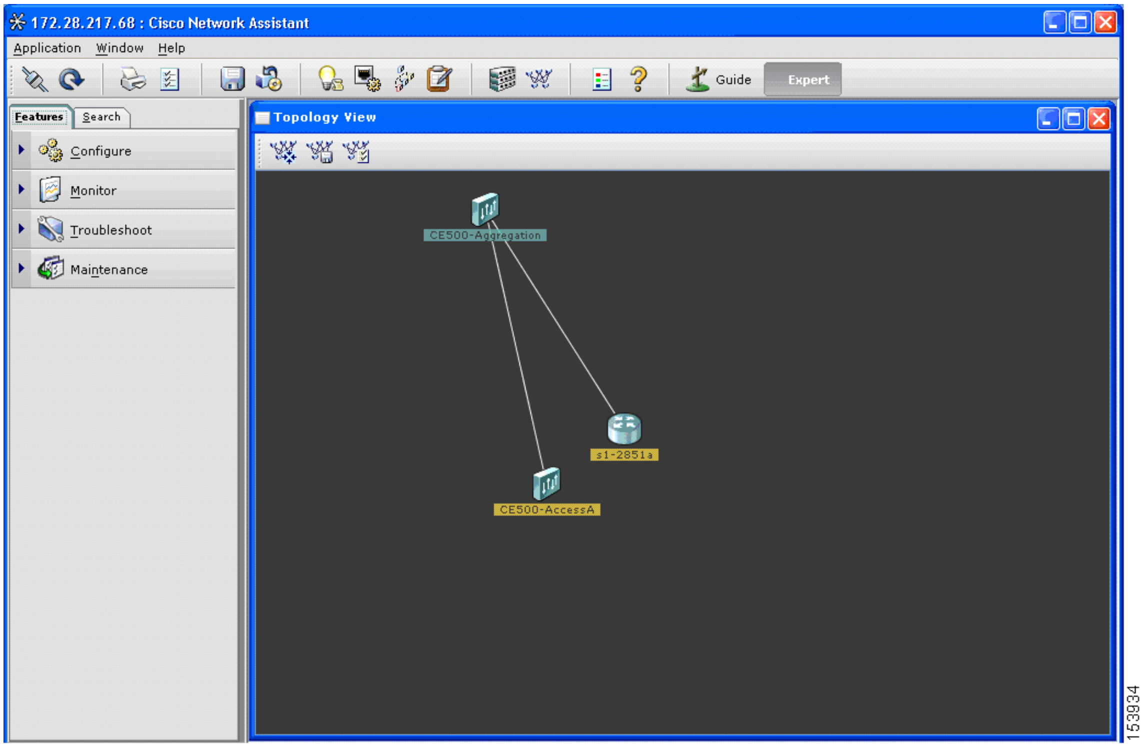
http://www.cisco.com/en/US/partner/products/ps6545/products_getting_started_guide09186a0080524310.html.

When installing Cisco Network Assistant for the first time it is important to follow the steps provided in *Getting Started with CNA 3*.1 at the following URL:

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

Figure 8 shows the CNA GUI interface that you use to configure the switches.

Figure 8 CNA GUI Interface



Configuring Port Settings

Perform the following steps to configure port settings on the access and aggregation switches.

Step 1 Highlight the appropriate switch in the Topology View window.

Step 2 In the left pane, click **Configure**.

Step 3 Click **Ports** and choose **Port Settings**.

Step 4 Choose a port in the Port Settings window, click **Modify**, and enter a description for the port.

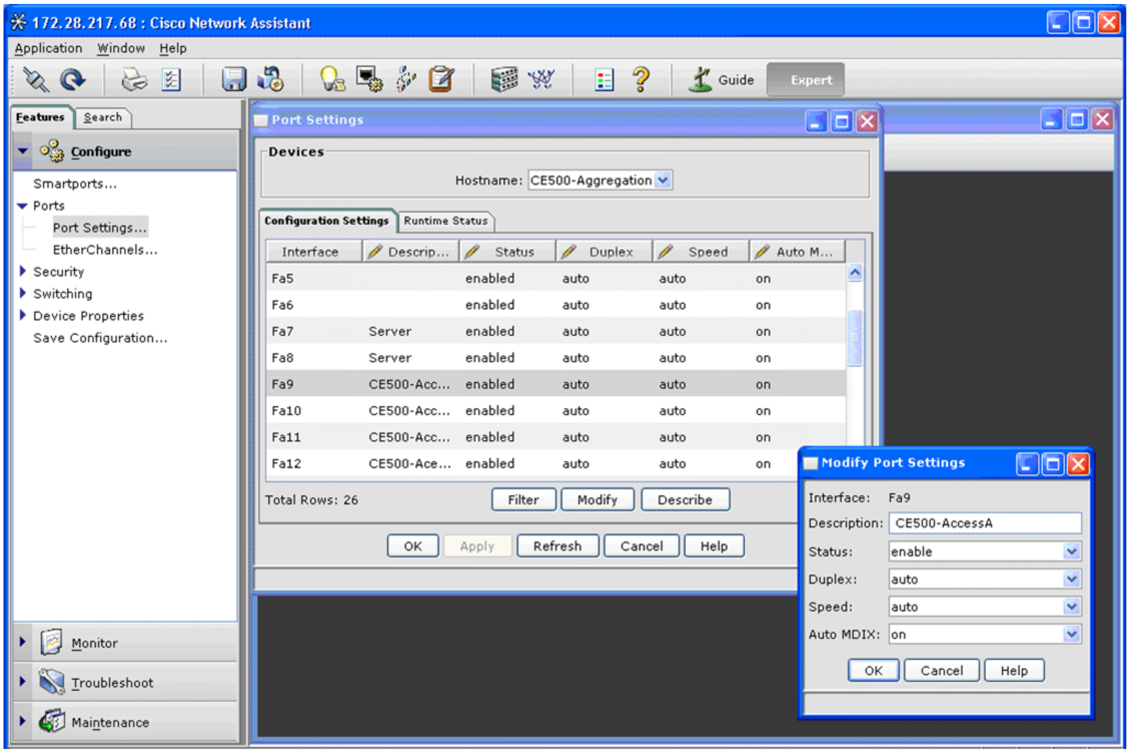
Leave the default settings for the other options unless the port is not used. If the port is not used, change the Status to Disabled to prevent any unauthorized devices from connecting to the network.

Step 5 Click **OK**.

Step 6 Click **Apply** to save all the Port Settings configuration changes and then click **OK** to close the Port Settings window.

Figure 9 displays the Port Settings configuration window.

Figure 9 Port Settings Configuration Window



Devices

Hostname: CE500-Aggregation

Interface	Descrip...	Status	Duplex	Speed	Auto M...
Fa5		enabled	auto	auto	on
Fa6		enabled	auto	auto	on
Fa7	Server	enabled	auto	auto	on
Fa8	Server	enabled	auto	auto	on
Fa9	CE500-Acc...	enabled	auto	auto	on
Fa10	CE500-Acc...	enabled	auto	auto	on
Fa11	CE500-Acc...	enabled	auto	auto	on
Fa12	CE500-Ace...	enabled	auto	auto	on

Total Rows: 26

Interface: Fa9
Description: CE500-AccessA
Status: enable
Duplex: auto
Speed: auto
Auto MDIX: on

Configuring Virtual Local Area Networks

Perform the following steps to configure Virtual Local Area Networks (VLANs) on the access and aggregation switches.

Step 1 Highlight the appropriate switch in the Topology View window.

Step 2 In the left pane, click **Configure**.

Step 3 Click **Switching** and choose **VLANs**.

Step 4 Click **Create** in the VLAN window.

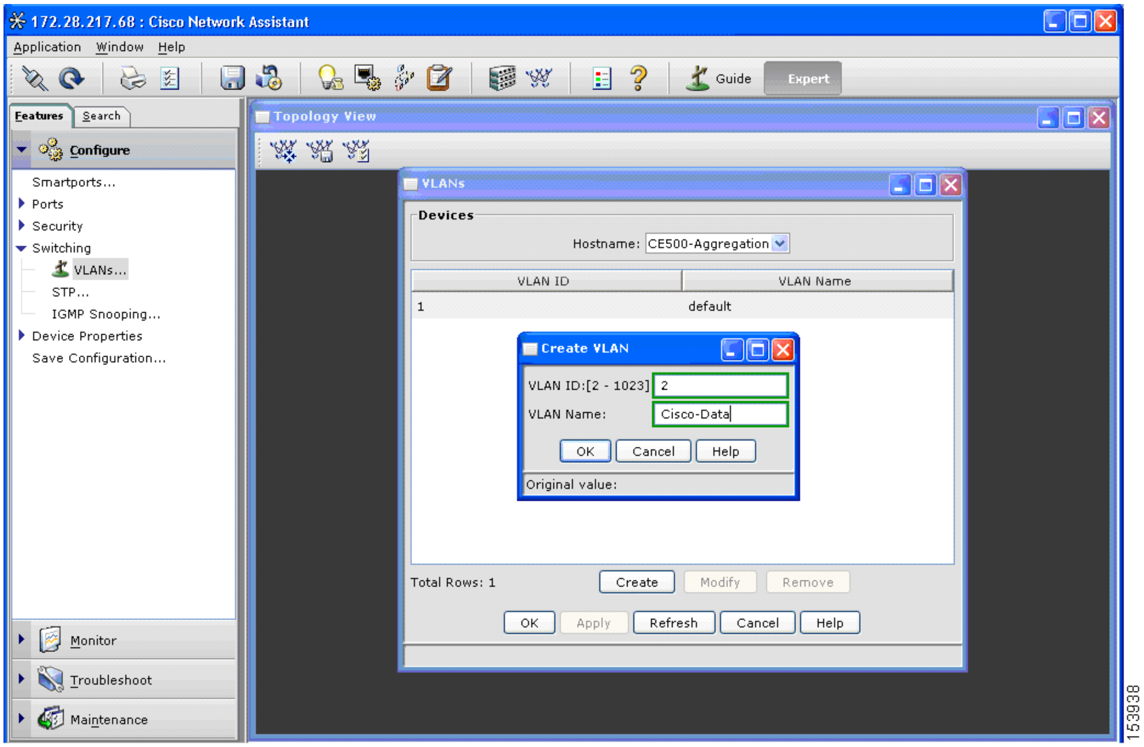
Step 5 Enter the VLAN ID (number) and the VLAN name (optional). For example, enter a VLAN ID of 2 and the VLAN name of Cisco-Data or a VLAN ID of 20 and the VLAN name of Cisco-Voice.

Step 6 In the Create VLAN window, click **OK**.

Step 7 Click **Apply** to save the VLAN configuration changes and then click **OK** to close the VLAN window.

Figure 10 displays the VLAN configuration window.

Figure 10 VLAN Configuration Window



172.28.217.68 : Cisco Network Assistant

Hostname: CE500-Aggregation

VLAN ID	VLAN Name
1	default

Create VLAN

VLAN ID:[2 - 1023] 2

VLAN Name: Cisco-Data

Original value:

Total Rows: 1

Configuring Security

Perform the following steps to configure security on the access and aggregation switches.

Step 1 Highlight the appropriate switch in the Topology View window.

Step 2 In the left pane, click **Configure**.

Step 3 Click **Security** and choose **Network Security Settings**.

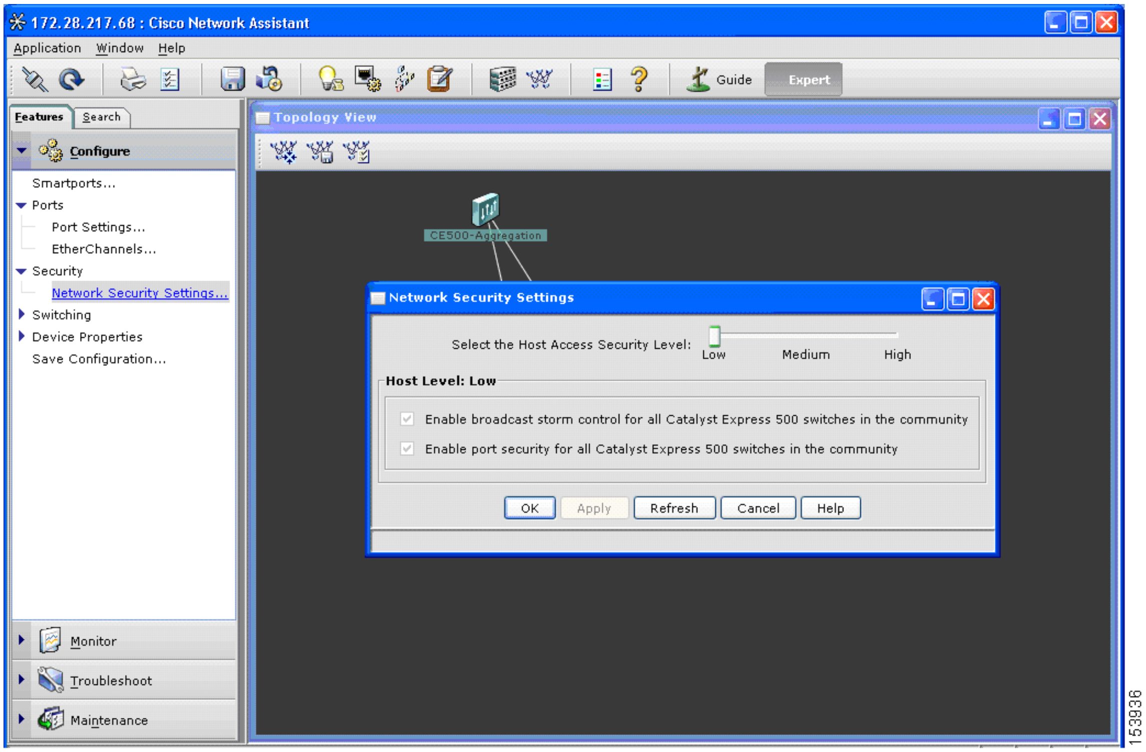
Step 4 Ensure that the default setting of Low is selected.

This setting enables Broadcast Storm Control which prevents broadcast traffic from flooding the LAN and degrading network performance. This setting also enables Port Security, which limits the number of devices that can connect to a switch port; the number of devices is determined by the Smartports role assigned to the port.

Step 5 Click **OK** to close the Network Security Settings window.

Figure 11 displays the Security configuration window.

Figure 11 Security Configuration Window



Select the Host Access Security Level: Low

Host Level: Low

☑ Enable broadcast storm control for all Catalyst Express 500 switches in the community

☑ Enable port security for all Catalyst Express 500 switches in the community

Configuring Smartports

Perform the following steps to configure Smartports on the access and aggregation switches.

Step 1 Highlight the appropriate switch in the Topology View window.

Step 2 In the left pane, click **Configure**.

Step 3 Click **Smartports**.

Step 4 Choose a port on the switch in the Smartports window and click **Modify**.

Step 5 Choose the Role for the port and choose the VLANs, then click **OK**.

Table 2 provides the recommended Smartports roles for the ports on both the access and aggregation switches.

Table 2 Recommended Smartports Configuration

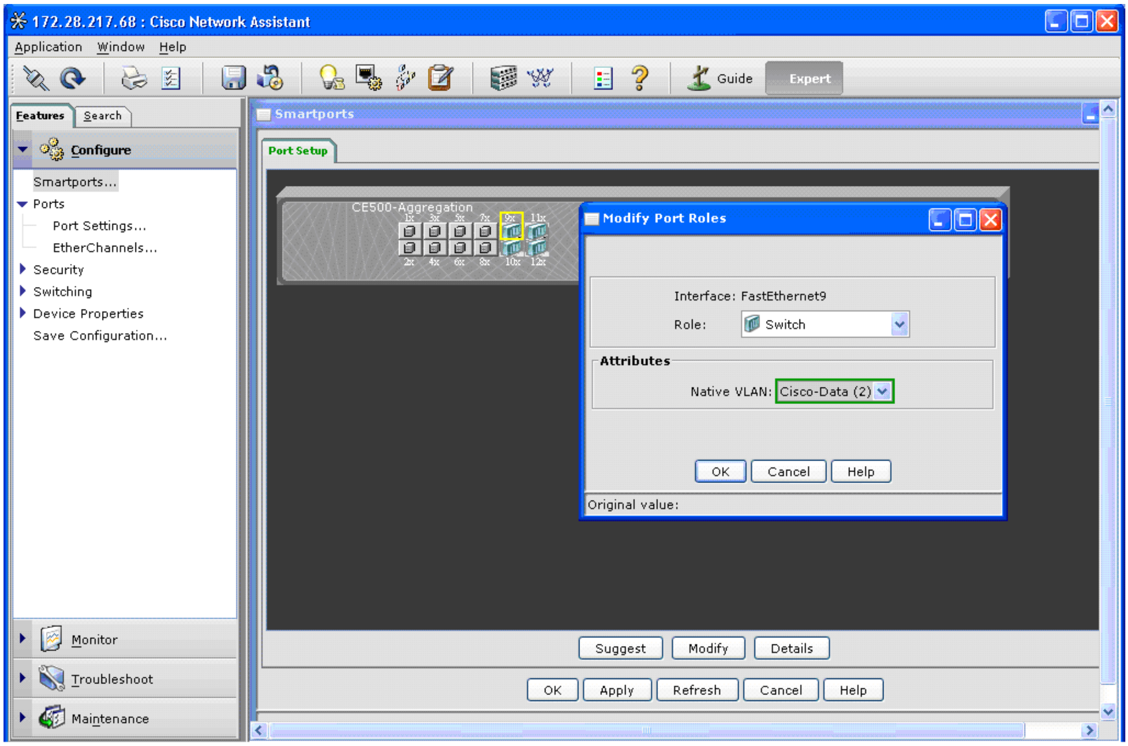
Switch	Port Type and Number	Recommended Port Role
Access	Fast Ethernet ports 1 to 24	IP Phone+Desktop
	Gigabit Ethernet port 1	Switch (connects to Aggregation)
Aggregation	Gigabit Ethernet port 1	Router
	Gigabit Ethernet ports 2 to 8	Server
	Gigabit Ethernet ports 9 to 12	Switch (connects to Access)

Step 6 Click **Yes** to confirm and then click **Apply** to save the Smartports configuration changes.

Step 7 Click **Yes** to confirm and then click **OK** to close the Smartports window.

Figure 12 displays the Smartports configuration window.

Figure 12 Smartports Configuration Window



Interface: FastEthernet9

Role: Switch

Native VLAN: Cisco-Data (2)

Original value:

Connectivity Tests

This section provides tests that can be used to ensure that WAN and LAN connectivity is working correctly.

Testing the WAN

Perform the following steps to ensure that the WAN interface of the router has connectivity to the service provider.

Step 1 From the Main menu, click **Tools** and choose **Ping**.

Step 2 Enter the source IP Address in the **Source** box. The IP address of the WAN interface should be used for the first test however one or more of the LAN interface IP addresses could also be used for this test.

Step 3 Enter the destination IP address in the **Destination** box. This is the IP address of the default gateway provided by the service provider.

Step 4 Click the **Ping** button.

Step 5 After the ping test is complete, the output is displayed in the box on the right-hand side of the Ping window.

Step 6 After a successful ping test, click **Close**. If the test is not successful, verify that all of the addresses used in the test and in the configuration are correct and perform the test again.

Testing the LAN

The following test ensures that the LAN interfaces on the router have connectivity to the LAN aggregation switch, LAN access switch, data end points, and voice end points.

Step 1 From the Main menu, click **Tools** and choose **Ping**.

Step 2 Enter the source IP Address in the **Source** box. One set of tests should be run using the Cisco-Data VLAN interface and another set run using the Cisco-Voice VLAN to ensure connectivity everywhere.

Step 3 Enter the destination IP address in the **Destination** box. Multiple tests should be run to ensure connectivity to the LAN aggregation switch, LAN access switches, data end points and voice end points.

Step 4 Click the **Ping** button.

Step 5 After the ping test is complete, the output is displayed in the box on the right-hand side of the Ping window.

Step 6 After a successful ping test, click **Close**. If the test is not successful, verify that all of the addresses used in the test and in the configuration are correct and perform the test again.

2851 ISR Configuration

This section provides the Command Line Interface (CLI) configuration for the Cisco 2851 ISR used in the design.

```
Current configuration : 7570 bytes
!
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname s1-2851a
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 debugging
no logging console
enable secret 5 $1$PHWX$phcbeZ..63XnS0nOj0pcm0
enable password 7 13061E01080355
!
aaa new-model
!
!
aaa authentication login local_authen local
aaa authorization exec local_author local
!
aaa session-id common
!
resource policy
!
clock timezone Pacific -8
clock summer-time PAST date Apr 5 2003 23:00 Oct 25 2003 23:00
ip subnet-zero
no ip source-route
ip tcp synwait-time 10
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.20.31.1 10.20.31.19
ip dhcp excluded-address 10.20.41.1 10.20.41.19
!
ip dhcp pool sdm-pool1
   network 10.20.31.0 255.255.255.0
   default-router 10.20.31.1
!
ip dhcp pool sdm-pool2
   import all
   network 10.20.41.0 255.255.255.0
   default-router 10.20.41.1
   option 150 ip 10.20.41.1
!
!
no ip bootp server
no ip domain lookup
ip ssh time-out 60
ip ssh authentication-retries 2
ip inspect name SDM_LOW cuseeme
ip inspect name SDM_LOW dns
ip inspect name SDM_LOW ftp
ip inspect name SDM_LOW h323
ip inspect name SDM_LOW icmp
ip inspect name SDM_LOW imap
ip inspect name SDM_LOW pop3
ip inspect name SDM_LOW netshow
ip inspect name SDM_LOW rcmd
ip inspect name SDM_LOW realaudio
ip inspect name SDM_LOW rtsp
ip inspect name SDM_LOW esmtp
ip inspect name SDM_LOW sqlnet
ip inspect name SDM_LOW streamworks
ip inspect name SDM_LOW tftp
ip inspect name SDM_LOW tcp
ip inspect name SDM_LOW udp
ip inspect name SDM_LOW vdolive
ip inspect name SDM_LOW https
ip ips sdf location flash://256MB.sdf
ip ips notify SDEE
ip ips name sdm_ips_rule
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-103639936
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-103639936
 revocation-check none
 rsakeypair TP-self-signed-103639936
!
!
crypto pki certificate chain TP-self-signed-103639936
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31303336 33393933 36301E17 0D303630 33323231 38343533
  355A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3130 33363339
  39333630 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  A8335196 7C705CE4 1FB93300 F2DCEDB0 57C5DCDB C20B86CF 802FED4B C3A7D4DF
  4594CBC1 3AC7F1DD 568B0488 415676A1 BE7C4CD6 4976C927 2349E6E9 030577A6
  FB3E746A B6F38838 92AD98FC 7AF39C9C 71B96C05 E3F1DD47 CCA7A43A 5FEDE011
  D4C140FD 62FC2CC6 42B6EB08 7BE4468E 7E7B4E77 C5E2AA4B 87E928F4 7A73ED9B
  02030100 01A36930 67300F06 03551D13 0101FF04 05300301 01FF3014 0603551D
  11040D30 0B820973 312D3238 3531612E 301F0603 551D2304 18301680 14DD5458
  45F42B92 AA9E3A47 07BF8F41 0CCEB9F6 8E301D06 03551D0E 04160414 DD545845
  F42B92AA 9E3A4707 BF8F410C CEB9F68E 300D0609 2A864886 F70D0101 04050003
  81810001 D5C29A23 053C6ABA 70ADB7C8 E93A1ADB 55C2E13B 6F0620DC A0A8E1E6
  6070FD3C 826B6E39 39DD554B 08D0B6D3 E5CAA262 E391D7D0 DB9066C9 703DF908
  6228CAB1 FDC9464A 5D23AFCC 93D74E6F 6E2D6439 DD4DB155 C60DAFB1 B4129680
  875B8187 A1FA6E1C C59C3FED 2D9CCD8A 5725055C D2E51E92 E7012FCC 55CDA3D6 0B86D3
  quit
username cse privilege 15 password 7 13061E010803557878
!
!
!
!
!
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet0/0
 description $ETH-WAN$$FW_OUTSIDE$
 ip address 100.100.1.2 255.255.255.0
 ip access-group 102 in
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat outside
 ip inspect SDM_LOW out
 ip virtual-reassembly
 ip route-cache flow
 load-interval 30
 duplex auto
 speed 10
 no cdp enable
 no mop enabled
!
interface Service-Engine0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip virtual-reassembly
 ip route-cache flow
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip route-cache flow
 duplex auto
 speed auto
 no mop enabled
!
interface GigabitEthernet0/1.1
 description $ETH-LAN$$FW_INSIDE$
 encapsulation dot1Q 2 native
 ip address 10.20.31.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat inside
 ip virtual-reassembly
 no snmp trap link-status
!
```

```
interface GigabitEthernet0/1.2
 description $ETH-LAN$$FW_INSIDE$
 encapsulation dot1Q 3
 ip address 10.20.41.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip virtual-reassembly
 no snmp trap link-status
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.100.1.254
!
!
ip http server
ip http access-class 2
ip http authentication local
ip http secure-server
ip http timeout-policy idle 5 life 86400 requests 10000
ip nat inside source list 1 interface GigabitEthernet0/0 overload
!
logging trap debugging
logging 1.1.1.1
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 10.10.31.0 0.0.0.255
access-list 1 permit 10.20.31.0 0.0.0.255
access-list 2 remark HTTP Access-class list
access-list 2 remark SDM_ACL Category=1
access-list 2 permit 10.10.41.0 0.0.0.255
access-list 2 permit 10.10.31.0 0.0.0.255
access-list 2 deny   any
access-list 100 remark VTY Access-class list
access-list 100 remark SDM_ACL Category=1
access-list 100 permit ip 10.10.41.0 0.0.0.255 any
access-list 100 permit ip 10.10.31.0 0.0.0.255 any
access-list 100 deny   ip any any
access-list 101 remark auto generated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
access-list 101 deny   ip 100.100.1.0 0.0.0.255 any
access-list 101 deny   ip host 255.255.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 permit ip any any
access-list 102 remark auto generated by SDM firewall configuration
access-list 102 remark SDM_ACL Category=1
access-list 102 deny   ip 10.10.31.0 0.0.0.255 any
access-list 102 permit icmp any host 100.100.1.2 echo-reply
access-list 102 permit icmp any host 100.100.1.2 time-exceeded
access-list 102 permit icmp any host 100.100.1.2 unreachable
access-list 102 permit tcp any host 100.100.1.2 eq 443
access-list 102 permit tcp any host 100.100.1.2 eq 22
access-list 102 permit tcp any host 100.100.1.2 eq cmd
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any
access-list 102 deny   ip 100.100.0.0 0.0.255.255 any
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any
access-list 102 deny   ip 127.0.0.0 0.255.255.255 any
access-list 102 deny   ip host 255.255.255.255 any
access-list 102 deny   ip host 0.0.0.0 any
access-list 102 deny   ip any any log
!
!
!
!
control-plane
!
```

```
!
!
!
!
!
!
!
!
banner login ^CHello & welcome!^C
!
line con 0
 login authentication local_authen
 transport output telnet
line aux 0
 login authentication local_authen
 transport output telnet
line 194
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output all
line vty 0 4
 access-class 100 in
 authorization exec local_author
 login authentication local_authen
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Bill of Materials

Table 3 provides the bill of materials used to build the validated system described in this document.

Table 3 Bill of Materials for the Validated 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