cisco.



Software Configuration Guide, Cisco IOS XE Fuji 16.9.x (Catalyst 9500 Switches)

First Published: 2018-07-18

Americas Headquarters

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883 © 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE	Preface v
	Document Conventions v
	Related Documentation vii
	Obtaining Documentation and Submitting a Service Request vi
CHAPTER 1	Contents 1
CHAPTER 2	Configuring the Switch Using the Web User Interface 3
	Setting up the Switch 3
	Connecting to the Switch 4
	Creating User Accounts 6
	Choosing Setup Options 7
	Configuring Basic Device Settings 7
	Configuring Your Device Based on a Site Profile 9
	Configuring VLAN Settings 12
	Configure STP Settings 12
	Configuring DHCP, NTP, DNS and SNMP Settings 13
	Configuring Port Settings 14

Notices 17

Contents



Preface

- \bullet Document Conventions , on page v
- Related Documentation, on page vii
- Obtaining Documentation and Submitting a Service Request, on page vii

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in bold font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> font.
Courier font	Terminal sessions and information the system displays appear in courier font.
Bold Courier font	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
$[x \mid y]$	Optional alternative keywords are grouped in brackets and separated by vertical bars.
$\{x \mid y\}$	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Description
[x {y z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!,#	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note	Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.
\mathcal{P}	
Тір	Means the following information will help you solve a problem.
Â	
ion	Means <i>reader be careful</i> . In this situation, you might do something that could result in equipment damage or loss of data.
D	
/er	Means <i>the described action saves time</i> . You can save time by performing the action described in the paragraph.
ß	
ıg	IMPORTANT SAFETY INSTRUCTIONS
	This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation



Before installing or upgrading the device, refer to the device release notes.

- Cisco Catalyst 9500 Series Switchesdocumentation, located at: http://www.cisco.com/go/c9500
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at: http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- Cisco Validated Designs documents, located at:

http://www.cisco.com/go/designzone

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER

Contents

Audio Video Bridging Cisco TrustSec High Availability Interface and Hardware Components IP **IP Multicast Routing** IPv6 Layer 2 Multiprotocol Label Switching Network Management Programmability Quality of Service Routing Security System Management VLAN

Contents

I



Configuring the Switch Using the Web User Interface

Note

Any figures included in the document are shown for illustrative purposes only.

- Setting up the Switch, on page 3
- Connecting to the Switch, on page 4
- Creating User Accounts, on page 6
- Choosing Setup Options, on page 7
- Configuring Basic Device Settings, on page 7
- Configuring Your Device Based on a Site Profile, on page 9
- Configuring VLAN Settings, on page 12
- Configure STP Settings, on page 12
- Configuring DHCP, NTP, DNS and SNMP Settings, on page 13
- Configuring Port Settings, on page 14

Setting up the Switch

After you complete the hardware installation, you need to setup the switch with configuration required to enable traffic to pass through the network. On your first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured.

The Web User Interface (Web UI) is an embedded GUI-based device-management tool that provides the ability to provision the device, to simplify device deployment and manageability, and to enhance the user experience. It comes with the default image, so there is no need to enable anything or install any license on the device. You can use WebUI to build configurations, and to monitor and troubleshoot the device without having CLI expertise.

Connecting to the Switch

Before you begin

Set up the DHCP Client Identifier on the client to get the IP address from the switch, and to be able to authenticate with Day 0 login credentials.

Setting up the DHCP Client Identifier on the client for Windows

- 1. Type regedit in the Windows search box on the taskbar and press enter.
- 2. If prompted by User Account Control, click Yes to open the Registry Editor.
- 3. Navigate to

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\ and locate the Ethernet Interface Global Unique Identifier (GUID).

4. Add a new REG_BINARY DhcpClientIdentifier with Data 77 65 62 75 69 for webui. You need to manually type in the value.

Figure 1: Setting up DHCP Client Identifier on Windows

computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentContro			p\Paramet	ers\Inter	faces\{4	6836ffc-6	358-4da1-t	o9f8-a2a10f1a0c48)			
stexstor		lame				Type		Data			
stisvc		🖄 (Default)				REG_SZ	2	(value not set)			
storahci	1	Address	ype			REG_D	WORD	0x00000000 (0)		
storfit	2	DhcpClie	ntldentifie			REG_BI	NARY	77 65 62 75 69			
stornyme		Edit Binary	Value							×	
storqosfit StorSvc		Luit billiary	value							~	le 01 00 79 00 00 00 00 00
storufs		Value name:									
storvsc	ſ	DhcpClientle	dentifier								
svsvc		Value data:									
swenum		0000	77	65	62	75	69		webu		
swprv		0000	177	05	62	/5	69		webu	1	
SynaMetSMI											
Synth3dVsc											
SynTP											
SynTPEnhService											
SysMain											
SystemEventsBroker											
SzCCID											
TabletInputService											
TapiSrv									ОК	Cancel	
E Tcpip										Calicer	
- Linkage	10	<u>وااد</u>				REO_D	WORD	UXJCHUOIS (1J	00271091)		
- Parameter											
Parameters Adapters											
> DNSRegisteredAdapters											
> ■ DivskegisteredAdapters > ■ Interfaces											
A line fraces											
[2e6a118d-8ff9-45c8-b861-13bbbf590a22]											
- {3f99fba7-ae95-43f6-b34c-e2fbdde8cb40}											
46836ffc-6358-4da1-b9f8-a2a10f1a0c48											
4828db99-4092-4a20-903b-e304a283e9f0											
- {7baa2017-910a-4c77-b968-a9beb40c9646											
- [{922467f8-ace4-4789-93b6-9a3799a7b574}											
- [(b20b01ef-9511-4f8d-af8d-c03a948db0e1)											
(b5fdd031-2580-445b-8430-074e5248bd14											

5. Restart the PC for the configuration to take effect.

Setting up the DHCP Client Identifier on the client for MAC

1. Go to System Preferences >Network >Advanced >TCP >DHCP Client ID: and enter webui.

L

				Netw	ork		Q Search
📄 Wi-Fi							
•	Wi-Fi	TCP/IP	DNS	WINS	802.1X	Proxies	Hardware
Config	jure IPv4:	Using DI	HCP			\$	
IPv4	Address:	XXXXXXXXXXX	16X XX 8				Renew DHCP Lease
Subr	net Mask:	2222/000	(12)55/2X(3)		DHCP	Client ID:	
	Router:	100000000	10XXXX				(If required)
Config	jure IPv6:	Automat	ically			\$	
	Router:	texexxxexx	S MXDexi	8X3496X			
IPv6	Address:	20087742	0050000	*****	KKK BXXXX	****	
Prefi	x Length:	162 8 X					
							Cancel
							Cancer

Figure 2: Setting up DHCP Client Identifier on MAC

2. Click **OK** to save the changes.

The bootup script runs the configuration wizard, which prompts you for basic configuration input: (Would you like to enter the initial configuration dialog? [yes/no]:). To configure Day 0 settings using the web UI, do not enter a response. Perform the following tasks instead:

- **Step 1** Make sure that no devices are connected to the switch.
- **Step 2** Connect one end of an ethernet cable to one of the downlink (non-management) ports on the active supervisor and the other end of the ethernet cable to the host (PC/MAC).
- **Step 3** Set up your PC/MAC as a DHCP client, to obtain the IP address of the switch automatically. You should get an IP address within the 192.168.1.x/24 range.

Figure 3: Obtaining the IP Address

ems > Network Connectio	ins		~ Ū	Search Network C
his connection Rename	e this connection View s	tatus of this connection	Change settings of this	connection 🖷
Cisco AnyConnect Secu Mobility Client Connec Disabled	tion 🦰 🌄 Uni	ernet dentified network el(R) Ethernet Connectio	Enable	Loopback Adapter d Loopback Adapter
VMware Network Ada VMnet8	Network Connection Details	s	×	
	Property Connection-specific DNS S Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask Lease Obtained Lease Expires IPv4 Default Gateway IPv4 DHCP Server IPv4 DHCP Server IPv4 DNS Server IPv4 WINS Server NetBIOS over Tcpip Enabl	Intel(R) Ethernet Connection 54-EE-75-DC-9F-06 Yes 192.168.1.3 255.255.255.0 Tuesday, June 11, 2019.8.25 Wednesday, June 12, 2019 192.168.1.1 192.168.1.1	:33 AM	

It may take up to three mins. You must complete the Day 0 setup through the web UI before using the device terminal.

- **Step 4** Launch a web browser on the PC and enter the device IP address (https://192.168.1.1) in the address bar.
- **Step 5** Enter the Day 0 username webui and password serial number of the switch.

The serial number is case sensitive.

What to do next

Create a user account.

Creating User Accounts

Setting a username and password is the first task you will perform on your device. Typically, as a network administrator, you will want to control access to your device and prevent unauthorized users from seeing your network configuration or manipulating your settings.

Step 1 Log on using the default username and password provided with the device.

Step 2 Set a password of up to 25 alphanumeric characters. The username password combination you set gives you privilege 15 access. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Figure 4: Create Account

Configuration Se	etup Wizard				
CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
Create New Account				Hardware and Software	details of the device.
Login Name				Platform Type:	
Password				IOS Installed:	
Confirm password				Serial Number:	
				Modules:	
				License Installed:	
		Create New Account			Basic Device Settings >

Choosing Setup Options

Select **Wired Network** to configure your device based on a site profile, and continue to configure switch wide settings. Otherwise, continue to the next step and configure only basic settings for your device.

Configuring Basic Device Settings

On the **Basic Device Settings** page configure the following information:

Step 1 In the **Device ID and Location Settings** section, type a unique name to identify your device in the network.

Step 2 Choose the date and time settings for your device. To synchronize your device with a valid outside timing mechanism, such as an NTP clock source, choose Automatic, or choose Manual to set it yourself.

Configuration Setup Wizard							
CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY		
Device ID and Location Settings				HELP A	ND TIPS		
Device Name			① Device name is mandatory				
Date & Time Mode	Automatic	•		device name is an identification that is gi			
				If manual time is set then the difference configuring the device.	n time will be adjusted at the time of		
Device Management Settings	Mon Aug 13 2018 14:18:06			The management VRF is a dedicated, se manage the router inband on switched v interfaces.			
Management Interface	gigabitethernet0/0			Select this to enable access to the devic password to authenticate user access to	e using Telnet. Configure a username and the device.		
Management IP	x.x.x.x			Select this to enable secure remote according to a configure a username and password to a configure a secure and password to a configure a secure according to a contract the secure according to contract the secure according to	ess to the device using Secure Shell (SSH). authenticate user access to the device.		
Subnet Mask	x.x.x.x			Enable transparent mode if you do not w transparent switch does not advertise its	ant the switch to participate in VTP. A VTP VLAN configuration and does not		
Default Gateway (optional)	x.x.x.x (optional)			synchronize its VLAN configuration base transparent switches do forward VTP ad	d on received advertisements, but vertisements that they receive out their trunk		
< Setup Options					Site Profile >		

Figure 5: Basic Settings - Device ID and Location Settings

- **Step 3** In the **Device Management Settings** section, assign an **IP address** to the management interface. Ensure that the IP address you assign is part of the subnet mask you enter.
- **Step 4** Optionally, enter an **IP** address to specify the default gateway.
- **Step 5** To enable access to the device using telnet, check the **Telnet** check box.
- **Step 6** To enable secure remote access to the device using Secure Shell (SSH), check the **SSH** check box.
- Step 7 Check the VTP transparent mode check box to disable the device from participating in VTP.

If you did not select **Wired Network**, in the earlier step, continue to the next screen to verify your configuration on the **Day 0 Config Summary** screen, and click **Finish**. To automatically configure your device based on a site profile, click **Setup Options**, and select **Wired Network**.

Figure 6: Basic Settings - Device Management Settings

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
	Mon Aug 13 2018 14:18:37			HELP /	AND TIPS
vice Management Settings					
lanagement Interface	gigabitethernet0/0			device name is an identification that is g	
fanagement IP	x.x.x.x			If manual time is set then the difference configuring the device.	in time will be adjusted at the time of
ubnet Mask	X.X.X.X			The management VRF is a dedicated, so manage the router inband on switched interfaces.	
efault Gateway (optional)	x.x.x.x (optional)			Select this to enable access to the devi password to authenticate user access to	ce using Telnet. Configure a username and o the device.
elnet				Select this to enable secure remote acc Configure a username and password to	ess to the device using Secure Shell (SSH authenticate user access to the device.
SH				Enable transparent mode if you do not w transparent switch does not advertise it	vant the switch to participate in VTP. A VT
TP transparent mode				synchronize its VLAN configuration base	
< Setup Options					Site Profile >

Configuring Your Device Based on a Site Profile

To ease your configuration tasks and save time, choose a site profile based on where your device may be installed and managed in your network. Based on the site profile you choose, your device is automatically configured according to Cisco best practices. You can easily modify this default configuration, from the corresponding detailed configuration screens.

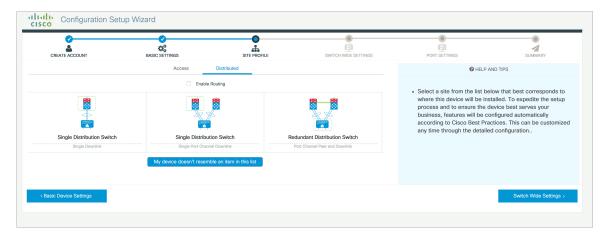
Choosing a site profile as part of Quick Setup allows you to configure your device based on the business needs of your enterprise. For example, you could use your device as an access switch, to connect client nodes and endpoints on your network, or as a distribution switch, to route packets between subnets and VLANs.

Setting	Single Distribution Switch (Single Downlink)	Single Distribution Switch (Single Port Channel Downlink)	Redundant Distribution Switch (Port Channel Peer and Downlink)
Hostname	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup
Spanning Tree Mode	RPVST+	RPVST+	RPVST+
VTP	Mode Transparent	Mode Transparent	Mode Transparent
UDLD	Enabled	Enabled	Enabled
Error Disable Recovery	Recovery mode set to Auto	Recovery mode set to Auto	Recovery mode set to Auto
Port Channel Load Balance	Source Destination IP	Source Destination IP	Source Destination IP
SSH	Version 2	Version 2	Version 2
SCP	Enabled	Enabled	Enabled
VTY Access to Switch	Enabled	Enabled	Enabled
Service Timestamp	Enabled	Enabled	Enabled
VLAN	The following VLANs are created:	The following VLANs are created:	The following VLANs are created:
	• Default VLAN	• Default VLAN	• Default VLAN
	• Data VLAN	• Data VLAN	• Data VLAN
	Voice VLAN	• Voice VLAN	• Voice VLAN
	Management VLAN	Management VLAN	Management VLAN

Table 1: Default Configuration Loaded with Each Site Profile (Distribution Switches)

Setting	Single Distribution Switch (Single Downlink)	Single Distribution Switch (Single Port Channel Downlink)	Redundant Distribution Switch (Port Channel Peer and Downlink)
Management Interface	Layer 3 settings	Layer 3 settings	Layer 3 settings
	configured on the	configured on the	configured on the
	management port, based	management port, based	management port, based
	on Quick Setup	on Quick Setup	on Quick Setup
QoS Policy	QoS Policy for	QoS Policy for	QoS Policy for
	Distribution defined	Distribution defined	Distribution defined
Uplink Interfaces	Selected uplink ports	Selected uplink ports	Selected uplink ports
	connect to other	connect to other	connect to other
	distribution or core	distribution or core	distribution or core
	switches	switches	switches
Downlink Interfaces	Downlink connections to	Downlink connections to	Downlink connections to
	access switches	access switches	access switches
	configured in Trunk mode	configured in Trunk mode	configured in Trunk mode
Port-channel	Port-channel to core created	Port-channel to core or access created	Port-channel to core or distribution created

Figure 7: Site Profile - Distribution Switches



CREATE ACCOUNT	C BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
	Access Dist	ibuted		() HELP A	ND TIPS
Single Downlink (Routed Access)	Enable Rousing Single Distribution SV Single Pot Channel Downlak (Rou My device doesn't resemble an	itch R Port Cr	edundant Distribution Switch	Select a site from the list below that been installed. To expected the setup process business, business,	and to ensure the device best serves omatically according to Cisco Best Pra
Basic Device Settings					Switch Wide Setting

Figure 8: Site Profile - Distribution Switches (with Routed Access)

Table 2: Default Configuration Loaded with Each Site Profile (Core Switches)

Setting	Standalone Core Switch (with ECMP Peers)	Standalone Collapsed Core Switch (with ECMP Peer and Port Channel Downlink)
Hostname	The hostname or device name you provided as part of Quick Setup	The hostname or device name you provided as part of Quick Setup
UDLD	Enabled	Enabled
Error Disable Recovery	Recovery mode set to Auto	Recovery mode set to Auto
Port Channel Load Balance	Source Destination IP	Source Destination IP
SSH	Version 2	Version 2
SCP	Enabled	Enabled
VTY Access to Switch	Enabled	Enabled
Mitigate Address Spoofing	Unicast RPF (uRPF) in strict mode	Unicast RPF (uRPF) in strict mode
Service Timestamp	Enabled	Enabled
Management Interface	Layer 3 settings configured on the management port, based on Quick Setup	Layer 3 settings configured on the management port, based on Quick Setup
QoS Policy	QoS Policy for Distribution/Core defined	QoS Policy for Distribution/Core defined
Uplink Interfaces	Selected uplink ports connect to MAN/WAN device	Selected uplink ports connect to MAN/WAN device
Downlink Interfaces	Downlink connections to access switches	Downlink connections to distribution switches

Setting	Standalone Core Switch (with ECMP Peers)	Standalone Collapsed Core Switch (with ECMP Peer and Port Channel Downlink)
Cross-connect Interfaces	Selected ports connect to other core switches	Selected ports connect to other core switches

Figure 9: Site Profile - Core Switches

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
	Access Distributed	Core		O HELP	AND TIPS
Standalone Core Switch with ECMP Peers		Standalone Collap with ECMP Peer and Pe		 Select a site from the list behavior will be inspected with the inspected will be inspected and the ensure the difference of the ensurement of	talled. To expedite the setu evice best serves your busi utomatically according to C

Configuring VLAN Settings

- **Step 1** In the VLAN Configuration section, you can configure both data and voice VLANs. Type a name for your data VLAN.
- Step 2 To configure a data VLAN, ensure that the Data VLAN check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.
- **Step 3** To configure a voice VLAN, ensure that the **Voice VLAN** check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate a VLAN range.

Configure STP Settings

- **Step 1** RPVST is the default STP mode configured on your device. You can change it to PVST from the **STP Mode** drop-down list.
- **Step 2** To change a bridge priority number from the default value 32748, change **Bridge Priority** to Yes and choose a priority number from the drop-down list.

Figure 10: VLAN and STP Settings

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
/LAN Configuration				HELP A	ND TIPS
Data VLAN Voice VLAN Management V Switch Wide Settings STP Configuration STP Mode Bridge Priority	RPVST	•		service by configuring ports phones on a specific VLAN. STP is to prevent bridge loops and the br	I allows you to enhance VoIP to carry IPvoice traffic from IP oadcast radiation that results from them. titles it as belonging to a particular domain. Device, use a severity level of warnings
Bridge Priority Number	32768	•		Protocol for network management and its network devices, such as switches, and re	collecting information from, and configuring outers on an IP network.
eneral Configuration					
< Site Profile					Port Settings >

Configuring DHCP, NTP, DNS and SNMP Settings

Step 1	In the Domain Details section, enter a domain name that the software uses to complete unqualified hostnames.
Step 2	Type an IP address to identify the DNS server. This server is used for name and address resolution on your device.
Step 3	In the Server Details section, type the IP address of the DNS server that you want to make available to DHCP clients.
Step 4	In the Syslog Server field, type the IP address of the server to which you want to send syslog messages.
Step 5	To ensure that your device is configured with the right time, date and timezone, enter the IP address of the NTP server with which you want to synchronize the device time.
Step 6	In the Management Details section, type an IP address to identify the SNMP server. SNMPv1, SNMPv2, and SNMPv3 are supported on your device.

Step 7 Specify the **SNMP community** string to permit access to the SNMP protocol.

Figure 11: DHCP, NTP, DNS and SNMP Settings

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
ieneral Configuration				HELP A	AND TIPS
omain Details					
Domain Name					d to carry user-generated traffic.Voice VLAt configuring ports to carry IPvoice traffic from
DNS Server				STP is to prevent bridge loops and the b	proadcast radiation that results from them.
erver Details					ntifies it as belonging to a particular domain
DHCP Server				Configure Syslog Client within the Cisco through emergencies to generate error malfunctions.	
Syslog Server				 Protocol for network manag 	
NTP Server				information from, and config as switches, and routers on	guring, network devices, such an IP network.
anagement Details					
< Site Profile					Port Settings >

What to do next

Configure port settings.

Configuring Port Settings

Step 1 Based on the site profile chosen in the earlier step which is displayed in the left-pane, select the **Port Role** from among the following options:

- Uplink For connecting to devices towards the core of the network.
- Downlink For connecting to devices further down in the network topology.
- Access For connecting guest devices that are VLAN-unaware.
- **Step 2** Choose an option from the **Select Switch** drop-down list.
- **Step 3** Make selections from the **Available** list of interfaces based on how you want to enable them and move them to the **Enabled** list.

Figure 12: Port Settings

CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY
	Port Role O Uplink O / Select Switch ALL	Access			
100 T S	Available (16)	Enabled (0)		
	Uplinks 😒	Interfaces			
	GigabitEthernet1/1/1	<i>></i>			
	GigabitEthernet1/1/2	÷			
S	GigabitEthernet1/1/3	>			
	GigabitEthernet1/1/4	>			
Switch Wide Settings					Day 0 Config Summary

What to do next

- Click Day 0 Config Summary to verify your setup.
- Click Finish.

Figure 13: Day 0 Config Summary

Configuration Set	tup Wizard							
CREATE ACCOUNT	BASIC SETTINGS	SITE PROFILE	SWITCH WIDE SETTINGS	PORT SETTINGS	SUMMARY			
SUMMARY					CLI Preview			
	This screen provides th	he summary of all the steps configured as a par	t of the day zero configuration. Please click Finish to configuration.	igure the device.				
> General Information	✓ User: test, ✓ Network Type: Wired	✓ User: test, ✓ Network Type: Wired , ✓ Site Profile: Single Access Switch - Single Uplink						
> Basic Device Configuration	🗸 Controller Name: test, 🗸 Managem	✓ Controller Name: test, ✓ Management Interface: gigabitethermet0/0(1.1.1.1),						
> Global Switch Settings	✓ Data VLAN: (), ✓ Voice VLAN: (not	✓ Data VLAN: (), ✓ Voice VLAN: (not configured), ✓ STP Mode: rapid-pvst, ✓ Bridge Priority: 32768, ✓ DNS Server: , ✓ DHCP Server: , ✓ NTP Server: , ✓ Syslag Server: , ✓ SNMP Server: , ✓ SNM						
> Port Configuration		Uplink Ports		Downlink Ports				
		No Ports were configured		No Ports were configured				
< Port Settings					Finish >			

Notices

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright [©] 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Notices