DHCP Zero Touch

The Cisco Dynamic Host Control Protocol (DHCP) Zero Touch feature enables a device to retrieve configuration files from the remote DHCP server during initial deployment with no end-user intervention.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About DHCP Zero Touch

DHCP Zero Touch Overview

The DHCP Zero Touch feature enables a device to retrieve configuration files from the remote Dynamic Host Configuration Protocol (DHCP) server during the initial device deployment without end-user intervention. You need a bootstrap configuration to communicate between the device and the remote server. The bootstrap configuration provides specific information about a device. This bootstrap configuration can be pre-installed on the device or can be retrieved from the DHCP server. The DHCP Zero Touch feature introduces another method of retrieving bootstrap configuration information: using the DHCP Option 43 message. To accommodate

situations where devices cannot have a pre-installed bootstrap configuration, a deployment model that uses DHCP Option 43 messages is used. Cisco recommends using DHCP Option 43 messages based on RFC 2132. You can use the DHCP Option 43 message to provide vendor-specific information in the form of ASCII codes to the DHCP server.

The DHCP Option 43 message supplies the necessary information that is normally provided in the bootstrap configuration to the DHCP client. When the DHCP client issues a DHCP IP address request to the DHCP server, the DHCP server sends out the IP address and a DHCP Option 43 message, if the DHCP Option 43 message is preconfigured on the DHCP server. Within this DHCP Option 43 message, predefined parameterized commands are provided to the DHCP client. A timer for three minutes is set. After the timeout, if the file download is successful, the process is complete. If the file download fails, check the generated DHCP Option 43 message and correct any problems. Power cycle the device to retry the DHCP Option 43 message process.

Initiating DHCP Option 43 Messages with WSMA

At router system initiation time, there are two ways to initiate the DHCP IP address request to enable the DHCP Option 43 message to be sent to the device:

1. If the device is enabled with startup configuration, zero touch deployment can be enabled by using the **ip address dhcp** and the **wsma dhcp** configuration commands.
2. If the device is not enabled with startup configuration, the Autoinstall feature automatically initializes the **ip address dhcp** configuration command, which enables the zero touch deployment. For more information about the Autoinstall feature, see the "Overview—Basic Configuration of a Cisco Networking Device" module in the *Configuration Fundamentals Configuration Guide*.

WSMA Parameterized Commands

The values configured using the **wsma id**, **wsma agent**, and **wsma profile initiator** commands are used as parameters to construct the DHCP Option 43 message to enable zero touch deployment (ZTD). The DHCP Option 43 message provides these predefined parameterized commands to the Dynamic Host Control Protocol (DHCP) client, which enables the client to decode and read the messages sent by the DHCP server.

Constructing a DHCP Option 43 Message

The DHCP Option 43 message is presented in the type/value (TV) format. The DHCP Option 43 message is used by clients and servers to exchange vendor-specific information. When you use the vendor-specific option (Option 43), you must specify the data using hexadecimal ASCII values. For more information on the **option** command, refer to the Cisco IOS IP Addressing Services Command Reference.

Note The maximum DHCP Option 43 size is 2500 bytes.

Following are the parameters used by the WSMA to construct the DHCP Option 43 message to enable ZTD:

```
<DHCP-typecode><feature-opcode><version><debug-option>;<arglist>
```

Table 1: Parameters of DHCP Option 43 Message

Parameter	Description
DHCP-typecode	Specifies the DHCP suboption type. The DHCP suboption type for WSMA is 4.
feature-opcode	There are two types of feature operation codes—Active (A) and Passive (P). The feature operation code for WSMA is Active (A) template. This code initiates a connection to the management server and sends a hello message to it. If the management server cannot be reached, the device keeps trying to connect until it gets through.
version	Indicates the version of template to be used by the WSMA.
debug-option	Indicates if debug messages have to be generated during the processing of the DHCP Option 43 messages. Debug OFF is recommended for normal processing and debug ON can be used for debugging the processing of DHCP Option 43 messages. The following are the two debug options: • D—debug option is ON • N—debug option is OFF
;	Delimiter used to separate the parameters.
arglist	List of named arguments for the command, separated by a semicolon. To use the default value for an argument, do not specify values for that parameter. Letter codes are used to identify the arguments. Name and value pairs can be listed in any order and are delimited by a semicolon.

The table below lists the arguments for configuring the WSMA ID and the initiator profile parameters used for configuring the WSMA configuration agent.

Table 2: Argument Lists for WSMA Active Template A (WSMA Indicators)

Parameter	Letter Code	Values	Parameter to CLI Mapping: Sample Letter Code	Parameter to CLI Mapping: Sample CLI Mapping
WSMA ID	A	(Optional) Indicates the WSMA ID. The default is hostname. 1—Indicates a custom string to be used. 2—Indicates the MAC address of the interface used. 3—Indicates the hardware serial number to be used. 4—Indicates Unified Display Interface (UDI).	A1881-ap A4	Device(config)# **wsma id string 881-ap** Device(config)# **wsma id udi**
Remote server IP ADDR	I	(Required) Indicates an IPv4 or IPv6 address or hostname. Set the DNS-server option for DHCP, if you use hostname.	I10.10.10.1-	Device(config-wsma-init)# **transport tls 10.10.10.1**
Remote server part	J	(Optional) Indicates the remote server part. The default port is 13000.	J10000	Device(config-wsma-init)# **transport tls 10.10.10.1.10090**
Transport protocol for WSMA initiator	K	(Required) Indicates the transport protocol for WSMA initiator. 1—TLS 2—SSH 3—HTTPS 4—HTTP	K1	Device(config)# **wsma profile intiator zero-touch** Device(config-wsma-init)# **transport tls 10.10.10.1 10090**
Encapsulation	B		B	Device(config-wsma-listener)# **encap soap12**

Parameter	Letter Code	Values	Parameter to CLI Mapping: Sample Letter Code	Parameter to CLI Mapping: Sample CLI Mapping
		(Optional) Indicates the encapsulation of a WSMA profile. The default is Simple Object Access Protocol (SOAP) 11. 1—SOAP 11 2—SOAP 12		
Max message C	C	(Optional) Indicates the maximum size limit for incoming messages. The default is 50 KB. Numeric string between 1 KB and 2000 KB.	C	Device(config-wsma-listener)# **max-message 50**
CA Server IP address	L	(Required) Indicates the IP address or hostname of certificate authority (CA) server for the Transport Layer Security (TLS) or Secure HTTP (HTTPS) protocol.	L	Device(ca-trustpoint)# **enrollment url** **http://10.1.43.216:80**
Source interface	M	Indicates the source interface name. It is applicable for the TLS protocol.	M11011	Device(config-wsma-initiator)# **transport tls name1** **11011 source** **fastethernet 0/1**
User name	N	(Required) Specifies the Username for SSH protocol. It is not applicable for the TLS protocol.	N11011	Device(config-wsma-initiator)# **transport ssh user1** **11011 path remote-cmd-text** **user username password**
User password	O	(Required) Specifies the password for accessing the SSH protocol. It is not applicable for the TLS protocol.	O11011	Device(config-wsma-initiator)# **transport ssh user1** **11011 path** **remote-cmd-text user** **username password**
Connect string/path	P		P11011	

Parameter	Letter Code	Values	Parameter to CLI Mapping: Sample Letter Code	Parameter to CLI Mapping: Sample CLI Mapping
		(Required) Specifies a connect string command for SSH, or the path for HTTPS and HTTP. It is not applicable for the TLS protocol.		`Device(config-wsma-initiator)#` **`transport https user1`** **`11011 path remote-cmd-text`** **`user username password`**
idle-timeout	Q	(Optional) Specifies the timeout value in minutes. The default is 1.	`Q30`	`Device(config-atm-vc)#` **`idle-timeout 30`**
domain-name	R	(Optional) Specifies the name of the domain that hosts the DHCP client. This parameter is applicable for the TLS protocol.	`example.com`	`Device(config)#` **`ip domain list`** **`example.com`**
fingerprint	T	(Optional) Specifies a fingerprint that can be matched against the fingerprint of a certification authority (CA) certificate during authentication. It is applicable for the TLS protocol.	`T96E50E2C126CC31490B319E3BFD40FE663DB5664`	`Device(ca-trustpoint)#` **`fingerprint 96E50E2C126CC3149`** **`0B319E3BFD4`** **`0FE663DB5664`**
fqdn	U	(Optional) Specifies a hostname and a domain name. It is applicable for the TLS protocol.	`example.com`	`Device(ca-trustpoint)#` **`fqdn dp-7214.examplecom`**
Keepalive interval	V	(Optional) Specifies the number of keepalive intervals.	`V600`	`Device(config-wsma-initiator)#` **`keepalive 600`**
Keepalive retries	W	(Optional) Specifies the number of keepalive retries.	`W5`	`Device(config-wsma-initiator)#` **`keepalive 600 retries 5`**
Crypto cmd wait time	X		`X`	`NA`

Parameter	Letter Code	Values	Parameter to CLI Mapping: Sample Letter Code	Parameter to CLI Mapping: Sample CLI Mapping
		(Optional) Specifies the time taken in seconds before a crypto command is executed. 1—15 seconds 2—30 seconds 3—45 seconds 4—60 seconds 5—120 seconds 6—180 seconds		
Default gateway	Y	Specifies the system's default gateway that needs to be configured.	`Y0.0.0.0`	`Device(config)#` **`ip route 0.0.0.0 0.0.0.0 10.1.43.254`**

Note Backup servers are not available. Type 6 encryption cannot be provided for zero touch due to additional initial configuration required on the Cisco device. The device tries to reconnect every 60 seconds for 15 minutes. If the server cannot be reached within the specified time, the device accepts reconfiguration via the DHCP Option 43 message.

How to Configure DHCP Zero Touch

Enabling WSMA to Receive a DHCP Option 43 Message

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wsma dhcp**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wsma dhcp** **Example:** `Device(config)# wsma dhcp`	Enables WSMA with permission to process an incoming DHCP Option 43 message.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Enabling CNS to Receive a DHCP Option 43 Message

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns dhcp**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cns dhcp** **Example:** `Device(config)# cns dhcp`	Enables CNS with permission to process an incoming DHCP Option 43 message.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuration Examples for DHCP Zero Touch

Example: Using DHCP Option 43 to Retrieve the Initial Configuration File

Example 1

In this example, in response to a DHCP IP address request sent by the Dynamic Host Control Protocol (DHCP) client, the DHCP server sends an Option 43 message such as 4A1N;I10.10.10.1;K1 to the DHCP client. The DHCP client forwards the Option 43 message to the Web Services Management Agent (WSMA). The WSMA verifies if the Option 43 message is allowed to process. Option 43 messages are allowed to process by the WSMA if the **wsma dhcp** command is enabled on the WSMA.

The parameters for the 4A1N;I10.10.10.1;K1 message are mapped as follows:

- 4—DHCP-typecode for WSMA
- A—Active template code
- 1—Version number of the Active template
- N—Debug option, which is OFF
- ;—Delimiter before the argument list
- I10.10.10.1—IP address of the management server
- K1—Transport protocol for the initiator used in Transport Layer Security (TLS)

The WSMA constructs the following commands and sends them to the remote management server to request the initial configuration file. A timer is set for five minutes.

```
Device(config)# wsma agent config profile zero-touch
Device(config)# wsma profile initiator zero-touch
Device(config-wsma-initiator)# transport tls 10.10.10.1
Device(config-wsma-initiator)# no wsse authorization level 15
```

The initial configuration file that is downloaded is checked. If the file download is successful, the process is complete.

Example 2

In this example, in response to a DHCP IP address request sent by the DHCP client, the DHCP server sends an Option 43 message such as 4A1N;A1881-ap;D10.10.10.1;K1 to the DHCP client. The DHCP client forwards the Option 43 message to the WSMA. The WSMA verifies if the Option 43 message is allowed to process. Option 43 messages are allowed to process by the WSMA if the **wsma dhcp** command is enabled on the WSMA.

The parameters for the A1881-ap;D10.10.10.1;K1 message are mapped as follows:

- 4—DHCP-typecode for WSMA
- A—Active template code
- 1—Version number of the Active template
- N—Debug option, which is OFF
- ;—Delimiter before the argument list
- 881-ap—Active template string values
- D10.10.10.1—IP address of the management server
- K1—Transport protocol for initiator used in TLS

The WSMA constructs the following commands and sends them to the remote management server to request the initial configuration file. A timer is set for five minutes.

```
Device(config)# wsma agent config profile zero-touch
Device(config)# wsma profile initiator zero-touch
Device(config-wsma-initiator)# transport tls 10.10.10.1
Device(config-wsma-initiator)# no wsse authorization level 15
```

Feature Information for DHCP Zero Touch

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for DHCP Zero Touch

Feature Name	Releases	Feature Information
DHCP Zero Touch		The DHCP Zero Touch feature allows you to configure the attributes of a device at initial deployment from a DHCP server. DHCP option 43 allows hands-free zero touch deployments. The following commands were introduced or modified: **wsma dhcp**, **cns dhcp**.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
WSMA commands	Cisco IOS Web Services Management Agent Command Reference
IP access lists	*Security Configuration Guide: Access Control Lists* in the *Securing the Data Plan Configuration Guide Library*
Public Key Infrastructure	*Public Key Infrastructure Configuration Guide* in the *Secure Connectivity Configuration Guide Library*
Secure Shell and Secure Shell Version 2	*Secure Shell Configuration Guide* in the *Securing User Services Configuration Guide Library*
Security and IP access lists commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*

RFCs

RFC	Title
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*
RFC 2246	*The TLS Protocol Version 1.0*

RFC	Title
RFC 4251	*The Secure Shell (SSH) Protocol Architecture*
RFC 4252	*The Secure Shell (SSH) Authentication Protocol*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html