



Cisco SMB Support Assistant Site Survey

Home > [SMB Support Assistant Configuration Overview](#) > Cisco SMB Support Assistant Site Survey

Cisco SMB Support Assistant Site Survey

[Introduction](#)

[Requirements](#)

[Site Survey Overview](#)

[Site Survey Worksheets](#)

[Key Concepts](#)

[Site IP Addressing](#)

[Virtual LANs](#)

[Router Type](#)

[NAT](#)

[IP Address Assignments](#)

[Domain Name Service](#)

[Device Passwords](#)

[Internet Connection](#)

[Wall Jacks](#)

[Power over Ethernet](#)

[Wireless Site Survey](#)

[Wireless Access Point Types](#)

[Wireless Security](#)

[Wireless SSID](#)

[Internet Services](#)

[Virtual Private Networks](#)

[Overview Worksheet](#)

[LAN Addressing Worksheet](#)

[Router Worksheet](#)

[Integrated Services Router Worksheet](#)

[Internet Worksheet - ISDN](#)

[Internet Worksheet - DSL](#)

[Internet Worksheet - T1/E1](#)

[Internet Worksheet - Ethernet](#)

[Switch Port Assignment Worksheets](#)

[Switch SW1 \(Root Switch\)](#)

[Switch SW2-SW5](#)

[Management VLAN Worksheet](#)

[Secure Server VLAN Worksheet](#)

[Guest VLAN Worksheet](#)

[Internet Services Worksheet](#)

[Security Appliance Worksheet](#)

[Wireless Network Assignments Worksheet](#)

[Next Step](#)

[Glossary](#)

[Related Information](#)

Service Requests

[Open a service request](#)

[Update a service request](#)

Feedback

Please rate this document.

++ + +/- - --

This document solved my problem.

Yes No Just Browsing

Suggestions for improvement:

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Download PDF



[Cisco SMB Support Assistant Site Survey](#)

Full Name:
Email:

Introduction

The SMB Support Assistant Site Survey is a unique set of instructions designed to help you set up and document your network.

The SMB Support Assistant Site Survey provides these benefits:

- Network Address Translation (NAT) to control communication between the LAN and the Internet

- Unique internal IP addresses for up to 30 sites. These addresses are compatible to allow you to easily implement VPNs at any time.
- Firewall rules to block unauthorized traffic
- Stateful firewall rules to dynamically permit authorized traffic
- Support for internal servers including email, web, and VPN
- Four Virtual LANs (VLANs) with specialized levels of security for LAN users, network management devices, protected servers, and guest users
- Comprehensive documentation of your entire network

[Back to Top](#)

Requirements

These items are required to complete the site survey:

Site Survey Overview

An accurate and detailed site survey is a critical component in building a network. To complete a site survey, you need to obtain information from these sources:

- Internet service provider
- Local telephone company
- Building managers
- Facility planners
- Electricians
- Company management and employees

To help you with your site survey, we have provided [Site Survey Worksheets](#) that capture the required information. These worksheets are used throughout the SMB Support Assistant documentation. The worksheets provide documentation for effective ongoing network management and support, and can help new administrators to quickly understand your network. You should complete one set of worksheets for each site at your organization.

Note: The worksheets that you need to complete depend on the devices in your network. All the worksheets are contained in the Adobe Acrobat file.

Site Survey Worksheets

Download and print the [Site Survey Worksheets](#) and complete them in this order:

- Overview Worksheet
- Site IP Addressing Plan
- LAN Addressing Worksheet
- Router Worksheet
- Integrated Services Router Worksheet
- Internet Worksheet- ISDN
- Internet Worksheet- DSL
- Internet Worksheet- T1/E1
- Internet Worksheet- Ethernet
- Guest VLAN Worksheet

- Network Management VLAN Worksheet
- Secure Server VLAN Worksheet
- Internet Services Worksheet
- Switch Port Assignments Worksheets
- Security Appliance Worksheet
- Wireless Network Assignments Worksheet

[Back to Top](#)

Key Concepts

These are some concepts you need to be familiar with to complete the site survey.

Site IP Addressing

This site survey includes a site IP addressing plan designed to let you use compatible configurations at up to 30 sites. This addressing ensures similar configurations at each site and provides unique addressing so that you can easily implement a [Virtual Private Network](#) (VPN) between remote sites.

Site IP Addressing Plan				
Location	Default	Management	Secure Server	Guest
	VLAN 20	VLAN 21	VLAN 22	VLAN 23
Site 1	192.168.10.0	192.168.11.0	192.168.12.0	192.168.13.0
Site 2	192.168.18.0	192.168.19.0	192.168.20.0	192.168.21.0
Site 3	192.168.28.0	192.168.27.0	192.168.26.0	192.168.25.0
Site 4	192.168.34.0	192.168.35.0	192.168.36.0	192.168.37.0
Site 5	192.168.42.0	192.168.43.0	192.168.44.0	192.168.45.0
Site 6	192.168.50.0	192.168.51.0	192.168.52.0	192.168.53.0
Site 7	192.168.58.0	192.168.59.0	192.168.60.0	192.168.61.0
Site 8	192.168.66.0	192.168.67.0	192.168.68.0	192.168.69.0
Site 9	192.168.74.0	192.168.75.0	192.168.76.0	192.168.77.0
Site 10	192.168.82.0	192.168.83.0	192.168.84.0	192.168.85.0
Site 11	192.168.90.0	192.168.91.0	192.168.92.0	192.168.93.0
Site 12	192.168.98.0	192.168.99.0	192.168.100.0	192.168.101.0
Site 13	192.168.106.0	192.168.107.0	192.168.108.0	192.168.109.0
Site 14	192.168.114.0	192.168.115.0	192.168.116.0	192.168.117.0
Site 15	192.168.122.0	192.168.123.0	192.168.124.0	192.168.125.0
Site 16	192.168.130.0	192.168.131.0	192.168.132.0	192.168.133.0
Site 17	192.168.138.0	192.168.139.0	192.168.140.0	192.168.141.0
Site 18	192.168.146.0	192.168.147.0	192.168.148.0	192.168.149.0
Site 19	192.168.154.0	192.168.155.0	192.168.156.0	192.168.157.0
Site 20	192.168.162.0	192.168.163.0	192.168.164.0	192.168.165.0
Site 21	192.168.170.0	192.168.171.0	192.168.172.0	192.168.173.0
Site 22	192.168.178.0	192.168.179.0	192.168.180.0	192.168.181.0
Site 23	192.168.186.0	192.168.187.0	192.168.188.0	192.168.189.0
Site 24	192.168.194.0	192.168.195.0	192.168.196.0	192.168.197.0
Site 25	192.168.202.0	192.168.203.0	192.168.204.0	192.168.205.0
Site 26	192.168.210.0	192.168.211.0	192.168.212.0	192.168.213.0
Site 27	192.168.218.0	192.168.219.0	192.168.220.0	192.168.221.0
Site 28	192.168.226.0	192.168.227.0	192.168.228.0	192.168.229.0
Site 29	192.168.234.0	192.168.235.0	192.168.236.0	192.168.237.0
Site 30	192.168.242.0	192.168.243.0	192.168.244.0	192.168.245.0

Note: If your network uses a [Wireless LAN Controller Module](#) (WLCM), you must use a separate set of IP Addresses. For an overview of these addresses, refer to [Configure Your Router for the Wireless LAN Controller Module](#)

Virtual LANs

Virtual Local Area Networks (VLANs) allow you to divide your network into separate logical groups so that you can assign different levels of security, priority, and access to each group. Devices in one VLAN behave as though they were connected to the same network segment, even if they are physically distant from each other. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

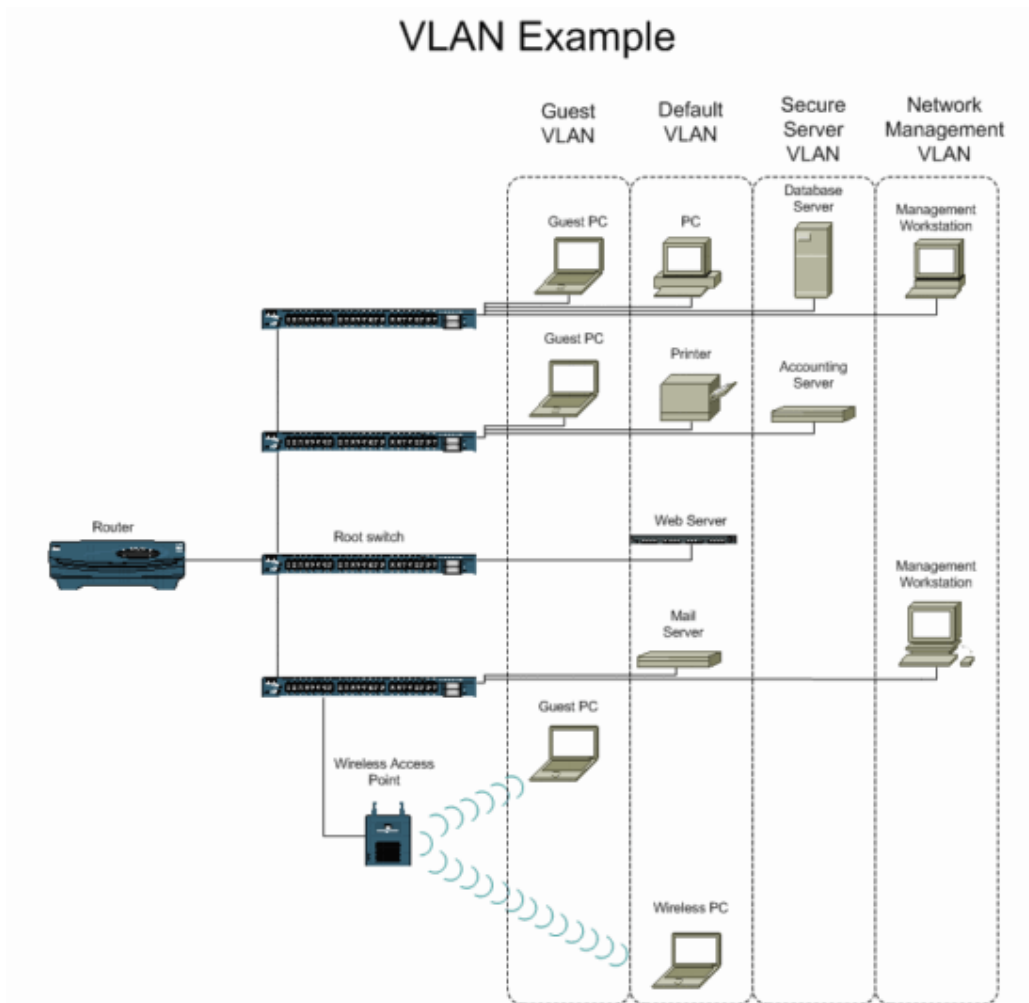
The table describes the recommended VLANs:

VLAN Name	VLAN ID	Description	Device Type
Default	20	Full access to the Internet and controlled access to other VLANs. All devices are in this VLAN by default.	General purpose VLAN; LAN PCs and servers

Network Management	21	Controlled access to other LAN devices and no access to the Internet	Network management devices
Secure Server	22	Controlled access to other VLANs and the Internet	Database servers or other devices with sensitive information
Guest	23	Full access to the Internet, no access to other VLANs	Guest users

Note: If your network uses a [Wireless LAN Controller Module \(WLCM\)](#), you must use a separate set of VLANs. For an overview of these VLANs, refer to [Configure Your Router for the Wireless LAN Controller Module](#).

The diagram shows an example of a network that uses VLANs:



Router Type

Cisco provides two types of router: Modular Routers and Integrated Services Routers. Modular routers are designed to be stand-alone routing devices, while Integrated Services Routers incorporate functions of a switch and/or wireless access point. Review the table to determine your router type:

Modular Router	Integrated Services Router
SB 100 series	

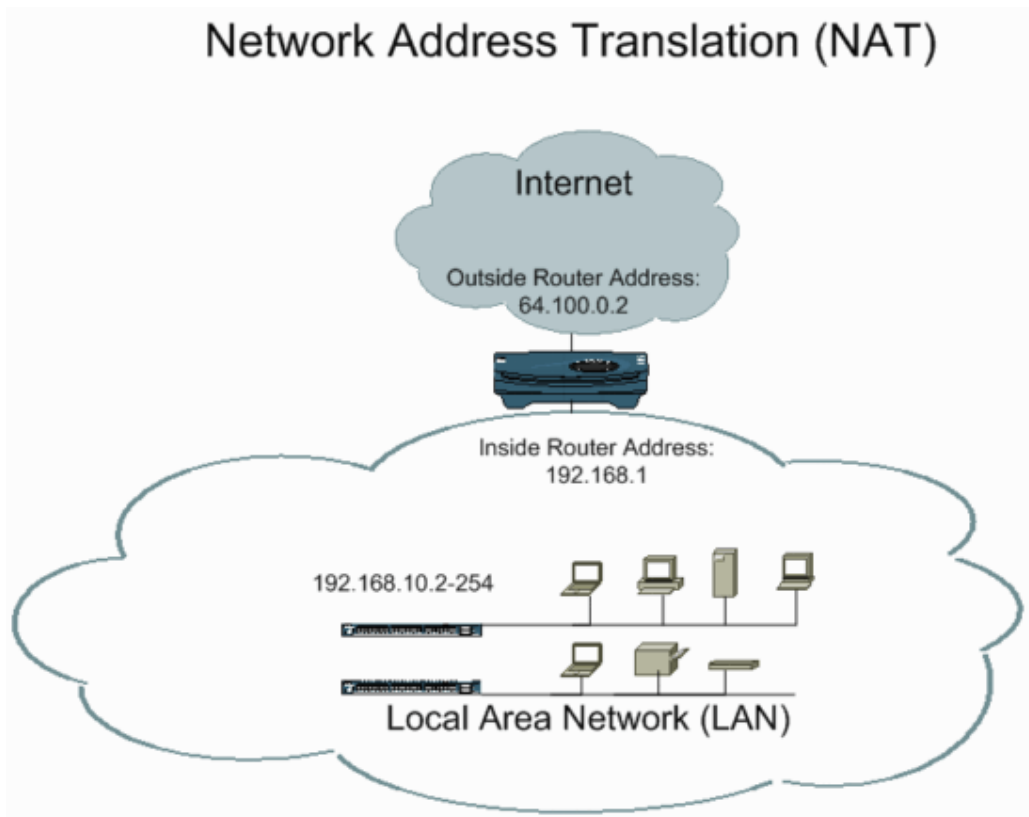
800 series	850 series, 870 series
1700 series	1800 series
2600 series	2800 series

NAT

The recommended configuration uses Network Address Translation to ease network configuration and add security.

The recommended configuration uses Network Address Translation (NAT) to simplify network configuration and add security. NAT translates between a single outside IP address and a set of internal IP addresses. NAT masks the IP addresses of devices inside the network while allowing them to communicate with the outside world.

The diagram illustrates the function of NAT within a network:



IP Address Assignments

There are two types of IP address assignment:

Static IP Address

A static IP address is an IP address that is permanently assigned to a network device. Static IP addresses are appropriate for servers or other network devices that require a known IP address.

The recommended configuration allows IP addresses .11 through .29 to be assigned statically. For example, the static IP addresses for the subnet 192.168.10.0 are 192.168.10.11 through 192.168.10.29.

DHCP

DHCP, or Dynamic Host Configuration Protocol, automatically assigns IP addresses to devices connected to the network. DHCP is appropriate for devices such as workstations that do not require a known IP address.

The recommended configuration is to configure the server to assign the IP addresses from .50 to .250. For example, the DHCP pool for the subnet 192.168.10.0 is 192.168.10.50 through 192.168.10.250.

To set up DHCP, you can enable the DHCP server included in Cisco routers or you can use an external non-Cisco DHCP server.

Note: Cisco does not support configurations with multiple VLANs on a non-Cisco DHCP server.

Domain Name Service

DNS, or Domain Name Service, resolves domain names such as www.cisco.com to a numeric IP address. DNS is required to access web sites and other services on the Internet. You can use DNS servers provided by your ISP, your own DNS servers, or a combination of both.

Device Passwords

To secure your site you need to create two types of access to your devices: an administrative username and password for read-only access and an enable password to modify configurations. It is important to use a strong password policy for all network passwords. Refer to the [Password Security](#) document for more information about how to create a strong password.

Internet Connection

There are four common Internet connection types:

- Ethernet
- T1/E1
- ISDN (BRI)
- DSL (ADSL/G.SHDSL)

Note: If you have an SDSL connection with a DSL modem, use the worksheets for an Ethernet connection.

Complete the section of the Internet worksheet for your connection type. The Internet worksheet contains a section for each Internet connection type and the available methods of encapsulation.

To complete the Internet Worksheet, you need to work with your Internet Service Provider (ISP), local telephone company, and building manager.

Note: Each type of Internet connection requires different equipment and configuration information. Be sure that you have completed and understood the information required for your Internet connection before you make any changes to your network design or purchase additional network equipment.

Encapsulation

Internet connections often use encapsulation as a way for network devices to communicate over disparate networks. Encapsulation places IP network traffic inside another protocol, such as point-to-point protocol (PPP) or Frame Relay, for delivery across a different kind of network.

These are the most common encapsulation types for T1 and E1 connections:

- HDLC
- PPP
- Frame Relay
- Ethernet
- PPP over Ethernet (PPPoE)

Channels

T1 and E1 connections use a certain number of the available channels on the physical circuit. The table summarizes the most common channel settings for T1 and E1 connections:

Circuit Type	Start Channel	End Channel

T1	1	24
E1	1	32

Encoding and Framing

T1 and E1 connections commonly utilize a line encoding method and data framing standard to send traffic over the network. The table summarizes the most common configurations for E1 and T1 connections:

Circuit Type	Encoding	Framing	Speed
T1	B8ZS	ESF	1.536 Mbps
E1	HDB3	CRC4	2.048 Mbps

Authentication

Your ISP may require authentication to verify your identity on the network. Authentication consists of a hostname and password used to connect to the ISP network. Authentication is common for ISDN links, and is used for some PPPoE, T1/E1, and ADSL connections.

ISP Address Assignment Method

In addition to the ISP information, you need to obtain information about your IP addresses from your ISP. These are the IP configuration types:

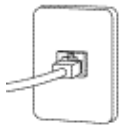
- **Dynamically Assigned IP Address:** The ISP automatically assigns your equipment an IP address with DHCP, but that address may change at any time without warning. Dynamic IP addresses are typical of residential cable modem and ISDN services.
- **Static IP Address:** The ISP assigns you a single static IP address that never changes, but you must configure your equipment with the IP address. Static IP addresses are often used for dedicated Internet circuits.

Shared devices on the network such as servers, printers, and scanners require a static IP address.

- **Range of IP Addresses:** The ISP assigns you a range or block of sequential IP addresses. You must configure your equipment with the IP addresses. Blocks of IP addresses are commonly available for dedicated Internet circuits. This documentation provides instructions on how to use the first IP address of a range of IP addresses.

Wall Jacks

Buildings with internal network cabling often have network jacks that are labeled with a number to identify each connection to the main telephone closet. If you have labeled wall jacks in your building, use the fields in the LAN addressing worksheet to document the wall jack number for each device in your network. If you have a computer that is not connected to a wall jack or if you do not have wall jacks in your building, leave these fields blank.



Power over Ethernet

Power over Ethernet (PoE) allows you to provide power to a network device over an Ethernet cable. PoE is commonly used to power wireless access points and IP phones. PoE requires a PoE-enabled device to run power over the Ethernet cable, such as a PoE-compatible switch or power injector. If you want to use PoE, refer to the documentation included with your PoE device for more information.

Wireless Site Survey

When you implement a wireless network, you need to perform a site survey to determine proper locations to mount each wireless access point to ensure proper communication across the network. If you want to implement a wireless network, refer to the documentation included with your wireless access point for instructions on how to perform a wireless site survey.

Wireless Access Point Types

Cisco wireless access points can operate in two modes: autonomous mode and lightweight mode. Autonomous access points have individual policies and configurations, while Lightweight Access Points (LAPs) receive policies and configurations from a centralized wireless LAN controller.

Note: The wireless access point module included on Cisco Integrated Services Routers (ISR) cannot be converted to lightweight mode.

If you want to use LAPs on your network, you must have a wireless LAN controller such as the Cisco Wireless LAN Controller Module (WLCM) and an external RADIUS server for client authentication.

Wireless Security

SMB SA documentation provides instructions for these authentication according to access point type:

- Autonomous Access Points: 802.1x/LEAP
- Lightweight Access Points (LAPs): 802.11i/WPA2

If you use LAPs, two security options are available:

- External RADIUS Server: The wireless network uses an external RADIUS server to authenticate users. This option provides greater security and requires that you provide an external RADIUS server.
- WPA2 Pre-Shared Key: A pre-shared password or passphrase is used to provide access to the wireless network. This option is less secure and requires that you create a [strong password](#) for the wireless network.

Wireless SSID

The Secure Session ID (SSID) is a name that identifies the wireless network to your users. The SSID should be a non-descriptive single word that does not identify the network, such as “zebra” or “kilo.” An SSID such as “tsunami,” “AcmeInc,” or “123mains” is a poor choice because it identifies the network.

Internet Services

If you have servers inside your network, you need to modify the network security configuration to allow incoming traffic to your servers.



Caution: If you change your security configuration, you can make your network vulnerable to attacks which can damage devices in your network. Ensure that you have properly secured and patched your servers before you make changes to your security configuration.

Internal Email Server

If you have an internal email server, you can enable incoming SMTP email traffic on ports 25 and 465 so that your email server can communicate with devices on the Internet. You do not need to allow incoming email if your email server is located at your ISP.

Internal Web Server

If you have an internal web server, you can enable incoming HTTP web traffic on ports 80 and 443 so that your web server can communicate with devices on the Internet. You do not need to allow incoming web traffic if your web server is located at your ISP.

Internal VPN Server

If you have an internal VPN server, you can enable incoming VPN traffic on so that your VPN server can communicate with external users. You do not need to allow incoming VPN traffic if your web server is located at your ISP.

Virtual Private Networks

A Virtual Private Network (VPN) allows computers at remote locations to communicate as though they were

directly connected. A VPN creates an encrypted "tunnel" through the Internet so that network can pass securely between two or more locations.

The Site IP Addressing plan provides unique IP addresses at each location to allow you to easily set up VPN connections.

[Back to Top](#)

Overview Worksheet

The overview worksheet is the first step in setting up a new device or network. Follow these steps to complete the overview worksheet:

1. If you have multiple sites in your organization, verify which site you are working on and assign it a number from 1 to 30. If you have only one site, use site number 1. Enter the site number in field A1 of the Overview Worksheet.
2. Consult the Site IP Addressing Plan and locate the the Default VLAN subnet for your site number. For example, the Default VLAN subnet for Site 1 is 192.168.10.0. Copy the Default VLAN subnet to field A2 of the Overview Worksheet.
3. Determine which VLANs you want to use in your network. Review the description of each VLAN to ensure that each device in the network is assigned to the appropriate VLAN. For more information on VLANs, see [Virtual LANs](#).

Note: Cisco does not support a non-Cisco DHCP server for multiple VLANs.

4. In field A3, check each VLAN you want to use, and copy the VLAN subnets for your site number to field A3 of the Overview Worksheet. For example, the Guest VLAN subnet for Site 1 is 192.168.13.1.
5. Determine whether you will run a Cisco or non-Cisco DHCP server. Note that a non-Cisco DHCP server is not supported for multiple VLANs. Check the DHCP server type you want to use in field A4.
6. Determine who is providing your DNS and check the appropriate box in field A5. For more information about DNS, see [Domain Name Service](#).
7. Determine what type of Internet connection you have and check the appropriate box in field A6. For more information about Internet connections, see [Internet Connection](#).
8. Verify what kind of router you have and check the appropriate box in field A7. For more information about router types, see [Router Type](#).

[Back to Top](#)

LAN Addressing Worksheet

Use this table to complete the LAN Addressing Worksheet:

Field Number	Field Name	Description
L1A	Subnet	Copy the subnet from field A2 of the Overview Worksheet to field L1A.
L2A	Subnet Mask	Enter 255.255.255.0 in field L2A.

L3A	DHCP Server	<ul style="list-style-type: none"> If you selected Cisco DHCP server in the Overview Worksheet, copy the router IP address from field L6A to field L3A. Otherwise, enter the IP address of your internal DHCP server. <p>For more information on DHCP, see DHCP.</p>
L4	DNS Server 1	<ul style="list-style-type: none"> If you have an internal DNS server, enter the IP address of the DNS server. If you use an ISP DNS server, copy the IP address in field B50 of the Internet Worksheet. <p>For more information about DNS, see Domain Name Service.</p>
L5	DNS Server 2	<ul style="list-style-type: none"> If you have an internal DNS server, enter the IP address of the DNS server in field L5. If you use an ISP DNS server, copy the IP address in field B51 of the Internet Worksheet to field L5. <p>For more information about DNS, see Domain Name Service.</p>
L6A	Router IP Address	Copy the subnet in field L1A to field L6A.
L7A	VLAN Number	<p>The Default VLAN is VLAN 20</p> <p>For more information about VLANs, see Virtual LANs.</p>
L8	Root-Switch IP Address	Copy the subnet in field L1A to field L8.
L9	Switch #2 IP Address	Copy the subnet in field L1A to field L9.
L10	Switch #3 IP Address	Copy the subnet in field L1A to field L10.
L11	Switch #4 IP Address	Copy the subnet in field L1A to field L11.
L12	Switch #5 IP Address	Copy the subnet in field L1A to field L12.
L13	Wireless Access Point	Copy the subnet in field L1A to field L13.
L14	Security Appliance-External	Copy the subnet in field L1A to field L14.

L15	Security Appliance-Internal	Copy the subnet in field L1A to field L14.
L16-L34	Static IP Assignments	<p>For devices in the Default VLAN that you want to assign a permanent IP address, follow these steps:</p> <ol style="list-style-type: none"> 1. Enter a description of the computer in the first field beginning with L16. 2. Copy the subnet in field L1A to the field next to the description to complete the IP address. 3. Ensure that the device is configured with the correct IP address. <p>Note: For more information about IP address assignment, see IP Address Assignment.</p>
L40A	VPN User Start Range	<p>Copy the subnet in field L1A to field L40A.</p> <p>The IP addresses in fields L40 and L41 are dynamically assigned to incoming VPN connections.</p> <p>For more information on VPNs, see Virtual Private Networks.</p>
L41A	VPN User End Range	<p>Copy the subnet in field L1A to field L41A.</p> <p>The IP addresses in fields L40 and L41 are dynamically assigned to incoming VPN connections.</p> <p>For more information on VPNs, see Virtual Private Networks.</p>
L50A	DHCP Start Range	<p>Copy the subnet in field L1A to field L50A.</p> <p>This is the first address in the pool of IP addresses that the DHCP server automatically distributes.</p> <p>Note: For more information about IP address assignment, see IP Address Assignment.</p>
L51A	DHCP End Range	<p>Copy the subnet in field L1A to field L51A.</p> <p>This is the last address in the pool of IP addresses that the DHCP server automatically distributes.</p> <p>Note: For more information about IP address assignment, see IP Address Assignment.</p>

[Back to Top](#)

Router Worksheet

Use this table to complete the Router Worksheet:

Note: If you have an Integrated Services Router, complete the [Integrated Services Router Worksheet](#).

Worksheet Field	Worksheet Field Name	Description
B9	Connection Type	<p>Check the type of Internet connection in field B9.</p> <p>For more information about Internet connections, see Internet Connection.</p>
B10	Administrative Account	<p>Enter the administrative account for the router in field B10. The recommended username is "admin".</p> <p>For more information about administrative accounts, see Device Passwords.</p>
B11	Administrative Password	<p>Create an administrative password for the router and enter it in field B11.</p> <p>For more information about administrative accounts, see Device Passwords.</p>
B12	Enable Password	<p>Create an enable password for the router and enter it in field B12.</p> <p>For more information about passwords, see Device Passwords.</p>
B13	Hours from GMT	Enter the number of hours from Greenwich Mean Time at the site in field B13.
B14	Time Zone	Enter the time zone for the site in field B14.
B15	Summer Time Zone	Enter the summer time zone for the site in field B15.
B16	Cisco DHCP Server?	If you are using a Cisco router as the DHCP server for the network, check Yes in field B16. Otherwise, check No .
B30	Router Model	<p>Enter the router model number in field B30.</p> <p>Note: The model number is required to obtain support from the SMB Technical Assistance Center (SMB TAC). The model number is printed on the back panel of the router.</p>
B31	Router Serial Number	<p>Enter the router serial number in field B31.</p> <p>Note: The serial number is required to obtain support from the SMB Technical Assistance Center (SMB TAC). The serial number is printed on the back panel of the router.</p> <p>Note: If you cannot locate the serial number, try the Cisco Product Identification Tool.</p>

B32	Router IOS Version	<p>Enter the router Cisco IOS® version in field B32.</p> <p>Note: If you do not have this information, you can retrieve it when you configure the router.</p>
B33	Router DRAM Memory	<p>Enter the amount of router DRAM memory in field B33.</p> <p>Note: If you do not have this information, you can retrieve it when you configure the router.</p>
B34	Router Flash Memory	<p>Enter the amount of flash memory in the router in field B34.</p> <p>Note: If you do not have this information, you can retrieve it when you configure the router.</p>
B35	LAN Interfaces	<p>LAN interfaces are router Ethernet ports that connect to LAN users. Routers typically have two or more built-in Ethernet interfaces.</p> <p>There are two types of Ethernet interfaces for LAN connections:</p> <ul style="list-style-type: none"> • FastEthernet • GigabitEthernet <p>Note: FastEthernet Interfaces are labeled 10/100 Ethernet ports in SDM.</p> <p>Interface numbers are often labeled on the router case. The document Configure Your Router with Security Device Manager provides further instructions on how to verify the interface numbers for your LAN interfaces.</p>
B36	Switch Port Interfaces	<p>Switch port interfaces act as a set of Ethernet ports and are configured a group.</p> <p>Switch port interfaces are labeled Ethernet Switch Ports in SDM.</p> <p>The document Configure Your Router with Security Device Manager provides instructions on how to verify these interface numbers.</p>
B37	Internet Interfaces	<p>Internet Interfaces are network interfaces built to support an Internet connection.</p> <p>Note: Some routers have a FastEthernet interface used for an Internet connection. This Interface is typically labeled WAN or Internet.</p> <p>The document Configure Your Router with Security Device Manager provides instructions on how to verify these interface numbers.</p>

B38	VLAN Interfaces	<p>A VLAN interface is a virtual interface used to configure built-in switch ports as a group. All routers with built-in switch port interfaces include a VLAN interface.</p> <p>The document Configure Your Router with Security Device Manager provides instructions on how to verify these interface numbers.</p>
-----	-----------------	--

[Back to Top](#)

Integrated Services Router Worksheet

Use this table to complete the Integrated Services Router Worksheet:

Note: If you have a wireless access point module or Wireless LAN Controller Module installed in your ISR, complete the wireless fields included in this worksheet. If you have an external wireless Access Point (AP), complete wireless fields in the [Wireless Network Assignments Worksheet](#).

Worksheet Field	Field Name	Description
B30	Router Model	<p>Enter the router model number in field B30.</p> <p>Note: The model number is required to obtain support from the SMB Technical Assistance Center (SMB TAC). The model number is printed on the back panel of the router.</p>
B31	Router Serial Number	<p>Enter the router serial number in field B31.</p> <p>Note: The serial number is required to obtain support from the SMB Technical Assistance Center (SMB TAC). The serial number is printed on the back panel of the router.</p> <p>Note: If you cannot locate the serial number, try the Cisco Product Identification Tool.</p>
B32	Router IOS Version	<p>Enter the router Cisco IOS® version in field B32.</p> <p>Note: If you do not have this information, you can retrieve it when you configure the router.</p>
B33	Router DRAM Memory	<p>Enter the amount of router DRAM memory in field B33.</p> <p>Note: If you do not have this information, you can retrieve it when you configure the router.</p>
B34	Router Flash Memory	<p>Enter the amount of flash memory in the router in field B34.</p> <p>Note: If you do not have this information, you can retrieve it when you configure the router.</p>
B9	Connection Type	<p>Check the type of Internet connection in field B9.</p> <p>For more information about Internet connections, see Internet Connection.</p>

B10	Administrative Account	<p>Enter the administrative account for the router in field B10. The recommended username is "admin".</p> <p>For more information about administrative accounts, see Device Passwords.</p>
B11	Administrative Password	<p>Create an administrative password for the router and enter it in field B11.</p> <p>For more information about administrative accounts, see Device Passwords.</p>
B12	Enable Password	<p>Create an enable password for the router and enter it in field B12.</p> <p>For more information about passwords, see Device Passwords.</p>
B13	Hours from GMT	Enter the number of hours from Greenwich Mean Time at the site in field B13.
B14	Time Zone	Enter the time zone for the site in field B14.
B15	Summer Time Zone	Enter the summer time zone for the site in field B15.
B16	Cisco DHCP Server	If you are using a Cisco router as the DHCP server for the network, check Yes in field B16. Otherwise, check No .
W10	Router IP Address	Copy the IP address of the router from field L6A of the LAN Addressing Worksheet to field W10.
W13	DNS Server	Copy the DNS server IP address from field L4 of the LAN Addressing Worksheet to field W13.
W14	Wireless Network Name	<p>Enter an SSID to identify the wireless network in field W16.</p> <p>For more information about SSIDs, see Wireless SSID.</p> <p>Note: This field applies only to an integrated access point module. If you have a wireless LAN Controller Module, complete field W26. For more information, see Wireless Access Point Types.</p>
W15	RADIUS Key	<p>Enter a password that you want users to use to log on to the network in field W18.</p> <p>Note: This field applies only to an integrated access point module. If you have a wireless LAN Controller Module, complete field W28. For more information, see Wireless Access Point Types.</p>

W34	Network	<p>Default</p> <p>Note: This field applies only to an integrated access point module. If you have a wireless LAN Controller Module, complete field W30. For more information, see Wireless Access Point Types.</p>
W36	Wireless Security	<p>802.1x / WPA</p> <p>Note: This field applies to autonomous access points only. If you have a wireless LAN Controller Module, see field W31. For more information, see Wireless Access Point Types.</p>
B35	LAN Interfaces	<p>LAN interfaces are router Ethernet ports that connect to LAN users. Routers typically have two or more built-in Ethernet interfaces.</p> <p>There are two types of Ethernet interfaces for LAN connections:</p> <ul style="list-style-type: none"> • FastEthernet • GigabitEthernet <p>Note: FastEthernet Interfaces are labeled 10/100 Ethernet ports in SDM.</p> <p>Interface numbers are often labeled on the router case. The document Configure Your Router with Security Device Manager provides further instructions on how to verify the interface numbers for your LAN interfaces.</p> <p>Enter the LAN interface numbers in field B35.</p>
B36	Switch Port Interfaces	<p>Switch port interfaces act as a set of Ethernet ports and are configured a group.</p> <p>Switch port interfaces are labeled Ethernet Switch Ports in SDM.</p> <p>The document Configure Your Router with Security Device Manager provides instructions on how to verify these interface numbers.</p> <p>Enter the switch interface numbers in field B36.</p>
B37	Internet Interfaces	<p>Internet Interfaces are network interfaces built to support an Internet connection.</p> <p>Note: Some routers have a FastEthernet interface used for an Internet connection. This Interface is typically labeled WAN or Internet.</p> <p>The document Configure Your Router with Security Device Manager provides instructions on how to verify these interface numbers.</p> <p>Enter the Internet interface number(s) in field B37.</p>

B38	VLAN Interfaces	<p>A VLAN interface is a virtual interface used to configure built-in switch ports as a group. All routers with built-in switch port interfaces include a VLAN interface.</p> <p>The document Configure Your Router with Security Device Manager provides instructions on how to verify these interface numbers.</p> <p>Enter the VLAN interface numbers in field B38.</p>
B39	Wireless LAN Controller	<p>The Wireless LAN Controller (WLCM) is an optional module centralizes management of policies and configurations for Lightweight Access Points (LAPs) on the wireless network. For more information on LAPs, see Wireless Access Point Types.</p> <p>The document Configure Your Router with Security Device Manager provides instructions on how to verify these interface numbers.</p> <p>Enter the WLCM interface number in field B39.</p>
W16	Controller Name	Enter the name for the WLCM in field W16.
W17	Controller Model	Enter the model number of the WLCM in field W17.
W18	Serial Number	Enter the serial number of the WLCM in field W18.
W19	Management IP Address	Enter the Management IP Address of the WLCM in field W19.
W20	Controller Manager IP Address	Enter the Controller Manager IP Address of the WLCM in field W20.
W21	Default Gateway	Enter the Default Gateway for the WLCM in field W21.
W22	RADIUS Server IP Address	If your network uses a RADIUS server for wireless security, enter the IP Address of the RADIUS server for the WLCM in field W22. For more information about wireless security, see Wireless Security .
W24	Admin Password	Enter the Admin Password for the WLCM in field W24.
W26	Wireless Network Name	Enter the names of your wireless networks, such as Default and Guest, in field W26.
W27	WPA Pre-Shared Key	If your wireless network uses a WPA Pre-Shared Key, enter the key in field W27. For more information about wireless security, see Wireless Security .
W28	RADIUS Key	Enter the RADIUS key used to authenticate wireless users in field W28.

W30	Network	Default
W31	Wireless Security	WPA2
W32	Lightweight APs	<p>Complete these fields for each Lightweight Access Point (LAP) in your wireless network:</p> <ul style="list-style-type: none"> • AP Name • Location • Model • Serial Number • Ethernet Jack • Switch Port
W33	Wireless Users	<p>Complete these fields for each wireless user in your wireless network:</p> <ul style="list-style-type: none"> • Create Date • Username • Full Name • Extension/Phone • Notes
S5-52	Switch Port Assignments	<p>If your Integrated Services Router (ISR) has a switch port module installed, use fields S5 through S52 to indicate this information about each switch port:</p> <ul style="list-style-type: none"> • Network: Indicate the VLAN for the switchport. • Wall Jack: If the device attached to the switchport is attached to a wall jack, indicate the wall jack number. • User: Provide a description of the device attached to the switchport. • Notes: Provide any additional comments about the user. <p>Note: If your network uses a Wireless LAN Controller Module (WLCM), you must use a separate set of VLANs. For an overview of these VLANs, refer to Configure Your Router for the Wireless LAN Controller Module.</p>

[Back to Top](#)

Internet Worksheet - ISDN

To complete the Internet Worksheet for ISDN, work with your Internet Service Provider to obtain this information:

Worksheet Field	Field Name	Description
B1	ISP Name	Enter the name of the company that provides your Internet service in field B1.
B2	ISP Support Number	Enter the number you call for ISP support in field B2.
B3	ISP Circuit ID	Enter the ISP customer ID or circuit ID that identifies your Internet connection in field B3.
B4	ISP Sales Contact	Enter the number for your ISP sales contact in field B4.
B5	Local Phone Carrier (LEC)	Enter your local telephone company in field B5. The local phone carrier is also known as the local exchange carrier (LEC).
B6	Local Phone Carrier (LEC) Circuit ID	<p>If you have a T1 or E1 circuit, enter the local phone carrier (LEC) circuit ID in field B6. If you have an ISDN line, enter the full telephone number or circuit ID.</p> <p>Note: If your ISP does not have the LEC circuit ID, you may be able to locate the circuit ID at your site. The LEC Circuit ID is often on a sticker on the telephone company jack where the circuit terminates. The telephone company jack is sometimes known as a smart jack. The jack is commonly located at the telephone company point of demarcation or demarc, which is typically in the main telephone closet on the ground floor of a building. In some cases, the telephone company extends the circuit inside the building to an office or another telephone closet. If your jack is located in the main telephone closet, you may need to contact your building management to gain access to the closet.</p>
B7	Demarc location	Enter the location in the network jack where your ISP terminates your Internet connection in field B7. The demarc is commonly located in the master telephone closet for the building, known as the minimum point of entry (MPOE). In some cases the demarc is extended to another location past the MPOE.

B8	Local Phone Carrier (LEC) Support Number	<p>Enter the customer service number for your phone line in field B8.</p> <p>Note: This field is required ISDN and DSL connections only.</p>
B40	Address Range	<p>Enter the IP address range assigned by your ISP in field B40.</p> <p>For more information about ISP IP assignments, see ISP Address Assignment Method.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p>
B41	Subnet Mask	<p>Enter the subnet mask assigned by your ISP in field B41.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p>
B43	Router IP Address Method	<p>Enter the router IP address method that your ISP uses in field B43.</p> <p>For more information about IP address assignment methods, see ISP Address Assignment Method.</p>
B45	IP Assignment Protocol	<p>If your Internet connection uses a dynamically assigned IP address, check the IP Assignment Protocol in field B45.</p> <p>For more information about IP address assignment methods, see ISP Address Assignment Method.</p>
B46	Router IP Address	<p>Enter the router IP Address in field B46.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p> <p>Note: If you have an ASA Security Appliance, use a public address from the pool in field B40.</p>
B47	ISP Router IP Address	<p>Enter the ISP router IP Address in field B47.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p>
B48	Domain Name	<p>Enter the Internet connection domain name in field B48.</p>

B50	DNS Server 1	<p>Enter the IP address of the first Domain Name Service (DNS) server in field B50.</p> <p>For more information about DNS, see Domain Name Service.</p>
B51	DNS Server 2	<p>Enter the IP address of the second Domain Name Service (DNS) server in field B51.</p> <p>For more information about DNS, see Domain Name Service.</p>
B52	Local Router Name	Enter your local router name in field B52.
A30	ISP Switch Type	<p>Enter the ISDN switch type in field A30.</p> <p>Note: You may need to contact your Local Phone Carrier (LEC) to complete this field.</p>
A31	Phone Number 1	<p>Enter the ISDN phone numbers in fields A31 and A32.</p> <p>Note: You may need to contact your Local Phone Carrier (LEC) to complete this field.</p>
A32	Phone Number 2	<p>Enter the ISDN phone numbers in fields A31 and A32.</p> <p>Note: You may need to contact your Local Phone Carrier (LEC) to complete this field.</p>
A33	SPID1	<p>If you have a 5ESS switch, enter the service profile identifier (SPID) numbers in fields A33 and A34.</p> <p>Note: You may need to contact your Local Phone Carrier (LEC) to complete this field.</p>
A34	SPID2	<p>If you have a 5ESS switch, enter the service profile identifier (SPID) numbers in fields A33 and A34.</p> <p>Note: You may need to contact your Local Phone Carrier (LEC) to complete this field.</p>
A35	ISP ISDN Access Number	Enter the ISDN access number in field A35.
A36	Call Data Rate	Enter the call speed for your connection in field A36, such as 56 Kbps.

A37	Authentication Type	<p>If your connection uses authentication, enter the authentication method for your connection in field A37.</p> <p>For more information about authentication, see Authentication.</p>
A38	Remote Host Name	<p>If your connection uses authentication, enter the remote host name in field A38.</p> <p>For more information about authentication, see Authentication.</p>
A39	Shared Secret	<p>If your connection uses authentication, enter the shared secret in field in A39.</p> <p>For more information about authentication, see Authentication.</p>
R21	VPN Group Name	<p>If your site has a VPN connection, enter the VPN group name in field R21. This name should be a non-descriptive single word that does not identify the network, such as "zebra" or "kilo." SSIDs such as "tsunami," "AcmeInc," or "123mainst" are poor choices because they identify the network.</p> <p>For more information on how to create strong passwords, refer to Password Security.</p>
R22	VPN Group Password	<p>If your site has a remote VPN connection, create strong password for the VPN group and enter it in field R22. The group password should differ from the admin and enable passwords because it is shared with end users.</p> <p>Refer to Password Security for information on how to create strong passwords.</p>
R32	Security Method	<p>If your site has a remote VPN connection, Cisco recommends 3DES as the VPN Security Method.</p>
R33	Remote VPN Address	<p>If your site has a remote VPN connection, enter the remote VPN address in field R33.</p>
R40	Remote VPN Users	<p>Enter information about each remote VPN user in the table beginning with field R40.</p> <p>Note: Do not record user passwords in this table.</p>

[Back to Top](#)

Internet Worksheet - DSL

To complete the Internet Service Provider Information, you need to work with your Internet Service Provider to obtain this information:

If you have an ADSL/G.SHDSL Internet connection, work with your ISP to complete these fields in the ADSL/G.SHDSL section of the Internet worksheet:

Worksheet Field	Field Name	Description
B1	ISP Name	Enter the name of the company that provides your Internet service in field B1.
B2	ISP support number	Enter the number you call for ISP support in field B2.
B3	ISP Circuit ID	Enter the ISP customer ID or circuit ID that identifies your Internet connection in field B3.
B4	ISP Sales Contact	Enter the number for your ISP sales contact in field B4.
B5	Local Phone Carrier (LEC)	Enter your local telephone company in field B5. The local phone carrier is also known as the local exchange carrier (LEC).
B6	Local Phone Carrier (LEC) Circuit ID	<p>If you have a T1 or E1 circuit, enter the local phone carrier (LEC) circuit ID in field B6. If you have an ISDN line, enter the full telephone number or circuit ID.</p> <p>Note: If your ISP does not have the LEC circuit ID, you may be able to locate the circuit ID at your site. The LEC Circuit ID is often on a sticker on the telephone company jack where the circuit terminates. The telephone company jack is sometimes known as a smart jack. The jack is commonly located at the telephone company point of demarcation or demarc, which is typically in the main telephone closet on the ground floor of a building. In some cases, the telephone company extends the circuit inside the building to an office or another telephone closet. If your jack is located in the main telephone closet, you may need to contact your building management to gain access to the closet.</p>

B7	Local Phone Carrier (LEC) Support Number	Enter the location in the network jack where your ISP terminates your Internet connection in field B7. The demarc is commonly located in the master telephone closet for the building, known as the minimum point of entry (MPOE). In some cases the demarc is extended to another location past the MPOE.
B8	Local Phone Carrier (LEC) Support Number	Enter the customer service number for your phone line in field B8. Note: This field is required ISDN and DSL connections only.
B40	Address Range	Enter the IP address range assigned by your ISP in field B40. For more information about ISP IP assignments, see ISP Address Assignment Method . Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.
B41	Subnet Mask	Enter the subnet mask assigned by your ISP in field B41. Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.
B43	Router IP Address Method	Enter the router IP address method that your ISP uses in field B43. For more information about IP address assignment methods, see ISP Address Assignment Method .
B45	IP Assignment Protocol	If your Internet connection uses a dynamically assigned IP address, check the IP Assignment Protocol in field B45. For more information about IP address assignment methods, see ISP Address Assignment Method .
B46	Router IP Address	Enter the router IP Address in field B46. Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank. Note: If you have an ASA Security Appliance, use a public address from the pool in field B40.

B47	ISP Router IP Address	<p>Enter the ISP router IP Address in field B46.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p>
B48	Domain Name	Enter the Internet connection domain name in field B48.
B50	DNS Server 1	<p>Enter the IP address of the first Domain Name Service (DNS) server in field B50.</p> <p>For more information about DNS, see Domain Name Service.</p>
B51	DNS Server 2	<p>Enter the IP address of the second Domain Name Service (DNS) server in field B51.</p> <p>For more information about DNS, see Domain Name Service.</p>
B52	Local Router Name	Enter your local router name in field B52.
A50	Circuit Speed	Enter the circuit speed in Kilobits per second (Kbps) in field A50.
A51	Encapsulation	<p>Enter the encapsulation for your connection in field A51. PPP over ATM encapsulation is the most common protocol for ADSL and G.SHDSL circuits.</p> <p>For more information about encapsulation, see Encapsulation.</p>
A52	ATM ILMI	<p>If your connection uses PPP over ATM encapsulation, enter the Interim Local Management Interface (ILMI) number in field A52.</p> <p>For more information about encapsulation, see Encapsulation.</p>
A53	ATM VC	<p>If your connection uses PPP over ATM encapsulation, enter the virtual path identifier/virtual channel identifier (VPI/VCI) for your connection in field A53.</p> <p>For more information about encapsulation, see Encapsulation.</p>

A54	Authentication Type	<p>If your connection uses authentication, enter the authentication method in field A54.</p> <p>For more information about authentication, see Authentication.</p>
A55	Remote Host Name	<p>If your connection uses authentication, enter the remote host name in field A55.</p> <p>For more information about authentication, see Authentication.</p>
A56	Shared Secret	<p>If your connection uses authentication, enter the shared secret in field in A56.</p> <p>For more information about authentication, see Authentication.</p>
R21	VPN Group Name	<p>If your site has a remote VPN connection, enter the VPN group name in field R21. This name should be a non-descriptive single word that does not identify the network, such as “zebra” or “kilo.” SSIDs such as “tsunami,” “AcmeInc,” or “123mainst” are poor choices because they identify the network.</p> <p>For more information on how to create strong passwords, refer to Password Security.</p>
R22	VPN Group Password	<p>If your site has a remote VPN connection, create strong password for the VPN group and enter it in field R22. The group password should differ from the admin and enable passwords because it is shared with end users.</p> <p>Refer to Password Security for information on how to create strong passwords.</p>
R32	Security Method	<p>If your site has a remote VPN connection, Cisco recommends 3DES as the VPN Security Method.</p>
R33	Remote VPN Address	<p>If your site has a remote VPN connection, enter the remote VPN address in field R33.</p>
R40	Remote VPN Users	<p>Enter information about each remote VPN user in the table beginning with field R40.</p> <p>Note: Do not record user passwords in this table.</p>

[Back to Top](#)

Internet Worksheet - T1/E1

To complete the Internet Service Provider Information, you need to work with your Internet Service Provider to obtain this information:

Worksheet Field	Field Name	Description
B1	Internet Service Provider	Enter the name of the company that provides your Internet service in field B1.
B2	Help Desk Phone	Enter the number you call for ISP support in field B2.
B3	ISP Circuit ID	Enter the ISP customer ID or circuit ID that identifies your Internet connection in field B3.
B4	Sales Contact	Enter the number for your ISP sales contact in field B4.
B5	Local Phone Carrier (LEC)	Enter your local telephone company in field B5. The local phone carrier is also known as the local exchange carrier (LEC).
B6	Local Phone Carrier (LEC) Circuit ID	<p>If you have a T1 or E1 circuit, enter the local phone carrier (LEC) circuit ID in field B6. If you have an ISDN line, enter the full telephone number or circuit ID.</p> <p>Note: If your ISP does not have the LEC circuit ID, you may be able to locate the circuit ID at your site. The LEC Circuit ID is often on a sticker on the telephone company jack where the circuit terminates. The telephone company jack is sometimes known as a smart jack. The jack is commonly located at the telephone company point of demarcation or demarc, which is typically in the main telephone closet on the ground floor of a building. In some cases, the telephone company extends the circuit inside the building to an office or another telephone closet. If your jack is located in the main telephone closet, you may need to contact your building management to gain access to the closet.</p>

B7	Circuit Demarc	<p>Enter the location in the network jack where your ISP terminates your Internet connection in field B7. The demarc is commonly located in the master telephone closet for the building, known as the minimum point of entry (MPOE). In some cases the demarc is extended to another location past the MPOE.</p>
B8	Local Phone Carrier (LEC) Support Number	<p>Enter the customer service number for your phone line in field B8.</p> <p>Note: This field is required ISDN and DSL connections only.</p>
B40	Address Range	<p>Enter the IP address range assigned by your ISP in field B40.</p> <p>For more information about ISP IP assignments, see ISP Address Assignment Method.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p>
B41	Subnet Mask	<p>Enter the subnet mask assigned by your ISP in field B41.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p>
B43	Router IP Address Method	<p>Enter the router IP address method that your ISP uses in field B43.</p> <p>For more information about IP address assignment methods, see ISP Address Assignment Method.</p>
B45	IP Assignment Protocol	<p>If your Internet connection uses a dynamically assigned IP address, check the IP Assignment Protocol in field B45.</p> <p>For more information about IP address assignment methods, see ISP Address Assignment Method.</p>
B46	Router IP Address	<p>Enter the router IP Address in field B46.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p> <p>Note: If you have an ASA Security Appliance, use a public address from the pool in field B40.</p>

B47	ISP Router IP Address	<p>Enter the ISP router IP Address in field B46.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p>
B48	Domain Name	Enter the Internet connection domain name in field B48.
B50	DNS Server 1	<p>Enter the IP address of the first Domain Name Service (DNS) server in field B50.</p> <p>For more information about DNS, see Domain Name Service.</p>
B51	DNS Server 2	<p>Enter the IP address of the second Domain Name Service (DNS) server in field B51.</p> <p>For more information about DNS, see Domain Name Service.</p>
B52	Local Router Name	Enter your local router name in field B52.
A20	Encoding	<p>Check the encoding type for your connection in field A20.</p> <p>For more information about encoding, see Encoding and Framing.</p>
A21	Framing	<p>Check the framing type for your connection in field A21.</p> <p>For more information about framing, see Encoding and Framing.</p>
A22	Encapsulation	<p>Check the encapsulation type for your connection in field A22.</p> <p>For more information about encapsulation, see Encapsulation.</p>
A23	Channel Assignments	<p>For field A23, indicate the channels that your circuit uses for data. If you have additional channels that carry another traffic type such as voice, label the channels accordingly.</p> <p>For more information about channels, see Channels.</p>

A24	Frame Relay DLCI	<p>Enter the data link connection identifier (DLCI) for your connection in field A24.</p> <p>Note: If your connection does not use Frame Relay encapsulation, leave this field blank.</p>
A25	Authentication Type	<p>If your connection uses authentication, enter the authentication method for your connection in field A25.</p> <p>For more information about authentication, see Authentication.</p>
A26	Remote Host Name	<p>If your connection uses authentication, enter the remote host name in field A26.</p> <p>For more information about authentication, see Authentication.</p>
A27	Shared Secret	<p>If your connection uses authentication, enter the shared secret in field in A27.</p> <p>For more information about authentication, see Authentication.</p>
R21	VPN Group Name	<p>If your site has a remote VPN connection, enter the VPN group name in field R21. This name should be a non-descriptive single word that does not identify the network, such as "zebra" or "kilo." SSIDs such as "tsunami," "AcmeInc," or "123mainst" are poor choices because they identify the network.</p> <p>For more information on how to create strong passwords, refer to Password Security.</p>
R22	VPN Group Password	<p>If your site has a remote VPN connection, create strong password for the VPN group and enter it in field R22. The group password should differ from the admin and enable passwords because it is shared with end users.</p> <p>Refer to Password Security for information on how to create strong passwords.</p>
R32	Security Method	<p>If your site has a remote VPN connection, Cisco recommends 3DES as the VPN Security Method.</p>
R33	Remote VPN Address	<p>If your site has a remote VPN connection, enter the remote VPN address in field R33.</p>

R40	Remote VPN Users	<p>Enter information about each remote VPN user in the table beginning with field R40.</p> <p>Note: Do not record user passwords in this table.</p>
-----	------------------	--

[Back to Top](#)

Internet Worksheet - Ethernet

To complete the Internet Service Provider Information, you need to work with your Internet Service Provider to obtain this information:

Worksheet Field	Field Name	Description
B1	Internet Service Provider	Enter the name of the company that provides your Internet service in field B1.
B2	Help Desk Phone	Enter the number you call for ISP support in field B2.
B3	ISP Circuit ID	Enter the ISP customer ID or circuit ID that identifies your Internet connection in field B3.
B4	Sales Contact	Enter the number for your ISP sales contact in field B4.
B5	Local Phone Carrier (LEC)	Enter your local telephone company in field B5. The local phone carrier is also known as the local exchange carrier (LEC).
B6	Local Phone Carrier (LEC) Circuit ID	<p>If you have a T1 or E1 circuit, enter the local phone carrier (LEC) circuit ID in field B6. If you have an ISDN line, enter the full telephone number or circuit ID.</p> <p>Note: If your ISP does not have the LEC circuit ID, you may be able to locate the circuit ID at your site. The LEC Circuit ID is often on a sticker on the telephone company jack where the circuit terminates. The telephone company jack is sometimes known as a smart jack. The jack is commonly located at the telephone company point of demarcation or demarc, which is typically in the main telephone closet on the ground floor of a building. In some cases, the telephone company extends the circuit inside the building to an office or another telephone closet. If your jack is located in the main telephone closet, you may need to contact your building management to gain access to the</p>

		closet.
B7	Circuit Demarc	Enter the location in the network jack where your ISP terminates your Internet connection in field B7. The demarc is commonly located in the master telephone closet for the building, known as the minimum point of entry (MPOE). In some cases the demarc is extended to another location past the MPOE.
B8	Local Phone Carrier (LEC) Support Number	Enter the customer service number for your phone line in field B8. Note: This field is required ISDN and DSL connections only.
B40	Address Range	Enter the IP address range assigned by your ISP in field B40. For more information about ISP IP assignments, see ISP Address Assignment Method . Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.
B41	Subnet Mask	Enter the subnet mask assigned by your ISP in field B41. Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.
B43	Router IP Address Method	Enter the router IP address method that your ISP uses in field B43. For more information about IP address assignment methods, see ISP Address Assignment Method .
B45	IP Assignment Protocol	If your Internet connection uses a dynamically assigned IP address, check the IP Assignment Protocol in field B45. For more information about IP address assignment methods, see ISP Address Assignment Method .
B46	Router IP Address	Enter the router IP Address in field B46. Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank. Note: If you have an ASA Security Appliance, use a public address from the pool in field B40.

B47	ISP Router IP Address	<p>Enter the ISP router IP Address in field B46.</p> <p>Note: If your Internet connection uses a dynamically assigned IP address, leave this field blank.</p>
B48	Domain Name	Enter the Internet connection domain name in field B48.
B50	DNS Server 1	<p>Enter the IP address of the first Domain Name Service (DNS) server in field B50.</p> <p>For more information about DNS, see Domain Name Service.</p>
B51	DNS Server 2	<p>Enter the IP address of the second Domain Name Service (DNS) server in field B51.</p> <p>For more information about DNS, see Domain Name Service.</p>
B52	Local Router Name	Enter your local router name in field B52.
B60	Encapsulation	<p>Check the encapsulation type for your connection in field B60.</p> <p>For more information about encapsulation, see Encapsulation.</p>
B62	Authentication Type	<p>If your connection uses authentication, enter the authentication method in field A62.</p> <p>For more information about authentication, see Authentication.</p>
B63	Remote Host Name	<p>If your connection uses authentication, enter the remote host name in field B63.</p> <p>For more information about authentication, see Authentication.</p>
B64	Shared Secret	<p>If your connection uses authentication, enter the shared secret in field in B64.</p> <p>For more information about authentication, see Authentication.</p>

R21	VPN Group Name	<p>If your site has a remote VPN connection, enter the VPN group name in field R21. This name should be a non-descriptive single word that does not identify the network, such as "zebra" or "kilo." SSIDs such as "tsunami," "AcmeInc," or "123mainst" are poor choices because they identify the network.</p> <p>For more information on how to create strong passwords, refer to Password Security.</p>
R22	VPN Group Password	<p>If your site has a remote VPN connection, create strong password for the VPN group and enter it in field R22. The group password should differ from the admin and enable passwords because it is shared with end users.</p> <p>Refer to Password Security for information on how to create strong passwords.</p>
R32	Security Method	<p>If your site has a remote VPN connection, Cisco recommends 3DES as the VPN Security Method.</p>
R33	Remote VPN Address	<p>If your site has a remote VPN connection, enter the remote VPN address in field R33.</p>
R40	Remote VPN Users	<p>Enter information about each remote VPN user in the table beginning with field R40.</p> <p>Note: Do not record user passwords in this table.</p>

[Back to Top](#)

Switch Port Assignment Worksheets

The site survey provides Switch Port Assignment worksheets to document up to five Ethernet switches with 48 ports each, or 200 total users. Worksheet S1 is for the first switch in the network, the "root" switch in the network. Additional worksheets are provided for additional, "non-root" switches. Use one non-root switch worksheet for each additional switch. All non-root switches are connected to the root switch.

The worksheets include this information for each port on the switch:

- Port number
- VLAN (Default, Network Management, Secure Server, or Guest). For more information about VLANs, see the [VLANs](#) section.
- Wall jack number

Note: If you have a computer that is not connected to a wall jack or if you do not have wall jacks in your building, leave this field blank. For more information about wall jacks, see [Wall Jacks](#).

- User description
- Additional notes

Complete one worksheet for each switch in your network. If you have a switch with 24 or fewer ports, omit the second page of the Switch Port Assignment worksheet.

Switch SW1 (Root Switch)

Worksheet Field	Field Name	Description
S1	Switch Name	The root switch is identified in field S1.
S2	Switch Model	<p>Enter the switch model number and switch serial number in field S2. The serial number is required to obtain support from the SMB Technical Assistance Center (SMB TAC). The serial number is printed on the back panel of the switch.</p> <p>Note: If you cannot locate the serial number, try the Cisco Product Identification Tool.</p>
S3	Description	Enter a brief description of the switch in field S3.
S4	Location	Enter the physical location of the switch in field S4.
S5	Admin Password, Enable Password	Enter the Admin password and Enable password for the switch in field S5.
S6	Port 1	If you have an external workstation or device to manage the switch, connect it to port 1 of the switch. Enter the management device wall jack number and any additional notes in field S6.
S7	Port 2	If you have a router, connect the router Ethernet interface to port 2 of the root switch. Enter the router wall jack number and any additional notes in field S6.
S8	Port 3	<p>Field S7 is reserved for future use of VOIP devices.</p> <p>Note: Cisco recommends that you reserve port 3 of the root switch for future use of Voice over IP (VOIP) devices.</p>
S9	Port 4	If you have a PIX Security Appliance, connect the inside interface to port 4 of the root switch. Enter the wall jack number and any additional notes in field S9.

S10	Port 5	If you have a PIX Security Appliance, connect the outside interface to port 5 of the root switch. Enter the wall jack number and any additional notes in field S10.
S11	Port 6	If you have a Wireless Access Point (AP) or Wireless Controller, connect the Ethernet interface to port 6 of the root switch. Enter the device IP address, wall jack number, and comments in field S11.
S12-S15	Ports 7-10	If you have non-root switches, connect them to ports 7-10 of the root switch. Enter the wall jack numbers and any additional notes about each non-root switch in fields S12 through S15. Note: It is important to connect each non-root switch directly to the root switch to maximize network performance and reliability.
S16-S53	Ports 11-48	Fields S16 through S53 list additional devices connected to the root switch. Enter the VLAN (Default, Network Management, Secure Server, or Guest), wall jack number, user description, and additional notes for each device in fields S16 through S53.

Switch SW2-SW5

Complete these fields on worksheet SW2 to document the second switch:

Worksheet Field	Field Name	Description
S60	Switch name	Enter the switch name in field S60.
S61	Switch model	Enter the switch model number and switch serial number in field S61. The serial number is required to obtain support from the SMB Technical Assistance Center (SMB TAC) . The serial number is printed on the back panel of the switch. Note: If you cannot locate the serial number, try the Cisco Product Identification Tool .
S62	Description	Enter a brief description of the switch in field S62.
S63	Location	Enter the physical location of the switch in field S63.
S64	Admin Password, Enable Password	Enter the Admin password and Enable password for the switch in field S64.

S65	Port 1	Connect port 1 of the switch to port 6 of the root switch. Enter the wall jack number of the root switch in field S65.
S66	Ports 2-48	Enter the VLAN (Default, Network Management, Secure Server, or Guest), wall jack number, user description, and additional notes for each device attached to the switch beginning at field S66.

Use the same instructions to complete the worksheets for switches SW3, SW4, and SW5. Use one copy of the non-root worksheets for each non-root switch.

[Back to Top](#)

Management VLAN Worksheet

Use this table to complete the Management VLAN Worksheet:

Field Number	Field Name	Explanation
L1B	Subnet	Copy the network management subnet from field A3 of the Overview Worksheet to field L1B.
L2B	Subnet Mask	Enter 255.255.255.0 in field L2B.
L3B	DHCP Server	Copy the subnet from field L1B to field L3B. Note: Cisco does not support multiple VLANs on a non-Cisco DHCP server.
L4	DNS Server 1	Copy the IP address you entered in field L4 of the LAN Addressing Worksheet to field L4.
L5	DNS Server 2	Copy the IP address you entered in field L5 of the LAN Addressing Worksheet to field L5.
L6B	Router IP Address	Copy the subnet from field L1B to field L6B.
L7B	VLAN Number	The Management VLAN is VLAN 21.
L8-L35	Static IP Assignments	Complete address and enter a description of each device with a static address in fields L8 through L35.
L50B	DHCP Start Range	Copy the subnet in field L1B to field L50B. This is the first address in the pool of IP addresses that the DHCP server automatically distributes. For more information on DHCP, see DHCP .

L51B	DHCP End Range	<p>Copy the subnet in field L1B to field L51B.</p> <p>This is the last address in the pool of IP addresses that the DHCP server automatically distributes.</p> <p>For more information on DHCP, see DHCP.</p>
------	----------------	---

[Back to Top](#)

Secure Server VLAN Worksheet

Use this table to complete the Secure Server VLAN Worksheet:

Field Number	Field Name	Explanation
L1C	Subnet	Copy the secure server subnet from field A3 of the Overview Worksheet to field L1C.
L2C	Subnet Mask	Enter 255.255.255.0 in field L2C.
L3C	DHCP Server	<p>Copy the subnet from field L1C to field L3C.</p> <p>Note: Cisco does not support multiple VLANs on a non-Cisco DHCP server.</p>
L4	DNS Server 1	Copy the IP address you entered in field L4 of the LAN Addressing Worksheet to field L4.
L5	DNS Server 2	Copy the IP address you entered in field L5 of the LAN Addressing Worksheet to field L5.
L6C	Router IP Address	Copy the subnet from field L1C to field L6C.
L7C	VLAN Number	The Secure Server VLAN is VLAN 22.
L8-L35	Static IP Assignments	Complete address and enter a description of each device with a static address in fields L8 through L35.
L50C	DHCP Start Range	<p>Copy the subnet in field L1C to field L50C.</p> <p>This is the first address in the pool of IP addresses that the DHCP server automatically distributes.</p> <p>For more information on DHCP, see DHCP.</p>
L51C	DHCP End Range	<p>Copy the subnet in field L1C to field L51C.</p> <p>This is the last address in the pool of IP addresses that the DHCP server automatically distributes.</p> <p>For more information on DHCP, see DHCP.</p>

[Back to Top](#)

Guest VLAN Worksheet

Use this table to complete the GuestVLAN Worksheet:

Field Number	Field Name	Explanation
L1D	Subnet	Copy the guest subnet from field A3 of the Overview Worksheet to field L1D.
L2D	Subnet Mask	Enter 255.255.255.0 in field L2D.
L3D	DHCP Server	Copy the subnet from field L1D to field L3D. Note: Cisco does not support multiple VLANs on a non-Cisco DHCP server.
L4	DNS Server 1	Copy the IP address you entered in field L4 of the LAN Addressing Worksheet to field L4.
L5	DNS Server 2	Copy the IP address you entered in field L5 of the LAN Addressing Worksheet to field L5.
L6D	Router IP Address	Copy the subnet from field L1D to field L6D.
L7D	VLAN Number	The Guest VLAN is VLAN 23.
L8-L35	Static IP Assignments	Complete address and enter a description of each device with a static address in fields L8 through L35.
L50D	DHCP Start Range	Copy the subnet in field L1D to field L50D. This is the first address in the pool of IP addresses that the DHCP server automatically distributes. For more information on DHCP, see DHCP .
L51D	DHCP End Range	Copy the subnet in field L1D to field L51D. This is the last address in the pool of IP addresses that the DHCP server automatically distributes. For more information on DHCP, see DHCP .

[Back to Top](#)

Internet Services Worksheet

The firewall blocks incoming email, web services, and Microsoft PPTP VPN services by default. If you have internal servers within your network such as email servers, web servers, or VPN servers, you can modify the firewall to allow this traffic.



Caution: Do not enable the services in this section unless they are required. If you open these services

this can subject internal machines to attack. For more information about Internet Services, see [Internet Services](#).

Use this table to complete the Internet Services Worksheet:

Field Number	Field Name	Explanation
F1	Internal Email Server IP Address	<p>If you have an internal email server, enter the IP address of your email server in field F1.</p> <p>Note: You do not need to make changes to the firewall if your email server is located at your ISP.</p>
F4	Internal Web Server IP Address	<p>If you have an internal web server, enter the internal IP address of the web server in field F4.</p> <p>Note: You do not need to make changes to the firewall if your web server is located at your ISP.</p>
F5	Microsoft PPTP VPN Server IP Address	<p>If you have remote users that use Microsoft PPTP VPN server to access your network, enter the IP address of the PPTP VPN server in field F5.</p> <p>Note: You do not need to make changes to the firewall if your VPN server is located at your ISP.</p>

For more information about Internet Services, see [Internet Services](#).

[Back to Top](#)

Security Appliance Worksheet

Use this table to complete the Security Appliance Worksheet:

Field Number	Field Name	Explanation
R1	Device Name	Enter the device name in field R1.
R2	Device Model	Enter the device model in field R2.
R3	Location	Enter the physical location of the security appliance in field R3.
R5	Serial Number	<p>Enter the security appliance serial number in field R5. The serial number is required to obtain support from the SMB Technical Assistance Center (SMB TAC). The serial number is printed on the back panel of the device.</p> <p>Note: If you cannot locate the serial number, try the Cisco Product Identification Tool.</p>

R7	External Interface	If you have an ASA 5500 Security Appliance, indicate the interface that is connected to the external network or the Internet. The recommended interface is interface 0 (FastEthernet 0/0).
R8	Internal Interface	If you have an ASA 5500 Security Appliance, indicate the interface that is connected to the internal network. The recommended interface is interface 1 (FastEthernet 0/1).
R9	Management IP Address	If you have an ASA 5500 Security Appliance, use the subnet from field L1A of the LAN Addressing Worksheet to complete the Management IP Address. This address provides administrative access to manage the security appliance. This field does not apply to the PIX Security Appliance.
R10	External IP Address	Enter the first available IP address in the IP Address range that you entered in field B40 of the Internet Worksheet. For example, if you are assigned the IP addresses 64.0.0.1-10 and 64.0.0.1 is assigned to your router, use 64.0.0.2 for the External IP Address.
R12	Internal IP Address	Enter the first address in the subnet that you entered in field L1A of the LAN Addressing Worksheet. For example, if the subnet in L1A is 192.168.10.0, enter 192.168.10.1. Note: If you have a security appliance, it acts as the default gateway for the network instead of the router.
R13	PAT IP Address	Enter an IP address from the IP Address range that you entered in field B40 of the Internet Worksheet. Note: The PAT IP address cannot be the same as the external or internal IP address.
R14	Default Gateway	Copy the IP address from field B46 of the Internet Worksheet to field R14.
R16	DNS Server	Copy the DNS server address from field L4 of the LAN worksheet to field R16.
R19	Administrative Password	Copy the administrative password from field B11 of the Router worksheet to field R19.
R20	Enable Password	Copy the enable password from field B12 of the Router worksheet to field R20.
R21	VPN Group Name	Enter the VPN group name in field R21. This name should be a non-descriptive single word that does not identify the network, such as "zebra" or "kilo." SSIDs such as "tsunami," "AcmeInc," or "123mainst" are poor choices because they identify the network. For more information on how to create strong passwords, refer to Password Security .

R22	VPN Group Password	<p>Create strong password for the VPN group and enter it in field R22. The group password should differ from the admin and enable passwords because it is shared with end users.</p> <p>Refer to Password Security for information on how to create strong passwords.</p>
R30	Untrusted Port	If you have a PIX Security Appliance, connect the untrusted port to your Internet connection.
R31	Switch Port	Enter the switch and port number connected to the security appliance. Cisco recommends that you connect the security appliance to port 4 of the Root Switch.
R32	Security Method	3DES is the recommended encryption method.
R33	Remote VPN Address	Enter the remote VPN address in field R33.
R40	Remote Users	<p>Enter information about each VPN user in the table beginning with field R40.</p> <p>Note: Do not record user passwords in this table.</p>

[Back to Top](#)

Wireless Network Assignments Worksheet

Use this table to complete the Wireless Network Assignments Worksheet:

Note: If your wireless network uses Lightweight Access Points (LAPs), complete the wireless fields included in the [Integrated Services Router Worksheet](#). For more information, see [Wireless Access Point Types](#).

Field Number	Field Name	Explanation
W1	Access Point Name	Enter the access point name in field W1.
W2	Model	Enter the model number of the Wireless Access Point (AP) in field W2.
W3	Location	Enter the installation location of the AP in field W3.
W4	Serial Number	<p>Enter the AP serial number in field W4. The serial number is required to obtain support from the SMB Technical Assistance Center (SMB TAC). The serial number is printed on the bottom panel of the AP.</p> <p>Note: If you cannot locate the serial number, try the Cisco Product Identification Tool.</p>
W5	Access Point IP Address	Copy the IP address of the AP from field L13 of the LAN Addressing Worksheet to field W5.

W6	Default Gateway	Copy the default gateway from field L6A of the LAN Addressing Worksheet to field W6.
W7	DNS Server	Copy the DNS server IP address from field L4 of the LAN Addressing Worksheet to field W7.
W8	Admin Password	Copy the admin password in field B11 of the Internet Worksheet to field W8.
W9	Enable Password	Copy the enable password in field B12 of the Internet Worksheet to field W9.
W10	Wireless Network Name	Enter an SSID to identify the wireless network in field W10. For more information about SSIDs, see Wireless SSID .
W11	RADIUS Key	Enter the RADIUS key used to authenticate wireless users in field W11.
W12	Ethernet Jack	Enter the Ethernet wall jack number that the AP is attached to in field W12.
W13	Switch Port	Enter the switch and port number connected to the AP. If you have a single AP, Cisco recommends that you connect the AP to Switch 1, Port 5.
W14	Network	Default
W15	Wireless Security	802.1x / WPA
W33	Wireless users	Enter contact information about each wireless user in field W33. Note: Do not record user passwords in this table.

[Back to Top](#)

Next Step

You have completed the site survey and worksheets. You can now begin the equipment installation process.

Choose the appropriate link to begin configuring your network. If you have multiple devices in your network, configure the router and switch(es) first.

Routers	Switches	Wireless	Security Appliance
Set Up Your Router	Set Up Your Catalyst Switch	Set Up Your Access Point	Set Up Your Security Appliance

[Back to Top](#)

Glossary

ADSL: Asymmetric Digital Subscriber Line. ADSL is a type of DSL connection designed to deliver more bandwidth downstream to the customer site than upstream.

Authentication: A way to verify the identity of a user on a network.

B8ZS: Binary 8-zero substitution. A common encoding type for T1 circuits.

CHAP: Challenge Handshake Authentication Protocol. A security feature supported on lines with PPP encapsulation that prevents unauthorized access.

Demarc: The point of demarcation between carrier network equipment and customer network equipment. In an office building the demarc is typically located in the ground floor or first floor telephone closet.

DHCP: Dynamic Host Configuration Protocol. A protocol that dynamically assigns IP addresses to devices on a network so that addresses are reused when hosts no longer need them.

DLCI: Data Link Connection Identifier. A network identifier used for Frame Relay connections.

DNS: Domain Name System. A system of servers that resolve domain names such as www.yahoo.com to a numeric IP address. DNS is required to access web sites and other services on the Internet.

ESF: Extended Super Frame. A common framing type for T1 circuits.

G.SHDSL: A DSL standard that delivers speeds of 192 Kbps up to 2.3 Mbps for upload and download.

HDLC: High-level Data Link Control. An encapsulation for serial network connections.

HTTP: HyperText Transfer Protocol. The protocol used to transfer network traffic related to the World Wide Web (www).

ILMI: Interim Local Management Interface. A configuration option for ADSL WAN connections

IP Address: A numeric address used to identify a network device.

ISDN: Integrated Services Digital Network. A communication protocol offered by telephone companies that permits telephone networks to carry data, voice, and other source traffic.

ISP: Internet Service Provider. A company that provides Internet access to other companies and individuals.

LAP: Lightweight Access Point. A wireless access point that is connected to a wireless LAN controller that manages the configuration for the wireless network.

LEC: Local Exchange Carrier. A telephone company that provides customer access to the world-wide public switched network through one of its central offices.

MPOE: Minimum Point of Entry. In a building with multiple demarcs, the MPOE is the demarc the furthest distance inside the building, typically the basement or first floor telephone closet.

PAP: Password Authentication Protocol. A security feature supported on lines with PPP encapsulation that prevents unauthorized access.

PPP: Point-to-Point Protocol. A network protocol used to connect different types of networks together. PPP is often used for high-speed Internet connections. PPP has an extension to dynamically assign an IP address when a hosts connects, similar to DHCP.

PPPoA: PPP over ATM. A common encapsulation type used for DSL connections.

PPPoE: PPP over Ethernet. A common encapsulation type used for DSL connections.

PPTP: Point-to-Point Tunneling Protocol. A protocol that creates a PPP tunnel to allow for transfer of other types of traffic such as VPN.

RADIUS: Remote Authentication Dial-In User Service. A method to verify the identity of users who remotely connect to a network. RADIUS is commonly used for wireless users and dial-up Internet connections.

SMTP: Secure Mail Transfer Protocol. A protocol for sending email messages between servers.

SSID: Service Set Identifier. A unique name used to identify a wireless network.

T1/E1: A high-speed network connection through the telephone-switching network. T1 and E1 connections provide high-speed connections to other networks or the Internet. T1 is a North American standard that provides a 1.544 Mbps connection. E1 is a primarily European standard that provides a 2.048 Mbps connection.

Wall Jack: Buildings with internal network cabling often have network jacks that are labeled with a number to identify each connection to the main telephone closet.

VPN: Virtual Private Network. A virtual network connection that enables computers at remote locations to communicate as though they were on the same physical network. A VPN can be encrypted with protocols such as IPSEC to secure the connection. VPNs are often used to connect remote users to a physical network or to connect networks in different physical locations.

[Back to Top](#)

Related Information

- [Site Survey Worksheets](#)
- [Password Security](#)