Provisioning

Zero-Touch Provisioning

Zero-Touch Provisioning (ZTP) automates the initial provisioning of Cisco network devices, reducing manual configuration efforts and enabling scalable deployment in heterogeneous network environments.

The Zero-Touch Provisioning feature is enabled automatically; no configuration is required.

Note:

The Zero-Touch Provisioning feature is enabled automatically; no configuration is required.

Key Features of Zero-Touch Provisioning

This section provides information about the DHCP server configuration, DHCPv6 support, Secure ZTP, bootstrapping information, and so on.

What is ZTP

Zero-touch provisioning (ZTP) is a network device provisioning method that:

- Automates the configuration of devices in heterogeneous network environments,
- Eliminates the need for manual intervention during initial installation, and
- Allows devices to self-configure using bootstrap interfaces. Guest Shell:

Guest Shell is a secure Linux-based container built into network devices that provides an environment for running Python automation scripts.

How ZTP works

- When a device supporting ZTP starts without a startup configuration, it enters ZTP mode.
- The device:
  - searches for a DHCP server,
  - configures its interface IP address, gateway, and DNS server IP address, and
  - enables Guest Shell.
- Guest Shell downloads a Python script from an HTTP or TFTP server to apply the initial configuration.
- After provisioning, Guest Shell remains enabled for further automation.

ZTP simplifies device provisioning, reduces operational delays, and ensures standardization in network setup.

DHCP server configuration for ZTP

A DHCP server configuration for Zero-Touch Provisioning (ZTP) is a network setup that:

- Enables automated device provisioning without manual intervention,
- Requires the DHCP server to operate on the same network as the new device, and
- Uses specific DHCP options to transmit operational data like script paths and server information.

In ZTP, the DHCP server plays a critical role in enabling automated provisioning. When a new device is powered on:

- It retrieves the IP address and information (HTTP/TFTP server address and Python script path) from the DHCP server.
- The DHCP server informs the device using:
  - Option 150: (Optional) Provides a list of IP addresses for the HTTP/TFTP server hosting the Python scripts.
  - Option 67: Supplies the file path of the Python script on the HTTP/TFTP server.

After receiving this information, the device:

- Connects to the HTTP/TFTP server and downloads the specified script.
- Uses the DHCP-provided default route to reach the server, as it initially lacks a configured route.

DHCP Client Behavior

From the Cisco IOS XE Amsterdam 17.2.1 release onwards, DHCP client options include advanced identification information such as:

Device Information	DHCPv4	DHCPv6
Product ID	124	16/toggles
Serial number	61/toggles	16/toggles

Device Information	DHCPv4	DHCPv6
MAC address	61/toggles	1
Cisco Network PnP	60	15

DHCPv6 and zero-touch provisioning

DHCP Version 6 (DHCPv6) support is implemented to enhance the Zero-Touch Provisioning feature. Notably, DHCPv6 operates by default on any Catalyst 9350 Series Switches that

initiate without existing configuration:

DHCPv6 is activated by default when devices boot without startup configurations. These devices are supported exclusively on Catalyst 9350 Series Switches.

The device leverages TFTP and HTTP protocols for downloading Python scripts, though both configurations revert to factory settings upon download failure.

For configuration, ensure appropriate HTTP or TFTP file paths are integrated within the DHCP configuration to facilitate DHCPv4 and DHCPv6 functionality effectively.

In deployment settings with both DHCPv4 and DHCPv6 options available, it is advisable to select either the IPv4 or IPv6 option to prevent conflicts. Consider scenarios where the same interface can possess both IP versions or manage traffic across separate interfaces with distinct IP protocols.

The following is a sample DHCPv4: {/etc/dhcp/dhcpd.conf:} host <hostname> {

hardware ethernet xx:xx:xx:xx:xx:xx;

option dhcp-client-identifier "xxxxxxxxxxxxx"; option host-name "<hostname>".

option log-servers x.x.x.x; fixed-address x.x.x.x;

if option vendor-class-identifier = "..." { option vendor-class-identifier "...";

if exists user-class and option user-class = "iPXE" { filename "http://x.x.x.x/…/<image>";

} else {

filename "http://x.x.x.x/…/<script-name>";

}

}

}

Secure ZTP protocols

Secure ZTP is a provisioning technique that:

- ensures devices validate their deployment in authorized networks,
- mandates integrity checks on provisioning data, and
- employs secure transport protocols for communication.

Secure ZTP remains enabled by default and coexists with classic ZTP, activating based on DHCP server responses and specific configuration options.

To use Secure ZTP, users must obtain an ownership voucher from a Cisco MASA server. Unlike classic ZTP, Secure ZTP exclusively supports Python scripts.

How secure ZTP works

Secure ZTP automates the onboarding process of Cisco devices by securely obtaining and validating bootstrapping data from trusted servers. The key components involved in this process are:

- Device: Enters ZTP mode, initiates the process, and validates bootstrapping data.
- DHCP server: Provides the IP address and ZTP-related options.
- Bootstrapping server: Provides signed data for device provisioning and redirection.
- Ownership voucher: Ensures the authenticity of the device and bootstrapping data. The process involves the following stages:

1. Device startup and DHCP option validation: When the device boots up and does not find the startup configuration, it enters ZTP mode and communicates with the DHCP server to obtain required options (143 for DHCPv4 or 136 for DHCPv6).
2. Recursive bootstrapping: The device iterates over bootstrapping servers in a recursive manner to retrieve valid bootstrapping data. If redirect data is returned, new servers are added to the list. This process continues until the required data is obtained or the server list is exhausted.
3. TLS handshake and server validation: The device authenticates itself using the Cisco Secure Unique Device Identifier (SUDI) certificate during the TLS handshake. It validates the server certificate either by using a previously learned server-trust anchor or without verification.
4. Retrieving and validating bootstrapping data:The device sends a RESTCONF POST request to the bootstrapping server, which responds with either onboarding or redirect data. The onboarding data is signed and validated using the device's private SUDI key for decryption (if required).
5. OS verification and update: The device checks if the running OS version matches the required version. If not, it downloads and installs the specific OS version, then reboots to restart the ZTP process.
6. Configuration application: After receiving onboarding information, the device starts the Guest Shell to execute customer-specific scripts and apply configuration data (in CLI or NETCONF format). Once completed, the Guest Shell is shut down.
7. Completion:

If the device is connected to a trusted server, it sends progress messages to indicate successful bootstrapping.

Result:

The Secure ZTP process securely provisions the device with the required configuration and software, ensuring it is ready for deployment in a trusted environment.

Secure ZTP Transport Protocol

Secure ZTP uses HTTPS as the transport protocol when communicating with the RESTCONF bootstrapping servers.

When establishing a connection, the device provides its Cisco Secure Unique Device Identifier (SUDI) certificate during the TLS handshake. The certificate serves as an

authentication token. No other authentication is supported. The SUDI certificate validates the device on the server side.

The bootstrapping server provides its own certificate during the TLS handshake to the

device. If the device has the server-trust anchor corresponding to this server, the device performs an X.509 certificate validation of the server certificate against the server-trust anchor. (The device can get the server-trust anchor from the redirect server.)

If the device does have a server-trust anchor, but the X.509 certificate is not validated

successfully, the device must discard the server-trust anchor, accept the connection, and mark the server as not trusted.

If the device does not have a server-trust anchor, it accepts the server certificate, but marks it as not trusted.

According to the RESTCONF protocol, a device must first initiate the root-resource discovery, before it can proceed with RPC requests. The following is a sample root-discovery request:

GET /.well-known/host-meta HTTP/1.1 Host: example.com

Accept: application/xrd+xml

The following is a sample root-discovery response:

HTTP/1.1 200 OK

Content-Type: application/xrd+xml Content-Length: nnn

<XRD xmlns='http://docs.oasis-open.org/ns/xri/xrd-1.0'>

<Link rel='restconf' href='/restconf_root'/>

</XRD>

The value in the HREF attribute is used in the follow-up requests to the RESTCONF server, for example, when

href='/restconf_root'

is received, the header for the get-bootstrapping-data RPC is POST /restconf_root/operations/ietf-sztp-bootstrap-server:

get-bootstrapping-data HTTP/1.1

The device receives a plain XML file, and the fields in the file are Base64 encoded. The

device runs Base64 decoding before extracting the information and attempting to recognize its structure. The decoded structure format can either be JSON or XML.

Dhcp options for secure ZTP

DHCP options for Secure ZTP are dynamic network configuration options used in Zero-Touch Provisioning (ZTP) systems that:

- support the provisioning of IPv4 and IPv6 clients with server URI information for secure bootstrapping,
- include Option 136 (DHCPv6) and Option 143 (DHCPv4), specifically designed for Secure ZTP, and
- initiate Secure ZTP handling functions when received by a ZTP-enabled device.

When a device in ZTP mode sends a DHCP discovery request and receives Options 136 and 143, it triggers the Secure ZTP bootstrapping process. The handling procedures continue indefinitely if the process fails, until successful completion or user intervention interrupts

it.

Bootstrapping servers

A bootstrapping server is a RESTCONF server that:

- uses the HTTPS data transport protocol,
- can serve as either a redirect server or an onboarding server, and
- facilitates initial device configuration through bootstrapping data. The bootstrapping process involves the following types of data:
- Required updated image: The required OS version, URLs for downloading the image, and instructions on validating the downloaded image.
- Preconfiguration script: A Python script to be executed before applying initial device configuration.
- Configuration: The initial device configuration in either Cisco IOS CLI format or NETCONF edit-config format.
- Postconfiguration script: A Python script to be executed after the initial device configuration is applied.

Bootstrapping servers can be categorized as trusted or untrusted:

- Trusted servers: These servers can provide unsigned bootstrapping data because they are pre-validated.
- Untrusted servers: These servers require validation of their certificate against the server's trust anchor. A trusted server can become untrusted if its certificate fails validation during the TLS handshake.

Bootstrapping data

Bootstrapping data is information a device obtains during the bootstrapping process which can be:

- signed, ensuring the data and sender have been verified,
- unsigned, accepted only under certain conditions, and
- composed of ownership vouchers, owner certificates, and conveyance artifacts when signed.

Signed Data:

- Trusted and requires presence of ownership voucher and owner certificate.
- Trusted servers can use signed data; however, this does not imply the server itself is trusted beyond the data exchange.

Unsigned Data:

- Accepted if received from a trusted server or if only redirect data.
- Not trusted if received from an untrusted onboarding server, leading the device to continue searching for data from other servers.

Trust Implications:

- Receiving signed data implies trust in the data itself, not the server.
- Servers providing unsigned data must be trusted to avoid errors. Examples:
- Redirect information being saved by the device for future TLS handshakes if signed.
- Unsigned onboarding information should result in an error if from an untrusted server.

Ownership vouchers

An ownership voucher is a cryptographic artifact that:

- securely assigns a pledge to an owner,
- contains YANG-modeled data encoded in a Cryptographic Message Syntax (CMS) structure, and
- is used in bootstrapping mechanisms to validate device ownership. Key Attributes:
- The voucher is signed using the device’s private key and verified using the device’s public key (trust anchor).
- It ensures secure communication between the Cisco MASA server and the device.
- The YANG-modeled data in the voucher includes metadata such as `serial-number`, `created-on`, `expires-on`, and `pinned-domain-cert`.

This is a sample ownership voucher:

yang-data voucher-artifact:

+ voucher

+---- created-on yang:date-and-time

+---- expires-on? yang:date-and-time

+---- assertion enumeration

+---- serial-number string

+---- idevid-issuer? binary

+---- pinned-domain-cert binary

+ domain-cert-revocation-checks? boolean

+---- nonce? binary

+---- last-renewal-date? yang:date-and-time

- Ownership vouchers are signed using the private key from the Cisco MASA server, which is securely stored in the Cisco Software Image Management (SWIM) server.
- Devices use their trust anchor (public key) to verify the voucher's signature.
- Fields like `created-on` and `expires-on` validate the voucher’s timeframe. Missing or invalid fields lead to rejection of the voucher.

Failure Conditions

If the signature validation fails or any required fields (e.g., `serial-number`) are incorrect, the bootstrapping process is deemed invalid. The device does not proceed with the

assigned configuration.

Owner certificates

An owner certificate is an X.509 certificate that:

- binds an owner's identity to a public key,
- enables a device to validate signatures in conveyed information, and
- plays a role in the bootstrapping process of device authentication.

Base64 encoding and decoding:

The data field in the bootstrapping process contains an owner certificate that is Base64 encoded. During validation, the Base64 encoding is decoded into a degenerate CMS structure.

Degenerate CMS structure:

This is a commonly used format for distributing X.509 certificates. A degenerate structure contains no signatures but can carry attached intermediate certificates.

After verifying the ownership voucher, the device extracts the pinned domain certificate and uses it to validate the owner certificate. The decoding process generates a DER-

encoded CMS structure of type "signedData." Examples:

- In a secure IoT deployment, the owner certificate ensures that devices can trust the conveyed information.
- A device receiving bootstrapping data validates the attached owner certificate before proceeding with configuration.

Uses of conveyed information

Conveyed information is a bootstrapping artifact that

- encodes essential redirect and onboarding data for devices,
- uses Base64 encoding for data fields, and
- undergoes signature verification using CMS structure certificates.

The process involves the device decoding Base64, then verifying the signature through owner certificate CMS structure and pinned domain certificate as the trust anchor.

Image update support process

The process of image update support ensures that a device runs the appropriate OS version during bootstrapping. It involves verifying the current OS version, downloading the required image, verifying it, and installing it if necessary.

The key components involved in this process are:

- Device: Checks, downloads, verifies, installs, and reboots the OS image based on the bootstrapping data.

- Bootstrapping data: Contains the required OS version, URLs for image downloads, and verification data.
- URLs: Used by the device to download the necessary OS image.
- Verification algorithm: Used to compare and validate the downloaded image against the provided hash in the bootstrapping data.

The process involves the following stages:

1. Verification of current version: The device checks if the current OS version matches the specified version in the bootstrapping data.
2. Downloading the image: If a mismatch occurs, the device downloads the OS image from the given URLs without modifying the URL or adding authentication information.
3. Image verification: The device calculates the image hash using the specified algorithm(s) and compares it against the provided hash.
4. Installation and reboot: Once verified, the device installs the image and reboots. It then enters the Secure ZTP process until the correct image is confirmed and proceeds with applying the on-boarding information.

Progress reporting

The device sends progress reports to the bootstrapping server. RFC 8572 provides more information on progress reporting.

When a bootstrapping server is trusted, it receives appropriate POST-request messages with the *ietf-sztp-bootstrap-server:report-progress* RPC.

There are two types of progress report messages—mandatory and optional. The mandatory reports indicate the start or termination of the bootstrapping process and include the

following types of reports:

- bootstrap-initiated
- bootstrap-error
- bootstrap-complete
- boot-image-installed-rebooting
- config-error
- parsing-error
- pre-script-error
- post-script-error

The rest of progress report messages are optional. Optional progress report messages are only sent to the server if the bootstrapping data has set the *reporting-level* parameter to *verbose*.

This is a sample report-progress request from the device to the server:

POST /restconf/operations/ietf-sztp-bootstrap-server:report-progress/HTTP/1.1 HOST: example.com

Content-Type: application/yang.data+xml

<input xmlns="urn:ietf:params:xml:ns:yang:ietf-sztp-bootstrap-server">

<progress-type>bootstrap-error</progress-type>

<message>Failed to decode data</message>

</input>

This is a sample *No content* response from the server:

HTTP/1.1 204 No Content

Date: Sat, 31 May 2021 17:02:40 GMT

Server: example-server

Sample configurations for zero-touch provisioning

This reference provides a step-by-step example of configuring a DHCP server on a device's management port using TFTP copy. This configuration is applicable for devices like Catalyst 3850, Catalyst 3650, and ISR 4000 when the DHCP server is connected through a management port.

The management port configuration enables devices to obtain a script or required files from a designated TFTP server during a Plug and Play (PnP) process. The DHCP scope is configured to provide the necessary IP parameters to the device.

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp excluded-address 10.1.1.1
Device(config)# ip dhcp excluded-address vrf Mgmt-vrf 10.1.1.1 10.1.1.10
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# vrf Mgmt-vrf
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 150 ip 203.0.113.254
Device(config-dhcp)# option 67 ascii /sample_python_dir/python_script.py
Device(config-dhcp)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# no ip dhcp client request tftp-server-address
Device(config-if)# end
```

NOTE:

- The option 150 command specifies the IP address of the TFTP server for device configuration purposes.
- The management VRF (Mgmt-vrf) ensures isolation of out-of-band management traffic from production data planes.
- Scripts downloaded using option 67 can automate device setup during the PnP process.

Configure a DHCP Server on a Management Port Using HTTP Copy

This is a sample DHCP server configuration using HTTP copy when the DHCP server is connected through the management port on a device. This configuration enables you to set up a DHCP pool and specify HTTP-based file transfer for device initialization:

Procedure

Configure a DHCP server on a device's management port using HTTP copy.

Example:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# vrf Mgmt-vrf
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 67 ascii http://198.51.100.1:8000/sample_python_2.py
Device(config-dhcp)# end
```

DHCP server configuration using TFTP in-band

This reference provides a sample configuration for setting up a DHCP server on a device using TFTP copy over an in-band port. The configuration is essential when working with devices like the Catalyst 3850 series, ensuring seamless operation and integration:

Device> enable

Device# configure terminal

Device(config)# ip dhcp excluded-address 10.1.1.1 Device(config)# ip dhcp pool pnp_device_pool

Device(config-dhcp)# network 10.1.1.0 255.255.255.0

Device(config-dhcp)# default-router 10.1.1.1

Device(config-dhcp)# option 150 ip 203.0.113.254

Device(config-dhcp)# option 67 ascii /sample_python_dir/python_script.py Device(config-dhcp)# exit

Device(config)# interface gigabitethernet 1/0/2

Device(config-if)# no ip dhcp client request tftp-server-address Device(config-if)# end

This configuration is designed to optimize DHCP operations through the in-band port while ensuring efficient management of network operations.

Configure a DHCP Server for In-Band Port Using HTTP

To configure a DHCP server using HTTP copy when the DHCP server is connected through an in-band port, follow this command sequence:

Procedure

Configure a DHCP server using HTTP copy.

Example:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp excluded-address 10.1.1.1
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 67 ascii http://192.0.2.1:8000/sample_python_2.py
Device(config-dhcp)# end
```

This configuration enables devices connected to the in-band port to automatically receive IP addresses and network configuration information.

Sample DHCP server configuration for script deployment on Linux Ubuntu devices

This reference provides sample configurations for a DHCP server on a Linux Ubuntu device to demonstrate how Python scripts can be copied to devices over a TFTP or HTTP server.

Prerequisites

Procedure

- A working Linux Ubuntu system with a DHCP server installed (e.g., `isc-dhcp-server`).
- Access to Python scripts hosted on a TFTP or HTTP server.
- A device (e.g., Catalyst 3850 switch) configured to receive DHCP configuration from the server.

What to do next

Configuration 1: Using a TFTP Server

The following sample DHCP server configuration retrieves a Python script from a TFTP server:

root@ubuntu-server:/etc/dhcp# more dhcpd.conf subnet 10.1.1.0 netmask 255.255.255.0 {

range 10.1.1.2 10.1.1.255;

host 3850 {

fixed-address 10.1.1.246 ;

hardware ethernet CC:D8:C1:85:6F:00;

option bootfile-name !<opt 67> " /python_dir/python_script.py"; option tftp-server-name !<opt 150> "203.0.113.254";

}

}

Configuration 2: Using an HTTP Server

The following sample DHCP server configuration retrieves a Python script hosted on an HTTP server:

Day0_with_mgmt_port_http

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.2 192.168.1.255;

host C2-3850 {

fixed-address 192.168.1.246 ; hardware ethernet CC:D8:C1:85:6F:00;

option bootfile-name "http://192.168.1.46/sample_python_2.py";

}

}

Device Activation: After starting the DHCP server, power on the management network-connected device. The rest of the configuration (e.g., downloading and running the Python script) is automatic.

- • Range Specification: Ensure the `range` command specifies a valid IP range that matches the subnet configuration.
  - Script Path: Confirm that the Python script paths are correctly specified for TFTP/HTTP servers.

These configurations automate script deployment to devices during DHCP initialization.

Configure a DHCPv6 Server on a Management Port Using TFTP Copy

This section provides a sample configuration of a DHCPv6 server connected to the management port and using TFTP to copy the required boot file. This example assumes VLAN 20 is configured, and the device is running in IPv6 mode.

Ensure the TFTP server address and file path are correct and reachable from the management port.

Validate the DHCPv6 pool after configuration using the **show ipv6 dhcp pool** command.

Procedure

Configure DHCPv6 server on a management port and use TFTP to copy the required boot file.

Example:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp pool pnp_device_pool
Device(config-dhcp)# vrf Mgmt-vrf
Device(config-dhcp)# network 10.1.1.0 255.255.255.0
Device(config-dhcp)# default-router 10.1.1.1
Device(config-dhcp)# option 67 ascii
http://198.51.100.1:8000/sample_python_2.py Device(config-dhcp)# end
```

Sample Python provisioning script

The sample Python script provided can be used from either an HTTP server or a TFTP server to execute various commands on a network device. This script performs the following

actions:

print "\n\n *** Sample ZTP Day0 Python Script *** \n\n" # Importing cli module

import cli

print "\n\n *** Executing show platform *** \n\n" cli_command = "show platform"

cli.executep(cli_command)

print "\n\n *** Executing show version *** \n\n" cli_command = "show version"

cli.executep(cli_command)

print "\n\n *** Configuring a Loopback Interface *** \n\n"

cli.configurep(["interface loop 100", "ip address 10.10.10.10 255.255.255.255", "end"]) print "\n\n *** Executing show ip interface brief *** \n\n"

cli_command = "sh ip int brief" cli.executep(cli_command)

print "\n\n *** ZTP Day0 Python Script Execution Complete *** \n\n"

This script is designed to automate preliminary configurations and checks on a network device, providing a streamlined approach to initial setup.

Boot logging and zero-touch provisioning output on Cisco 4000 Series Integrated Services Routers

This document presents a sample Zero-Touch Provisioning (ZTP) boot log for Cisco 4000 Series Integrated Services Routers, showcasing successful Guest Shell activation, Python script execution, and provisioning of the device for day-zero operations. The following sections provide an overview of the process and analysis of the key elements.

Overview

Zero-Touch Provisioning (ZTP) automatically configures a router upon boot-up without

manual intervention, simplifying device initialization. The provided boot log demonstrates critical events during provisioning, such as:

- Guest Shell activation,
- Execution of a Python script to configure device interfaces, and
- Successful configuration verification post-script execution.

Cryptographic Notice

This product includes cryptographic features and complies with U.S. and local regulations governing import, export, and usage. For details on U.S. laws concerning Cisco

cryptographic products, visit [Cisco Cryptographic Export

Compliance](http://www.cisco.com/wwl/export/crypto/tool/stqrg.html). If further assistance is required, email: export@cisco.com.

Sample ZTP Boot Log

The following is the full boot log output from a Zero-Touch Provisioning session:

% failed to initialize nvram

! <This message indicates that the startup configuration

is absent on the device. This is the first indication that the Day Zero work flow is going to start.>

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

*** Sample ZTP Day0 Python Script ***

*** Configuring a Loopback Interface *** Line 1 SUCCESS: interface loop 100

Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255

Line 3 SUCCESS: end

*** Executing show ip interface brief ***

Interface IP-Address OK? Method Status Protocol GigabitEthernet0/0/0 unassigned YES unset down down GigabitEthernet0/0/1 unassigned YES unset down down GigabitEthernet0/0/2 unassigned YES unset down down GigabitEthernet0/0/3 192.168.1.246 YES DHCP up up GigabitEthernet0 192.168.1.246 YES DHCP up up

Loopback100 10.10.10.10 YES TFTP up up

*** ZTP Day0 Python Script Execution Complete *** Press RETURN to get started!

The day zero provisioning is complete, and the Cisco IOS prompt is accessible.

Zero-Touch Provisioning successfully initializes the Cisco ISR 4000 Series Router, configures network interfaces via Python scripting, and verifies the setup, enabling seamless day-zero deployment.

Sample boot logs for Cisco Catalyst 9350 Series switches

The following sections display sample Zero-Touch Provisioning boot logs. These logs shows that Guest Shell is successfully enabled, the Python script is downloaded to the Guest Shell, and the Guest Shell executes the downloaded Python script and configures the

```
device for Day Zero.
=
% Checking backup nvram
% No config present. Using default config
FIPS: Flash Key Check : Begin
FIPS: Flash Key Check : End, Not Found, FIPS Mode Not Enabled
! <This message indicates that the startup configuration
is absent on the device. This is the first indication that the Day Zero work flow is going
 to start.>
```

Cisco IOS XE Everest 16.6.x to Cisco IOS XE Fuji 16.8.x

The following example shows the sample boot logs before the .py script is run:

*** Sample ZTP Day0 Python Script ***

...

*** ZTP Day0 Python Script Execution Complete ***

```
The following example shows how to configure the device for Day Zero provisioning:
Initializing Hardware...
System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P) Compiled Thu 02/20/2020
23:47:51.50
by rel
Current ROMMON image : Primary Last reset cause : SoftwareReload
C9350-48UXM platform with 8388608 Kbytes of main memory
Preparing to autoboot. [Press Ctrl-C to interrupt] 0
boot: attempting to boot from [flash:cat9k_iosxe.16.06.05.SPA.bin] boot: reading file
cat9k_iosxe.16.06.05.SPA.bin
##########################################################################
##########################
Both links down, not waiting for other switches Switch number is 1
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph
(c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19
and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec.
252.227-7013.
cisco Systems, Inc. 170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.5,
RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2018 by Cisco Systems,
 Inc.
Compiled Mon 10-Dec-18 12:52 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed
 under GPL
Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute
and/or
modify such GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software, or the applicable
 URL provided
on the flyer accompanying the IOS-XE
software.
% Checking backup nvram
% No config present. Using default config
FIPS: Flash Key Check : Begin
FIPS: Flash Key Check : End, Not Found, FIPS Mode Not Enabled
This product contains cryptographic features and is subject to United States and local
country laws governing
import, export, transfer and use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption. Importers, exporters,
 distributors and
users are responsible for compliance with U.S. and local country laws. By using this product
 you agree to
comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

```
If you require further assistance please contact us by sending email to export@cisco.com.
cisco C9350-48UXM (X86) processor with 1392780K/6147K bytes of memory. Processor board ID
FCW2144L045
2048K bytes of non-volatile configuration memory. 8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:. 11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.
Base Ethernet MAC Address : ec:1d:8b:0a:68:00 Motherboard Assembly Number : 73-17959-06
Motherboard
Serial Number : FOC21418FPQ
Model Revision Number : B0 Motherboard Revision Number : A0
Model Number : C9350-48UXM
System Serial Number : FCW2144L045
%INIT: waited 0 seconds for NVRAM to be available
SETUP: new interface Vlan1 placed in "shutdown" state
Press RETURN to get started!

*Sep 4 20:36:43.586: [IOX DEBUG] Waiting for another 5 secs Guestshell enabled successfully
*Sep 4 20:37:45.321: [IOX DEBUG] Checking for guestshell mount path
*Sep 4 20:37:45.321: [IOX DEBUG] Validating if guestshell is ready for use
*Sep 4 20:37:45.321: [IOX DEBUG] Guestshell enabled successfully
```

*** Sample ZTP Day0 Python Script ***

*** Executing show platform ***

```
Switch  Ports    Model                Serial No.   MAC address     Hw Ver.       Sw Ver.
------  -----   ---------             -----------  --------------  -------       --------
 1       68     C9350-48P             FVH2935LDJT  68d9.726c.1b00  V01           17.18.01

Mac persistency wait time: Indefinite
                                      Current
Switch#   Role        Priority      State
-----------------------------------------
1       Active          1          Ready
```

Switch Ports Model Serial No. MAC address Hw Ver. Sw Ver.

1 62 C9350-48UXM FCW2144L045 ec1d.8b0a.6800 V01 16.6.5

Switch/Stack Mac Address : ec1d.8b0a.6800 - Local Mac Address Mac persistency wait time: Indefinite

Current Switch# Role Priority State

*1 Active 1 Ready

*** Executing show version ***

```
ZTP_1: Executing Show Version
Cisco IOS XE Software, Version 17.18.01
Cisco IOS Software [IOSXE], Cisco L3 Switch Software (CISCO9K_IOSXE), Version 17.18.1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Wed 06-Aug-25 03:45 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 17.18.1r[FC3], RELEASE SOFTWARE (P)
C9350 uptime is 8 weeks, 6 days, 18 hours, 3 minutes
Uptime for this control processor is 8 weeks, 6 days, 18 hours, 6 minutes
System returned to ROM by PowerOn
System image file is "flash:packages.conf"
Last reload reason: PowerOn

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                      Technology-package
Current                       Type                         Next reboot
------------------------------------------------------------------------------
advantage               Smart License                    advantage


Smart Licensing Status: Smart Licensing Using Policy

cisco C9350-48P (X86) processor with 2099157K/6147K bytes of memory.
Processor board ID FVH2935LDJT
2 Virtual Ethernet interfaces
96 Gigabit Ethernet interfaces
8 TwentyFive Gigabit Ethernet interfaces
8 Fifty Gigabit Ethernet interfaces
20 Hundred Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
3072000K bytes of Crash Files at crashinfo:.
12582912K bytes of Flash at flash:.
3072000K bytes of Crash Files at crashinfo-2:.
12582912K bytes of Flash at flash-2:.

Base Ethernet MAC Address          : 68:d9:72:6c:1b:00
Motherboard Assembly Number        : 73-103862-02
Motherboard Serial Number          : FVH29341FH5
Model Revision Number              : B0
Motherboard Revision Number        : B0
Model Number                       : C9350-48P
System Serial Number               : FVH2935LDJT
CLEI Code Number                   : INMSF00ARA
Cloud ID                           : Q5CG-9BQ8-XKN6


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 68    C9350-48P          17.18.01          CISCO9K_IOSXE         INSTALL
```

Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.5, RELEASE SOFTWARE (fc3)

Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2018 by Cisco Systems, Inc.

Compiled Mon 10-Dec-18 12:52 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.

All rights reserved. Certain components of Cisco IOS-XE software are

licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the

documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE

software.

ROM: IOS-XE ROMMON

BOOTLDR: System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P) Switch uptime is 2 minutes

Uptime for this control processor is 4 minutes System returned to ROM by Reload Command

System image file is "flash:cat9k_iosxe.16.06.05.SPA.bin" Last reload reason: Reload Command

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

Technology-package Technology-package Current Type Next reboot

network-advantage Permanent network-advantage

cisco C9350-48UXM (X86) processor with 1392780K/6147K bytes of memory. Processor board ID FCW2144L045

36 Ethernet interfaces

1 Virtual Ethernet interface 4 Gigabit Ethernet interfaces

20 Ten Gigabit Ethernet interfaces 2 Forty Gigabit Ethernet interfaces

2048K bytes of non-volatile configuration memory. 8388608K bytes of physical memory.

1638400K bytes of Crash Files at crashinfo:. 11264000K bytes of Flash at flash:.

0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address : ec:1d:8b:0a:68:00 Motherboard Assembly Number : 73-17959-06 Motherboard Serial Number : FOC21418FPQ

Model Revision Number : B0 Motherboard Revision Number : A0

Model Number : C9350-48UXM

System Serial Number : FCW2144L045

Switch Ports Model SW Version SW Image Mode

* 1 62 C9350-48UXM 16.6.5 CAT9K_IOSXE BUNDLE

Configuration register is 0x102

*** Configuring a Loopback Interface ***

Line 1 SUCCESS: interface loop 100

Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255

Line 3 SUCCESS: end

*** Executing show ip interface brief ***

Interface IP-Address OK? Method Status Protocol Vlan1 unassigned YES unset administratively down down

GigabitEthernet0/0 10.127.128.3 YES DHCP	up	up
Tw1/0/1 unassigned YES unset down		down
Tw1/0/2 unassigned YES unset down		down
Tw1/0/3 unassigned YES unset down		down
Tw1/0/4 unassigned YES unset down		down
Tw1/0/5 unassigned YES unset down		down
Tw1/0/6 unassigned YES unset down		down
Tw1/0/7 unassigned YES unset down		down
Tw1/0/8 unassigned YES unset down		down
Tw1/0/9 unassigned YES unset down		down
Tw1/0/10 unassigned YES unset down		down
Tw1/0/11 unassigned YES unset down		down
Tw1/0/12 unassigned YES unset down		down
Tw1/0/13 unassigned YES unset down		down

Tw1/0/14	unassigned	YES unset down	down
Tw1/0/15	unassigned	YES unset down	down
Tw1/0/16	unassigned	YES unset down	down
Tw1/0/17	unassigned	YES unset down	down
Tw1/0/18	unassigned	YES unset down	down
Tw1/0/19	unassigned	YES unset down	down
Tw1/0/20	unassigned	YES unset down	down
Tw1/0/21	unassigned	YES unset down	down
Tw1/0/22	unassigned	YES unset down	down
Tw1/0/23	unassigned	YES unset down	down
Tw1/0/24	unassigned	YES unset down	down
Tw1/0/25	unassigned	YES unset down	down
Tw1/0/26	unassigned	YES unset down	down

Tw1/0/27	unassigned	YES unset down	down
Tw1/0/28	unassigned	YES unset down	down
Tw1/0/29	unassigned	YES unset down	down
Tw1/0/30	unassigned	YES unset down	down
Tw1/0/31	unassigned	YES unset down	down
Tw1/0/32	unassigned	YES unset down	down
Tw1/0/33	unassigned	YES unset down	down
Tw1/0/34	unassigned	YES unset down	down
Tw1/0/35	unassigned	YES unset down	down
Tw1/0/36	unassigned	YES unset down	down
Te1/0/37	unassigned	YES unset down	down
Te1/0/38	unassigned	YES unset down	down
Te1/0/39	unassigned	YES unset down	down

Te1/0/40	unassigned	YES unset down	down
Te1/0/41	unassigned	YES unset down	down
Te1/0/42	unassigned	YES unset down	down
Te1/0/43	unassigned	YES unset down	down
Te1/0/44	unassigned	YES unset down	down
Te1/0/45	unassigned	YES unset down	down
Te1/0/46	unassigned	YES unset down	down
Te1/0/47	unassigned	YES unset down	down
Te1/0/48	unassigned	YES unset up	up

GigabitEthernet1/1/1 unassigned YES unset down down GigabitEthernet1/1/2 unassigned YES unset down down GigabitEthernet1/1/3 unassigned YES unset down down GigabitEthernet1/1/4 unassigned YES unset down down Te1/1/1 unassigned YES unset down down Te1/1/2 unassigned YES unset down down Te1/1/3 unassigned YES unset down down Te1/1/4 unassigned YES unset down down Te1/1/5 unassigned YES unset down down Te1/1/6 unassigned YES unset down down Te1/1/7 unassigned YES unset down down Te1/1/8 unassigned YES unset down down Fo1/1/1 unassigned YES unset down down Fo1/1/2 unassigned YES unset down down

Loopback100 10.10.10.10 YES TFTP up up

*** Configuring username, password, SSH ***

Line 1 SUCCESS: username cisco privilege 15 password cisco Line 2 SUCCESS: ip domain name domain

Line 3 SUCCESS: line vty 0 15 Line 4 SUCCESS: login local

Line 5 SUCCESS: transport input all Line 6 SUCCESS: end

*** ZTP Day0 Python Script Execution Complete ***

C9350 support for Cisco IOS XE 17.18.x and beyond

The following example shows the sample boot logs before the .py script is run:

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: The process for the command is not

responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable

guestshell installed successfully Current state is: DEPLOYED

guestshell activated successfully Current state is: ACTIVATED

guestshell started successfully Current state is: RUNNING

Guestshell enabled successfully

The following example shows how to configure the device for Day Zero provisioning:

Both links down, not waiting for other switches Switch number is 1

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc. 170 West Tasman Drive

San Jose, California 95134-1706

Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.4, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compiled Thu 22-Aug-19 18:14 by mcpre

PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE, AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE

"SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement (EULA) and any relevant supplemental terms (SEULA) found at

http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

You hereby acknowledge and agree that certain Software and/or features are licensed for a particular term, that the license to such Software and/or features is valid only for the applicable term and that such Software and/or features may be shut down or otherwise terminated by Cisco after expiration

of the applicable license term (e.g., 90-day trial period). Cisco reserves the right to terminate any such Software feature electronically or by any other means available. While Cisco may provide alerts, it is your sole responsibility to monitor your usage of any such term Software feature to ensure that your systems and networks are prepared for a shutdown of the Software feature.

% Checking backup nvram

% No config present. Using default config

FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled

cisco C9350-48UXM (X86) processor with 1419044K/6147K bytes of memory. Processor board ID FCW2144L045

2048K bytes of non-volatile configuration memory. 8388608K bytes of physical memory.

1638400K bytes of Crash Files at crashinfo:. 11264000K bytes of Flash at flash:.

0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address : ec:1d:8b:0a:68:00 Motherboard Assembly Number : 73-17959-06 Motherboard Serial Number : FOC21418FPQ

Model Revision Number : B0 Motherboard Revision Number : A0

Model Number : C9350-48UXM

System Serial Number : FCW2144L045

%INIT: waited 0 seconds for NVRAM to be available

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: The process for the command is not

responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is

otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable

The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable The process for the command is not responding or is otherwise unavailable guestshell installed successfully

Current state is: DEPLOYED

guestshell activated successfully Current state is: ACTIVATED

guestshell started successfully Current state is: RUNNING

Guestshell enabled successfully

HTTP server statistics:

Accepted connections total: 0

*** Sample ZTP Day0 Python Script ***

*** Executing show platform ***

```
Device#show platform
Switch  Ports    Model               Serial No.   MAC address     Hw Ver.       Sw Ver.
------  -----   ---------            -----------  --------------  -------       --------
 1       68     C9350-48P            FVH2935LDJT  68d9.726c.1b00  V01           17.18.01

Mac persistency wait time: Indefinite
                                    Current
Switch#   Role        Priority      State
-----------------------------------------
1       Active          1          Ready
```

*** Executing show version ***

```
ZTP_1: Executing Show Version
Cisco IOS XE Software, Version 17.18.01
Cisco IOS Software [IOSXE], Cisco L3 Switch Software (CISCO9K_IOSXE), Version 17.18.1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Wed 06-Aug-25 03:45 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
```

```
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 17.18.1r[FC3], RELEASE SOFTWARE (P)
C9350 uptime is 8 weeks, 6 days, 18 hours, 3 minutes
Uptime for this control processor is 8 weeks, 6 days, 18 hours, 6 minutes
System returned to ROM by PowerOn
System image file is "flash:packages.conf"
Last reload reason: PowerOn

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                      Technology-package
Current                         Type                       Next reboot
------------------------------------------------------------------------------
advantage              Smart License                    advantage


Smart Licensing Status: Smart Licensing Using Policy

cisco C9350-48P (X86) processor with 2099157K/6147K bytes of memoExecutingry.
Processor board ID FVH2935LDJT
2 Virtual Ethernet interfaces
96 Gigabit Ethernet interfaces
8 TwentyFive Gigabit Ethernet interfaces
8 Fifty Gigabit Ethernet interfaces
20 Hundred Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
3072000K bytes of Crash Files at crashinfo:.
12582912K bytes of Flash at flash:.
3072000K bytes of Crash Files at crashinfo-2:.
12582912K bytes of Flash at flash-2:.

Base Ethernet MAC Address          : 68:d9:72:6c:1b:00
Motherboard Assembly Number        : 73-103862-02
Motherboard Serial Number          : FVH29341FH5
Model Revision Number              : B0
Motherboard Revision Number        : B0
Model Number                       : C9350-48P
System Serial Number               : FVH2935LDJT
CLEI Code Number                   : INMSF00ARA
Cloud ID                           : Q5CG-9BQ8-XKN6


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 68    C9350-48P          17.18.01          CISCO9K_IOSXE         INSTALL
```

Cisco IOS XE Software, Version 16.09.04

Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.4, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2019 by Cisco Systems, Inc. Compiled Thu 22-Aug-19 18:14 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.

All rights reserved. Certain components of Cisco IOS-XE software are

licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the

documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE

software.

ROM: IOS-XE ROMMON

BOOTLDR: System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P) Switch uptime is 4 minutes

Uptime for this control processor is 5 minutes System returned to ROM by Reload Command

System image file is "flash:cat9k_iosxe.16.09.04.SPA.bin" Last reload reason: Reload Command

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

Technology-package Technology-package Current Type Next reboot

network-advantage Smart License network-advantage None Subscription Smart License None

Smart Licensing Status: UNREGISTERED/EVAL EXPIRED

cisco C9350-48UXM (X86) processor with 1419044K/6147K bytes of memory. Processor board ID FCW2144L045

36 Ethernet interfaces

1 Virtual Ethernet interface 4 Gigabit Ethernet interfaces

20 Ten Gigabit Ethernet interfaces

2 TwentyFive Gigabit Ethernet interfaces 2 Forty Gigabit Ethernet interfaces

2048K bytes of non-volatile configuration memory. 8388608K bytes of physical memory.

1638400K bytes of Crash Files at crashinfo:. 11264000K bytes of Flash at flash:.

0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address : ec:1d:8b:0a:68:00

Motherboard Assembly Number : 73-17959-06 Motherboard Serial Number : FOC21418FPQ Model Revision Number : B0

Motherboard Revision Number : A0

Model Number : C9350-48UXM

System Serial Number : FCW2144L045

Switch Ports Model SW Version SW Image Mode

* 1 64 C9350-48UXM 16.9.4 CAT9K_IOSXE BUNDLE

Configuration register is 0x102

*** Configuring a Loopback Interface ***

Line 1 SUCCESS: interface loop 100

Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255

Line 3 SUCCESS: end

*** Executing show ip interface brief ***

Any interface listed with OK? value "NO" does not have a valid configuration Interface IP-Address OK? Method Status Protocol

Vlan1 unassigned NO unset up up

GigabitEthernet0/0 10.127.128.5 YES DHCP	up	up
Tw1/0/1 unassigned YES unset down		down
Tw1/0/2 unassigned YES unset down		down
Tw1/0/3 unassigned YES unset down		down
Tw1/0/4 unassigned YES unset down		down
Tw1/0/5 unassigned YES unset down		down
Tw1/0/6 unassigned YES unset down		down
Tw1/0/7 unassigned YES unset down		down
Tw1/0/8 unassigned YES unset down		down
Tw1/0/9 unassigned YES unset down		down
Tw1/0/10 unassigned YES unset down		down
Tw1/0/11 unassigned YES unset down		down
Tw1/0/12 unassigned YES unset down		down
Tw1/0/13 unassigned YES unset down		down
Tw1/0/14 unassigned YES unset down		down
Tw1/0/15 unassigned YES unset down		down
Tw1/0/16 unassigned YES unset down		down
Tw1/0/17 unassigned YES unset down		down

Tw1/0/18 unassigned YES unset down		down
Tw1/0/19 unassigned YES unset down		down
Tw1/0/20 unassigned YES unset down		down
Tw1/0/21 unassigned YES unset down		down
Tw1/0/22 unassigned YES unset down		down
Tw1/0/23 unassigned YES unset down		down
Tw1/0/24 unassigned YES unset down		down
Tw1/0/25 unassigned YES unset down		down

Tw1/0/26	unassigned	YES unset down	down
Tw1/0/27	unassigned	YES unset down	down
Tw1/0/28	unassigned	YES unset down	down
Tw1/0/29	unassigned	YES unset down	down
Tw1/0/30	unassigned	YES unset down	down
Tw1/0/31	unassigned	YES unset down	down
Tw1/0/32	unassigned	YES unset down	down
Tw1/0/33	unassigned	YES unset down	down
Tw1/0/34	unassigned	YES unset down	down
Tw1/0/35	unassigned	YES unset down	down
Tw1/0/36	unassigned	YES unset down	down
Te1/0/37	unassigned	YES unset down	down
Te1/0/38	unassigned	YES unset down	down
Te1/0/39	unassigned	YES unset down	down
Te1/0/40	unassigned	YES unset down	down
Te1/0/41	unassigned	YES unset down	down
Te1/0/42	unassigned	YES unset down	down
Te1/0/43	unassigned	YES unset down	down
Te1/0/44	unassigned	YES unset down	down
Te1/0/45	unassigned	YES unset down	down
Te1/0/46	unassigned	YES unset down	down
Te1/0/47	unassigned	YES unset down	down
Te1/0/48	unassigned	YES unset up	up

GigabitEthernet1/1/1	unassigned	YES unset down	down
GigabitEthernet1/1/2	unassigned	YES unset down	down

GigabitEthernet1/1/3	unassigned	YES unset down	down

GigabitEthernet1/1/4 unassigned YES unset down down Te1/1/1 unassigned YES unset down down Te1/1/2 unassigned YES unset down down Te1/1/3 unassigned YES unset down down Te1/1/4 unassigned YES unset down down Te1/1/5 unassigned YES unset down down Te1/1/6 unassigned YES unset down down Te1/1/7 unassigned YES unset down down Te1/1/8 unassigned YES unset down down Fo1/1/1 unassigned YES unset down down Fo1/1/2 unassigned YES unset down down TwentyFiveGigE1/1/1 unassigned YES unset down down TwentyFiveGigE1/1/2 unassigned YES unset down down Loopback100 10.10.10.10 YES TFTP up up

*** Configuring username, password, SSH ***

Line 1 SUCCESS: username cisco privilege 15 password cisco

**CLI Line # 1: WARNING: Command has been added to the configuration using a type 0 password.

However, type 0 passwords will soon be deprecated. Migrate to a supported password type

Line 2 SUCCESS: ip domain name domain Line 3 SUCCESS: line vty 0 15

Line 4 SUCCESS: login local

Line 5 SUCCESS: transport input all Line 6 SUCCESS: end

*** ZTP Day0 Python Script Execution Complete *** Press RETURN to get started!

C9350 support for Cisco IOS XE 17.18.x and beyond

The following example shows the sample boot logs before the .py script is run:

--- System Configuration Dialog ---

```
Would you like to enter the initial configuration dialog? [yes/no]: day0guestshell installed
 successfully
Current state is: DEPLOYED
day0guestshell activated successfully Current state is: ACTIVATED
day0guestshell started successfully Current state is: RUNNING
Guestshell enabled successfully
```

*** Sample ZTP Day0 Python Script ***

...

*** ZTP Day0 Python Script Execution Complete ***

```
Guestshell destroyed successfully
The following example shows how to configure the device for Day Zero provisioning:
Both links down, not waiting for other switches Switch number is 1
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph
(c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19
and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec.
252.227-7013.
Cisco Systems, Inc. 170 West Tasman Drive
San Jose, California 95134-1706
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems,
 Inc.
Compiled Tue 28-Apr-20 09:37 by mcpre
This software version supports only Smart Licensing as the software licensing mechanism.
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR LICENSE
KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE, AND/OR
SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE
```

```
"SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL ACCEPTANCE
OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING
TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.
Your use of the Software is subject to the Cisco End User License Agreement (EULA) and any
 relevant
supplemental terms (SEULA) found at
http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.
You hereby acknowledge and agree that certain Software and/or features are licensed for a
particular term,
that the license to such Software and/or features is valid only for the applicable term and
 that such Software
and/or features may be shut down or otherwise terminated by Cisco after expiration of the
applicable license
term (e.g., 90-day trial period). Cisco reserves
the right to terminate any such Software feature electronically or by any other means
available. While Cisco
may provide alerts, it is your sole responsibility to monitor your usage of any such term
Software feature to
ensure that your systems and networks are prepared for a shutdown of the Software feature.
% Checking backup nvram
% No config present. Using default config
FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled
All TCP AO KDF Tests Pass
cisco C9350-48UXM (X86) processor with 1343703K/6147K bytes of memory. Processor board ID
FCW2144L045
2048K bytes of non-volatile configuration memory. 8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:. 11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.
Base Ethernet MAC Address : ec:1d:8b:0a:68:00 Motherboard Assembly Number : 73-17959-06
Motherboard
Serial Number : FOC21418FPQ
Model Revision Number : B0 Motherboard Revision Number : A0
Model Number : C9350-48UXM
System Serial Number : FCW2144L045
```

--- System Configuration Dialog ---

```
Would you like to enter the initial configuration dialog? [yes/no]: day0guestshell installed
 successfully
Current state is: DEPLOYED
day0guestshell activated successfully Current state is: ACTIVATED
day0guestshell started successfully Current state is: RUNNING
Guestshell enabled successfully
HTTP server statistics:
Accepted connections total: 0
```

*** Sample ZTP Day0 Python Script ***

*** Executing show platform ***

```
Device#show platform
Switch  Ports    Model               Serial No.   MAC address     Hw Ver.       Sw Ver.
------  -----   ---------            -----------  --------------  -------       --------
 1       68     C9350-48P            FVH2935LDJT  68d9.726c.1b00  V01           17.18.01

Mac persistency wait time: Indefinite
                                    Current
Switch#   Role        Priority      State
-----------------------------------------
1       Active          1          Ready
```

*** Executing show version ***

```
ZTP_1: Executing Show Version
Cisco IOS XE Software, Version 17.18.01
Cisco IOS Software [IOSXE], Cisco L3 Switch Software (CISCO9K_IOSXE), Version 17.18.1,
```

```
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
Compiled Wed 06-Aug-25 03:45 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2025 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 17.18.1r[FC3], RELEASE SOFTWARE (P)
C9350 uptime is 8 weeks, 6 days, 18 hours, 3 minutes
Uptime for this control processor is 8 weeks, 6 days, 18 hours, 6 minutes
System returned to ROM by PowerOn
System image file is "flash:packages.conf"
Last reload reason: PowerOn

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                      Technology-package
Current                       Type                         Next reboot
------------------------------------------------------------------------------
advantage              Smart License                    advantage


Smart Licensing Status: Smart Licensing Using Policy

cisco C9350-48P (X86) processor with 2099157K/6147K bytes of memory.
Processor board ID FVH2935LDJT
2 Virtual Ethernet interfaces
96 Gigabit Ethernet interfaces
8 TwentyFive Gigabit Ethernet interfaces
8 Fifty Gigabit Ethernet interfaces
20 Hundred Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
16777216K bytes of physical memory.
3072000K bytes of Crash Files at crashinfo:.
12582912K bytes of Flash at flash:.
3072000K bytes of Crash Files at crashinfo-2:.
12582912K bytes of Flash at flash-2:.

Base Ethernet MAC Address          : 68:d9:72:6c:1b:00
Motherboard Assembly Number        : 73-103862-02
Motherboard Serial Number          : FVH29341FH5
Model Revision Number              : B0
Motherboard Revision Number        : B0
Model Number                       : C9350-48P
System Serial Number               : FVH2935LDJT
CLEI Code Number                   : INMSF00ARA
Cloud ID                           : Q5CG-9BQ8-XKN6
```

```
Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 68    C9350-48P          17.18.01          CISCO9K_IOSXE         INSTALL
```

RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems, Inc.

Compiled Tue 28-Apr-20 09:37 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2020 by cisco Systems, Inc.

All rights reserved. Certain components of Cisco IOS-XE software are

licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the

documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE

software.

ROM: IOS-XE ROMMON

BOOTLDR: System Bootstrap, Version 17.2.1r[FC1], RELEASE SOFTWARE (P)

Switch uptime is 4 minutes

Uptime for this control processor is 9 minutes System returned to ROM by Reload Command

System image file is "flash:cat9k_iosxe.16.12.03a.SPA.bin" Last reload reason: Reload Command

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

Technology-package Technology-package Current Type Next reboot

network-advantage Smart License network-advantage None Subscription Smart License None

AIR License Level: AIR DNA Advantage

Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: UNREGISTERED/EVAL EXPIRED

cisco C9350-48UXM (X86) processor with 1343703K/6147K bytes of memory. Processor board ID FCW2144L045

1 Virtual Ethernet interface 4 Gigabit Ethernet interfaces

36 2.5 Gigabit Ethernet interfaces 20 Ten Gigabit Ethernet interfaces

2 TwentyFive Gigabit Ethernet interfaces 2 Forty Gigabit Ethernet interfaces

2048K bytes of non-volatile configuration memory. 8388608K bytes of physical memory.

1638400K bytes of Crash Files at crashinfo:. 11264000K bytes of Flash at flash:.

0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address : ec:1d:8b:0a:68:00 Motherboard Assembly Number : 73-17959-06 Motherboard Serial Number : FOC21418FPQ

Model Revision Number : B0 Motherboard Revision Number : A0

Model Number : C9350-48UXM

System Serial Number : FCW2144L045

Switch Ports Model SW Version SW Image Mode

* 1 65 C9350-48UXM 16.12.3a CAT9K_IOSXE BUNDLE

Configuration register is 0x102

*** Configuring a Loopback Interface ***

Line 1 SUCCESS: interface loop 100

Line 2 SUCCESS: ip address 10.10.10.10 255.255.255.255

Line 3 SUCCESS: end

*** Executing show ip interface brief ***

Interface IP-Address OK? Method Status Protocol Vlan1 unassigned YES unset up up

GigabitEthernet0/0 10.127.128.10 YES DHCP	up	up
Tw1/0/1 unassigned YES unset down		down
Tw1/0/2 unassigned YES unset down		down
Tw1/0/3 unassigned YES unset down		down
Tw1/0/4 unassigned YES unset down		down
Tw1/0/5 unassigned YES unset down		down
Tw1/0/6 unassigned YES unset down		down
Tw1/0/7 unassigned YES unset down		down
Tw1/0/8 unassigned YES unset down		down
Tw1/0/9 unassigned YES unset down		down
Tw1/0/10 unassigned YES unset down		down
Tw1/0/11 unassigned YES unset down		down
Tw1/0/12 unassigned YES unset down		down
Tw1/0/13 unassigned YES unset down		down
Tw1/0/14 unassigned YES unset down		down
Tw1/0/15 unassigned YES unset down		down

Tw1/0/16 unassigned YES unset down		down
Tw1/0/17 unassigned YES unset down		down
Tw1/0/18 unassigned YES unset down		down
Tw1/0/19 unassigned YES unset down		down

Tw1/0/20	unassigned	YES unset down	down
Tw1/0/21	unassigned	YES unset down	down
Tw1/0/22	unassigned	YES unset down	down
Tw1/0/23	unassigned	YES unset down	down
Tw1/0/24	unassigned	YES unset down	down
Tw1/0/25	unassigned	YES unset down	down
Tw1/0/26	unassigned	YES unset down	down
Tw1/0/27	unassigned	YES unset down	down
Tw1/0/28	unassigned	YES unset down	down
Tw1/0/29	unassigned	YES unset down	down
Tw1/0/30	unassigned	YES unset down	down
Tw1/0/31	unassigned	YES unset down	down
Tw1/0/32	unassigned	YES unset down	down
Tw1/0/33	unassigned	YES unset down	down
Tw1/0/34	unassigned	YES unset down	down
Tw1/0/35	unassigned	YES unset down	down
Tw1/0/36	unassigned	YES unset down	down
Te1/0/37	unassigned	YES unset down	down
Te1/0/38	unassigned	YES unset down	down
Te1/0/39	unassigned	YES unset down	down
Te1/0/40	unassigned	YES unset down	down
Te1/0/41	unassigned	YES unset down	down
Te1/0/42	unassigned	YES unset down	down
Te1/0/43	unassigned	YES unset down	down
Te1/0/44	unassigned	YES unset down	down
Te1/0/45	unassigned	YES unset down	down

Te1/0/46	unassigned	YES unset down	down
Te1/0/47	unassigned	YES unset down	down
Te1/0/48	unassigned	YES unset up	up

GigabitEthernet1/1/1 unassigned YES unset down down GigabitEthernet1/1/2 unassigned YES unset down down GigabitEthernet1/1/3 unassigned YES unset down down GigabitEthernet1/1/4 unassigned YES unset down down Te1/1/1 unassigned YES unset down down Te1/1/2 unassigned YES unset down down Te1/1/3 unassigned YES unset down down Te1/1/4 unassigned YES unset down down Te1/1/5 unassigned YES unset down down Te1/1/6 unassigned YES unset down down Te1/1/7 unassigned YES unset down down Te1/1/8 unassigned YES unset down down Fo1/1/1 unassigned YES unset down down Fo1/1/2 unassigned YES unset down down TwentyFiveGigE1/1/1 unassigned YES unset down down TwentyFiveGigE1/1/2 unassigned YES unset down down Ap1/0/1 unassigned YES unset up up

Loopback100 10.10.10.10 YES TFTP up up

*** Configuring username, password, SSH ***

Line 1 SUCCESS: username cisco privilege 15 password cisco

**CLI Line # 1: WARNING: Command has been added to the configuration using a type 0 password.

However, type 0 passwords will soon be deprecated. Migrate to a supported password type

Line 2 SUCCESS: ip domain name domain Line 3 SUCCESS: line vty 0 15

Line 4 SUCCESS: login local

Line 5 SUCCESS: transport input all Line 6 SUCCESS: end

*** ZTP Day0 Python Script Execution Complete *** Guestshell destroyed successfully

Press RETURN to get started!

This following example shows the sample boot logs before the .py script is run:

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Acquired IPv4 address 10.127.128.8 on Interface GigabitEthernet0/0 Received following DHCPv4 options:

bootfile : test.py

tftp-server-ip : 159.14.27.2 OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode Entering enable mode will stop pnp-discovery

Attempting bootfile tftp://159.14.27.2/test.py day0guestshell activated successfully Current state is: ACTIVATED

day0guestshell started successfully Current state is: RUNNING

Guestshell enabled successfully

*** Sample ZTP Day0 Python Script ***

...

*** ZTP Day0 Python Script Execution Complete *** Guestshell destroyed successfully

The following example shows how to configure the device for Day Zero provisioning: Both links down, not waiting for other switches

Switch number is 1

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc. 170 West Tasman Drive

San Jose, California 95134-1706

Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.2.1, RELEASE SOFTWARE (fc4)

Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2020 by Cisco Systems, Inc.

Compiled Thu 26-Mar-20 03:29 by mcpre

This software version supports only Smart Licensing as the software licensing mechanism. PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE, AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE

"SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL

ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement (EULA) and any relevant supplemental terms (SEULA) found at

http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

You hereby acknowledge and agree that certain Software and/or features are licensed for a particular term, that the license to such Software and/or features is valid only for the applicable term and that such Software and/or features may be shut down or otherwise terminated by Cisco after expiration of the applicable license term (e.g., 90-day trial period). Cisco reserves

the right to terminate any such Software feature electronically or by any other means available. While Cisco may provide alerts, it is your sole responsibility to monitor your usage of any such term Software feature to ensure that your systems and networks are prepared for a shutdown of the Software feature.

% Checking backup nvram

% No config present. Using default config

FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled All TCP AO KDF Tests Pass

cisco C9350-48UXM (X86) processor with 1338934K/6147K bytes of memory. Processor board ID FCW2144L045

2048K bytes of non-volatile configuration memory. 8388608K bytes of physical memory.

1638400K bytes of Crash Files at crashinfo:. 11264000K bytes of Flash at flash:.

Base Ethernet MAC Address : ec:1d:8b:0a:68:00

Motherboard Assembly Number : 73-17959-06 Motherboard Serial Number : FOC21418FPQ Model Revision Number : B0

Motherboard Revision Number : A0

Model Number : C9350-48UXM

System Serial Number : FCW2144L045 CLEI Code Number :

No startup-config, starting autoinstall/pnp/ztp...

Autoinstall will terminate if any input is detected on console Autoinstall trying DHCPv4 on GigabitEthernet0/0 Autoinstall trying DHCPv6 on GigabitEthernet0/0

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Acquired IPv4 address 10.127.128.8 on Interface GigabitEthernet0/0 Received following DHCPv4 options:

bootfile : test.py

tftp-server-ip : 159.14.27.2 OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode Entering enable mode will stop pnp-discovery

Attempting bootfile tftp://159.14.27.2/test.py day0guestshell activated successfully Current state is: ACTIVATED

day0guestshell started successfully Current state is: RUNNING

Guestshell enabled successfully

Additional References for Zero-Touch Provisioning

Standards and RFCs

Standard/RFC	Title
RFC 5652	*Cryptographic Message Syntax (CMS)*
RFC 8040	*RESTCONF Protocol*
RFC 8366	*A Voucher Artifact for Bootstrapping Protocols*
RFC 8572	*Secure Zero Touch Provisioning (SZTP)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for	https://www.cisco.com/c/en/us/support/index.html

Description	Link

troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	