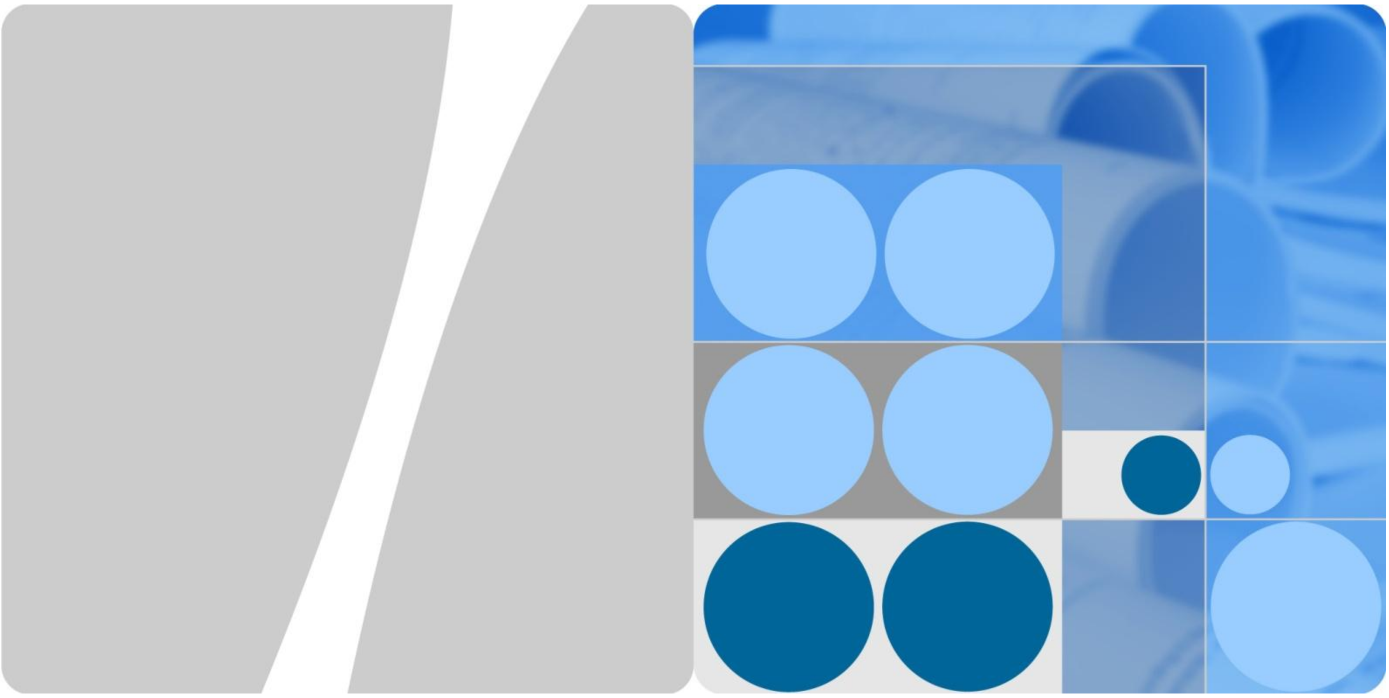


S Series Switches

Easy Operation Technology White Paper

Issue	01
Date	2013-05-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

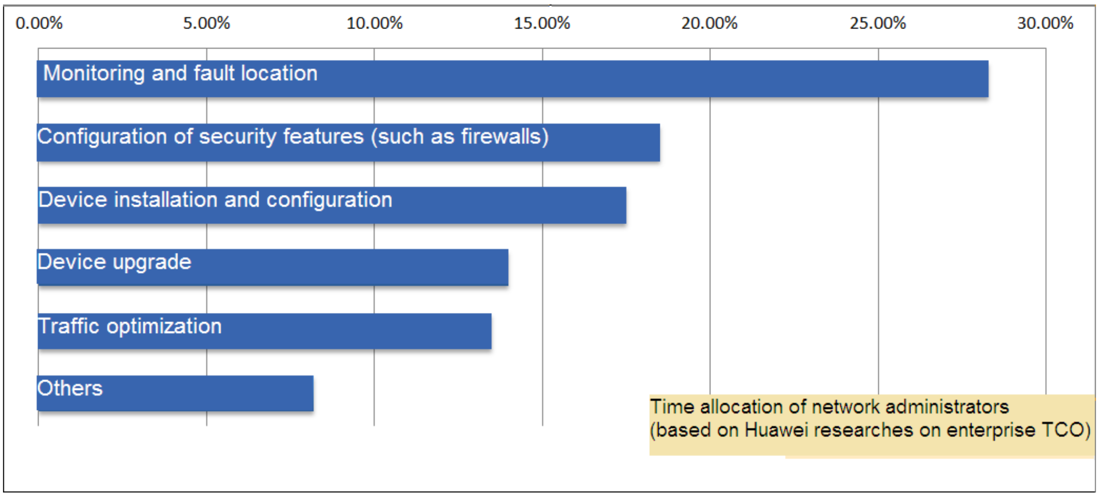
Email: support@huawei.com

Contents

1 Feature Introduction

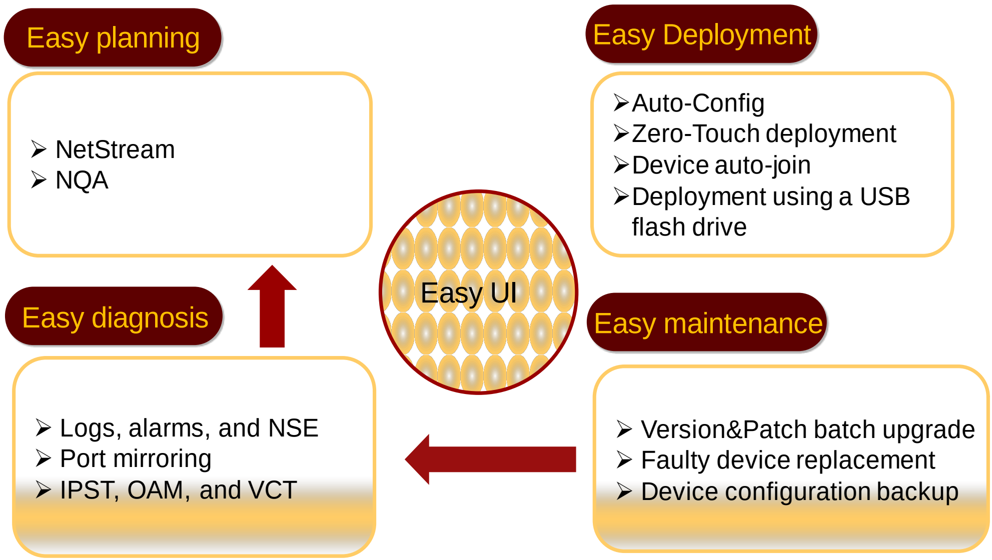
As network technologies develop and network scales expand, carriers or large enterprise customers have to manage and maintain dozens or even hundreds of devices. Network administrators spend much time in simple repetitive work, such as device installation, software upgrade, fault location, and device replacement. Therefore, there is an urgent need for simplified network device management, and batch device management becomes a great challenge for enterprise IT departments.

Figure 1-1 Driving force for smart device management



Huawei has therefore developed the Easy Operation solution to meet device management requirements on large-scale networks.

Figure 1-2 Easy Operation architecture



Easy Operation consists of five components: easy planning, easy deployment, easy maintenance, easy diagnosis, and eSight user interface (UI). Table 1-1 summarizes Easy Operation sub-components and their implementation.

Table 1-1 Easy Operation sub-components and implementation

Component	Sub-component	Implementation
Easy deployment	• Auto-Config • Zero-Touch deployment • Device auto-join	These features are implemented by exchanging EZOP packets based on the Client-Commander architecture, which is compatible with the Auto-Config process. These features are called EasyDeploy, which will be described in this document.
Easy maintenance	• Version and patch batch upgrade • Faulty device replacement • Device configuration backup	
Easy deployment	Deployment using a USB flash drive	This feature is already supported in V200R002C00.
Easy planning	NetStream and network quality analysis (NQA)	These features are well developed and therefore not mentioned in this document.
Easy diagnosis	• Logs, alarms, and Network Security Explorer (NSE) • Port mirroring • IPST, operation, administration, and management (OAM), and VCT.	

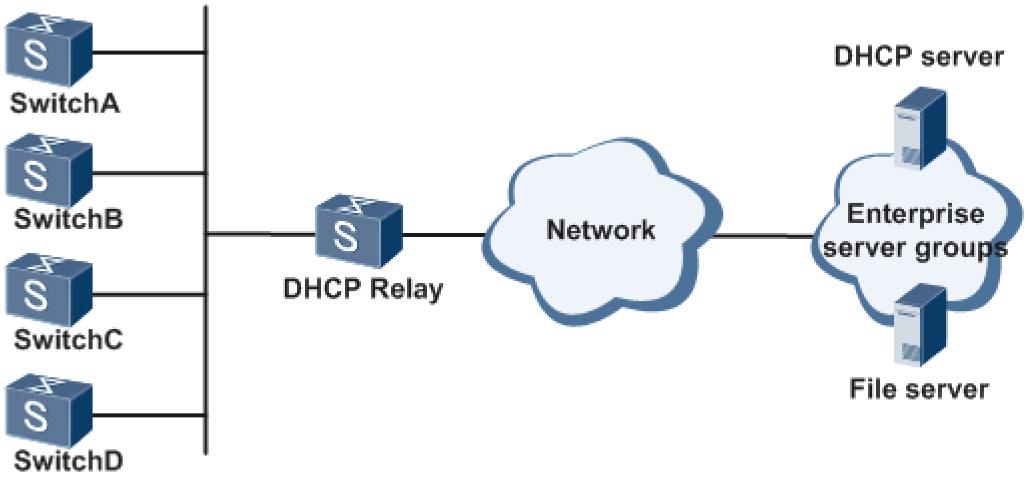
2 Technology Description

2.1 Auto-Config (Through the Option Fields or Intermediate Files)

With the Auto-Config function, the maintenance personnel only need to configure an IP address pool on the DHCP server, save the configuration file, system software package (optional), patch file (optional), and web page file (optional) to a specified file server. In this way, a device without configuration can automatically obtain files and activate downloaded files, reducing high costs of manual configuration on a large number of devices and improving device configuration efficiency.

2.1.1 Auto-Config Application Environment

Figure 2-1 Auto-Config application environment



As shown in Figure 2-1, SwitchA, SwitchB, SwitchC, and SwitchD have no configuration file. The switches need to use the Auto-Config function to automatically load and execute configuration files. By default, the Auto-Config function has been enabled on the four switches, and the enterprise server group has the DHCP server and file server deployed. If the switches and the DHCP server are on different network segments, a DHCP relay agent needs to be configured to enable interaction between the switches and the DHCP server. This ensures that DHCP Request packets of the switches are sent to the DHCP server.

SwitchA, SwichB, SwitchC, and SwitchD function as DHCP clients to periodically send DHCP Request packets to the DHCP server to obtain configuration information.

After receiving the DHCP Request packets, the DHCP server sends DHCP Reply packets that contain IP addresses assigned to the switches, egress gateway address, and Option parameters. Option parameters include the file server IP address, configuration file name, system software package name, version number information, patch file name, and web page file name. If Option parameters do not contain configuration file, the switches obtain the information from the intermediate file. The intermediate file needs to be edited and saved on the file server.

The switches automatically obtain version files from the specified file server according to information in the received DHCP Reply packets. The information includes the configuration file name, system software package name, patch file name, and web page file name. The switches specify the obtained version files for next startup. After the switches are restarted, they automatically load configuration files, system software package, patch files, and web page files.

2.1.2 Auto-Config Concepts

DHCP Server

In an Auto-Config application environment, the DHCP server provides network configuration information for devices that function as DHCP clients. An IP address pool, egress gateway address, and Option parameters need to be configured on the DHCP server. The IP address pool contains IP addresses to be assigned to interfaces of devices. Option parameters contain information about the IP address of the file server that the DHCP server assigns to DHCP clients, configuration file name, system software package name, version number, patch file name, and web page file name. In an Auto-Config application environment, any device that supports the DHCP server function can function as a DHCP server.

- IP address pool

  When a Huawei switch functions as a DHCP server, the DHCP server can configure a global IP address pool or a VLANIF interface IP address pool.

- Option parameters

  A DHCP server uses the Option field in a DHCP packet to carry control information and network configuration parameters to implement dynamic IP address allocation. In this way, the DHCP server provides network configuration information for devices that function as DHCP clients. Table 2-1 lists DHCP Option parameters related to the Auto-Config function.

Table 2-1 DHCP Option parameters

Option	Description
Option 67	Name of a configuration file assigned to a DHCP client. The file name extension must be .cfg or .zip.
Option 141	FTP/SFTP user name assigned to a DHCP client.
Option 142	FTP/SFTP password assigned to a DHCP client.
Option 143	FTP server IP address assigned to a DHCP client.
Option 145	Information about the non-configuration file assigned to a DHCP client.

Option	Description
Option 146	User-specified settings, including file deletion policy used when memory space is insufficient, configuration file activation delay.
Option 147	Authentication information used by devices to be configured to authenticate the DHCP server for device deployment. Option 147 is optional. If Option 147 is required, it must be configured as **AutoConfig**.
Option 149	SFTP server IP address and port number assigned to DHCP clients.
Option 150	TFTP server IP address assigned to a DHCP client.

Information about non-configuration files contained in Option 145 includes information about system software package, version number, patch file, and web page file. You can choose to configure the information as required. The information is in the format of vrpfile=VRPFILENAME;vrpver=VRPVERSION;patchfile=PATCHFILENAME;webfile=WEBFILE;.

Assume that a device needs to obtain the following information: system software package name **auto_V200R001C00.cc**, version number V200R001C00, patch file **auto_V200R001C00.pat**, and web page file **auto.web.zip**. The non-configuration file in Option 145 is in the format of vrpfile=auto_V200R001C00.cc;vrpver= V200R001C00;patchfile=auto_V200R001C00.pat;webfile=auto.web.zip;.

Pay attention to the following four points:

1. In versions earlier than V200R002, the system software package name in Option 145 must contain version number information as shown in the preceding example. In V200R002 and later versions, this limitation is removed.
2. From V200R002, you can configure Option 67 and Option 145 to specify the file path of the configuration file, system software package, patch file, and web page file in the root directory of the file server, and the length of the path cannot exceed 48 characters. For example, the file path can be vrpfile=/auto/S5700LI.cc;vrpver=V200R002C00;patchfile=/auto/V200R002C00.pat;webfile=/auto/auto.web.zip;.
3. From V200R001, Option 146 specifies intermediate file name. From V200R002, Option 146 specifies file path of the intermediate file, and the length of the directory cannot exceed 48 characters. The name and file path of the intermediate file in Option 146 must be the same as those of the intermediate file stored on the file server.
4. From V200R002, you can receive the files through SFTP server. Option149 specifies SFTP server IP address and port number assigned to DHCP clients. For example, if the SFTP server IP address is 10.10.10.1 and port number is 22, the Option 149 field is: option 149 ascii ipaddr=10.10.10.1;port=2.

File Server

The file server is FTP/TFTP/SFTP server, used to store files for devices that are running the Auto-Config function. When a device to be configured obtains the IP address of the file server from the DHCP server, the device downloads files it needs from the file server, including the intermediate file, configuration file, system software package, patch file, and web page file. In an Auto-Config application environment, any device that supports the file server function can function as an FTP/TFTP/SFTP server.

The device to be configured obtains the IP address of the TFTP server from Option 150 in Option parameters, and obtains the FTP user name, FTP password, and IP address of the FTP server from Option 141, Option 142, and Option 143 respectively. When both TFTP Option and FTP Option parameters are set on the DHCP server, FTP Option parameters take effect. Options 141, 142, and 149 enable DHCP clients to obtain the SFTP user name, SFTP password, and SFTP server IP address and port number.

Intermediate File

The intermediate file saves mapping between MAC address or ESN of the device to be configured and files the device needs, including system software package name, version number, patch file name, web page file name, and configuration file name. If Option 67 that contains configuration file is not configured on the DHCP server, the Auto-Config function enables the device to download the intermediate file from the file server. After analyzing the intermediate file, the device searches for the system software package name, version number, patch file name, web page file name, and configuration file name that match its own MAC address or ESN, and downloads files from the file server according to the obtained names.

Assume that the MAC address of a device is 0018-82C5-AA89, the ESN is 9300070123456789, the version file name is auto_V200R001C00.cc, the version number is V200R001C00, the patch file is auto_V200R001C00.pat, the configuration file is auto_V200R001C00.cfg, and the web page file is auto.web.zip. The contents of the intermediate file are as follows:

```
MAC=0018-82C5-AA89;vrpfile=auto_V200R001C00.cc;vrpver=
V200R001C00;patchfile=auto_V200R001C00.pat;cfgfile=auto_V200R001C00.cfg;webfile=a
uto.web.zip.
```

When configuring the intermediate file, note the following points:

If multiple devices need to be configured, each row in the intermediate file records the configuration of each device.

Either the MAC address or the ESN of a device can be chosen. You can use the following methods to obtain the MAC address and ESN of a device:

Check the label on the device.

If you can log in to the device, run the **display bridge mac-address** command to view the MAC address of the device and run the **display elabel** command to view the ESN of the device. The BarCode field in the **display elabel** command output displays the ESN.

In versions earlier than V200R002, the system software package name in the intermediate file must contain version number information. From V200R002, you can configure the intermediate file to specify the file path of the configuration file, system software package, patch file, and web page file in the root directory of the file server, which is similar to the configuration of Option 145.

In versions earlier than V200R001, the intermediate file name is **lswnet.cfg**. The intermediate file name in later versions can be edited. The intermediate file is in the text format. It can be edited on the file server. You can also edit the intermediate file on a PC and upload it to the file server.

DHCP Relay

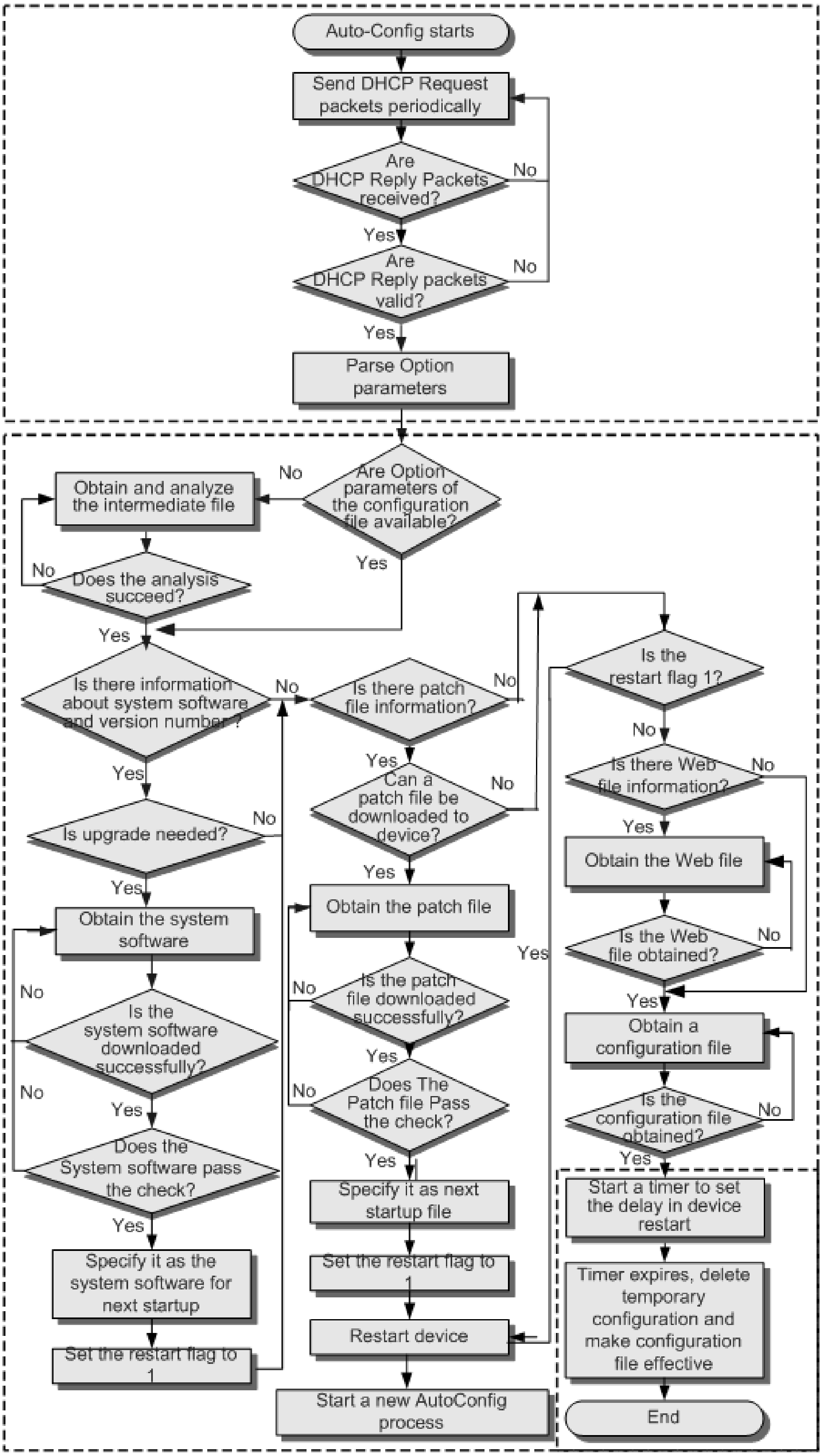
A device to be configured functions as a DHCP client, and broadcasts a DHCP Request packet to obtain an IP address. If the switches and the DHCP server are on different network segments, a DHCP relay agent needs to be configured to enable interaction between the switches and the DHCP server.

2.1.3 Auto-Config Workflow

Before configuring the Auto-Config function, pay attention to the following three points:

1. The device can be configured using either Auto-Config or USB deployment. The two methods cannot be used together.
2. Ensure that the device does not contain the configuration file. Except the web page file, the device cannot contain files with the file name extension .cfg or .zip.
3. Only interfaces added to the default VLAN (that is, VLAN1) support the Auto-Config function. By default, all interfaces are added to VLAN1.

Figure 2-2 Auto-Config workflow


Auto-Config starts
Send DHCP Request packets periodically
Are DHCP Reply Packets received?
No
Yes
Are DHCP Reply packets valid?
No
Yes
Parse Option parameters
Are Option parameters of the configuration file available?
No
Yes
Obtain and analyze the intermediate file
Does the analysis succeed?
No
Yes
Is there information about system software and version number ?
No
Yes
Is upgrade needed?
No
Yes
Obtain the system software
Is the system software downloaded successfully?
No
Yes
Does the System software pass the check?
No
Yes
Specify it as the system software for next startup
Set the restart flag to 1
Is there patch file information?
No
Yes
Can a patch file be downloaded to device?
No
Yes
Obtain the patch file
Is the patch file downloaded successfully?
No
Yes
Does The Patch file Pass the check?
No
Yes
Specify it as next startup file
Set the restart flag to 1
Restart device
Start a new AutoConfig process
Is the restart flag 1?
Yes
No
Is there Web file information?
No
Yes
Obtain the Web file
Is the Web file obtained?
No
Yes
Obtain a configuration file
Is the configuration file obtained?
No
Yes
Start a timer to set the delay in device restart
Timer expires, delete temporary configuration and make configuration file effective
End

As shown Figure 2-2, Auto-Config includes three steps:

A device obtains its IP address and configuration information from the DHCP server.

The device obtains files it needs from the file server.

The configuration takes effect.

Obtaining IP Address and Configuration Information from the DHCP Server

1. When a device without configuration starts, the device automatically enables the DHCP client function on an interface in Up state and broadcasts a DHCP Request packet through the interface. After receiving the DHCP Request packet, the DHCP server sends a DHCP Reply packet to the device. The packet contains the IP address assigned to the device, FTP/TFTP/SFTP server IP address, FTP/SFTP user name, FTP/SFTP password, and default gateway address.

2. The device checks whether the FTP/TFTP/SFTP server information in the DHCP Reply packet is valid. If so, the IP address is assigned to the device. When TFTP Option, FTP Option and SFTP Option parameters are set on the DHCP server, SFTP Option parameters take effect.

Obtaining Files the Device Needs from the File Server

Step 1 After obtaining an IP address, gateway address, and file server IP address, the device adds a route to the file server, and logs in to the file server to obtain files.

The device obtains files in either of the following methods:

- Option method.

  If the received DHCP Reply packet contains Option 67, the device analyzes Option 67 to obtain the configuration file and analyzes Option 145 to check whether the system software package, patch file, and web page file are available.

  This method applies to the scenario where a few devices need to be configured and load the same configuration file.

- Intermediate file method

  If the received DHCP Reply packet does not contain Option 67, the device does not analyze Option 145, and obtains files through the intermediate file. After obtaining the file server IP address, the device without configuration downloads and analyzes the intermediate file from the file server. The device records the configuration file name, system software package name, patch file name, and web page file name in the intermediate file and then deletes the intermediate file. The device downloads the configuration file, system software package, patch file, and web page file from the file server according to the recorded names.

  This method applies to the scenario where many devices need to be configured and load different configuration files.

Step 2 The Auto-Config module analyzes information about system software package and version number.

If no information about system software package and version number is available, go to Step 3.

If only system software package information or version number information is available, the Auto-Config process is suspended.

If both system software package information and version number information are available but they are not the same, the Auto-Config process is suspended.

If system software package information and version number information are the same, check whether the system software package and version number are the same as those for next startup. If not, the Auto-Config process is suspended. If so, go to the next step.

If the system software and version number are the same as the current system software, and the current system software is running, go to Step 3. If the current system software is not running, the Auto-Config process is suspended.

If system software information and version number information are the same but are different from the current system software or the device has no system software, the device downloads system software package form the file server.

After downloading system software package successfully, the device checks whether the system software package is correct. If not, the device deletes the system software package, records the error, stops the subsequent processes, suspends the Auto-Config process, and waits for human intervention. If the system software package is correct, the device automatically specifies the system software package for next startup. Go to Step 3.

If the device fails to obtain system software package because of insufficient memory space, the device determines whether to delete the existing system software package based on the setting of Option 146. By default, the existing system software package is not deleted. You can run the **display autoconfig-status** command to find out why the device fails to download the configuration file, system software package, web page file, and patch file.

Step 3 The Auto-Config module analyzes whether the patch file is available.

If no patch file is available, go to Step 4.

If the patch file is available, check whether the patch file is the same as the patch file for next startup. If not, the Auto-Config process is suspended. If so, go to the next step.

If the patch file is available and is the same as the current patch file, and the current patch file is running, go to Step 4. If the current patch file is not running, the Auto-Config process is suspended.

If the patch file is available, but it is different from the current patch file or the device has no patch file, the device downloads the patch file from the file server.

After downloading the patch file successfully, the device checks whether the patch file is correct. If not, the device deletes the patch file, records the error, stops the subsequent processes, suspends the Auto-Config process, and waits for human intervention. If the patch file is correct, the device specifies the patch file as the patch file for next startup. Go to Step 4.

Step 4 The Auto-Config module analyzes whether the web page file is available.

If no web page file is available, go to Step 5.

If web page file is available and is the same as the current web page file, the device deletes the current web page file. If the web page file cannot be deleted, the Auto-Config process is suspended. If the web page file is deleted, the device downloads a web page file from the file server.

If web page file is available, but it is different from the current web page file or the device has no web page file, the device downloads a web page file from the file server.

After the web page file is downloaded successfully, go to Step 5.

Step 5 The Auto-Config module analyzes configuration file name. The device downloads the configuration file from the file server. If the device fails to download the configuration file, the device suspends the Auto-Config process and waits for human intervention. After downloading the configuration file successfully, the device starts a delay timer for the configuration file to take effect. If no timer is configured, the configuration file takes effect immediately.

When the device is obtaining files from the file server, note the following point:

If the device fails to obtain the intermediate file, system software package, patch file, web page file, and configuration file, the Auto-Config process is suspended and the timer for periodically obtaining files is started. The system attempts to obtain the files every 30 minutes within 3 days and attempts to obtain the files every 2 hours 3 days later. If the system still fails to obtain the files 30 days later, the system stops obtaining the files and waits for human intervention. Then run the **autoconfig getting-file restart** command to obtain the intermediate file, system software package, patch file, web page file, and configuration file again and the Auto-Config process continues.

Validity Period of the Configuration

You can configure Option 146 on the DHCP server to set a delay timer for the configuration file to take effect. After the configuration file is downloaded successfully, the configuration file takes effect according to the setting of Option 146. If no Option 146 is configured, the configuration file takes effect immediately.

2.2 Zero-Touch (Through the Commander)

The Zero-Touch function in EasyDeploy applies to the initial stage of network deployment when most devices are newly installed and do not work due to lack of configuration files.

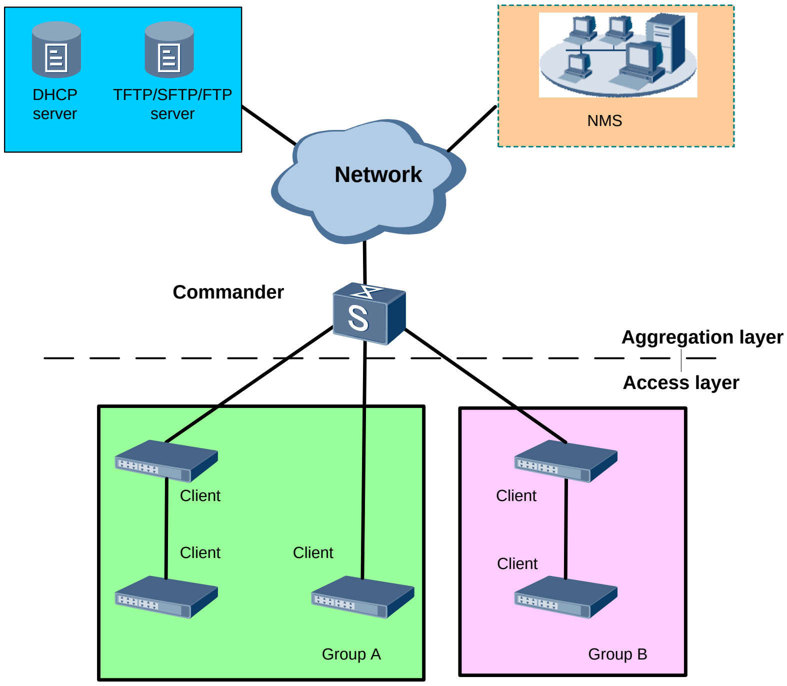
Based on the Auto-Config function, the Zero-Touch function uses the Client-Commander architecture and implements the device auto-join, faulty device replacement, and device configuration backup functions by exchanging EZOP packets.

With the Zero-Touch function, network administrators simply need to record device IDs, such as MAC addresses or equipment serial numbers (ESNs), and prepare configuration files for devices and other files to be loaded, such as system software packages, patch files, license files, and web page files. After the customer or agent installs devices onsite, network administrators load files on devices using the command line interface (CLI) or network management system (NMS) in a remote equipment room of the network center. Network administrators do not have to be onsite throughout the entire configuration process, effectively reducing the workload.

2.2.1 Network Architecture

Figure 2-3 shows a typical Zero-Touch network, including the Commander, clients, DHCP server, NMS (optional), and file server (optional).

Figure 2-3 Zero-Touch network



- The Commander is the network management device on which network administrators operate in the Zero-Touch scenario. The Commander provides the following functions:
  - Delivers the file server IP address, user name, password, and names of system software packages, configuration files, patch files, and web page files to clients.
  - Saves client deployment information in a database.
  - Manages all clients. Network administrators configure and query device deployment information on the Commander.

NOTE

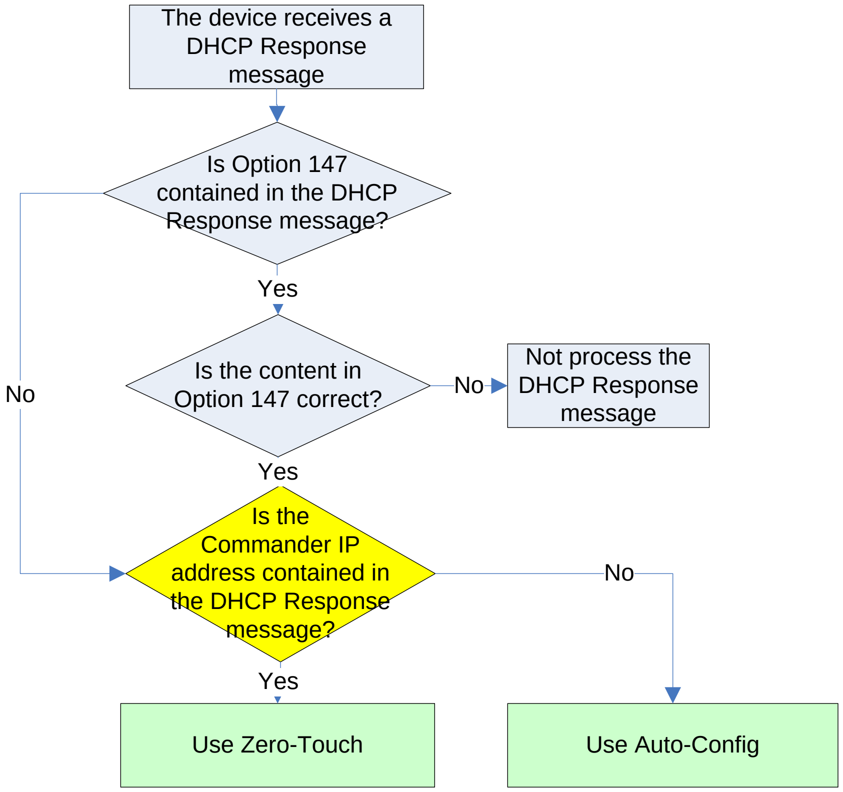
As shown in Figure 2-3, the Commander can be deployed in a Layer 2 or Layer 3 path along which clients exchange messages with the DHCP server. You can enable DHCP snooping or DHCP relay on the Commander depending on the Layer 2/Layer 3 network design. Alternatively, you can deploy the Commander in bypass mode, in which case the Commander only manages clients and does not allocate IP addresses to clients.

- A client is a device managed by the Commander. A client provides the following functions:
  - Obtains information from the Commander.
  - Sends its own information and information required by the Commander database to the Commander.
  - Responds to the Commander and performs operations according to instructions from the Commander.
- A group consists of multiple clients. Network administrators can create a group for clients with the same attributes. Clients in a group share the same settings, such as the names of system software packages, configuration files, patch files, and web page files, and the same patch or upgrade policies.

2.2.2 Relationship Between Zero-Touch and Auto-Config

The Zero-Touch function inherits the typical network and some functions of Auto-Config.

Figure 2-4 Relationship between Zero-Touch and Auto-Config


The device receives a DHCP Response message
Is Option 147 contained in the DHCP Response message?
Yes
No
Is the content in Option 147 correct?
No
Not process the DHCP Response message
Yes
Is the Commander IP address contained in the DHCP Response message?
No
Yes
Use Zero-Touch
Use Auto-Config

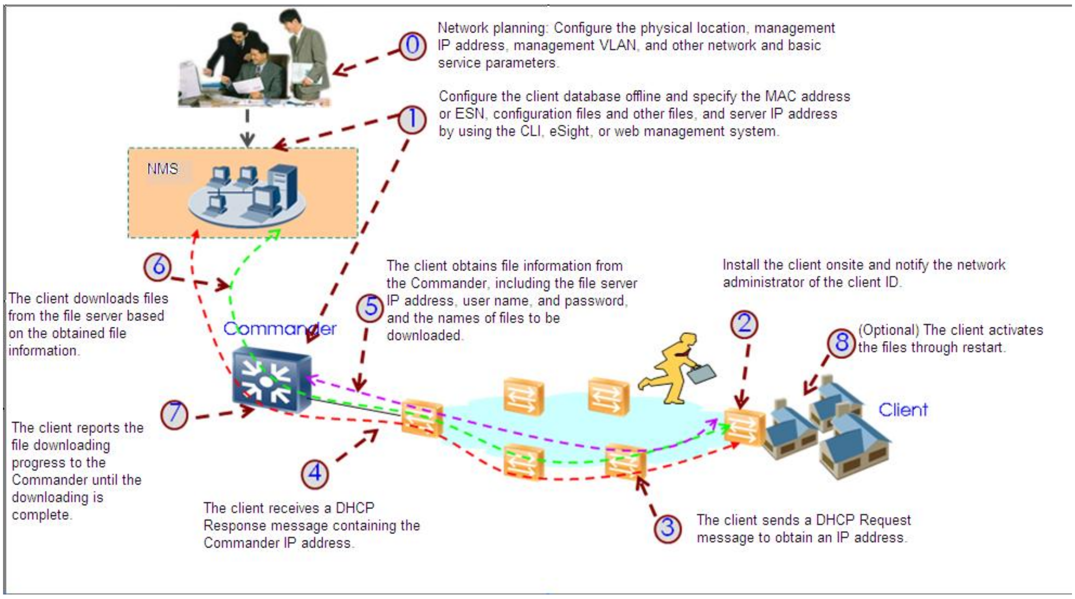
Same as Auto-Config, the Zero-Touch function is forward compatible. The Option 147 and 148 fields determine whether to use Zero-Touch or Auto-Config.

If the Option 147 field exists in the DHCP Response message, the value must be **Auto-Config**. Otherwise, the message is invalid and not processed.

If the Option 148 field exists in the DHCP Response message, Zero-Touch is used. Otherwise, Auto-Config is used.

2.2.3 Zero-Touch Process

Figure 2-5 Zero-Touch process


0
Network planning: Configure the physical location, management IP address, management VLAN, and other network and basic service parameters.
1
Configure the client database offline and specify the MAC address or ESN, configuration files and other files, and server IP address by using the CLI, eSight, or web management system.
NMS
6
The client downloads files from the file server based on the obtained file information.
Commander
5
The client obtains file information from the Commander, including the file server IP address, user name, and password, and the names of files to be downloaded.
2
Install the client onsite and notify the network administrator of the client ID.
8
(Optional) The client activates the files through restart.
Client
7
The client reports the file downloading progress to the Commander until the downloading is complete.
4
The client receives a DHCP Response message containing the Commander IP address.
3
The client sends a DHCP Request message to obtain an IP address.

The Zero-Touch process is as follows:

- **Step 0:** It is the planning stage in which files required by the devices are prepared. Details about this step are not mentioned here.
- **Step 1:** Network administrators configure the Commander. The Commander saves information about all clients, including MAC addresses, ESNs, and names of system software packages, patch files, and configuration files. Clients are upgraded based on the information, so the information must be configured on the Commander in advance.
- **Step 2:** The customer or agent installs clients onsite and notifies network administrators of the device MAC addresses or ESNs, which will be configured in the client database on the Commander.
- **Step 3:** Clients send DHCP packets to obtain IP addresses.
- **Step 4:** The DHCP server allocates IP addresses to the clients and sends the Commander IP address using Option 148 to the clients. The file server address, user name, password, and names of files to be downloaded may also be contained in the DHCP Response message. Clients choose to use Zero-Touch or Auto-Config depending on whether the DHCP Response message contains the valid Commander IP address. For details, see Figure 2-4.
- **Step 5:** Clients exchange packets with the Commander to obtain the file server IP address, user name, and password, and names of files to be downloaded.
- **Step 6**: Clients download specified files from the file server.
- **Step 7:** Clients download the files in a specified sequence. Once a file is downloaded or fails to be downloaded, the clients report the file downloading progress to the Commander.
- **Step 8**: According to the configuration on the Commander, clients decide whether to restart to make the downloaded files take effect.

2.2.4 Client Working Process in a Zero-Touch Scenario

Figure 2-6 Client working process in a Zero-Touch scenario

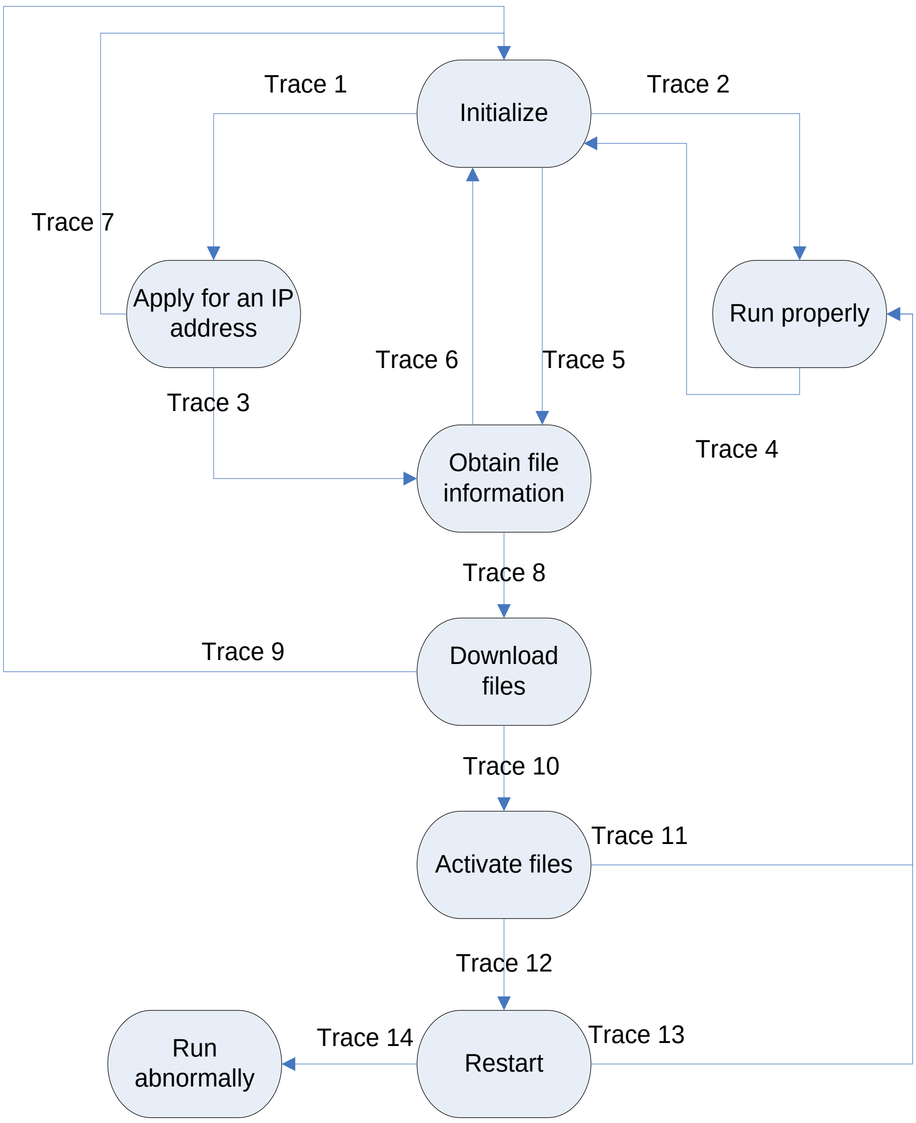


Table 2-2 Working process description

Trace N	Event
Trace 1	The client starts without any configuration.
Trace 2	The client starts properly with configuration files.
Trace 3	The client obtains the management IP address and other information and passes the validity check.
Trace 4 & Trace 5	The client triggers the upgrade commands.

Trace N	Event
Trace 6	The client fails to obtain file information.
Trace 7	The client fails to obtain an IP address.
Trace 8	The client obtains file information.
Trace 9	The client fails to download a file.
Trace 10	The client downloads all required files.
Trace 11	Downloaded files are activated without device restart.
Trace 12	Downloaded files can be activated only after the client restarts.
Trace 13	The client runs properly after a restart.
Trace 14	The client does not run properly after a restart.

- Initializing

  In initializing state, tasks start to run after a client starts properly. The client checks whether there is a configuration file on itself. If so, the client starts to run properly. If not, the client applies for an IP address using DHCP.

  If the client enters the initializing state from another state, data of that state exists on the client, including global variables and downloaded files. Information, except for file downloading results, can be deleted. You must delete files that are not successfully downloaded, but can retain or delete files that have been successfully downloaded.

- Running properly

  A client is running properly. Clients can transition from any state to the normal running state. They are in this state when they have a configuration file or after downloading all required files and restarting (if downloaded files take effect only after a restart).

- Applying for an IP address

  A client sends DHCP Request messages at an interval specified by the timer to apply for an IP address and obtains the Commander IP address. In this phase, the client exchanges messages with the DHCP server, but the Commander does not participate in this process.

  A client knows the Commander IP address in this phase and then can communicate with the Commander.

- Obtaining file information

  A client can obtain file information from the Commander in any of the following ways:

  - Network administrators define information about all required files in the DHCP Option fields, including the server IP address, user name, password, and names of files to be downloaded. For details, refer to the Auto-Config function in V200R002C00 and earlier versions. After obtaining file information, the client can directly download required files.
  - Network administrators define the server IP address, but not names of files to be downloaded, in the DHCP Option fields. The client needs to obtain the names of files to be downloaded through an intermediate file. For details, refer to the Auto-Config function in V200R002C00 and earlier versions.
  - Network administrators define only the Commander IP address in the DHCP Option fields. The client sends a request to the Commander to obtain all file information.

A client attempts to obtain file information at an interval of 1 minute. After five failures to obtain file information, the client switches to the initializing state.

- Downloading files

  Based on the obtained information, the client downloads the system software packages, patch files, web page files, license files, configuration files, and user-defined files in sequence.

  In a Zero-Touch scenario, only configurations files are mandatory. The client decides whether to download other files according to the configuration on the Commander. If other files are not required, the client notifies the Commander of the information using keepalive packets after the Zero-Touch function is implemented.

  A client attempts to download a file at an interval of 5 minutes. If the downloading fails for three times, the client stops downloading other files, enters the initializing state, and sends error information to the Commander. Users determine whether to delete the downloaded files.

- Activating files

  A client activates all downloaded files.

  If a system software package has been downloaded, the client restarts to activate all downloaded files by default. Otherwise, the client activates all downloaded files without restart.

  In V200R003C00, by default, patches are hot patches and patch files are not activated through restart. You can configure the client to activate patch files through restart.

  In a Zero-Touch scenario, configuration files are decompiled and written into the client line by line through a VRP interface, but not activated through restart by default.

2.2.5 Protocol Packet Format

In the Zero-Touch scenario, DHCP carries information by Option fields, and FTP, TFTP, and SFTP are used to download files. The elements that differ from Auto-Config lie in packet exchange between the Commander and clients and definition of Option fields.

The Commander and clients communicate with each other using unicast UDP packets (EZOP packets). In an EZOP packet, the source and destination IP addresses are the IP addresses of the Commander and client, and the default UDP port number is 60000. You can set the UDP port number by commands or Option fields.

If a client has multiple IP addresses, the source IP address is selected according to the following rules when it sends a packet to the Commander:

- If the client obtains an IP address using DHCP, this IP address is used as the source IP address.
- If the client uses a static IP address, the IP address of a loopback interface is used as the source IP address. If no IP address is configured on the loopback interface, use the source IP address obtained by searching the routing table through the Commander IP address.

DHCP Option Field

Table 2-3 lists the DHCP Option fields used in the Zero-Touch scenario. The Option 148 field specifies the Commander IP address, UDP port number, and address type. Other Option fields have been used in the Auto-Config function.

In the Zero-Touch scenario, you need to specify only DNS parameters and Option 148 on the DHCP server. Other parameters can be set on the Commander.

Table 2-3 Description of Option fields

Option	Description
Option 6	IP address of the DNS server.
Option 15	DNS domain name.
Option 66	Host name of the TFTP server.
Option 67	Name of the configuration file.
Option 141	SFTP/FTP user name.
Option 142	SFTP/FTP password.
Option 143	IP address of the FTP server.
Option 145	File information.
Option 146	Client operation, including the actions taken when the storage memory is insufficient and delay time of file activation. • **opervalue**: indicates whether to delete system software package from the file system when the storage memory is insufficient (0: no; 1: yes). The default value is **0**. • **delaytime**: indicates the delay before a downloaded file takes effect. The unit is in seconds. The default value is **0**. • **netfile**: indicates the intermediate file name. The intermediate file name contains a maximum of 48 bytes, consisting of digits (0 to 9), lowercase letters (a to z), uppercase letters (A to Z), hyphens (-), and underscores (_). The file name extension must be .cfg. • **intime**: indicates the file activation time, ranging from 00:00 to 23:59. • **actmode**: indicates how a file is activated. The value 0 indicates that the file is activated in default mode and 1 indicates that the file is activated by restarting the client. The default value is **0**. NOTE • *The maximum value of **delaytime** is one day, namely, 86400 seconds. A delay longer than one day is counted as one day.* • *If both **delaytime** and **intime** are configured, **delaytime** takes effect.*
Option 147	Authentication information. The client to be configured authenticates the DHCP server according to the authentication information. Option 147 is optional. If Option 147 is required, the value must be **AutoConfig**.
*Option 148	Commander IP address.
*Option 149	IP address of the SFTP server.

Option	Description
Option 150	IP address of the TFTP server.

- Example of the Option 148 field:
  - If the IPv4 address is 10.10.10.5 and the port number is 60000 (default port number), the Option 148 field can be any of the following:

    Option 148 = "ipaddr=10.10.10.5"

    Option 148 = "ipaddr=10.10.10.5; port=60000"

    Option 148 = "ipaddr=10.10.10.5; port=60000; type=ipv4"
  - If the IPv4 address is 10.10.10.5 and the port number is 50000, the Option 148 field can be either of the following:

    Option 148 = "ipaddr=10.10.10.5; port=50000"

    Option 148 = "ipaddr=10.10.10.5; port=50000; type= ipv4"
  - If the IPv6 address is 10:20::11:22 and the port number is 60000 (default port number), the Option 148 field can be either of the following:

    Option 148 = "ipaddr= 10:20::11:22; type= ipv6"

    Option 148 = "ipaddr= 10:20::11:22; port=60000; type= ipv6"
  - If the IPv6 address is 10:20::11:22 and the port number is 50000, the Option 148 field is:

    Option 148 = "ipaddr= 10:20::11:22; port=50000; type= ipv6".

  By default, the port number is 60000 and the IP address is an IPv4 address. In V200R003C00, IPv6 is not supported.
- Example of the Option 149 field:
  - If the IP address of the SFTP server is 10.10.10.5 and the port number is 22 (default port number), the Option 149 field can be either of the following:

    Option 149 = "ipaddr=10.10.10.5"

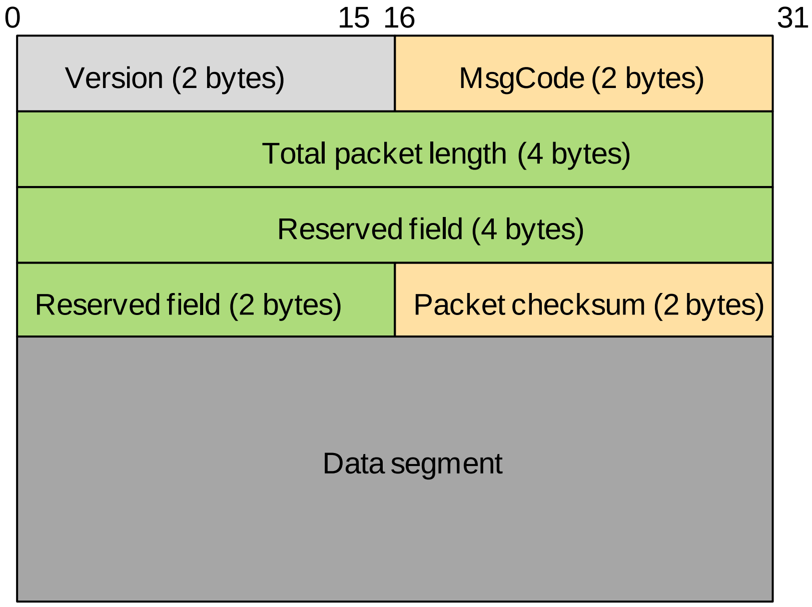
    Option 149 = "ipaddr=10.10.10.5; port=22"

If the Option 150, Option 143, and Option 149 fields are all contained in the DHCP message, Option 149, Option 150, and Option 143, that is, SFTP, TFTP, and FTP, take effect in sequence.

EZOP Packet

The Commander and clients communicate with each other using EZOP packets.

Figure 2-7 EZOP packet format



The **Version** field indicates the message version number, which is fixed at 01. This field is used to identify messages of different versions in the future. Table 2-4 lists values of the **MsgCode** field.

Table 2-4 Values of the MsgCode field

Value	Name	Description
0x0001	DOWNLOAD_INFO_REQUEST	Message code in the request packet that a client sends to the Commander for information about files to be downloaded.
0x0002	DOWNLOAD_INFO_RESPONSE	Message code in the packet that the Commander sends in response to the client's request packet.
0x0003	PROCCESS_INFO	Message code in packets that a client sends to the Commander to report the implementation progress. The client reports the progress to the Commander until the Zero-Touch process ends, regardless of whether the client is running properly.

Usage scenarios of EZOP packets are described in specific services.

2.2.6 Commander Database

The Commander saves client information in different databases, including the client database, group database, and global database. The Commander determines files to be loaded and upgrade modes for clients based on these databases. In addition, the Commander tracks the status of each client based on these databases for convenience for network administrators.

Client Database

The client database contains all information about a client managed by the Commander, including:

- Client ID and ID of the group to which the client belongs
- Client's MAC address and ESN
- Client's host name, device model, and device type
- File server
- Client's policies to activate files
- Information about files to be downloaded
- Files being upgraded on the client
- Information about files running on the client, including the system software package and its version, configuration files, patch files, web page files, and license files
- Configuration files backed up on the file server, and the status and result of configuration file backup
- Client's running status
- Client's running mode (Zero-Touch or active upgrade)
- Client's upgrade stages (such as applying for an IP address)
- Substatus in the client's upgrade stages
- Status of the file being downloaded
- Client's progress of downloading files
- Client's upgrade error description
- Number of keepalive packets sent by the client to the Commander. If the Commander does not receive any keepalive packets from a client for 120 seconds, the Commander considers that the client is lost.
- Whether the Commander IP address on the client is successfully changed
- Whether the client MAC address or ESN is matched
- Whether the client has restarted
- Description of a client's upgrade failure
- Whether the client is upgraded by command lines
- Number of upgrade attempts by command lines

The index in the client database can be only the MAC address or ESN.

In the client database, only MAC addresses and names of files to be downloaded can be configured using command lines before the Zero-Touch process starts. Other information is reported to the Commander by EZOP packets with the **MsgCode** field as **0x0004** after the Zero-Touch process starts.

Group Database

The group database contains information about a group of clients that have the same policies. You can configure the group database to implement simplified batch configuration. Each group has a matching policy. In Zero-Touch, groups can be classified into built-in groups and user-defined groups.

- Built-in groups are classified based on the device type, such as S5700-EI and S5700-HI. Table 2-5 lists the device models that support built-in groups in V200R003C00.

Table 2-5 Device models that support built-in groups in V200R003C00

Device Type	Description	Model
S2750-EI	S275x-EI series	S2750-28TP-PWR-EI-AC S2750-20TP-PWR-EI-AC S2750-28TP-EI-AC S2751-28TP-PWR-EI-AC
S5700-EI	S5700-EI series	S5700-28C-EI S5700-28C-EI-24S S5700-28C-PWR-EI S5700-52C-EI S5700-52C-PWR-EI
S5700-SI	S5700-SI series	S5700-24TP-SI-AC S5700-24TP-SI-DC S5700-48TP-SI-AC S5700-48TP-SI-DC S5700-24TP-PWR-SI S5700-48TP-PWR-SI S5700-28C-SI S5700-52C-SI S5700-28C-PWR-SI S5700-52C-PWR-SI S5700-26X-SI-12S-AC
S5700-P-LI	S5700-LI P series	S5700-28P-LI-AC S5700-28P-LI-DC S5700-52P-LI-AC S5700-52P-LI-DC S5700-28P-PWR-LI-AC S5700-52P-PWR-LI-AC
S5700-X-LI	S5700-LI X series	S5700-28X-LI-AC S5700-28X-LI-DC S5700-52X-LI-AC S5700-52X-LI-DC S5700-28X-PWR-LI-AC S5700-52X-PWR-LI-AC S5700-28X-LI-24S-AC S5700-28X-LI-24S-DC
S5700-10P-LI	S5700-10P-LI series	S5700-10P-LI-AC S5700-10P-PWR-LI-AC

Device Type	Description	Model
S5700S-LI	S5700S-LI series	S5700S-28P-LI-AC S5700S-52P-LI-AC
S5700-HI	S5700-HI series	S5700-28C-HI S5700-28C-HI-24S
S5710-EI	S5710-EI series	S5710-28C-EI S5710-52C-EI S5710-28C-PWR-EI-AC S5710-52C-PWR-EI S5710-52C-PWR-EI-AC
S5710-HI	S5710-HI series	S5710-108C-PWR-HI
S6700-EI	S6700-EI series	S6700-24-EI S6700-48-EI
S7700	S7700 series	S7703 S7706 S7712
S9700	S9700 series	S9703 S9706 S9712

- User-defined groups can be classified based on the following:
  - MAC address or ESN, such as 0026-0E4C-E02B
  - IP address, such as 192.168.110.0/24
  - Device model of the client, such as S5700-28X-LI-AC
  - Device type of the client, such as S5710-HI. User-defined groups of this type are similar to built-in groups and are compatible with the device type of new clients.

The Commander searches entries in the MAC address-, ESN-, IP address-, device model-, and device type-based and built-in group databases in sequence to match the client.

You can configure masks in MAC and IP address-based group databases to implement fuzzy matching.

Global Database

The global database contains information commonly used by clients and groups. Information is deployed in EZOP global mode through command lines. The global database also complements the client and group databases so that users can obtain configuration information that is not contained in the client and group databases. The global database contains the following information:

- Whether the Commander is enabled
- Whether the Easy Operation view is enabled

- Commander IP address and port number
- Whether a client automatically joins the management domain of the Commander. By default, a client does not automatically join the management domain of the Commander.
- Whether a client automatically deletes unnecessary files from the memory. By default, this function is disabled.
- File server
- File activation and configuration backup policies
- Files to be downloaded by default

Query Sequence

In the Zero-Touch scenario, when the Commander receives an EZOP packet from a client to request for file information, the Commander queries the client database and group database in sequence.

If the client matches an entry in the client database or group database that has no information, the client downloads information from the global database. The client also downloads some global configurations, such as the file deleting and backup policies, from the global database. The client downloads only existing files in the client or group database. If any file does not exist in the client database or group database, the client does not download the file from the global database, but directly downloads the next file.

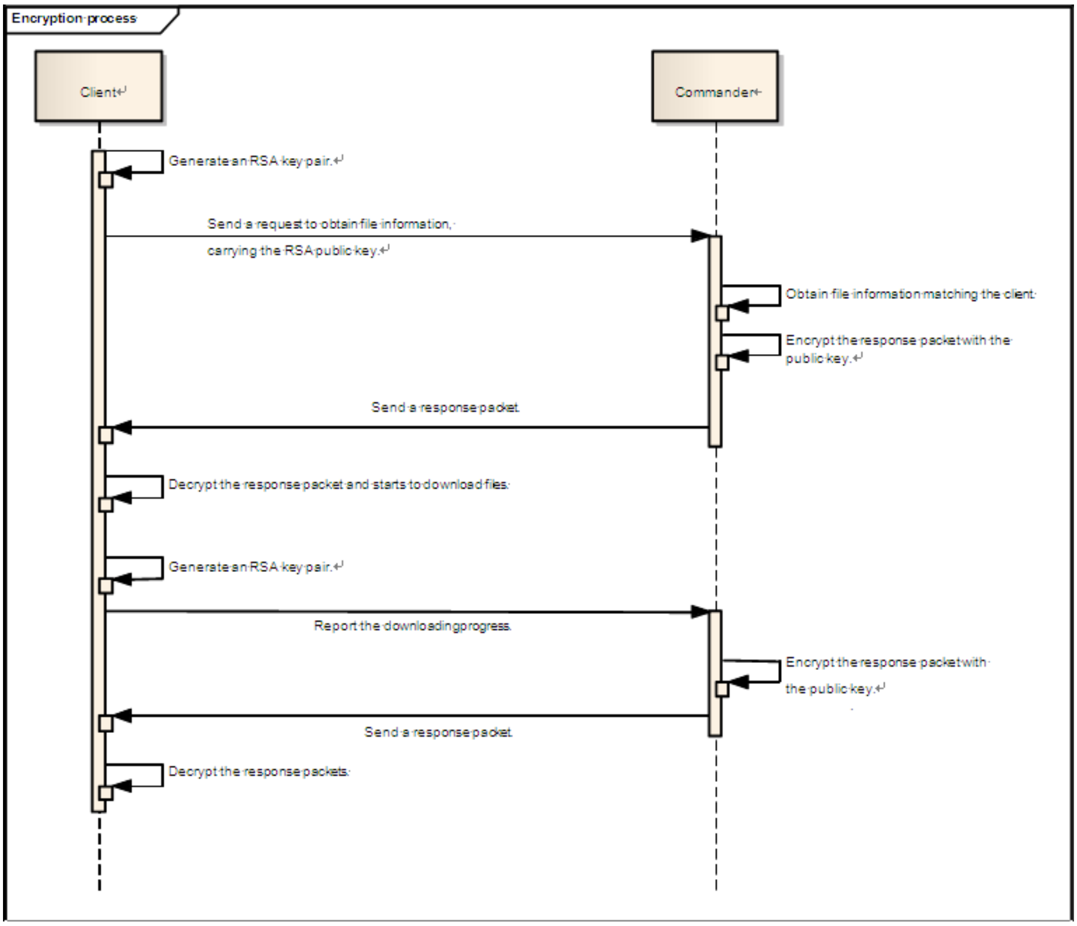
2.2.7 RSA Encryption and Decryption

TFTP/FTP/SFTP server information, such as the IP address, user name, and password, is secret and must be encrypted when the Commander responds to clients.

During message exchanges between the Commander and clients, an RSA key pair is generated on the client to protect secret information.

The RSA key pair is generated when the client starts. The client sends a request with the public key to the Commander. Then the Commander sends file information encrypted by the public key to the client and the client decrypts it with the private key.

Figure 2-8 RSA process in the Zero-Touch scenario

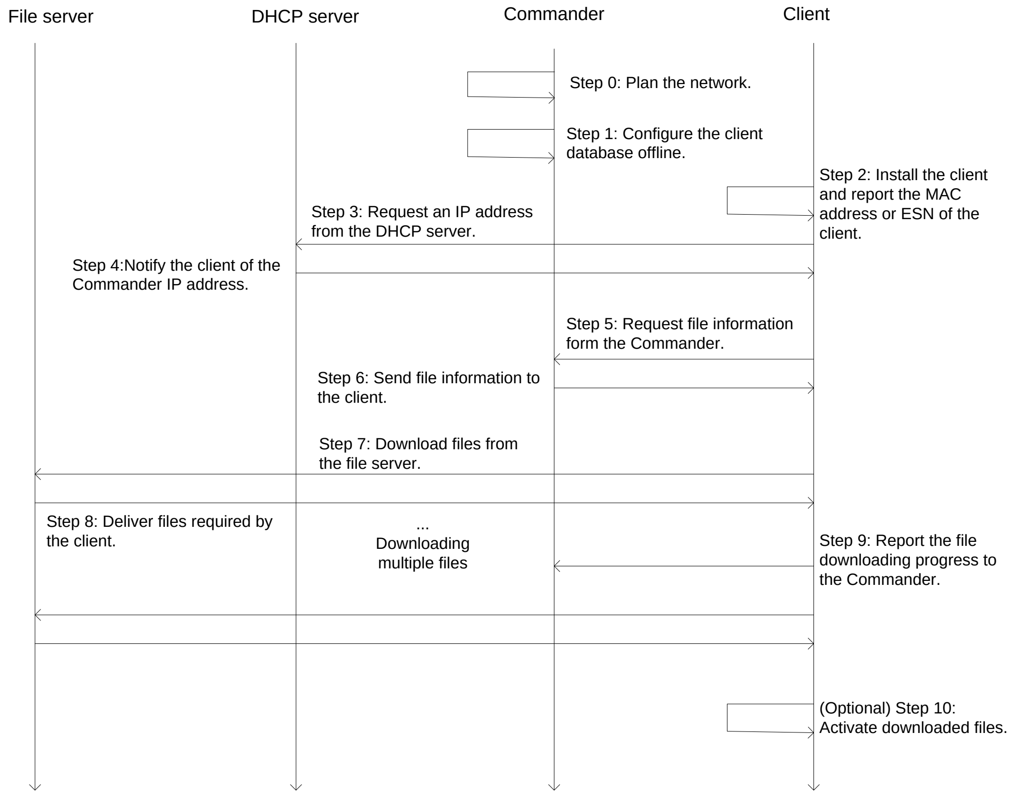

Encryption process
Client
Commander
Generate an RSA key pair.
Send a request to obtain file information, carrying the RSA public key.
Obtain file information matching the client
Encrypt the response packet with the public key.
Send a response packet
Decrypt the response packet and starts to download files
Generate an RSA key pair.
Report the downloadingprogress
Encrypt the response packet with the public key.
Send a response packet
Decrypt the response packets

Only packets with the **MsgCode** field as **0x0002** or **0x0005** are encrypted.

2.2.8 Zero-Touch Description

Figure 2-9 shows the Zero-Touch flowchart. For details about the Zero-Touch process, see Figure 2-5. Steps in Figure 2-9 are more detailed than those in Figure 2-5.

Figure 2-9 Zero-Touch flowchart


File server
DHCP server
Commander
Client
Step 0: Plan the network.
Step 1: Configure the client database offline.
Step 2: Install the client and report the MAC address or ESN of the client.
Step 3: Request an IP address from the DHCP server.
Step 4:Notify the client of the Commander IP address.
Step 5: Request file information form the Commander.
Step 6: Send file information to the client.
Step 7: Download files from the file server.
Step 8: Deliver files required by the client.
...
Downloading multiple files
Step 9: Report the file downloading progress to the Commander.
(Optional) Step 10: Activate downloaded files.

The following sections describe the Zero-Touch process in details from step 3.

Client Applying for an IP Address from the DHCP Server (Step 3)

By default, all ports on a client are added to VLAN 1, and VLANIF 1 is created. The client automatically sends DHCP Discovery messages in VLAN 1 after it is added to the network.

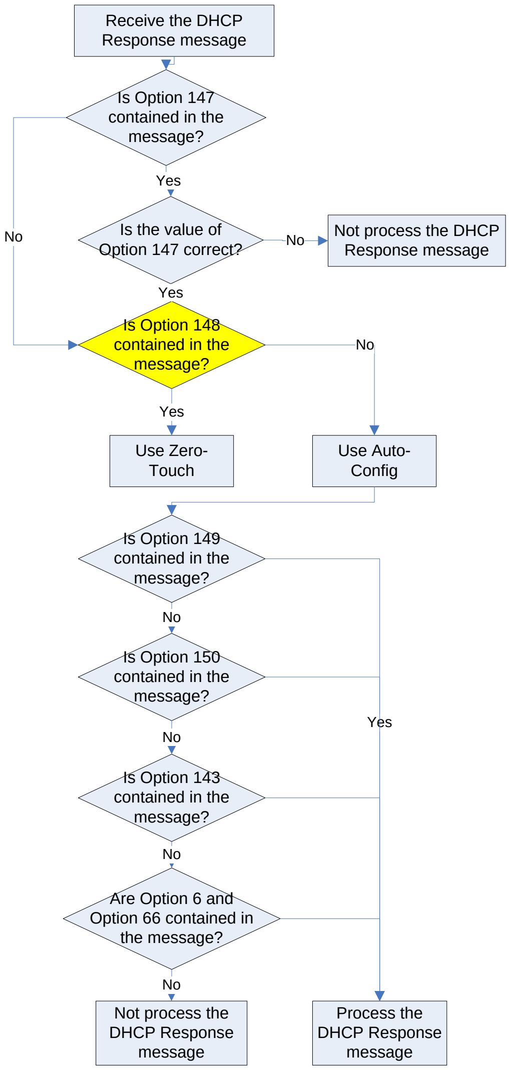
The client sends DHCP Discovery messages at an interval of 5 minutes until it obtains an IP address.

DHCP Server Notifying the Client of the Commander IP Address (Step 4)

To allow the client to obtain information about files to be downloaded, you have to specify the Commander IP address in the Option 148 field of the DHCP Response message sent by the DHCP server. After receiving the DHCP Response message, the client obtains information about files to be downloaded from the Commander specified in the Option 148 field.

Figure 2-10 shows the flowchart of the client's processing on the DHCP Response message.

Figure 2-10 Flowchart of the client's processing on the DHCP Response message


Receive the DHCP Response message
Is Option 147 contained in the message?
Yes
No
Is the value of Option 147 correct?
No
Not process the DHCP Response message
Yes
Is Option 148 contained in the message?
No
Yes
Use Zero-Touch
Use Auto-Config
Is Option 149 contained in the message?
No
Is Option 150 contained in the message?
Yes
No
Is Option 143 contained in the message?
No
Are Option 6 and Option 66 contained in the message?
No
Not process the DHCP Response message
Process the DHCP Response message

Client Requesting File Information from the Commander (Step 5)

The client requests file information from the Commander by sending the DOWNLOAD_INFO_REQUEST packet, with the **MsgCode** field as **0x0001**. Figure 2-11 shows the format of a DOWNLOAD_INFO_REQUEST packet.

Figure 2-11 Format of a DOWNLOAD_INFO_REQUEST packet

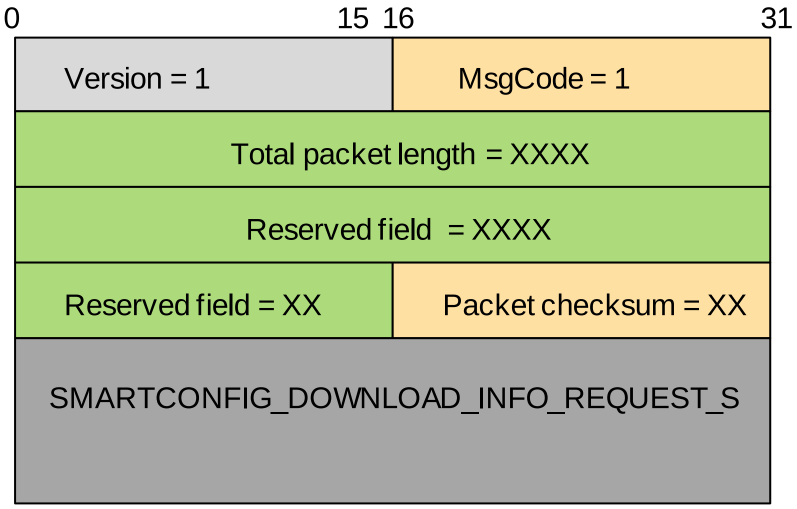


Table 2-6 lists fields in a DOWNLOAD_INFO_REQUEST packet.

Table 2-6 Fields in a DOWNLOAD_INFO_REQUEST packet

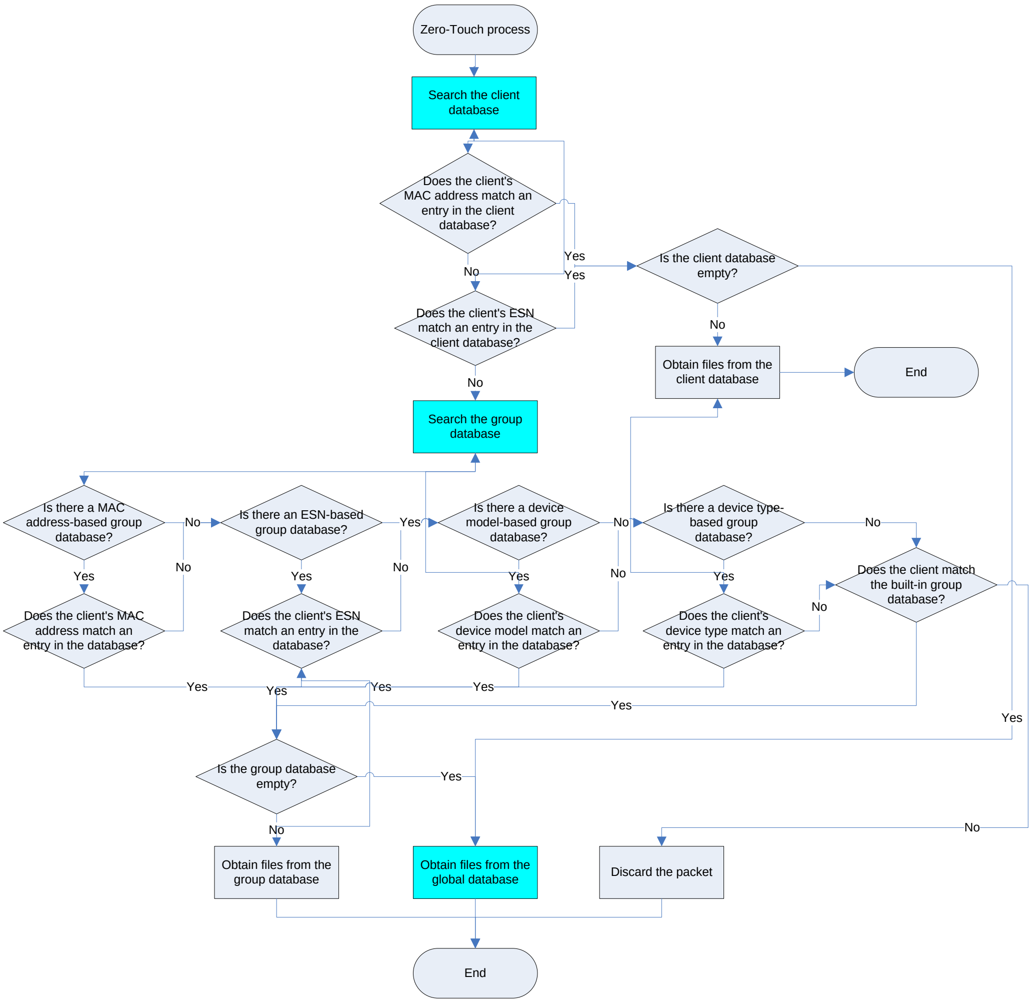
Field	Description
stClientIpAddr	IP address of the client that requests for file information.
ulClientRequestType	Type of a client's request for files to be downloaded, including Zero-Touch and upgrade. The value 0 indicates Zero-Touch and 1 indicates upgrade. Other values indicate Zero-Touch by default.
szClientMacAddr	MAC address of the client that requests for file information.
szClientModel	Device model of the client. The value must be the same as the formal model, such as S5700-28P-LI-AC.
szClientDeviceType	Device type of the client. The value must be the same as the formal type, such as S5700-LI.
szClientESN	ESN of the client.
ulGroupId	Group to which the client belongs.
szRsaPublicKey	RSA public key, which is used by the Commander to encrypt response packets.

Commander Sending File Information to the Client (Step 6)

After receiving DOWNLOAD_INFO_REQUEST packets from the client, the Commander searches the client database. The client database must be configured in advance and only the MAC address and ESN can be configured as indexes. If the client does not match any entry in the client database, the Commander searches the MAC address-, ESN-, IP address-, device model-, and device type-based and built-in group databases in sequence. If the client cannot match any entry, the Commander discards the request.

Figure 2-12 shows how the Commander searches databases for a client.

Figure 2-12 Commander searching databases


Zero-Touch process
Search the client database
Does the client's MAC address match an entry in the client database?
Yes
No
Yes
Is the client database empty?
Does the client's ESN match an entry in the client database?
No
Obtain files from the client database
End
No
Search the group database
Is there a MAC address-based group database?
No
Is there an ESN-based group database?
Yes
Is there a device model-based group database?
No
Is there a device type-based group database?
No
Yes
No
Yes
No
Yes
No
Yes
Does the client match the built-in group database?
No
Does the client's MAC address match an entry in the database?
Does the client's ESN match an entry in the database?
Does the client's device model match an entry in the database?
Does the client's device type match an entry in the database?
Yes
Yes
Yes
Yes
Yes
Yes
Is the group database empty?
Yes
No
No
Obtain files from the group database
Obtain files from the global database
Discard the packet
End

The client cannot detect packet discarding. The client sends request packets at an interval of 20 seconds until it receives responses from the Commander. If the client does not receive responses from the Commander after 15 attempts, the client sends a DHCP Request message to the DHCP server to request for the Commander IP address again.

After receiving the client's request to obtain file information, the Commander sends the client a DOWNLOAD_INFO_RESPONSE packet with file information and the **MsgCode** field as **0x0002**. Figure 2-13 shows the format of a DOWNLOAD_INFO_RESPONSE packet.

Figure 2-13 Format of a DOWNLOAD_INFO_RESPONSE packet

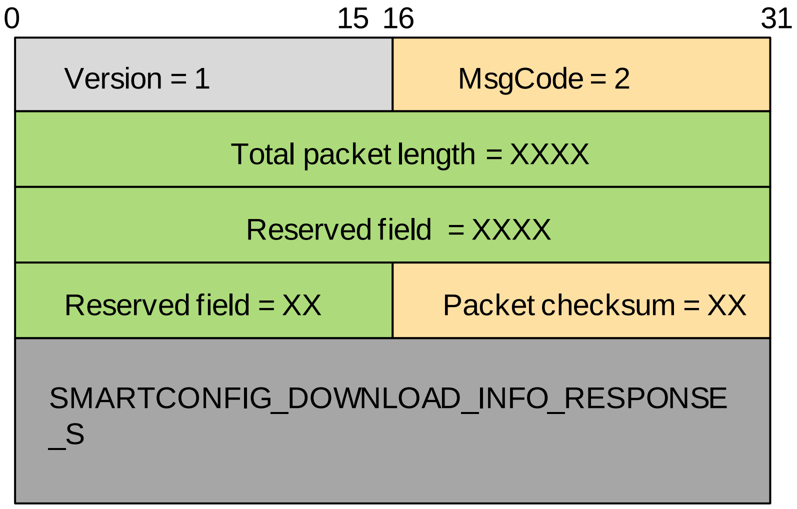


Table 2-7 lists fields in a DOWNLOAD_INFO_RESPONSE packet.

Table 2-7 Fields in a DOWNLOAD_INFO_RESPONSE packet

Field	Description
ulServerType	Type of the file server. The value 1 indicates a TFTP server, 2 indicates an FTP server, and 3 indicates an SFTP server. Other values indicate an SFTP server by default.
ulServerIpAddr	IP address of the file server.
ulServerIpAddrType	Type of the IP address. The value 0 indicates an IPv4 address and 1 indicates an IPv6 address. Other values indicate an IPv4 address by default.
szUserName	User name for logging in to the file server.
szPassword	Password for logging in to the file server.
szVrpFilename szVrpFileVersion szPatFilename szWebFilename szCfgFilename szLicFilename szUserDef1Filename szUserDef2Filename szUserDef3Filename	Names of files to be downloaded.

Field	Description
ulFlashCleanFlag	Whether to delete files from the flash memory. The value 0 indicates no and 1 indicates yes. Other values indicate yes by default. This flag applies only to system software. Disabled system software is deleted only when the flash memory is insufficient for downloading system software package. Whether clients automatically delete unnecessary files from the flash memory depends on the file server type. When clients download files from a TFTP server, they cannot obtain the size of files; therefore, the clients cannot automatically delete unnecessary files from the flash memory. When clients download files from an FTP or SFTP server that does not return the size of files, the clients also cannot automatically delete unnecessary files from the flash memory.
ulActivateMode	File activation mode. The value 0 indicates file activation without restart and 1 indicates file activation with restart. Other values indicate file activation without restart by default.
ulActivateDelayMode	File activation delay mode. The value 0 indicates immediate file activation, 1 indicates delayed file activation, and 2 indicates file activation after a specified period. Other values indicate immediate file activation.
ulActivateDelayTime	Delay time of file activation. The value ranges from 0 to 86400, in seconds. Other values indicate immediate file activation.
ulActivateInTime	Time of file activation. The value ranges from 00:00 to 23:59. Other values indicate immediate file activation.

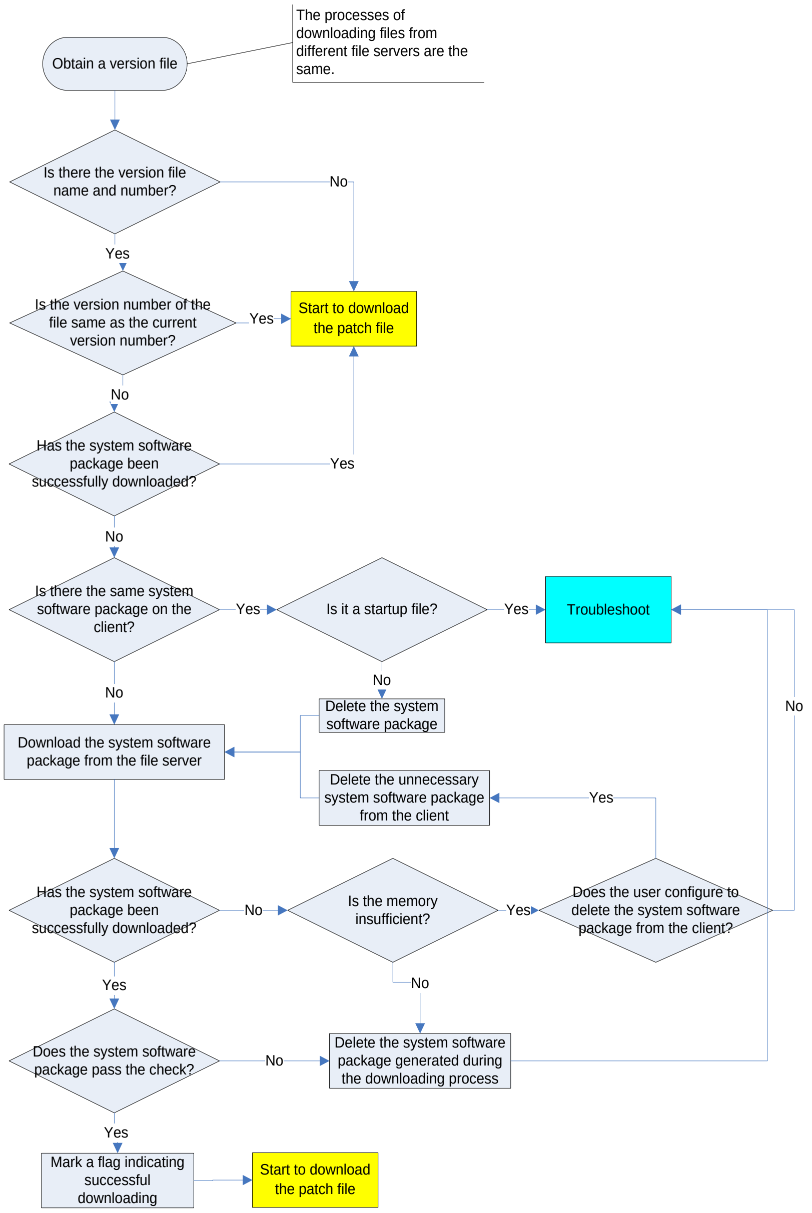
In this way, the client obtains the file server IP address, user name, and password and files to be downloaded from the Commander. Note that the DOWNLOAD_INFO_RESPONSE packets sent from the Commander are encrypted and the client must decrypt the packets using the private key.

Client Downloading Files from the File Server (Step 7&8)

The client downloads system software packages, patch files, web page files, license files, configuration files, and user-defined files in sequence. If any file does not exist in the client database or group database, the client directly downloads the next file. The following describes the downloading process of each file.

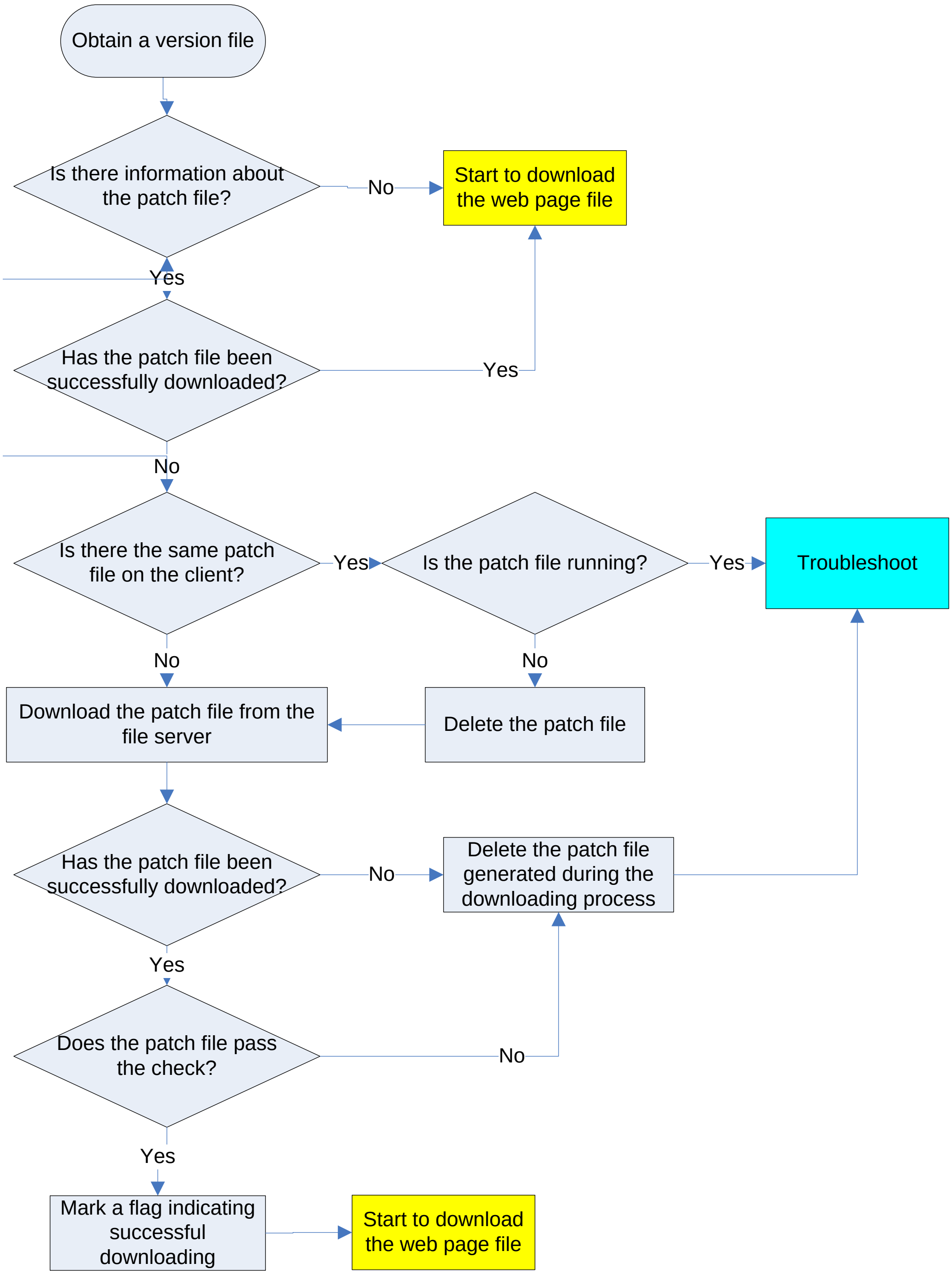
- System software package

Figure 2-14 Flowchart of downloading the system software package


Obtain a version file
The processes of downloading files from different file servers are the same.
Is there the version file name and number?
No
Yes
Is the version number of the file same as the current version number?
Yes
Start to download the patch file
No
Has the system software package been successfully downloaded?
Yes
No
Is there the same system software package on the client?
Yes
Is it a startup file?
Yes
Troubleshoot
No
No
Delete the system software package
No
Download the system software package from the file server
Delete the unnecessary system software package from the client
Yes
Has the system software package been successfully downloaded?
No
Is the memory insufficient?
Yes
Does the user configure to delete the system software package from the client?
Yes
No
Does the system software package pass the check?
No
Delete the system software package generated during the downloading process
Yes
Mark a flag indicating successful downloading
Start to download the patch file

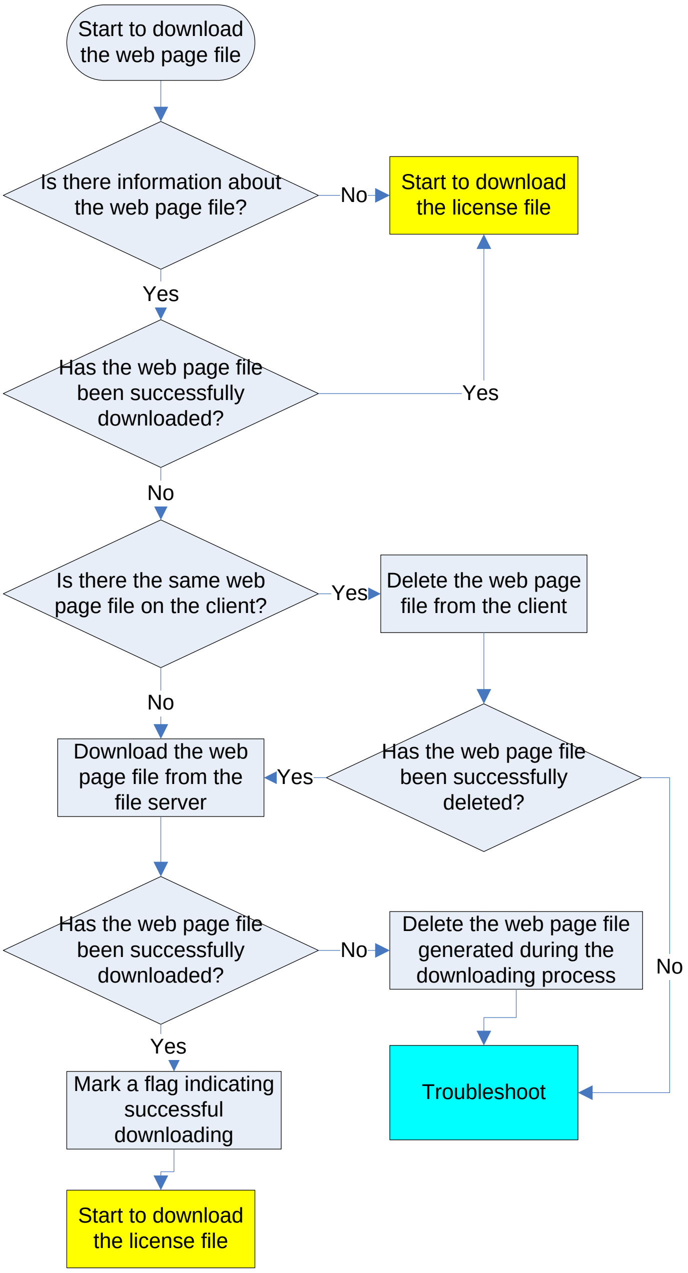
- Patch file

Figure 2-15 Flowchart of downloading the patch file


Obtain a version file
Is there information about the patch file?
No
Start to download the web page file
Yes
Has the patch file been successfully downloaded?
Yes
No
Is there the same patch file on the client?
Yes
Is the patch file running?
Yes
Troubleshoot
No
No
Download the patch file from the file server
Delete the patch file
Has the patch file been successfully downloaded?
No
Delete the patch file generated during the downloading process
Yes
Does the patch file pass the check?
No
Yes
Mark a flag indicating successful downloading
Start to download the web page file

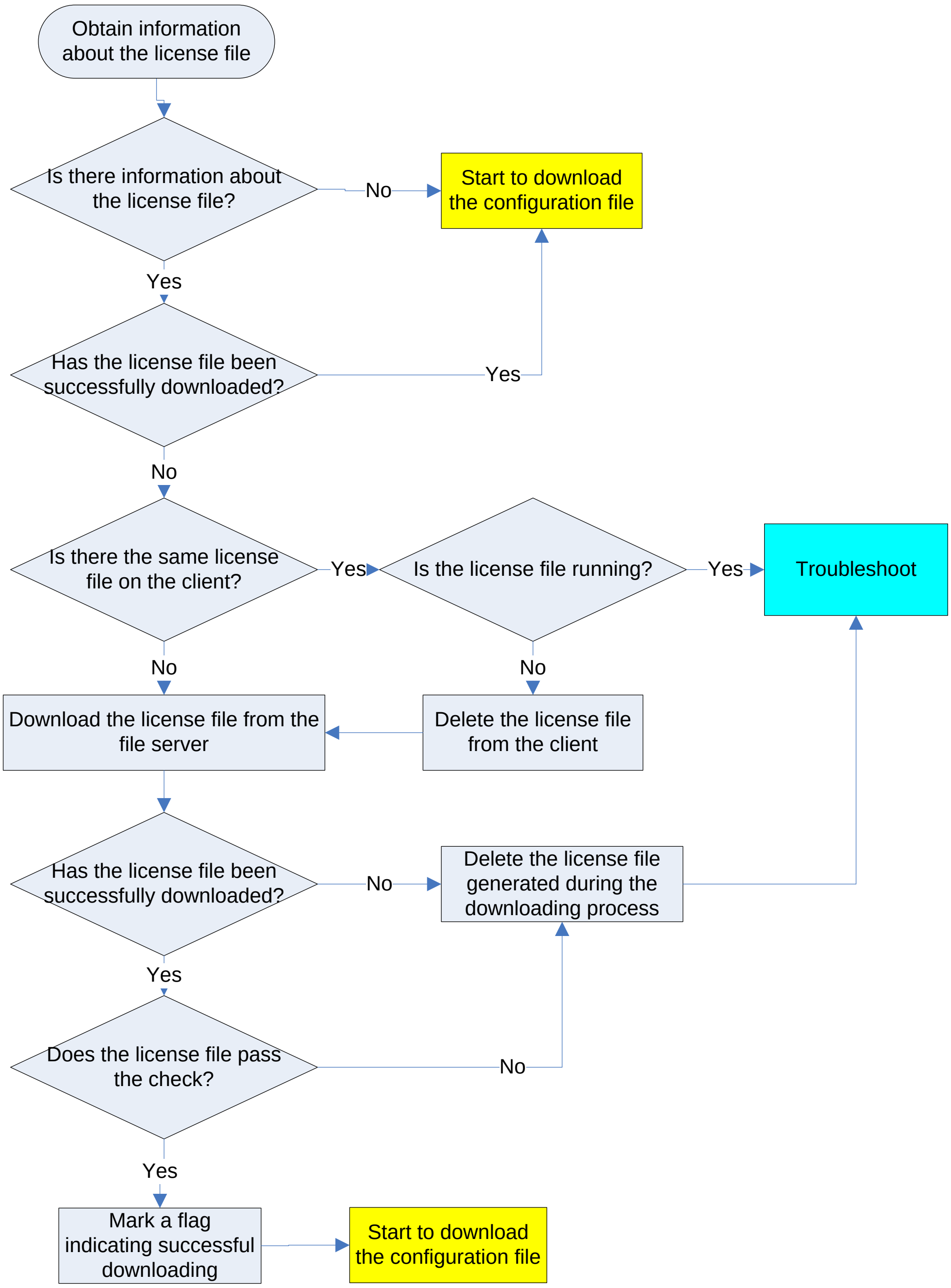
- Web page file

Figure 2-16 Flowchart of downloading the web page file


Start to download the web page file
Is there information about the web page file?
No
Start to download the license file
Yes
Has the web page file been successfully downloaded?
Yes
No
Is there the same web page file on the client?
Yes
Delete the web page file from the client
No
Download the web page file from the file server
Yes
Has the web page file been successfully deleted?
Has the web page file been successfully downloaded?
No
Delete the web page file generated during the downloading process
No
Yes
Mark a flag indicating successful downloading
Troubleshoot
Start to download the license file

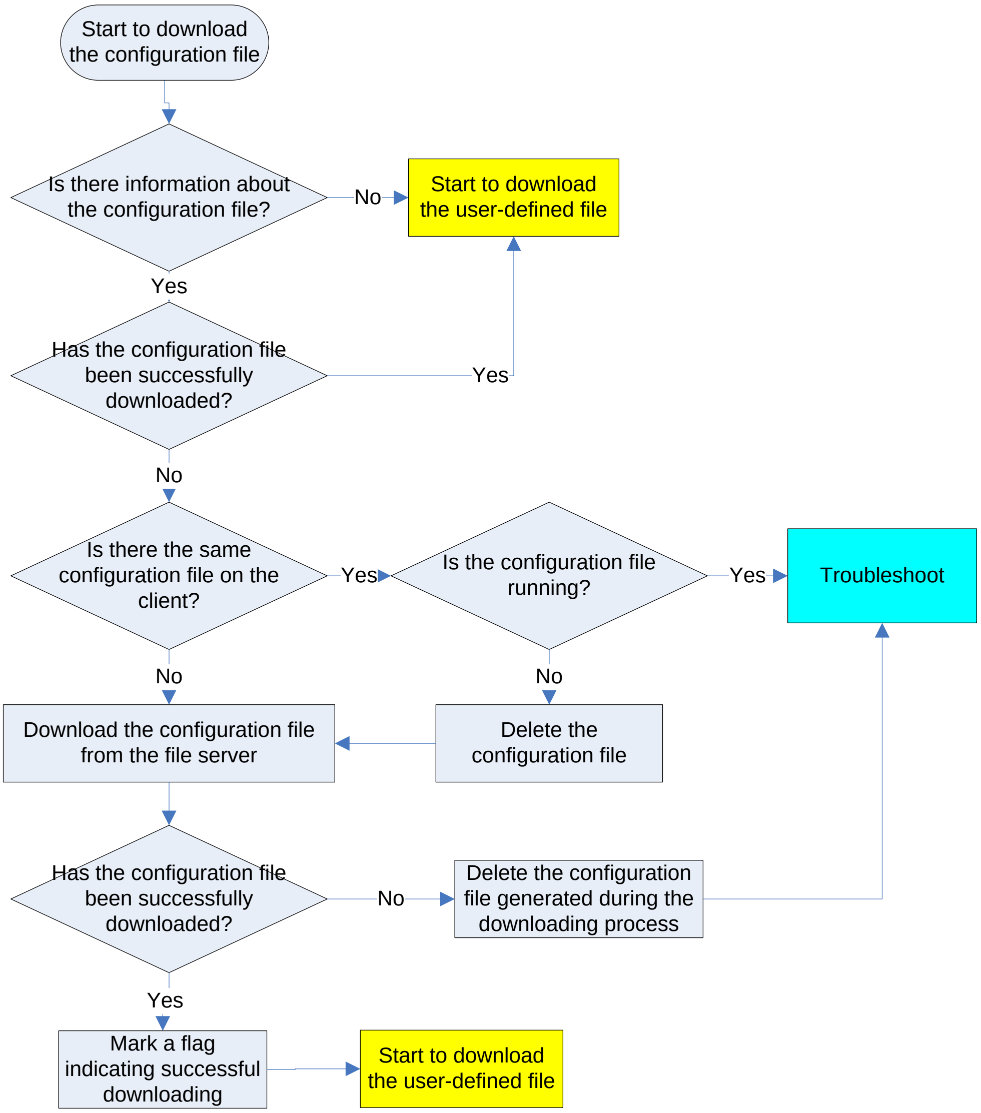
- License file (The client cannot download license files in the Zero-Touch scenario.)

Figure 2-17 Flowchart of downloading the license file


Obtain information about the license file
Is there information about the license file?
No
Start to download the configuration file
Yes
Has the license file been successfully downloaded?
Yes
No
Is there the same license file on the client?
Yes
Is the license file running?
Yes
Troubleshoot
No
No
Download the license file from the file server
Delete the license file from the client
Has the license file been successfully downloaded?
No
Delete the license file generated during the downloading process
Yes
Does the license file pass the check?
No
Yes
Mark a flag indicating successful downloading
Start to download the configuration file

- Configuration file

Figure 2-18 Flowchart of downloading the configuration file


Start to download the configuration file
Is there information about the configuration file?
No
Start to download the user-defined file
Yes
Has the configuration file been successfully downloaded?
Yes
No
Is there the same configuration file on the client?
Yes
Is the configuration file running?
Yes
Troubleshoot
No
No
Download the configuration file from the file server
Delete the configuration file
Has the configuration file been successfully downloaded?
No
Delete the configuration file generated during the downloading process
Yes
Mark a flag indicating successful downloading
Start to download the user-defined file

- User-defined file

  The downloading process of user-defined files is the same as that of the web page file, and not mentioned here.

Client Reporting the Downloading Progress to the Commander (Step 9)

When downloading files from the Commander, the client reports the downloading progress to the Commander through PROCESS_INFO packets until all files are successfully downloaded.

The Commander does not respond to the PROCESS_INFO packets.

Figure 2-19 Format of a PROCESS_INFO packet

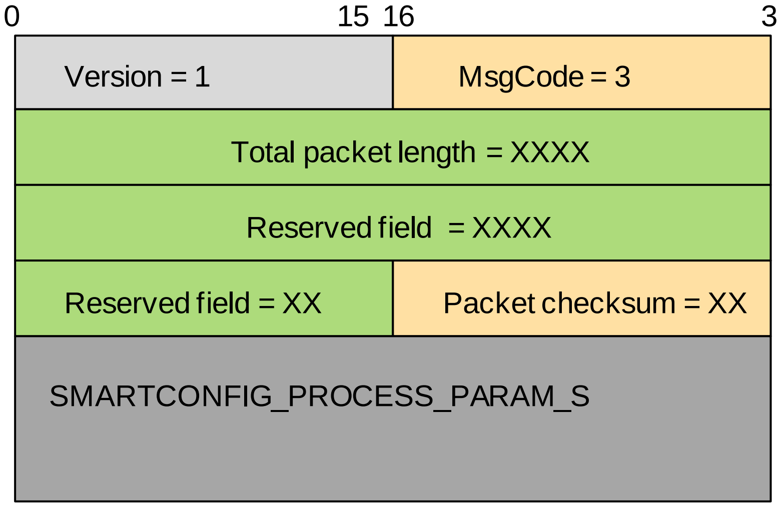


Table 2-8 lists fields in a PROCCESS_INFO packet.

Table 2-8 Fields in a PROCESS_INFO packet

Field	Description
ulClientIpAddr	IP address of the client.
ulClientIpAddrType	Type of the IP address. The value 0 indicates an IPv4 address and 1 indicates an IPv6 address. Other values indicate an IPv4 address by default.
szClientMacAddr	MAC address of the client.
szClientModel	Device model of the client. The value must be the same as the formal model, such as S5700-28P-LI-AC.
szClientDeviceType	Device type of the client. The value must be the same as the formal type, such as S5700-LI.
szClientESN	ESN of the client.
szClientHostName	Host name of the client.
szVrpFilename szVrpFileVersion szPatFilename szWebFilename szCfgFilename szLicFilename szUserDef1Filename szUserDef2Filename szUserDef3Filename	Names of files to be downloaded.

Field	Description
ulSmartconfgMethod	Method for deploying the client. For details, see Table 2-9.
ulEasy InstallPhase	Running state of the client's state machine. For details, see Table 2-10.
ulEasy InstallOptStat	State of the client during the file downloading process. For details, see Table 2-11.
ulEasy InstallDownPercent	File downloading progress, in percentage. This field is not supported currently and is reserved.
ulEasy InstallErrReson	Cause of errors. For details, see Table 2-12.
szErrResonDescr	Description of error causes.

Table 2-9 lists values of the **ulSmartconfgMethod** field.

Table 2-9 Values of the ulSmartconfgMethod field

Value	Description
0x00	Unknown state
0x01	Zero-Touch deployment
0x02	Automatic upgrade
0x03	Deployment using a USB flash drive

Table 2-10 lists values of the **ulEasy InstallPhase** field.

Table 2-10 Values of the ulEasy InstallPhase field

Value	Description
0x00	Unknown state
0x01	Initializing
0x02	Applying for an IP address from the DHCP server
0x03	Obtaining file information
0x04	Downloading files
0x05	Activating files
0x06	Running properly

Table 2-11 lists values of the **ulEasy InstallOptStat** field.

Table 2-11 Values of the ulEasy InstallOptStat field

Value	Description
0x00	Unknown state
0x01	Downloading the system software package
0x02	Downloading the configuration file
0x03	Downloading the patch file
0x04	Downloading the web page file
0x05	Downloading the license file
0x06	Downloading the first user-defined file
0x07	Downloading the second user-defined file
0x08	Downloading the third user-defined file

Table 2-12 lists values of the **ulEasy InstallErrReson** field.

Table 2-12 Values of the ulEasy InstallErrReson field

Value	Description
0x00	No error exists.
0x01	Failed to obtain file information from the Commander.
0x02	The file server is unreachable.
0x03	The user name or password is incorrect.
0x04	The file does not exist on the file server.
0x05	The MAC address is invalid.
0x06	The ESN is invalid.
0x07	The storage memory on the local device or card is insufficient.
0x08	The storage memory on other devices or cards is insufficient.
0x09	Failed to synchronize files with other devices.
0x0A	The name of the file to be downloaded is the same as the name of a system file on the local device or card.
0x0B	The name of the file to be downloaded is the same as the name of a system file on other devices or cards.
0x0C	Failed to pass the validity check.
0x0D	Failed to activate files.
0x0E	Failed to restart the device.

Value	Description
0x0F	The server type is incorrect.
0xFFFFFFFE	An unknown error exists.

During the Zero-Touch process, the client reports information about each state to the Commander through PROCESS_INFO packets. In this way, users can view the progress of each client on the Commander. If an error occurs in the downloading process, the client sends the error message to the Commander.

A PROCESS_INFO packet carries the current progress of the client. After sending a PROCESS_INFO packet, the client directly enters the next state without receiving any response from the Commander. A PROCESS_INFO packet is triggered in either of the following situations:

- An event occurs, including:
  - The status of the state machine changes.
  - A file has been downloaded.
  - An error occurs during the downloading process.
- The timer times out.

  The client receives no response to its PROCESS_INFO packets. To prevent packet loss, the client sends PROCESS_INFO packets to the Commander at an interval of 30 seconds until all files are successfully downloaded.

Client Activating Files (Step 10)

The client activates downloaded files based on the **ulActivateMode** field in the DOWNLOAD_INFO_RESPONSE packet.

The default file activation mode is used unless otherwise specified by users on the Commander. By default, all downloaded files, except for system software packages, are activated without restart. The client automatically activates downloaded files based on internal instructions, for example, configuring the system software package to be loaded at next startup and automatically activating patch files.

By default, patches are hot patches and patch files are not activated through restart. You can configure the client to activate patch files through restart.

In a Zero-Touch scenario, configuration files are decompiled and written into the client line by line through a VRP interface, but not activated through restart by default. The configuration files will be loaded at next startup.

In the Zero-Touch scenario of V200R003C00, web page files cannot be automatically activated.

2.2.9 Zero-Touch Application Scenario

The Zero-Touch function applies to devices without any configuration on newly-deployed networks.

Pay attention to the following points in a Zero-Touch scenario:

- The Commander must be specified on the network. You are advised to deploy the Commander at the aggregation layer or higher layers to manage downstream clients, and configure the Commander as the gateway of a network segment or the DHCP relay agent.
- The Commander and newly deployed clients on the Zero-Touch network must be of V200R003C00 or later versions.
- Unless multiple clients on the network have the same configurations, the administrator needs to register clients with the Commander one by one, specify corresponding files to be downloaded on the Commander, and upload configuration files for each client on the file server. To relieve workload, the administrator can fill in the templates with client information and import the information to the web management system. The system then automatically generates a client database.
- If files are stored on the Commander instead of a file server, the Commander must notify the client of the Commander IP address as the file server IP address.
- Chassis switches are recommended as the Commander.

2.3 Device Auto-Join

The device auto-join function is implemented based on the Commander-Client architecture and applies to the scenario where a running device wants to directly join the network.

Without EasyDeploy, you can ignore newly joined devices, but also cannot manage the devices. EasyDeploy manages clients in a unified manner, but client information must be configured on the Commander in advance.

To allow clients to join the network temporarily, EasyDeploy provides the device auto-join function. In this way, a running device can join a network of the Commander-Client architecture and register itself with the Commander as a client.

NOTE

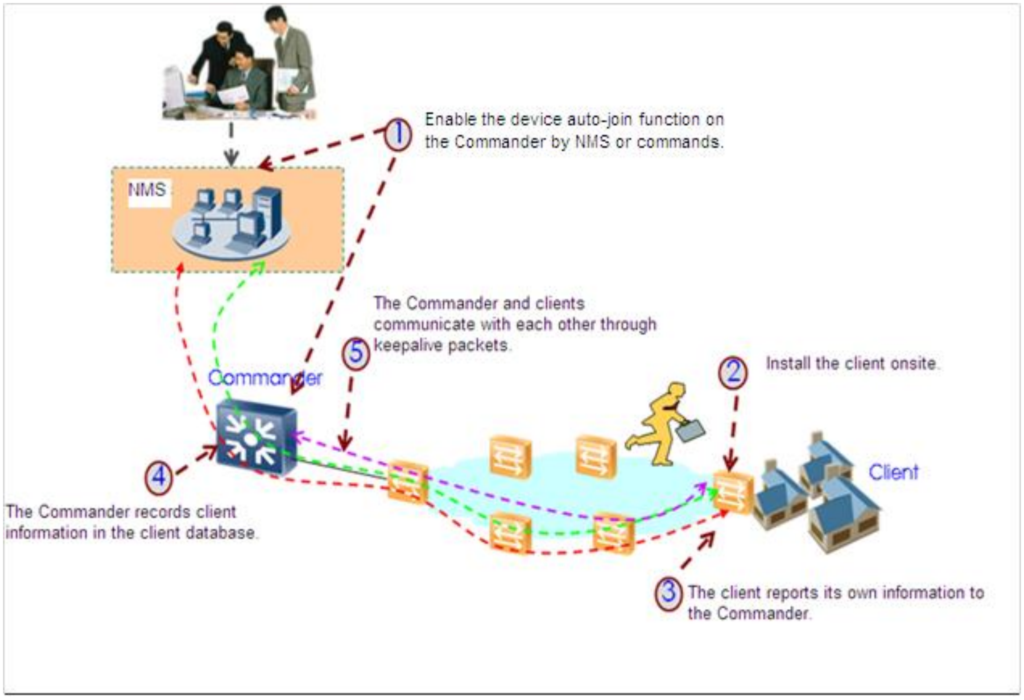
By default, the device auto-join function is disabled on the Commander.

2.3.1 Network Architecture

A typical network of device auto-join consists of the Commander, clients, DHCP server, NMS (optional), and file server (optional). The network is similar to the Zero-Touch network, and details are not provided here.

2.3.2 Device Auto-Join Process

Figure 2-20 Process of device auto-join


① Enable the device auto-join function on the Commander by NMS or commands.
NMS
⑤ The Commander and clients communicate with each other through keepalive packets.
② Install the client onsite.
Commander
Client
④ The Commander records client information in the client database.
③ The client reports its own information to the Commander.

The device auto-join process is as follows:

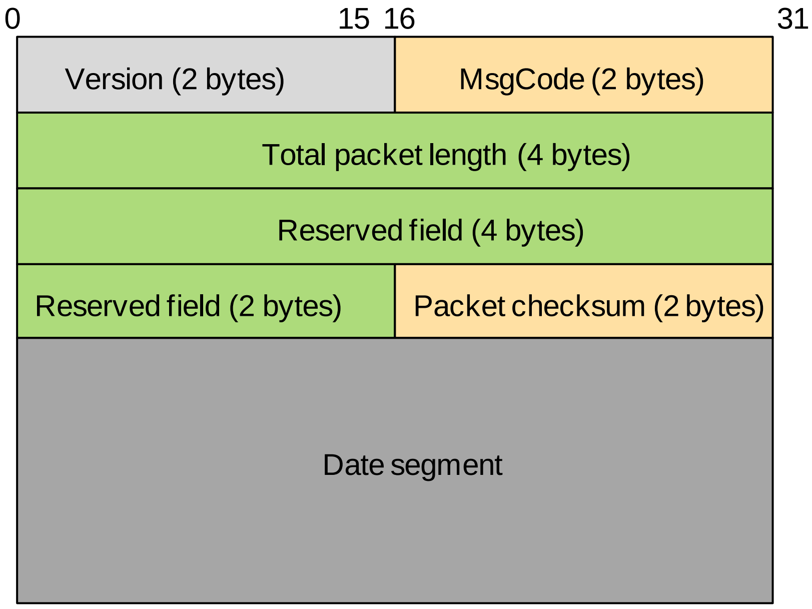
- **Step 1**: Enable the device auto-join function on the Commander.
- **Step 2**: Add a running client to the network.
- **Step 3**: The new client reports its own information to the Commander through keepalive packets.
- **Step 4**: The Commander records information about the new client in the client database.
- **Step 5**: The Commander responds to the keepalive packets sent by the client. The management link between the Commander and client is established.

2.3.3 Client Working Process in a Device Auto-Join Scenario

During a device auto-join process, the client keeps running properly, involving no status switch.

2.3.4 Protocol Packet Format

Figure 2-21 EZOP packet format



The **Version** field indicates the message version number, which is fixed at 01. This field is used to identify messages of different versions in the future. Table 2-13 lists values of the **MsgCode** field.

Table 2-13 Values of the MsgCode field

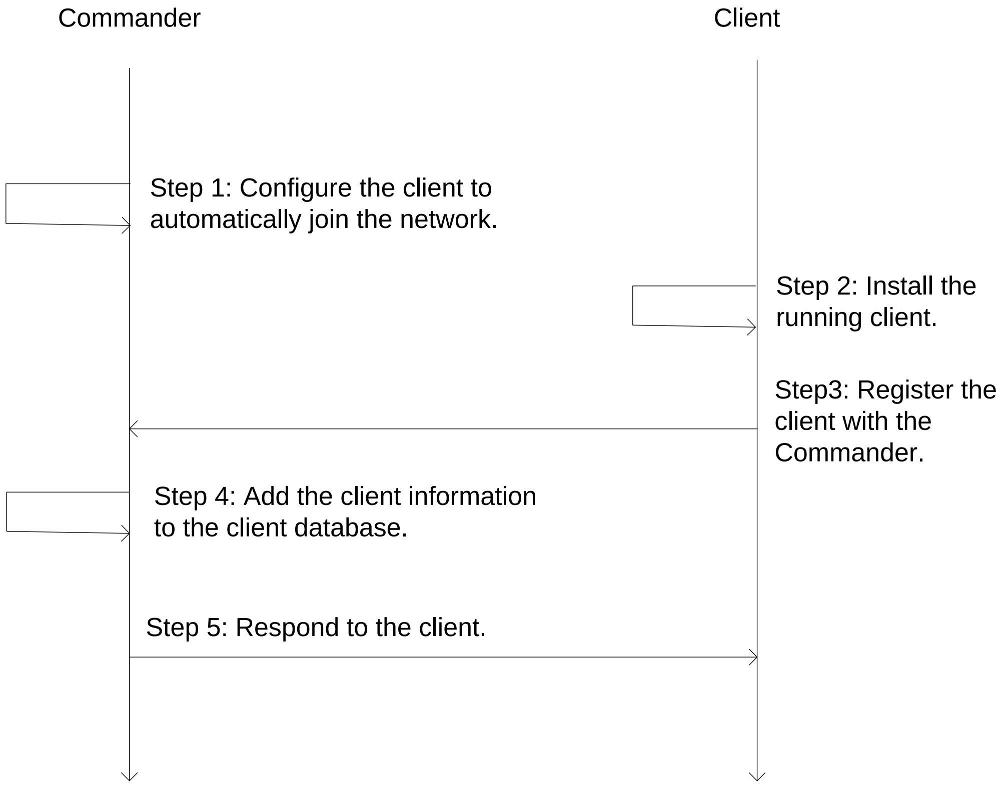
Value	Name	Description
0x0004	STATUS_INFO	Message code in the request packet that a client periodically sends to notify the Commander of the client's status. The packet is a keepalive packet and carries information about files on the client.
0x0005	STATUS_INFO _RESPONSE	Message code in the packet that the Commander sends in response to the client's request packet.

2.3.5 Commander Database

In a device auto-join process, the Commander updates its client database with information about the new client. Entries in this client database, also called the dynamic client database, are dynamically learned and share the client information with the client database manually configured by users.

2.3.6 Device Auto-Join Description

Figure 2-22 Device auto-join flowchart


Commander
Client
Step 1: Configure the client to automatically join the network.
Step 2: Install the running client.
Step3: Register the client with the Commander.
Step 4: Add the client information to the client database.
Step 5: Respond to the client.

The following sections describe the device auto-join process in details from step 3.

Client Registering with the Commander (Step 3)

The client sends a STATUS_INFO packet with the **MsgCode** field as **0x0004** to the Commander to notify its existence and report its information. Figure 2-23 shows the format of a STATUS_INFO packet.

Figure 2-23 Format of a STATUS_INFO packet

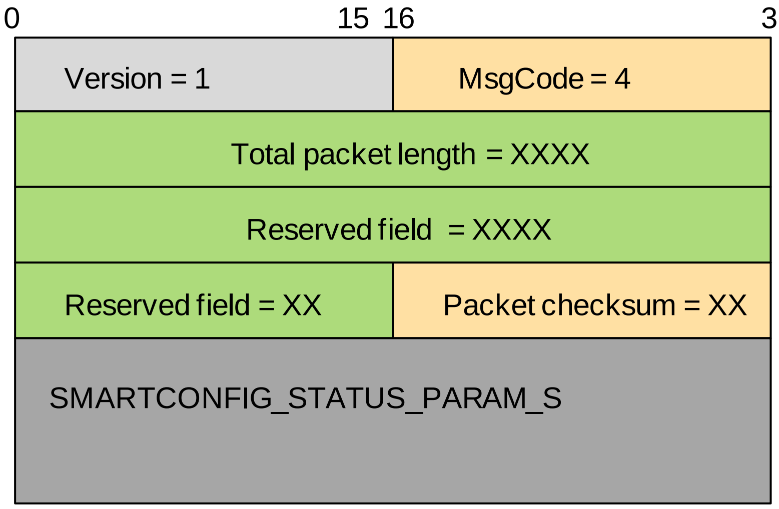


Table 2-14 lists fields in a STATUS_INFO packet.

Table 2-14 Fields in a STATUS_INFO packet

Field	Description
ulClientIpAddr	IP address of the client.
ulClientIpAddrType	Type of the IP address. The value 0 indicates an IPv4 address and 1 indicates an IPv6 address. Other values indicate an IPv4 address by default.
szClientMacAddr	MAC address of the client.
szClientModel	Device model of the client. The value must be the same as the formal model, such as S5700-28P-LI-AC.
szClientDeviceType	Device type of the client. The value must be the same as the formal type, such as S5700-LI.
szClientESN	ESN of the client.
szClientHostName	Host name of the client.
szVrpFilename szVrpFileVersion szPatFilename szWebFilename szCfgFilename szLicFilename	Names of files to be downloaded.
szBackupConfigName	Name of the backup configuration file.

Field	Description
ulBackupConfigErrReson	Cause for a configuration backup error.
szErrResonDescr	Result of backing up files to the file server. The value can be: • Backup configuration file by sftp successfully. • Backup configuration file by sftp failed.
szRsaPublicKey	RSA public key.

A STATUS_INFO packet carries client information as well as backup information about the configuration file. For details, see section 2.6 "Configuration Backup."

NOTE

The STATUS_INFO packets can be transmitted at an interval of 30 seconds as the keepalive packets between the Commander and clients. If the Commander does not receive any STATUS_INFO packets from a client for 120 seconds, the Commander considers that the client is lost.

Commander Storing Client Information (Step 4)

After the client has been registered with the Commander, information about the client is stored in the client database (also called the dynamic client database) on the Commander. The client database manually configured by users is called the static client database.

The dynamic and static client databases differ with each other only in the **ucMatchRuleType** field. If the value of the **ucMatchRuleType** field is **0**, the client is added to the dynamic client database. Otherwise, the client is added to the static client database.

Commander Responding to the Client (Step 5)

After receiving the STATUS_INFO packet from the client, the Commander responds to the client with a STATUS_INFO_RESPONSE packet with the **MsgCode** field as **0x0005**. Figure 2-24 shows the format of a STATUS_INFO_RESPONSE packet.

Figure 2-24 Format of a STATUS_INFO_RESPONSE packet

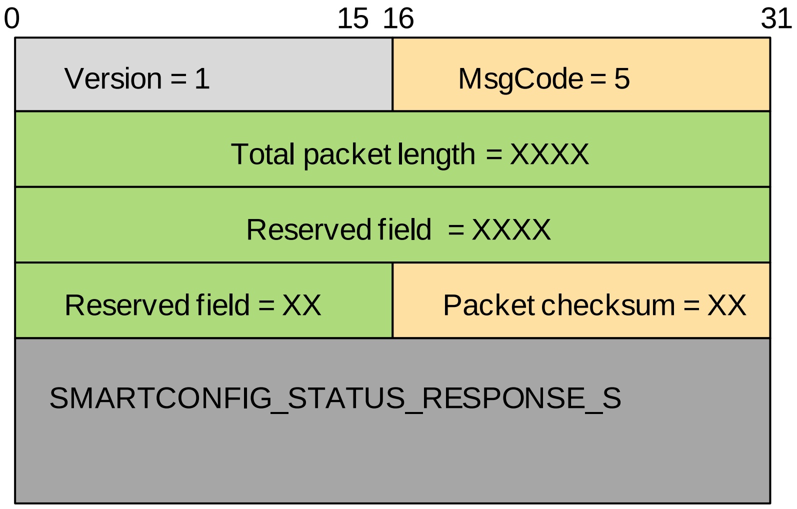


Table 2-15 lists fields in a STATUS_INFO_RESPONSE packet.

Table 2-15 Fields in a STATUS_INFO_RESPONSE packet

Field	Description
ulBackupEnableFlag	Flag of configuration file backup.
ulBackupInterval	Interval for backing up a configuration file.
ulBackupMode	Mode in which a configuration file is backed up.
ulBackupServerType	Type of the file server.
ulBackupServerIpAddr	IP address of the file server.
ulBackupServerIpAddrType	IP address type of the file server.
szUserName	User name for logging in to the file server.
szPassword	Password for logging in to the file server.

The STATUS_INFO_RESPONSE packet also carries backup information about configuration files.

NOTE

A STATUS_INFO_RESPONSE packet can function as the response packet to the keepalive packet sent by the client.

2.3.7 Application Scenario of the Device Auto-Join Function

The device auto-join function applies to the scenario where a running device wants to directly join a network of the Commander-Client architecture. The newly joined device can be a device with configurations, providing a flexible network deployment mode.

On a network running EasyDeploy, you can enable the device auto-join function on the Commander and configure the Commander IP address on the client. After routes between the Commander and clients are reachable, the Commander automatically learns basic information about clients and adds the information to the client database. Information about clients includes the MAC address, ESN, IP address, device type, device model, and names of the system software package, configuration file, and patch file installed on the clients. In this way, the Commander can monitor and manage basic information and version files of all clients on the network. In the batch upgrade scenario, the information can be used to specify devices to be upgraded.

After a client joins the network, the configuration file of this client can be backed up. However, other files such as the system software package and patch file cannot be backed up. If the client is faulty and needs to be replaced, only the configuration file of the original client can be inherited.

2.4 Batch Upgrade

The batch upgrade function applies to the enterprise networks where running devices need to be upgraded in a batch due to the end of service (EOS), software bugs, or new function launching.

Without EasyDeploy, network administrators have to load the target version to the devices one by one. The workload is heavy to upgrade a large number of devices.

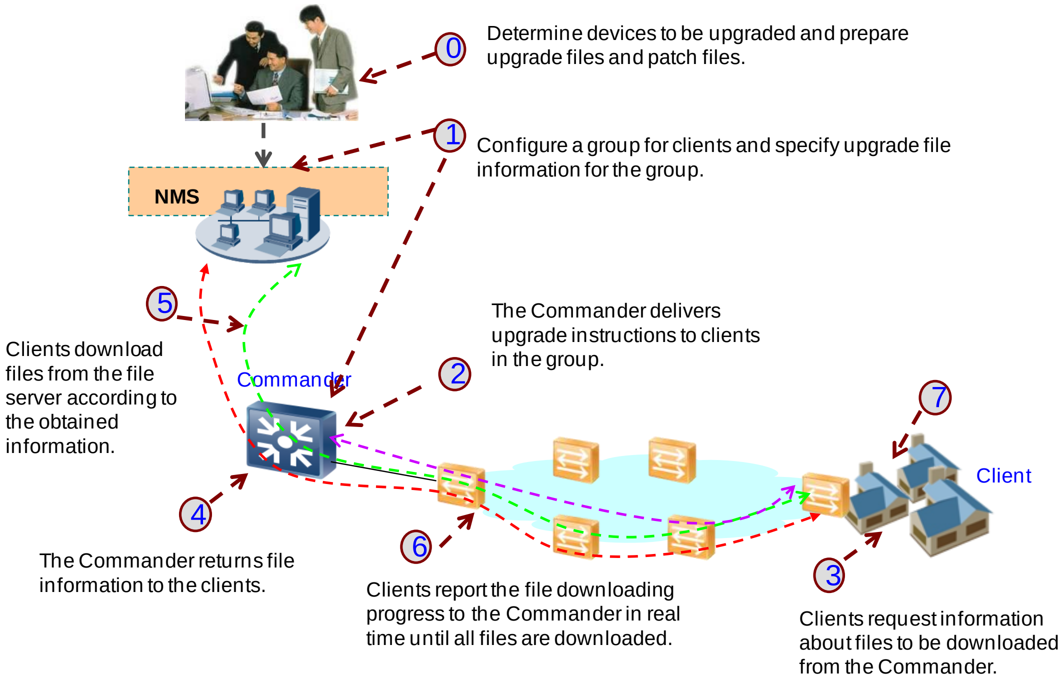
EasyDeploy provides the batch upgrade function to relieve workload for network administrators. Network administrators simply need to record the MAC addresses, ESNs, or types of the devices requiring the same target version and create a group for these devices. Then network administrators can complete the one-key batch upgrade using the CLI or NMS in a remote equipment room of the network center, effectively reducing the workload.

2.4.1 Network Architecture

A typical network of a batch upgrade consists of the Commander, clients, DHCP server, NMS (optional), and file server (optional). The network is similar to the Zero-Touch network, and details are not provided here.

2.4.2 Batch Upgrade Process

Figure 2-25 Batch upgrade process

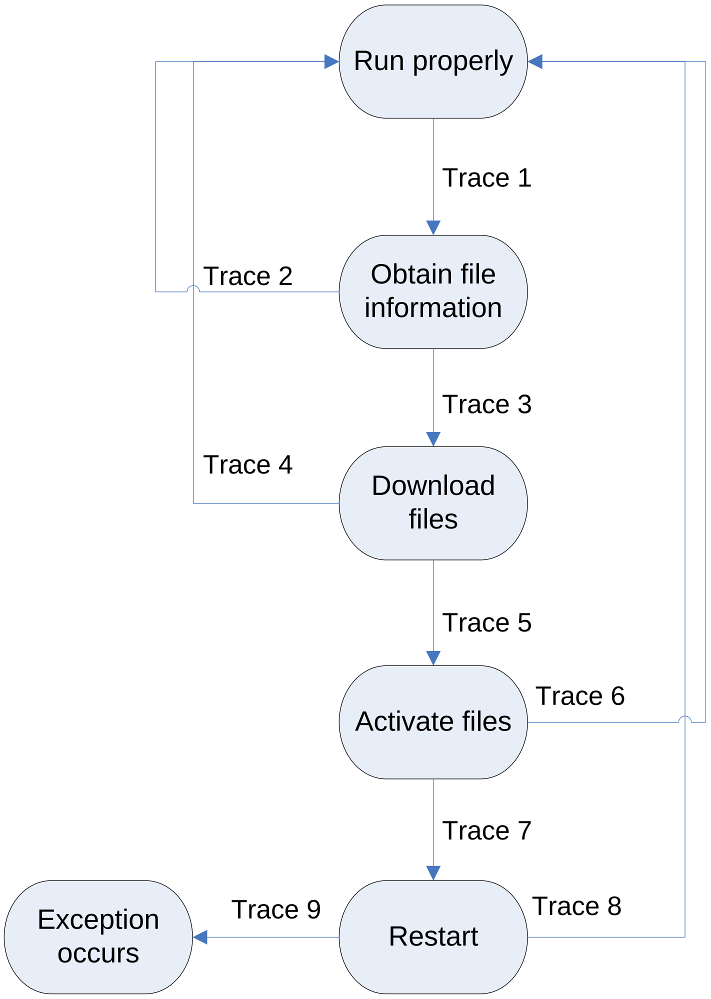

0
Determine devices to be upgraded and prepare upgrade files and patch files.
1
Configure a group for clients and specify upgrade file information for the group.
NMS
5
Clients download files from the file server according to the obtained information.
Commander
2
The Commander delivers upgrade instructions to clients in the group.
7
Client
4
The Commander returns file information to the clients.
6
Clients report the file downloading progress to the Commander in real time until all files are downloaded.
3
Clients request information about files to be downloaded from the Commander.

The batch upgrade process is as follows:

- **Step 0:** Network administrators determine devices to be upgraded, upgrade files, and which devices using the same upgrade file.
- **Step 1:** Network administrators group the devices using the same upgrade file and specify upgrade files for the group using the CLI or NMS.
- **Step 2:** Network administrators issue upgrade instructions to clients in the group using a command on the Commander. Before delivering the upgrade instructions, the Commander compares the current file of each client with the upgrade file. If the files are the same, the Commander stops the upgrade.
- **Step 3:** After receiving the upgrade instructions, the clients send request packets to the Commander for information about files to be downloaded.
- **Step 4:** The Commander, according to fields in the clients' request packets, determines that the clients meet upgrade requirements. The Commander then obtains file server information and file information from the group database matching the clients, and sends the information to the clients.
- **Step 5:** After obtaining file information, clients download files from the file server.
- **Step 6:** Clients download the files in a specified sequence. Once a file is downloaded or fails to be downloaded, the clients report the file downloading progress to the Commander.
- **Step 7:** According to the configuration on the Commander, clients decide whether to restart to make the downloaded files take effect.

2.4.3 Client Working Process During a Batch Upgrade

Figure 2-26 Client working process during a batch upgrade



Running Properly

Clients are running properly. Clients can transition from any state to the normal running state. They are in this state when they have a configuration file or after downloading all required files and restarting (if downloaded files take effect only after a restart).

Obtaining File Information

Clients obtain information about files to be downloaded and file server information from the Commander. A client attempts to obtain file information at an interval of 1 minute. After five failures to obtain file information, the client cancels the upgrade and enters the normal running state.

Downloading Files

Based on the obtained information, clients download the system software packages, patch files, web page files, license files, configuration files, and user-defined files in sequence.

All the files are optional for a batch upgrade. Clients decide whether to download the files according to the configuration on the Commander.

A client attempts to download a file at an interval of 5 minutes. If the downloading fails for three times, the client stops downloading files, enters the normal running state, and sends error information to the Commander. Users determine whether to delete the downloaded files.

Activating Files

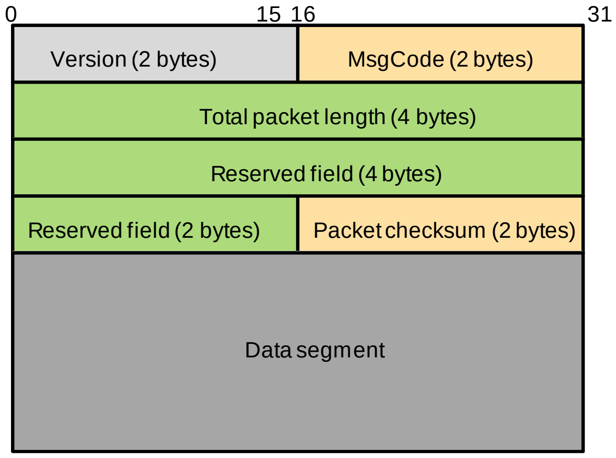
In this phase, clients activate all downloaded files. If clients have downloaded a system software package or configuration file, they restart to activate all downloaded files by default.

Table 2-16 Working process description

Trace N	Event
Trace 1	A running client receives an upgrade instruction from the Commander.
Trace 2	The client fails to obtain information about files to be downloaded.
Trace 3	The client obtains file information.
Trace 4	The client fails to download a file.
Trace 5	The client downloads all required files.
Trace 6	Downloaded files are activated without device restart.
Trace 7	Downloaded files can be activated only after the client restarts.
Trace 8	The client runs properly after a restart.
Trace 9	The client does not run properly after a restart.

2.4.4 Protocol Packet Format

Figure 2-27 EZOP packet format



The **Version** field indicates the message version number, which is fixed at 01. This field is used to identify messages of different versions in the future. Table 2-17 lists values of the **MsgCode** field.

Table 2-17 Values of the MsgCode field

Value	Name	Description
0x0001	DOWNLOAD_INFO_REQUEST	Message code in the request packet that a client sends to the Commander for information about files to be downloaded.
0x0002	DOWNLOAD_INFO_RESPONSE	Message code in the packet that the Commander sends in response to the client's request packet.
0x0003	PROCCESS_INFO	Message code in packets that a client sends to the Commander to report the batch upgrade progress. The client reports the batch upgrade progress to the Commander until the batch upgrade process ends, regardless of whether the client is running properly.
0x0006	UPGRADE_NOTICE	Message code in the upgrade instruction that the Commander sends to clients after network administrators execute the upgrade command.

2.4.5 Commander Database

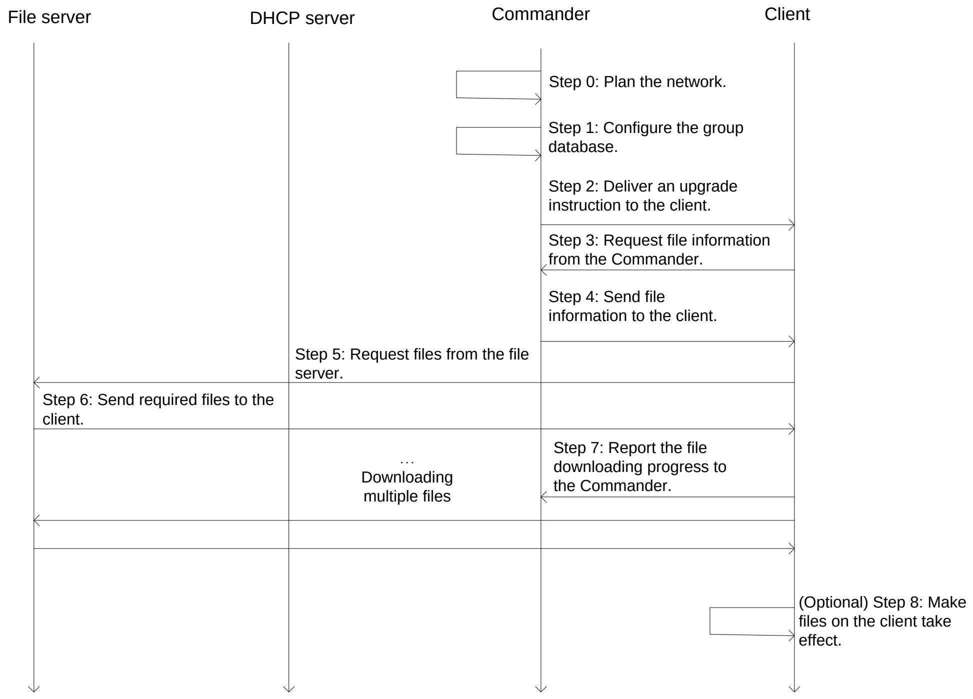
During a batch upgrade, the Commander still searches the client database and group database, which have been described in section 2.2.6 "Commander Database."

The database lookup sequence in a batch upgrade is different from that in the Zero-Touch scenario. When receiving EZOP request packets from clients for file information, the Commander searches only the group database for the file information. The Commander searches the client database to find client information and determines whether to send upgrade instructions to clients. The following section describes the detailed upgrade process.

2.4.6 Batch Upgrade Description

Figure 2-28 shows the batch upgrade flowchart. For details about the batch upgrade process, see Figure 2-25. Steps in Figure 2-28 are more detailed than those in Figure 2-25.

Figure 2-28 Batch upgrade flowchart


File server
DHCP server
Commander
Client
Step 0: Plan the network.
Step 1: Configure the group database.
Step 2: Deliver an upgrade instruction to the client.
Step 3: Request file information from the Commander.
Step 4: Send file information to the client.
Step 5: Request files from the file server.
Step 6: Send required files to the client.
…
Downloading multiple files
Step 7: Report the file downloading progress to the Commander.
(Optional) Step 8: Make files on the client take effect.

The following sections describe important steps in details.

Configuring the Group Database on the Commander (Step 1)

Table 2-18 lists fields in the group database.

Table 2-18 Fields in the group database

Field	Description
ulGroupId	Index of a group, which determines the group to which clients belong.
szGroupName	Name of the group, which is user-defined.
ulMatchRule	Rule matching type.
ulCurRuleNum	Number of matching rules.
szImgFile	Names and other information about files to be downloaded.

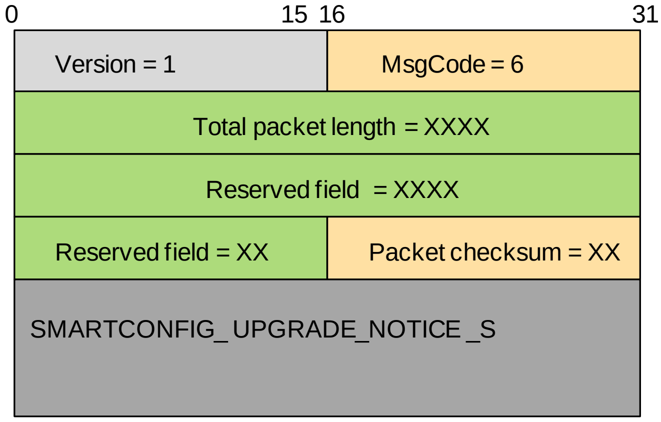
Field	Description
szImgVers szCfgFile szPatFile szWebFile szLicFile szCsmFile	
stActFile	Policy for activating files.
pstRuleHead pstRuleTail	Start and end matching rules in the group.
pNextGrp pPrevGrp	Next and previous matching rules of the current matching rule in the group.

Users can configure groups based on the MAC address, ESN, or other types of information on the Commander using the CLI or NMS. The group database contains key information listed in Table 2-18. It provides information about files for upgrading clients, based on which clients can obtain the required files.

Commander Delivering Upgrade Instructions (Step 2)

After the group database is configured on the Commander, the Commander sends UPGRADE_NOTICE packets to clients to instruct the clients to prepare for upgrades. The **MsgCode** field in UPGRADE_NOTICE packets is 0x0006. Figure 2-29 shows the format of a UPGRADE_NOTICE packet.

Figure 2-29 UPGRADE_NOTICE packet format



The batch upgrade command **upgrade group** [*group-name*] &<1-15> is executed on the Commander. The Commander obtains the group ID based on the group name and determines whether each client belongs to this group by traversing all client databases. The Commander sends UPGRADE_NOTICE packets only to clients belonging to this group.

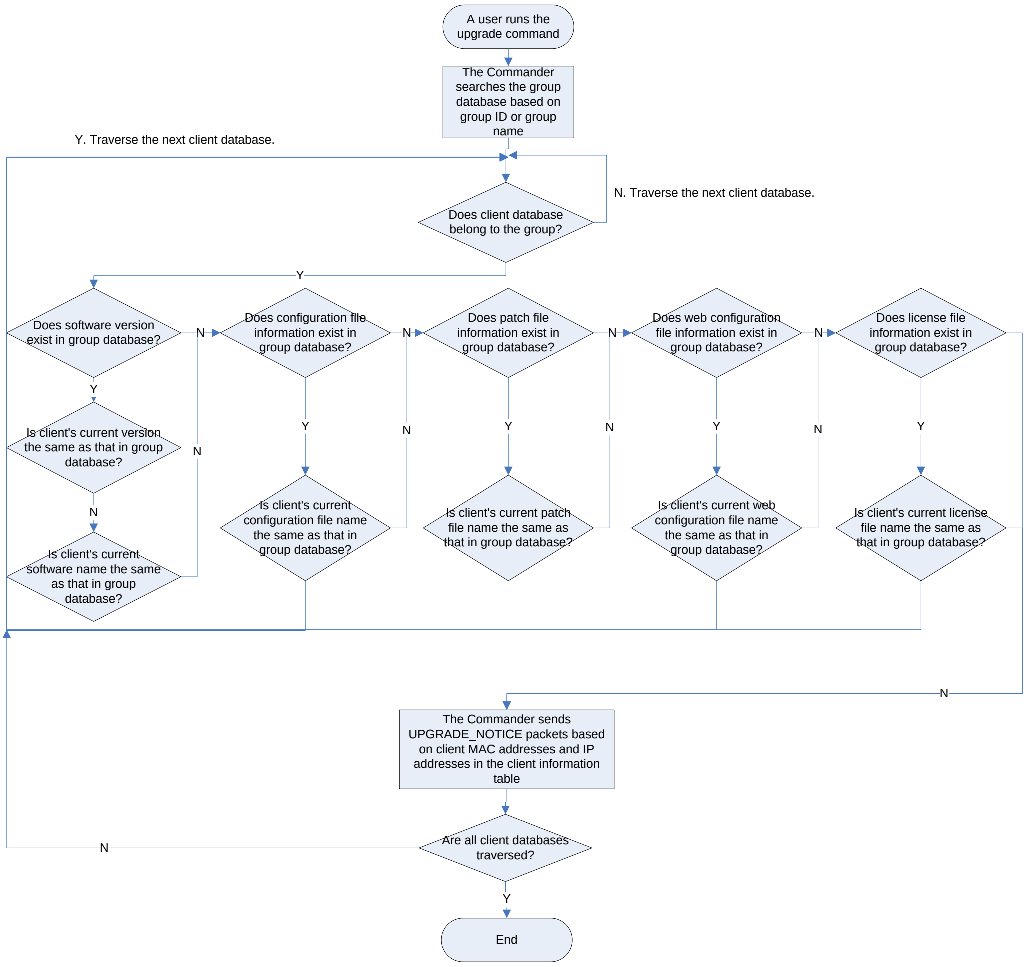
The Commander obtains the group ID and then sends UPGRADE_NOTICE packets carrying this group ID to clients. After receiving the packets, the clients send DOWNLOAD_INFO_REQUEST packets to the Commander.

After the upgrade command is executed on the Commander, the Commander delivers upgrade instructions to connected clients that are running properly and need to be upgraded. The Commander does not deliver an upgrade instruction to a client, but records error information, in any of following situations:

- The target version is the same as the current version of the client.
- The upgrade file name is the same as the current file name on the client. Names of user-defined files are not checked.
- The client is not running properly.

To prevent a large number of clients from starting the upgrade process at the same time, the Commander delivers upgrade instructions to each 50 clients at an interval of 5 seconds.

Figure 2-30 Process of sending an UPGRADE_NOTICE packet by the Commander


A user runs the upgrade command
The Commander searches the group database based on group ID or group name
Y. Traverse the next client database.
N. Traverse the next client database.
Does client database belong to the group?
Y
Does software version exist in group database?
N
Does configuration file information exist in group database?
N
Does patch file information exist in group database?
N
Does web configuration file information exist in group database?
N
Does license file information exist in group database?
Y
Is client's current version the same as that in group database?
N
N
Is client's current software name the same as that in group database?
Y
N
Is client's current configuration file name the same as that in group database?
Y
N
Is client's current patch file name the same as that in group database?
Y
N
Is client's current web configuration file name the same as that in group database?
Y
Is client's current license file name the same as that in group database?
N
The Commander sends UPGRADE_NOTICE packets based on client MAC addresses and IP addresses in the client information table
N
Are all client databases traversed?
Y
End

Clients Requesting File Information from the Commander (Step 3)

After receiving UPGRADE_NOTICE packets, clients send DOWNLOAD_INFO_REQUEST packets to the Commander for file information. The process is similar to "Client Requesting

File Information from the Commander (Step 5)" in section 2.2.8 "Zero-Touch Description", and is not provided here.

Values of the **ulClientRequestType** and **ulGroupId** fields in DOWNLOAD_INFO_REQUEST packets that clients send to the Commander in the batch upgrade scenario are different from those in the Zero-Touch scenario. In the batch upgrade scenario, the value of **ulClientRequestType** is **1**, indicating the upgrade process, and the **ulGroupId** field is set to the group ID delivered by the Commander. The Commander searches the group database for download information based on the two fields and sends the information to the clients.

Table 2-19 Description of key fields

Field	Description
ulClientRequestType	Type of a client's request for files to be downloaded, including Zero-Touch and upgrade. The value 0 indicates Zero-Touch and 1 indicates upgrade. Other values indicate Zero-Touch by default.
ulGroupId	Information about the group to which clients belong.

Subsequent Process (Steps 4 to 8)

Steps 4 to 8 in the batch upgrade scenario are similar to steps 6 to 10 in the Zero-Touch scenario, and details are not provided here.

2.4.7 Application Scenario

The batch upgrade function applies to the enterprise networks where running Huawei switches need to be upgraded in a batch due to the EOS, software bugs, or new function launching.

Common device upgrades include version upgrades and patch upgrades. You are advised to create a group based on the following rules:

- When clients to be upgraded are of the same model, classify the clients into the default group according to Table 2-5 in section 2.2.6 "Commander Database" for upgrade since the clients use the same upgrade file.
- When clients to be upgraded are of different models, classify clients of each model into the default group for upgrades since clients of the same model use the same upgrade file.
- In a few scenarios, clients to be upgraded are of diversified models and use different upgrade files, create groups based on client IP addresses. Compared with MAC address-based or ESN-based group planning, IP address-based group planning is easier and more convenient.

2.5 Faulty Device Replacement

Faulty device replacement applies to constructed networks where devices need to be replaced due to hardware failures or misoperations.

Without EasyDeploy, network administrators must replace faulty devices onsite and import configurations of faulty devices to the new devices. If the original devices and new devices use different system software package and patch files, network administrators must upgrade the system software package and patch files, resulting in heavy workload.

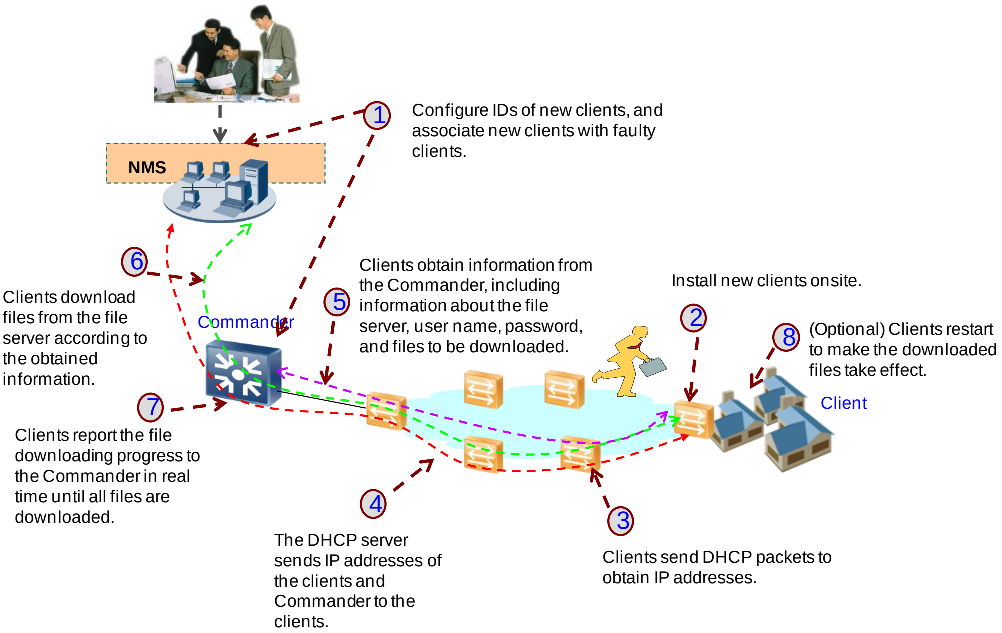
EasyDeploy provides the faulty device replacement function to relieve workload for network administrators. Before using this function, network administrators record IDs of new devices such as MAC addresses and ESNs, and specify IDs of the original devices. After the customer or agent installs new devices, network administrators associate the new devices with faulty devices using the CLI or NMS in a remote equipment room of the network center. Network administrators run only one command to configure new devices to automatically download files of the faulty devices, effectively reducing workload.

2.5.1 Network Architecture

A typical network of faulty device replacement consists of the Commander, clients, DHCP server, NMS (optional), and file server (optional). The network is similar to the Zero-Touch network, and details are not provided here.

2.5.2 Faulty Device Replacement Process

Figure 2-31 Faulty device replacement process


1
Configure IDs of new clients, and associate new clients with faulty clients.
NMS
6
Clients download files from the file server according to the obtained information.
Commander
5
Clients obtain information from the Commander, including information about the file server, user name, password, and files to be downloaded.
Install new clients onsite.
2
8
(Optional) Clients restart to make the downloaded files take effect.
Client
7
Clients report the file downloading progress to the Commander in real time until all files are downloaded.
4
The DHCP server sends IP addresses of the clients and Commander to the clients.
3
Clients send DHCP packets to obtain IP addresses.

The faulty device replacement process is as follows:

- **Step 1:** Network administrators associate new clients with faulty clients to allow the Commander to know a new device matches which faulty client's configuration file and other files.
- **Step 2:** The customer or agent installs new clients onsite.
- **Step 3:** Clients send DHCP packets to obtain IP addresses.
- **Step 4:** The DHCP server allocates IP addresses to the clients and sends the Commander IP address using Option 148 to the clients.

- **Step 5:** Clients exchange packets with the Commander. The Commander sends information about the configuration file, user-defined files, and file server to the clients based on the user configuration.
- **Step 6:** Clients download specified files from the file server.
- **Step 7:** Clients download the files in a specified sequence. Once a file is downloaded or fails to be downloaded, the clients report the file downloading progress to the Commander.
- **Step 8:** According to the configuration on the Commander, clients decide whether to restart to make the downloaded files take effect.

2.5.3 Client Working Process During Faulty Device Replacement

The working process on clients during faulty device replacement is the same as that during Zero-Touch.

For details, see section 2.2.4 "Client Working Process in a Zero-Touch Scenario."

2.5.4 Protocol Packet Format

The format of protocol packets in the faulty device replacement scenario is the same as that in the Zero-Touch scenario. For details, see section 2.2.5 "Protocol Packet Format."

2.5.5 Commander Database

During faulty device replacement, the Commander uses the client database and faulty device replacement database. For details about the client database, see section 2.2.6 "Commander Database."

The following sections describe the faulty device replacement database and the relationship between it and the client database.

Faulty Device Replacement Database

The Commander finds the faulty device replacement database based on MAC addresses or ESNs of new devices and finds the client database based on client IDs of faulty devices to associate information about new devices with information about faulty devices.

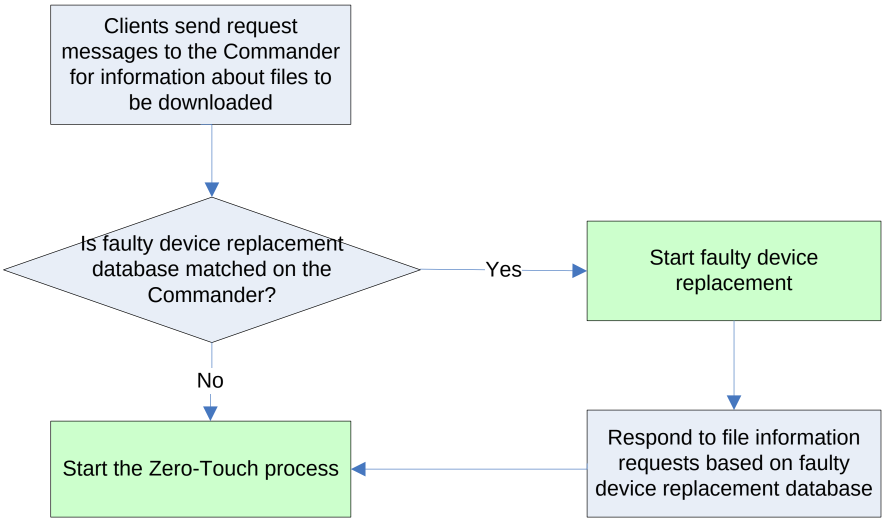
The faulty device replacement database includes the following information:

- IDs of original clients
- MAC addresses of new devices
- ESNs of new clients
- System software package of new clients
- System software version of new clients
- Patch file of new devices
- Web page file of new devices
- License file of new devices
- User-defined file of new devices

If a client fails to obtain information about the backup configuration file from the client database, the client attempts to obtain information about the configuration file from the client database. If no such information is found, the client uses information about the default configuration file. However, the default configuration file may differ from the configuration file on faulty clients.

2.5.6 Relationship Between Faulty Device Replacement and a Zero-Touch Scenario

Figure 2-32 Relationship between faulty device replacement and a Zero-Touch scenario


Clients send request messages to the Commander for information about files to be downloaded
Is faulty device replacement database matched on the Commander?
Yes
Start faulty device replacement
No
Start the Zero-Touch process
Respond to file information requests based on faulty device replacement database

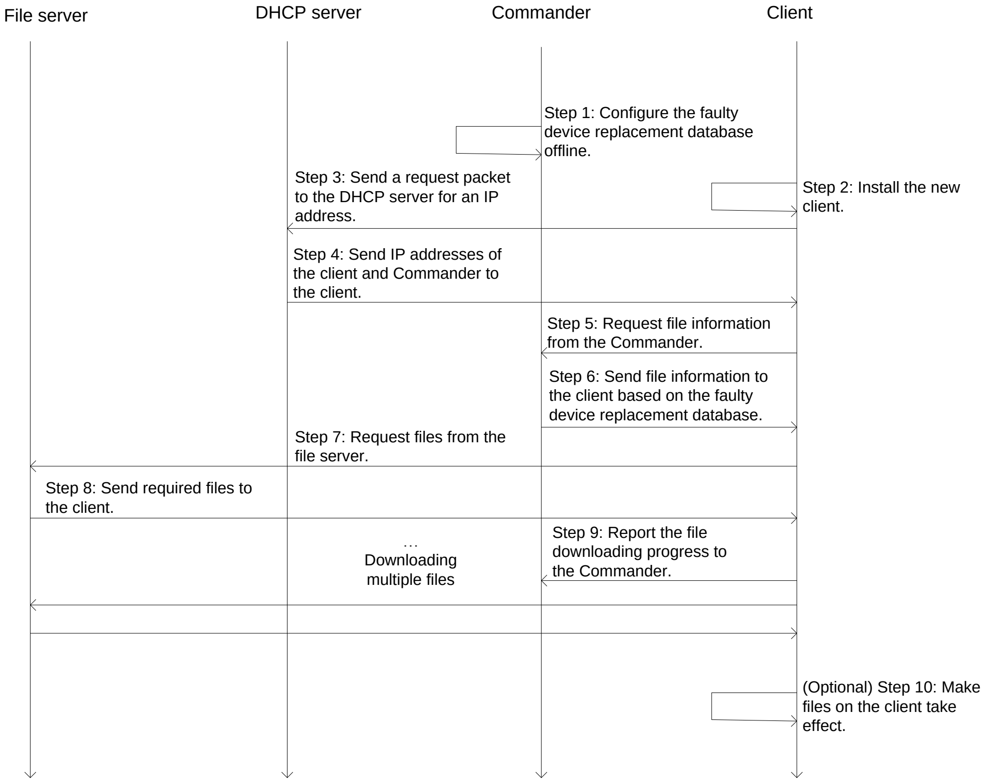
The faulty device replacement function is similar to the Zero-Touch function. The Zero-Touch function can be considered as a part of the faulty device replacement function.

After receiving an EZOP packet from a client requesting information about files to be downloaded, the Commander searches the faulty device replacement database for the information. If the information is found, the Commander sends the information to the client, and the subsequent process is the same as that in the Zero-Touch scenario. If no such information is found, the Commander searches the client database according to the Zero-Touch process.

2.5.7 Faulty Device Replacement Description

Figure 2-33 shows the faulty device replacement flowchart. For details about the faulty device replacement process, see Figure 2-31. Steps in Figure 2-33 are more detailed than those in Figure 2-31.

Figure 2-33 Faulty device replacement flowchart


File server
DHCP server
Commander
Client
Step 1: Configure the faulty device replacement database offline.
Step 2: Install the new client.
Step 3: Send a request packet to the DHCP server for an IP address.
Step 4: Send IP addresses of the client and Commander to the client.
Step 5: Request file information from the Commander.
Step 6: Send file information to the client based on the faulty device replacement database.
Step 7: Request files from the file server.
Step 8: Send required files to the client.
Step 9: Report the file downloading progress to the Commander.
…
Downloading multiple files
(Optional) Step 10: Make files on the client take effect.

Configuring the Faulty Device Replacement Database (Step 1)

For details about the faulty device replacement database, see section 2.5.5 "Commander Database."

The current version is V200R003C00. If information about the software version, patch file, web page file, and license file are configured using the CLI, the Commander sends the information and configuration file information obtained from the original faulty device database to clients. If the preceding information is not configured, the faulty device replacement database contains no such information, and new devices start with their own files except that the configuration file information is obtained from the original client database.

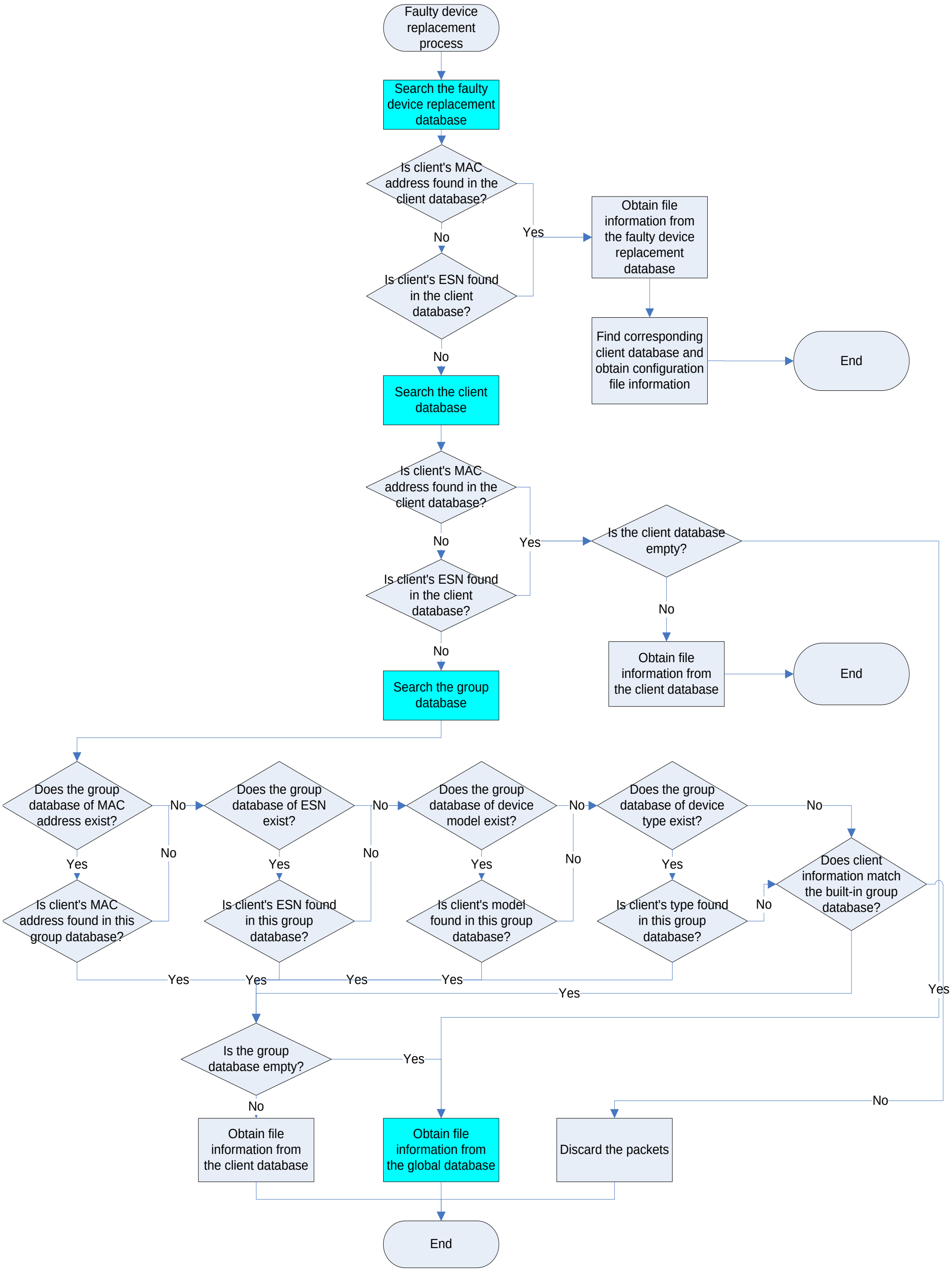
Installing New Clients and Requesting File Information (Steps 2 to 5)

Steps 2 to 5 are the same as steps 2 to 5 in the Zero-Touch scenario. For details, see section 2.2.8 "Zero-Touch Description."

Commander Sending File Information to Clients (Step 6)

After receiving DOWNLOAD_INFO_REQUEST packets from clients, the Commander searches the faulty device replacement database for file information. If no such information is found, the Zero-Touch process starts and the Commander searches the client database.

Figure 2-34 Commander searching databases


Faulty device replacement process
Search the faulty device replacement database
Is client's MAC address found in the client database?
No
Yes
Obtain file information from the faulty device replacement database
Is client's ESN found in the client database?
No
Find corresponding client database and obtain configuration file information
End
Search the client database
Is client's MAC address found in the client database?
No
Yes
Is the client database empty?
Is client's ESN found in the client database?
No
Obtain file information from the client database
End
No
Search the group database
Does the group database of MAC address exist?
No
Does the group database of ESN exist?
No
Does the group database of device model exist?
No
Does the group database of device type exist?
No
Yes
Yes
Yes
Yes
Does client information match the built-in group database?
Is client's MAC address found in this group database?
Is client's ESN found in this group database?
Is client's model found in this group database?
Is client's type found in this group database?
No
Yes
Is the group database empty?
Yes
No
Obtain file information from the client database
Obtain file information from the global database
Discard the packets
End

Subsequent Process (Steps 6 to 10)

Steps 6 to 10 in the faulty device replacement scenario are similar to steps 6 to 10 in the Zero-Touch scenario, and details are not provided here.

Note that the client database of faulty clients is deleted after new clients go online. That is, if the faulty clients are added to the network again after recovery, configure a new client database for them or execute the faulty device replacement process.

2.5.8 Application Scenario

Faulty device replacement applies to scenarios where Huawei switches have been used on enterprise networks and some switches need to be replaced due to hardware failures or misoperations.

V200R003C00 supports two faulty device replacement methods. One method is to configure information about all files except the configuration file required by new clients, so the clients can correctly download the files. Another method is that new clients download only the same configuration file as the original clients', and use other files of their own. The first method is recommended.

2.6 Configuration Backup

Configuration backup applies to constructed enterprise networks where configuration files of clients need to be backed up to a file server due to service changes.

Without EasyDeploy, network administrators must periodically back up configuration files of all devices to ensure that devices can recover from hardware failures. The workload is heavy if there are many devices.

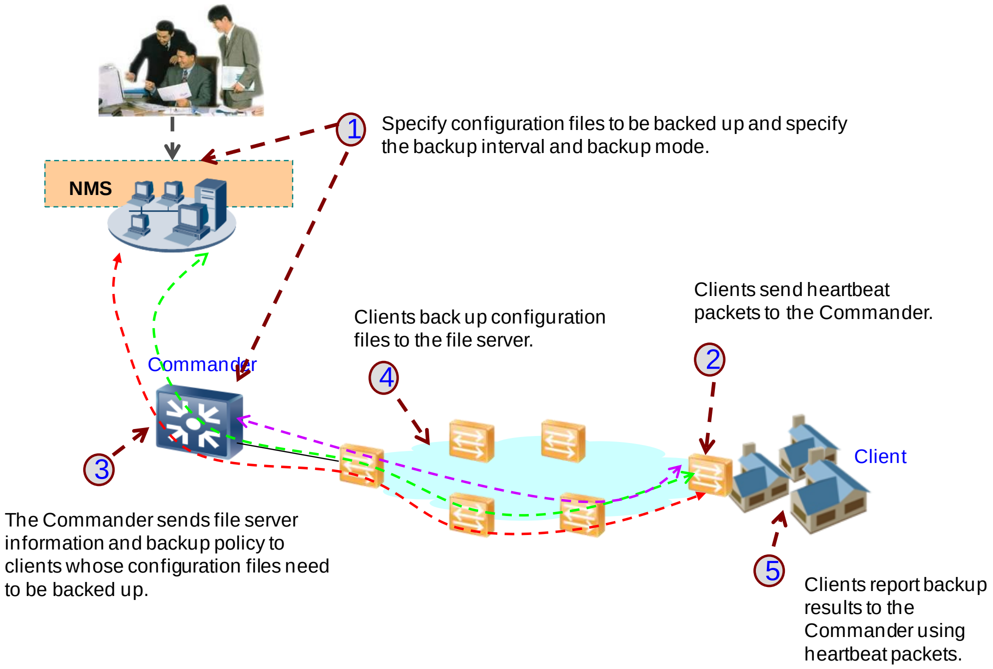
EasyDeploy provides the configuration backup function to relieve workload for network administrators. With this function, network administrators configure devices to periodically upload their configuration files to a file server using the CLI or NMS in a remote equipment room of the network center, simplifying operations and reducing workload.

2.6.1 Network Architecture

A typical network of configuration backup consists of the Commander, clients, DHCP server, NMS (optional), and file server (optional). The network is similar to the Zero-Touch network, and details are not provided here.

2.6.2 Configuration Backup Process

Figure 2-35 Configuration backup process


NMS
1
Specify configuration files to be backed up and specify the backup interval and backup mode.
Clients send heartbeat packets to the Commander.
2
Clients back up configuration files to the file server.
4
Commander
Client
3
The Commander sends file server information and backup policy to clients whose configuration files need to be backed up.
5
Clients report backup results to the Commander using heartbeat packets.

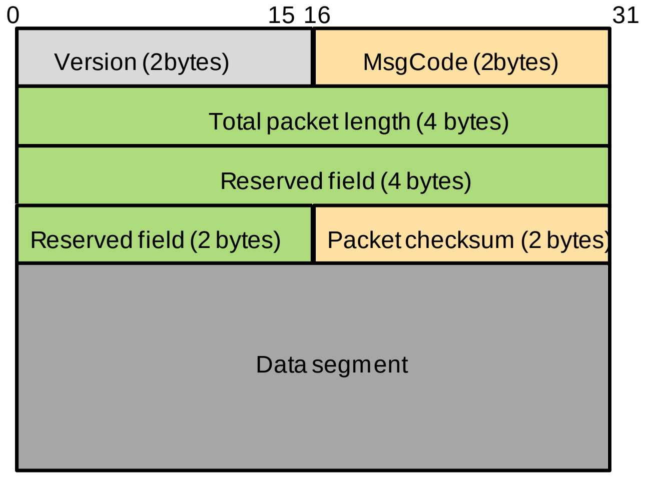
The configuration roadmap is as follows:

- **Step 1:** Network administrators specify device configuration files to be backed up and set backup parameters, including the backup interval and backup mode.
- **Step 2:** Clients that are running properly send keepalive packets to the Commander.
- **Step 3:** After receiving keepalive packets from clients, the Commander sends keepalive response packets carrying the backup interval, backup mode, and file server information to the clients if network administrators have configured the configuration backup function.
- **Step 4:** Clients back up configuration files to the file server in the specified period of time based on the configuration on the Commander.
- **Step 5:** Clients report backup results to the Commander using keepalive packets.

2.6.3 Client Working Process During Configuration Backup

During configuration backup, clients are always in normal running state, involving no status switching.

Figure 2-36 EZOP packet format



The **Version** field indicates the message version number, which is fixed at 01. This field is used to identify messages of different versions in the future. Table 2-20 lists values of the **MsgCode** field.

Table 2-20 Values of the MsgCode field

Value	Name	Description
0x0004	STATUS_INFO	Message code in the request packet that a client periodically sends to notify the Commander of the client's status. The packet is a keepalive packet and carries information about files on the client.
0x0005	STATUS_INFO _RESPONSE	Message code in the packet that the Commander sends in response to the client's request packet.

2.6.4 Commander Database

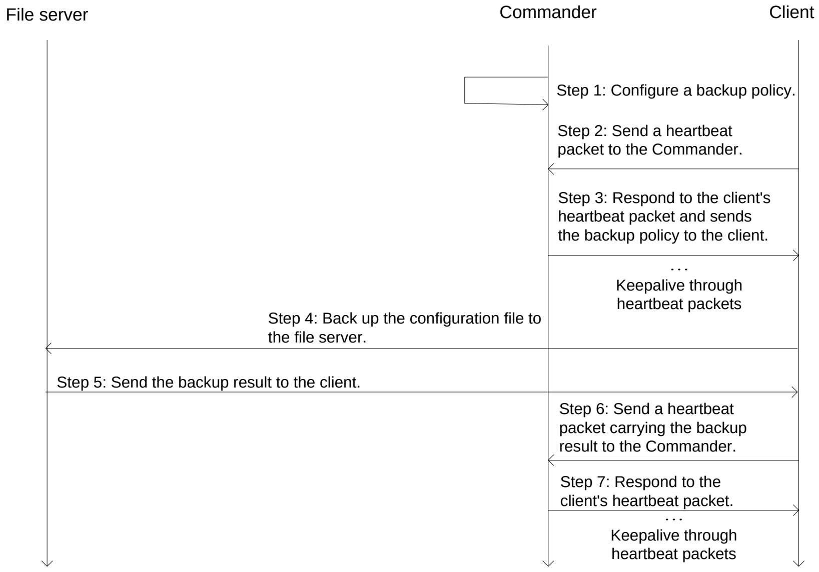
During configuration backup, the Commander mainly uses a client database.

When a client starts running properly, the client sends keepalive packets carrying the client's basic information to the Commander at an interval of 30 seconds. After receiving the packet, the Commander updates the client database.

2.6.5 Configuration Backup Description

Figure 2-37 shows the configuration backup flowchart. For details about the configuration backup process, see Figure 2-35. Steps in Figure 2-37 are more detailed than those in Figure 2-35.

Figure 2-37 Configuration backup flowchart


File server
Commander
Client
Step 1: Configure a backup policy.
Step 2: Send a heartbeat packet to the Commander.
Step 3: Respond to the client's heartbeat packet and sends the backup policy to the client.
. . .
Keepalive through heartbeat packets
Step 4: Back up the configuration file to the file server.
Step 5: Send the backup result to the client.
Step 6: Send a heartbeat packet carrying the backup result to the Commander.
Step 7: Respond to the client's heartbeat packet.
. . .
Keepalive through heartbeat packets

Configuring a Backup Policy on the Commander (Step 1)

After enabling the configuration backup function on the Commander, network administrators need to specify the interval at which clients back up configuration files to the file server and the backup mode including automatic file replacement and copy creation.

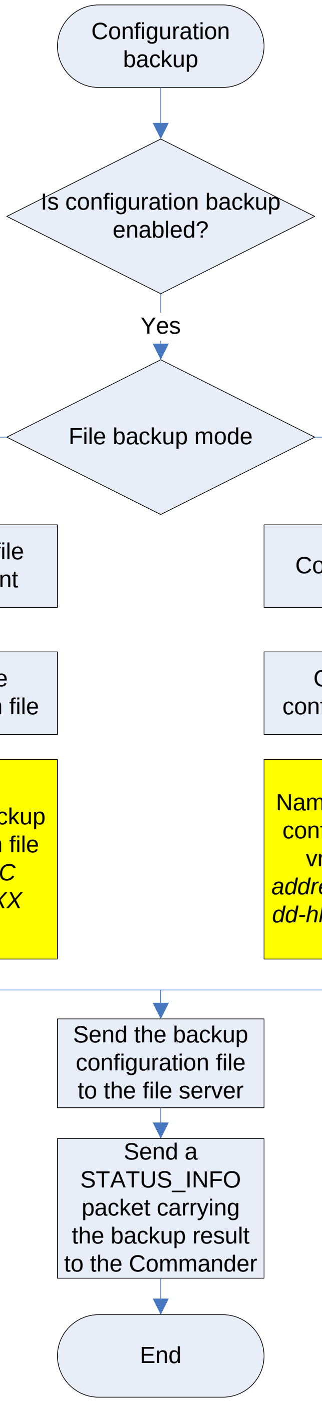
The backup command also takes effect on the Commander. Network administrators can configure the Commander to periodically back up its configuration file.

In automatic file replacement mode, each backup configuration file replaces the original configuration file on the file server, but keeps the file name unchanged.

In copy creation mode, backup configuration files on the file server have different names. The naming rule for a backup configuration file is vrpcfg-*MAC address-yyyy-mm-dd-hh-mm-ss.XXX*, in which *XXX* is the file name extension. The file name extension is the same as the startup configuration file on the device. When the startup configuration file is **vrpcfg.zip**, the naming rule is vrpcfg-*MAC address-yyyy-mm-dd-hh-mm-ss*.zip; when the startup configuration file is **vrpcfg.cfg**, the naming rule is vrpcfg-*MAC address-yyyy-mm-dd-hh-mm-ss*.cfg.

Note that only configurations in the current configuration file are backed up. The configurations that have been modified but not saved are not backed up.

Figure 2-38 Configuration backup process


Configuration backup
Is configuration backup enabled?
Yes
File backup mode
Automatic file replacement
Copy creation
Obtain the configuration file
Obtain the configuration file
Name the backup configuration file vrpcfg-*MAC address.XXX*
Name the backup configuration file vrpcfg-*MAC address-yyyy-mm-dd-hh-mm-ss.XXX*
Send the backup configuration file to the file server
Send a STATUS_INFO packet carrying the backup result to the Commander
End

Clients Sending Keepalive Packets to the Commander (Step 2)

Clients send EZOP packets (STATUS_INFO packets) to the Commander to inform the Commander of their status and basic information. The **MsgCode** field is set to **0x0004** in the STATUS_INFO packets. Figure 2-39 shows the format of a STATUS_INFO packet.

Figure 2-39 STATUS_INFO packet format

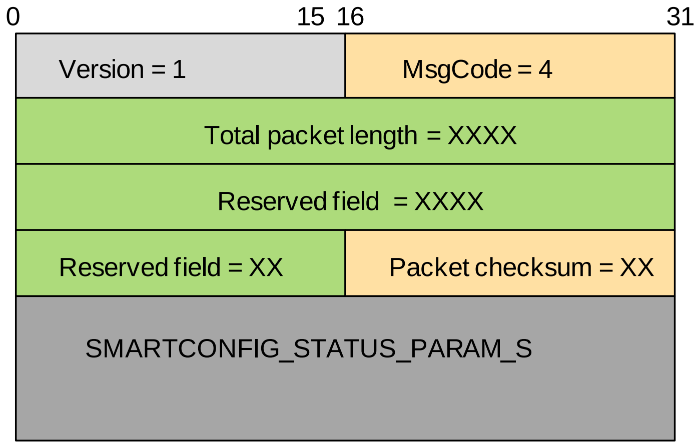


Table 2-21 lists fields in a STATUS_INFO packet.

Table 2-21 Fields in a STATUS_INFO packet

Field	Description
ulClientIpAddr	IP address of the client.
ulClientIpAddrType	Type of the IP address, including IPv4 and IPv6. The value 0 indicates an IPv4 address and 1 indicates an IPv6 address. Other values indicate an IPv4 address by default.
szClientMacAddr	MAC address of the client.
szClientModel	Device model of the client. The value must be the same as the formal model, such as S5700-28P-LI-AC.
szClientDeviceType	Device type of the client. The value must be the same as the formal type, such as S5700-LI.
szClientESN	ESN of the client.
szClientHostName	Host name of the client.
szVrpFilename szVrpFileVersion szPatFilename szWebFilename szCfgFilename szLicFilename	Names of system files and other information.
szBackupConfigName	Name of the backup configuration file.
ulBackupConfigErrReson	Cause for a configuration backup error. Table 2-22 lists the values.
szErrResonDesc	Result of backing up files to the file server. The value can

Field	Description
	be: ● Backup configuration file by sftp successfully. ● Backup configuration file by sftp failed.
szRsaPublicKey	RSA public key.

Table 2-22 lists values of the **ulBackupConfigErrReson** field.

Table 2-22 Values of the ulBackupConfigErrReson field

Value	Description
0x00	No error exists.
0x01	The configuration backup function is disabled.
0x02	The file server is unreachable.
0x03	The user name or password is incorrect.
0xFFFFFFFE	An unknown error exists.

STATUS_INFO packets have the following functions:

- Keepalive packets that a client periodically sends to the Commander. The Commander determines whether the client is always online based on the packets.
- Reporting backup information, including backup file names and backup results.

A client sends STATUS_INFO packets to the Commander at an interval of 30 seconds. If the Commander does not receive any STATUS_INFO packets from the client within 2 minutes, the Commander considers a client loss and changes the value of **usRunState** in the client database. For details about the client database, see section 2.2.6 "Commander Database."

Commander Responding to Clients' Keepalive Packets (Step 3)

After receiving STATUS_INFO packets from clients, the Commander returns STATUS_INFO_RESPONSE packets in which **MsgCode** is **0x0005** to the clients. The STATUS_INFO_RESPONSE packets are encrypted because they carry the user name and password of the file server. Figure 2-40 shows the format of a STATUS_INFO_RESPONSE packet.

Figure 2-40 STATUS_INFO_RESPONSE packet format

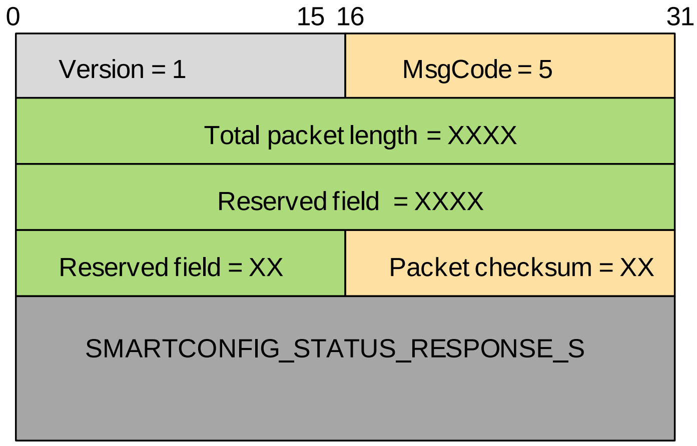


Table 2-23 Fields in a STATUS_INFO_RESPONSE packet

Field	Description
ulBackupEnableFlag	Flag of configuration file backup. The value 0 indicates non-scheduled backup and 1 indicates scheduled backup. Other values indicate non-scheduled backup.
ulBackupInterval	Interval for backing up a configuration file. The value ranges from 0 to 720, in hours. The value 0 indicates no backup. Other values indicate non-scheduled backup.
ulBackupMode	Mode in which a configuration file is backed up. The value 0 indicates automatic file replacement and 1 indicates copy creation. Other values indicate automatic file replacement.
ulBackupServerType	Type of the file server. The value 1 indicates a TFTP server, 2 indicates an FTP server, and 3 indicates an SFTP server. Other values indicate an SFTP server by default.
ulBackupServerIpAddr	IP address of the client.
ulBackupServerIpAddrType	Type of the IP address, including IPv4 and IPv6. The value 0 indicates an IPv4 address and 1 indicates an IPv6 address. Other values indicate an IPv4 address by default.
szUserName	User name for logging in to the file server.
szPassword	Password for logging in to the file server.

Clients do not sense the loss of STATUS_INFO_RESPONSE packets. That is, clients can still run properly even if they do not receive STATUS_INFO_RESPONSE packets in a long period.

Clients Backing Up Files to the File Server (Steps 4 and 5)

Clients obtain the IP address, user name, and password of the file server, backup time, and backup mode from STATUS_INFO_RESPONSE packets. Then the clients back up files to the file server, and the file server returns backup results.

Clients Reporting Backup Results to the Commander (Steps 6 and 7)

After backing up configuration files, clients send STATUS_INFO packets with backup results indicated by the **ulBackupConfigErrReson** and **szErrResonDescr** fields to the Commander. For details about the fields, see Table 2-21 and Table 2-22.

2.6.6 Application Scenario

Configuration backup applies to constructed enterprise networks where configuration files of clients need to be backed up to a file server due to service changes. Automatic configuration backup is recommended to ensure high reliability.

The recommended backup plan is as follows:

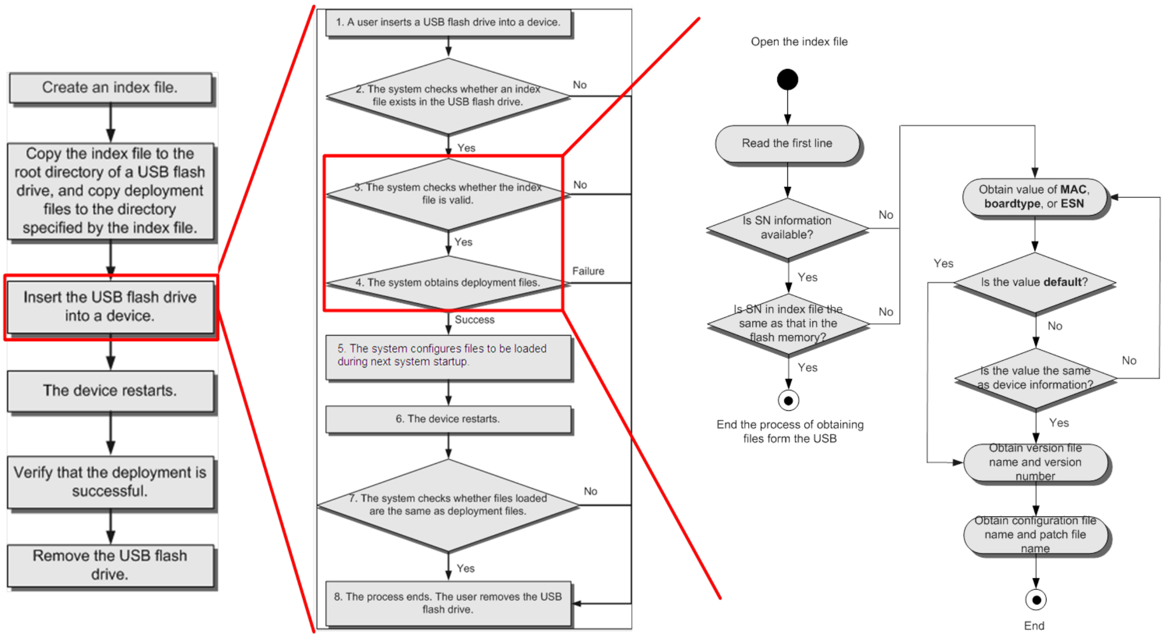
- Backup time: You are advised to back up configuration files at off-peak hours, with 0:00 to 4:00 recommended, every five days. The backup time varies according to characteristics of different enterprises.
- Backup mode: It differs based on enterprise users.
  - Enterprise users usually are not familiar with switches and rarely change switch configurations. Before changing the switch configurations, they confirm with the agent and Huawei technical support engineers to ensure high backup reliability. In this situation, automatic file replacement is recommended to reduce the load on the file server.
  - Copy creation is recommended in the scenario where a few enterprise users frequently change configuration files to conduct researches. They need to periodically clean up data on the file server.

2.7 Deployment Using a USB Flash Drive

Unlike common deployment modes, deployment using a USB flash drive implements automatic device file download and load, freeing users from using the CLI or NMS to perform manual configuration. This deployment mode is especially convenient for centrally deploying new devices in an enterprise.

Switches of earlier versions already support deployment using a flash drive. This section briefly describes this function. Figure 2-41 shows nested processes of deployment using a USB flash drive.

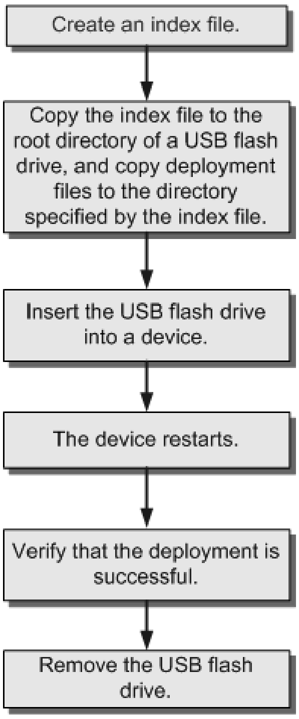
Figure 2-41 Nested processes of deployment using a USB flash drive


Create an index file.
Copy the index file to the root directory of a USB flash drive, and copy deployment files to the directory specified by the index file.
Insert the USB flash drive into a device.
The device restarts.
Verify that the deployment is successful.
Remove the USB flash drive.
1. A user inserts a USB flash drive into a device.
2. The system checks whether an index file exists in the USB flash drive.
No
Yes
3. The system checks whether the index file is valid.
No
Yes
4. The system obtains deployment files.
Failure
Success
5. The system configures files to be loaded during next system startup.
6. The device restarts.
7. The system checks whether files loaded are the same as deployment files.
No
Yes
8. The process ends. The user removes the USB flash drive.
Open the index file
Read the first line
Is SN information available?
No
Yes
Is SN in index file the same as that in the flash memory?
No
Yes
End the process of obtaining files form the USB
Obtain value of MAC, boardtype, or ESN
Yes
Is the value default?
No
Is the value the same as device information?
No
Yes
Obtain version file name and version number
Obtain configuration file name and patch file name
End

2.7.1 Overall Process

Before starting the deployment using a USB flash drive, create an index file named **usbload_config.txt**, save the index file to the root directory of the USB flash drive, and save deployment files to the directory specified in the index file. When the USB flash drive is plugged into the device, the device automatically loads the deployment files for software upgrades. Figure 2-42 shows the overall process of deployment using a USB flash drive.

Figure 2-42 Overall process of deployment using a USB flash drive


Create an index file.
Copy the index file to the root directory of a USB flash drive, and copy deployment files to the directory specified by the index file.
Insert the USB flash drive into a device.
The device restarts.
Verify that the deployment is successful.
Remove the USB flash drive.

NOTE

The index file created for deployment using a USB flash drive must be named **usbload_config.txt**.

The content of the **usbload_config.txt** file is as follows:

```
<time-sn=201105091219;/>
<usb-deployment password=huawei2012;/>
<mac=0018-8200-0001; vrpfile=; vrpver=; cfgfile=vrpcfg.cfg; webfile=; patchfile=;/>
<mac=0018-8200-0002; vrpfile=; vrpver=; cfgfile=; webfile=; patchfile=patch.pat;/>
```

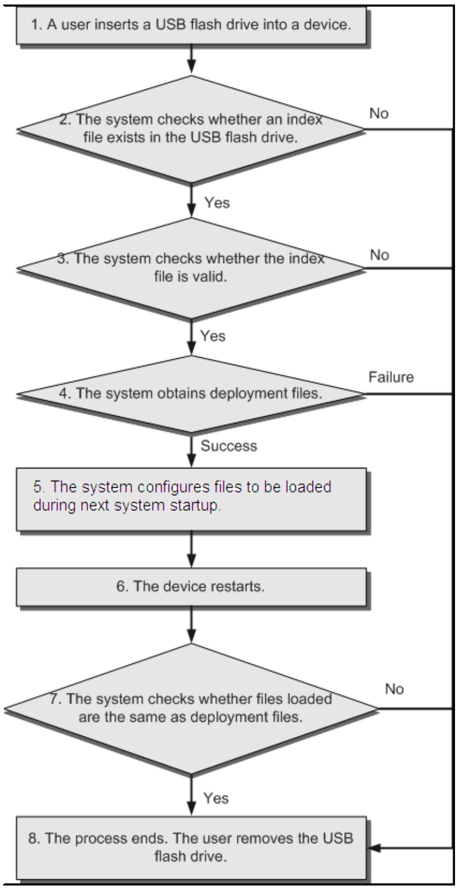
Table 2-24 describes key fields in an index file.

Table 2-24 Key fields in an index file

Field	Description
time-sn	Identification information of the index file.
usb-deployment password	Authentication password for deployment using a USB flash drive.
MAC	MAC address of the device, in the format of *XXXX-XXXX-XXXX*.
boardtype	Type of the device.
esn	ESN of the device.

2.7.2 Process of Deployment Using a USB Flash Drive

Figure 2-43 Process of deployment using a USB flash drive

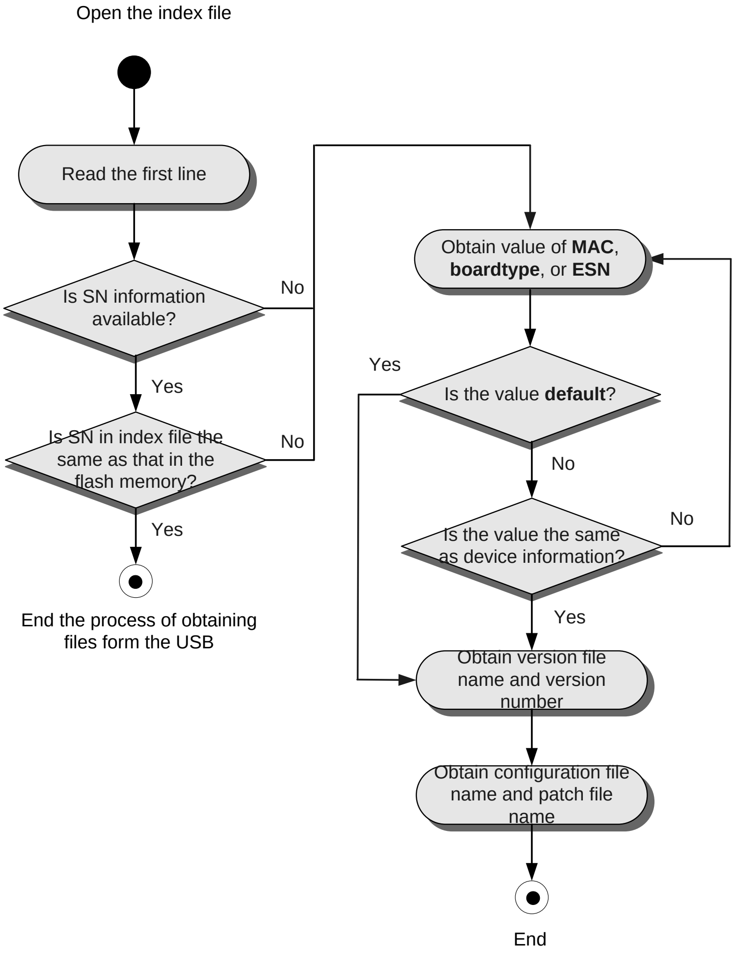

1. A user inserts a USB flash drive into a device.
2. The system checks whether an index file exists in the USB flash drive.
No
Yes
3. The system checks whether the index file is valid.
No
Yes
4. The system obtains deployment files.
Failure
Success
5. The system configures files to be loaded during next system startup.
6. The device restarts.
7. The system checks whether files loaded are the same as deployment files.
No
Yes
8. The process ends. The user removes the USB flash drive.

- **Step 2:** The device checks whether the **usbload_config.txt** file exists in the root directory of the USB flash drive. The file name must be correct; otherwise, the device considers that no index file exists.
- **Step 3:** If the index file exists, the device checks whether the index file content is in the format described in section 2.7.1 "Overall Process" to prevent bogus index files.
- **Step 4:** The device downloads deployment files from the USB flash drive based on the MAC address or ESN in the index file. If no matching file exists, the device exits the upgrade.
- **Steps 5 and 6:** When all deployment files are downloaded, the device configures the files to be loaded at next startup and restarts.
- **Step 7:** After a restart, the device checks whether the startup file names are the same as those in the USB flash drive. If so, the upgrade succeeds; if not, the upgrade fails.

2.7.3 Process of Reading the Index File

When reading the index file in the USB flash drive, Huawei switches check the file validity based on specified rules.

Figure 2-44 Process of reading the index file


Open the index file
Read the first line
Is SN information available?
No
Yes
Is SN in index file the same as that in the flash memory?
No
Yes
End the process of obtaining files form the USB
Obtain value of MAC, boardtype, or ESN
Yes
Is the value default?
No
Is the value the same as device information?
No
Yes
Obtain version file name and version number
Obtain configuration file name and patch file name
End

TimeSN Information

To prevent duplicate copies of deployment files, the first line of the index file must be **time-sn**, which is a string recording the index file generation date and time. The device also has such an SN in its flash memory. Before copying files, the device compares the value of **time-sn** in the index file with that in its flash memory. If they are the same, the device considers that the upgrade has been performed and does not copy the files. If they are different, the device starts copying the files. After copying the files, the device updates the value of **time-sn** in the flash memory to that in the index file. An index file without **time-sn** is considered invalid, and the device will stop copying the files.

Default Information

If the values of key fields including **MAC**, **boardtype**, and **esn** in the index file are all **default**, the device starts to copy files without comparing the values with information on the device. The following is an example:

```
MAC=default; vrpfile=s3328.cc; vrpver=V200R003C00; cfgfile=vrpcfg01.cfg;
```

If a field is not matched or found, the value of this field is considered empty. In the preceding example, the **patchfile** field is not found, so the device does not download any patch files.

Troubleshooting for Deployment Using a USB Flash Drive

If deployment using a USB flash drive is interrupted or fails due to an error, you can troubleshoot the fault using either of the following methods:

- View error information recorded in the **usbload_error.txt** file in the root directory of the USB flash drive. If multiple devices use the same USB flash drive for upgrades, all error information is saved to this file. The error information format is as follows:

```
===================================================
 Time        :2012-10-25 21:21:34
 MAC Address  :0200-0000-0001
 IP Address   :192.168.1.33
 Description  :
Failed to read the sn line of the file(usbload_config.txt), 'time-sn=' does not exist.
===================================================
```

  - Run debug commands to check the upgrade in real time.

3 Product Capabilities

NOTE
Information in this chapter is subject to changes without notices. To obtain product capabilities, see the specification list.

3.1 Basic Specifications

Table 3-1 Main specifications of EasyDeploy

Device Type	Functioning as a Commander	Functioning as a Client	Number of Clients Supported by the Device When Functioning as the Commander	Number of Groups Supported by the Device When Functioning as the Commander	Maximum Number of Matching Rules Supported
5700-LI	X	√	N/A	N/A	N/A
5700S-LI	X	√	N/A	N/A	N/A
5700-SI	√	√	64	256	• User-defined group: 256 • Device: 256
5700-EI	√	√	64	256	• User-defined group: 256 • Device: 256
5700-HI	√	√	128	256	• User-defined group: 256 • Device: 256
5706-LI	X	√	N/A	N/A	N/A
5710-EI	√	√	64	256	• User-defined

Device Type	Functioning as a Commander	Functioning as a Client	Number of Clients Supported by the Device When Functioning as the Commander	Number of Groups Supported by the Device When Functioning as the Commander	Maximum Number of Matching Rules Supported
					group: 256 - Device: 256
5710-HI	√	√	128	256	- User-defined group: 256 - Device: 256
6700-EI	√	√	128	256	- User-defined group: 256 - Device: 256
275x-EI	X	√	N/A	N/A	N/A
Chassis switch	√	√	255	256	- User-defined group: 256 - Device: 256

Only box switches support Auto-Config.

Only the S5700LI, S5700SI, 5710EI, S5700HI, 5710HI, and S6700EI series support deployment using a USB flash drive. Among the S5700LI series, only the S5700-28X-LI-24S-DC and S5700-28X-LI-24S-AC support deployment using a USB flash drive.

3.2 Main Restrictions

- When the clients are chassis switches, EasyDeploy can be applied only to the batch upgrade scenario.
- EasyDeploy of V200R003C00 does not support IPv6 or VPN.
- In the Zero-Touch (including the original Auto-Config scenario) or faulty device replacement scenario, if you log in to a device through the console port, the EasyDeploy process stops and the device switches to the normal running state.
- In Zero-Touch (including the original Auto-Config scenario) and faulty device replacement scenarios, only ports in the default VLAN (VLAN 1) support EasyDeploy. By default, all ports on a device belong to VLAN 1.
- Whether clients automatically delete unnecessary files from the flash memory depends on the file server type. When clients download files from a TFTP server, they cannot obtain the size of files; therefore, the clients cannot automatically delete unnecessary files from the flash memory. When clients download files from an FTP or SFTP server that does not return the size of files, the clients also cannot automatically delete unnecessary files from the flash memory.

4 Application Scenarios

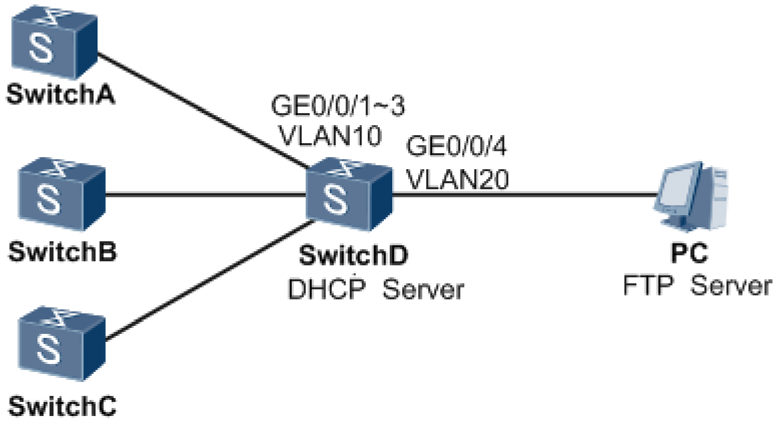
4.1 Auto-Config

Networking Requirements

As shown in Figure 4-1, in the network deployment for a residential community, the aggregation device SwitchD is connected to new Switches (such as SwitchA, SwitchB, and SwitchC) on each layer of buildings in the residential community.

Users want to load the same system software package, patch file, and configuration file on all the Switches on layers. Besides, to save manpower costs and time on deploying many Switches, the Switches must be automatically configured with the same configuration file.

Figure 4-1 Networking diagram for configuring Auto-Config for devices on the same network segment as the DHCP server



Configuration Roadmap

The configuration roadmap is as follows:

1. Directly connect the user PC to SwitchD and configure the PC as an FTP server.
2. Place the configuration file, system software package, and patch file to be loaded to the working directory of the FTP server to ensure that SwitchA, SwitchB, and SwitchC can obtain files to be loaded.

3. Configure SwitchD as the DHCP server to provide network configurations to SwitchA, SwitchB, and SwitchC. Configure information about the system software package, patch file, and configuration file in Option 67 and Option 145 because the same files are to be loaded on all the Switches.
4. Power on SwitchA, SwitchB, and SwitchC, so that the configuration file, system software package, and patch file are automatically loaded using Auto-Config.

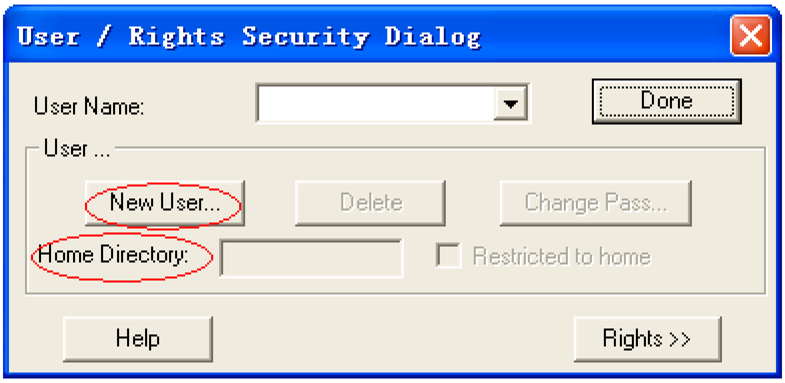
Procedure

Step 1 Configuring the FTP server

# Configure the FTP server IP address, user name, password, and working directory.

As shown in Figure 4-2, run an FTP server program on the PC, for example, wftpd32. Choose **Security** > **Users/rights**. Click **New User** in the displayed dialog box to set the user name to **user** and password to **huawei**. Enter the FTP working directory in the **Home Directory**: text box to set working directory to **D:\autoconfig**. Click **Done** to finish the setting and close the dialog box. Set the PC IP address to 192.168.1.6 and mask to 255.255.255.0.

Figure 4-2 Configuring the FTP server



Step 2 Upload system software package, configuration file, and patch file to the FTP server working directory **D:\autoconfig**. Procedures for uploading the files are not mentioned here.

Step 3 Configure the DHCP server.

```
<HUAWEI> system-view
[HUAWEI] sysname DHCP Server
[DHCP Server] dhcp enable
[DHCP Server] vlan batch 10 20
[DHCP Server] interface gigabitethernet 0/0/1
[DHCP Server-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[DHCP Server-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[DHCP Server-GigabitEthernet0/0/1] quit
[DHCP Server] interface gigabitethernet 0/0/2
[DHCP Server-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[DHCP Server-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[DHCP Server-GigabitEthernet0/0/2] quit
[DHCP Server] interface gigabitethernet 0/0/3
[DHCP Server-GigabitEthernet0/0/3] port hybrid pvid vlan 10
[DHCP Server-GigabitEthernet0/0/3] port hybrid untagged vlan 10
[DHCP Server-GigabitEthernet0/0/3] quit
```

```
[DHCP Server] interface gigabitethernet 0/0/4
[DHCP Server-GigabitEthernet0/0/4] port hybrid pvid vlan 20
[DHCP Server-GigabitEthernet0/0/4] port hybrid untagged vlan 20
[DHCP Server-GigabitEthernet0/0/4] quit
[DHCP Server] interface vlanif 10
[DHCP Server-Vlanif10] ip address 192.168.2.6 255.255.255.0
[DHCP Server-Vlanif10] dhcp select global
[DHCP Server-Vlanif10] quit
[DHCP Server] interface vlanif 20
[DHCP Server-Vlanif20] ip address 192.168.1.1 255.255.255.0
[DHCP Server-Vlanif20] quit
[DHCP Server] ip pool auto-config
[DHCP Server-ip-pool-auto-config] network 192.168.2.0 mask 255.255.255.0
[DHCP Server-ip-pool-auto-config] gateway-list 192.168.2.6
[DHCP Server-ip-pool-auto-config] option 67 ascii s_V200R002C00.cfg
[DHCP Server-ip-pool-auto-config] option 141 ascii user
[DHCP Server-ip-pool-auto-config] option 142 ascii huawei
[DHCP Server-ip-pool-auto-config] option 143 ip-address 192.168.1.6
[DHCP Server-ip-pool-auto-config] option 145 ascii
vrpfile=s_V200R002C00.cc;vrpver=V200R002C00;patchfile=s_V200R002C00.pat;
[DHCP Server-ip-pool-auto-config] quit
```

Step 4 Power on SwitchA, SwitchB, and SwitchC, and run the Auto-Config process.

Step 5 Verify the configuration.

# After Auto-Config is finished, log in to the Switches to be configured and run the **display startup** command to view the system software package, configuration file, and patch file for the startup of the Switch. SwitchA is used as an example.

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:      flash:/s_V200R002C00.cc
  Startup system software:               flash:/s_V200R002C00.cc
  Next startup system software:           flash:/s_V200R002C00.cc
  Startup saved-configuration file:        flash:/s_V200R002C00.cfg
  Next startup saved-configuration file:    flash:/s_V200R002C00.cfg
  Startup paf file:                     NULL
  Next startup paf file:                 NULL
  Startup license file:                  NULL
  Next startup license file:              NULL
  Startup patch package:                 flash:/s_V200R002C00.pat
  Next startup patch package:             flash:/s_V200R002C00.pat
```

Configuration Files

Configuration file of the DHCP server

```
#
 sysname DHCP Server
#
vlan batch 10 20
#
 dhcp enable
#
ip pool auto-config
 gateway-list 192.168.2.6
 network 192.168.2.0 mask 255.255.255.0
 option 67 ascii s_V200R002C00.cfg
 option 141 ascii user
 option 142 ascii huawei
 option 143 ip-address 192.168.1.6
 option 145 ascii
vrpfile=s_V200R002C00.cc;vrpver=V200R002C00;patchfile=s_V200R002C00.pat;
#
interface Vlanif10
 ip address 192.168.2.6 255.255.255.0
 dhcp select global
#
interface Vlanfi20
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
return
```

4.2 Zero-Touch

Networking Requirements

On the enterprise network shown in Figure 4-3, Switch1 and Switch2 have reachable routes to each other. The IP address of VLANIF 20 corresponding to GE0/0/1 on Switch1 is 192.168.10.90, and that corresponding to GE0/0/3 on Switch2 is 192.168.10.80. The IP address of VLANIF 10 corresponding to GE0/0/1 and GE0/0/2 on Switch2 is 192.168.1.6, and the IP address of the file server is 192.168.10.100.

New devices Client1, Client2, and Client3 need to be deployed on the enterprise network. The new clients and the DHCP server are in different network segments. To reduce labor costs and save time on device deployment, the enterprise wants to implement unified automatic batch configuration and maintenance of the new devices.

Figure 4-3 Application scenario of Zero-Touch

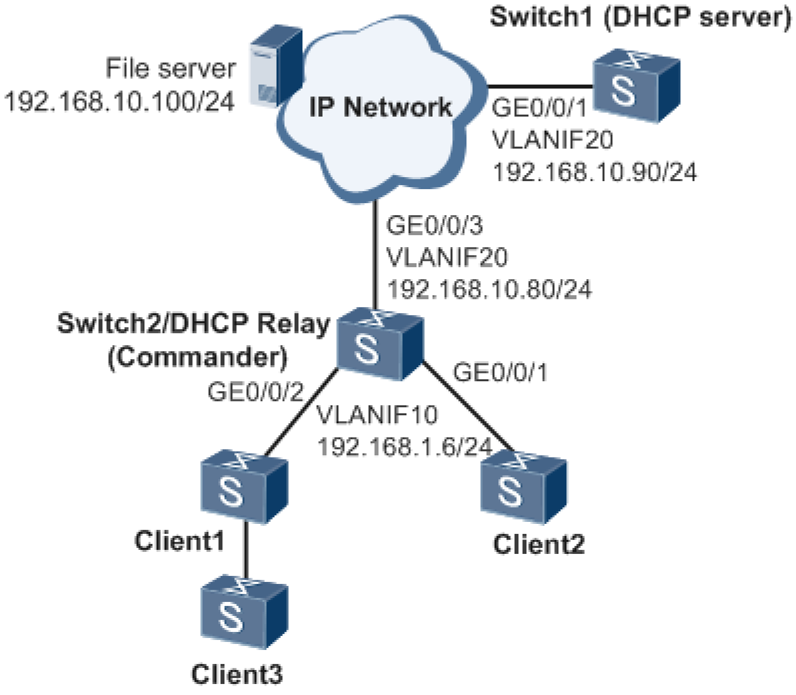


Table 4-1 describes new devices to be configured.

Table 4-1 New devices to be configured

New Device	Device Type	Files to Be Loaded
Client1	S5700-HI	• s5700-hi.cfg • User-defined file: header1.txt
Client2	S5700-HI	• s5700-hi.cfg • User-defined file: header1.txt
Client3	S5700-SI	• s5700-si.cfg • User-defined file: header2.txt

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure Switch1 as the DHCP server and Switch2 as the DHCP relay agent so that the new clients can automatically obtain IP addresses of their own and the Commander.
2. Configure the file server and save files to be loaded on the file server.
3. Configure Switch2 as the Commander to implement Zero-Touch through the Commander.
   - Configure basic functions of the Commander. Enable automatic configuration backup on the Commander to facilitate replacement of faulty devices in future maintenance.

  - Client1 and Client2 are devices of the same type and need to load the same configuration file. Therefore, you can configure a group based the device type of the two devices. Client3 needs to load a different configuration file. You can specify file information exclusively for Client3 or configure a group based on its device type. To specify file information exclusively for Client3, obtain the MAC address or ESN of Client3 first.
4. Start the Zero-Touch process.

Procedure

Step 1 Configure the DHCP service.

# Configure Switch1 as the DHCP server.

```
<HUAWEI> system-view
[HUAWEI] sysname DHCP Server
[DHCP Server] dhcp enable
[DHCP Server] interface vlanif 20
[DHCP Server-Vlanif20] dhcp select global
[DHCP Server-Vlanif20] quit
[DHCP Server] ip pool easy-operation
[DHCP Server-ip-pool-easy-operation] network 192.168.1.0 mask 255.255.255.0
[DHCP Server-ip-pool-easy-operation] gateway-list 192.168.1.6
[DHCP Server-ip-pool-easy-operation] option 148 ascii ipaddr=192.168.1.6;
[DHCP Server-ip-pool-easy-operation] quit
```

# Configure a static route on Switch1.

```
[DHCP Server] ip route-static 192.168.1.0 255.255.255.0 192.168.10.80
```

# Configure Switch2 (the Commander) as a DHCP relay agent.

```
<HUAWEI> system-view
[HUAWEI] sysname Commander
[Commander] dhcp enable
[Commander] interface gigabitethernet 0/0/1
[Commander-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[Commander-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[Commander-GigabitEthernet0/0/1] quit
[Commander] interface gigabitethernet 0/0/2
[Commander-GigabitEthernet0/0/2] port hybrid pvid vlan 10
[Commander-GigabitEthernet0/0/2] port hybrid untagged vlan 10
[Commander-GigabitEthernet0/0/2] quit
[Commander] interface vlanif 10
[Commander-Vlanif10] dhcp select relay
[Commander-Vlanif10] dhcp relay server-ip 192.168.10.90
[Commander-Vlanif10] quit
```

Step 2 Configure the file server.

Configure the file server according to the server manual. Ensure that the file server has reachable routes to the Commander and clients. After completing the configuration, save required files on the file server.

Step 3 Configure basic functions of the Commander.

```
[Commander] easy-operation commander ip-address 192.168.1.6
[Commander] easy-operation commander enable
```

```
[Commander] easy-operation
[Commander-easyoperation] sftp-server 192.168.10.100 username admin password
easyoperation
[Commander-easyoperation] backup configuration interval 2
```

Step 4 Configure information about files to be downloaded.

# On the Commander, configure a built-in group based on the device type of Client1 and Client2, and specify file information in the group.

```
[Commander-easyoperation] group build-in S5700-HI
[Commander-easyoperation-group-build-in-S5700-HI] configuration-file s5700-hi.cfg
[Commander-easyoperation-group-build-in-S5700-HI] custom-file header1.txt
[Commander-easyoperation-group-build-in-S5700-HI] quit
```

# Specify file information for Client3.

```
[Commander-easyoperation] client 3 mac-address 5489-9875-edff
[Commander-easyoperation] client 3 configuration-file s5700-si.cfg custom-file
header2.txt
[Commander-easyoperation] quit
```

Step 5 Verify the configuration.

# Check the global configuration on the Commander.

```
[Commander] display easy-operation configuration
---------------------------------------------------------------------------
 Role          : Commander
 Commander IP address        : 192.168.1.6
 Commander UDP port           : 60000
 IP address of file server     : 192.168.10.100
 Type of file server           : SFTP
 Username of file server        : admin
 Default system-software file   : -
 Default system-software version: -
 Default configuration file    : -
 Default patch file            : -
 Default Web page file             : -
 Default license file         : -
 Default custom file 1        : -
 Default custom file 2        : -
 Default custom file 3        : -
 Auto clear up : Disable
 Auto join in  : Disable
 Activating file time          : Immediately
 Activating file method        : Default
 Backup configuration file mode : Default
 Backup configuration file interval(hours): 2
---------------------------------------------------------------------------
```

Step 6 Power on the new clients to start the Zero-Touch process.

You can run the **display easy-operation download-status** command to check the file downloading progress on the clients.

```
[Commander] display easy-operation download-status
The total number of client in downloading files is : 3
```

```
-----------------------------------------------------------------------------
  ID    Mac address    IP address     Method     Phase        Status
-----------------------------------------------------------------------------
  1     00E0-FC12-A34B 192.168.1.254   zero-touch  Config-file  UPGRADING
  2     00E0-FC34-3190 192.168.1.253   zero-touch  Config-file  UPGRADING
  3     5489-9875-edff 192.168.1.252   zero-touch  Config-file  UPGRADING
```

----End

Configuration Files

# Configuration file of Switch1

```
#
 sysname DHCP Server
#
vlan 20
#
 dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 148 ascii ipaddr=192.168.1.6;
#
interface Vlanif20
 ip address 192.168.10.90 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
ip route-static 192.168.1.0 255.255.255.0 192.168.10.80
#
return
```

# Configuration file of Switch2

```
#
 sysname Commander
#
vlan batch 10
#
 dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.10.90
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
```

```
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
easy-operation commander ip-address 192.168.1.6
easy-operation commander enable
#
easy-operation
 sftp-server 192.168.10.100 username admin password %$%$"lcYC3a9)~67^c$uM%5ZQ>Uc%$%$
 backup configuration interval 2
 client 3 mac-address 5489-9875-EDFF
 client 3 configuration-file s5700-si.cfg
 client 3 custom-file header2.txt
 group build-in S5700-HI
  configuration-file s5700-hi.cfg
  custom-file header1.txt
#
return
```

4.3 Faulty Device Replacement

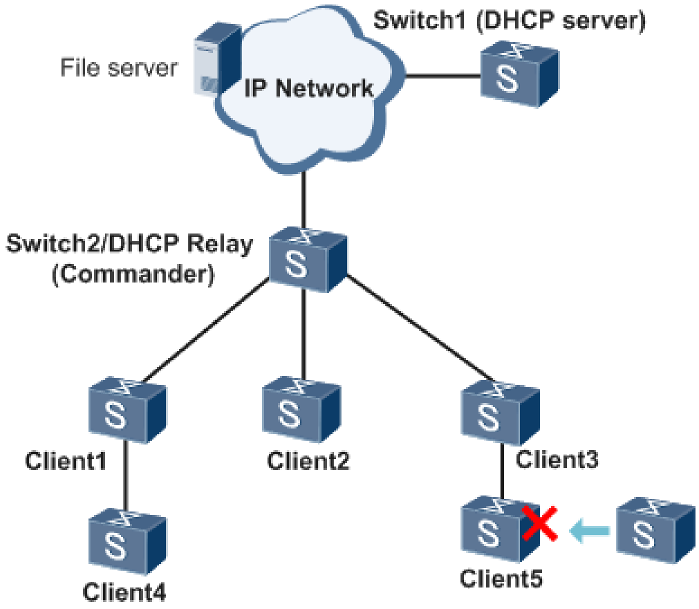
Networking Requirements

The enterprise network shown in Figure 4-4 supports the Easy-Operation function. Switch1, Switch2, and the file server have reachable routes to each other. Switch1 functions as the DHCP server, and Switch2 functions as a DHCP relay agent and Commander.

Client5 on the network fails, and services of users connected to Client5 are interrupted. To resume services for users, Client5 must be replaced by a new client. The new client needs to take over services of Client5 quickly to minimize impact of the fault.

The MAC address of the new client is 0200-0000-0000, and the new client needs to download the web page file **web_1.web.7z**.

Figure 4-4 Application scenario of faulty device replacement



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure faulty device replacement information on Switch2 so that the new client can obtain the backup configuration file of the faulty client.
2. Start the faulty device replacement process.

Procedure

Step 1 Configure faulty device replacement information on Switch2.

```
<HUAWEI> system-view
[HUAWEI] sysname Commander
[Commander] easy-operation
[Commander-easyoperation] client 5 replace mac-address 0200-0000-0000
[Commander-easyoperation] client 5 replace web-file web_1.web.7z
```

Step 2 Verify the configuration.

```
[Commander] display easy-operation client replace
The total number of replacement information is :  1

-----------------------------------------------------------
  ID     Replaced Mac    Replaced Esn
-----------------------------------------------------------
  5      0200-0000-0000   -
-----------------------------------------------------------
```

Install and power on the new client to start the faulty device replacement process. You can run the **display easy-operation client 5** command to check the status of the new client.

```
[Commander] display easy-operation client 5

-------------------------------------------------------------------------------
 ID   Mac address    ESN                         IP address       State
-------------------------------------------------------------------------------
 5    0200-0000-0000 2102353173107C800132        192.168.1.254    UPGRADING
-------------------------------------------------------------------------------
```

You can also run the **display easy-operation download-status** command to check the file downloading progress on the new client.

```
[Commander] display easy-operation download-status
The total number of client in downloading files is : 1

-------------------------------------------------------------------------------
 ID  Mac address     IP address         Method      Phase       Status
-------------------------------------------------------------------------------
 5   0200-0000-0000   192.168.1.254       Zero-touch   Web-file    UPGRADING
```

----End

Configuration Files

# Configuration file of Switch1

```
#
 sysname DHCP Server
#
vlan batch 20
#
 dhcp enable
#
ip pool easy-operation
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 148 ascii ipaddr=192.168.1.6;
#
interface Vlanif20
 ip address 192.168.10.90 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

# Configuration file of Switch2

```
#
 sysname Commander
#
vlan batch 10
#
 dhcp enable
#
interface Vlanif10
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.10.90
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
easy-operation commander ip-address 192.168.1.6
easy-operation commander enable
#
easy-operation
 sftp-server 192.168.10.100 username admin password %$%$"lcYC3a9)~67^c$uM%5ZQ>Uc%$%$
 backup configuration interval 2
 client 3 replace mac-address 0200-0000-0000
 client 3 replace web-file web_1.web.7z
#
```

```
return
```

4.4 Batch Upgrade

Networking Requirements

On the enterprise network shown in Figure 4-5, Client1 to Client6 in office buildings have reachable routes to the switch and file server. The IP address of the switch is 172.31.20.10/24, and that of the file server is 172.31.1.90. To reduce labor costs and facilitate subsequent upgrades and maintenance, the enterprise wants the clients to automatically obtain required files for batch upgrades.

Figure 4-5 Application scenario of a batch upgrade

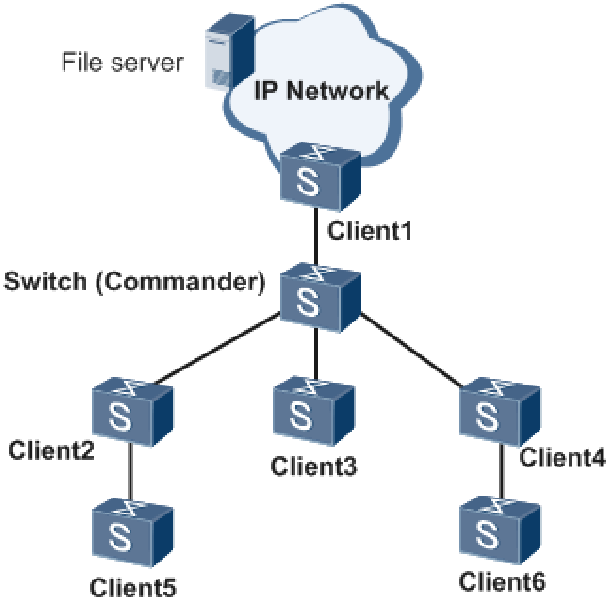


Table 4-2 describes information about Client1 to Client6 and files to be loaded. If you do not know information about the clients, check client information on the Commander after completing Step 4.

Table 4-2 Information about clients and files to be loaded

Client	Device Type	MAC Address	IP Address	Files to Be Loaded
Client1	S7700	N/A	172.31.20.100/24	• s7700.cc (V200R003C00) • license.dat • User-defined file: header1.txt
Client2	S5700-HI	N/A	N/A	s5700-hi.cc (V200R003C00)

Client	Device Type	MAC Address	IP Address	Files to Be Loaded
Client3	S5700-HI	N/A	N/A	s5700-hi.cc (V200R003C00)
Client4	S5700-EI	N/A	172.31.10.10/24	s5700-ei.cc (V200R003C00)
Client5	S5700-HI	N/A	N/A	s5700-hi.cc (V200R003C00)
Client6	S5700-SI	5489-9875-ea12	N/A	• web_1.web.7z • User-defined file: header.txt

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the file server and save files to be loaded on the file server.
2. Specify the switch IP address on the clients.
3. Configure the switch as the Commander to implement a batch upgrade through the Commander.
   - Configure basic functions of the Commander.
   - Configure groups for the clients based on the device type and specify files to be loaded in the groups.
   - Enable automatic configuration backup on the Commander to facilitate replacement of faulty devices in future maintenance.
4. Start the batch upgrade process.

Procedure

Step 1 Configure the file server.

Configure the file server according to the server manual. After completing the configuration, save required files on the file server.

Step 2 Specify the Commander IP address on the clients.

# Specify the Commander IP address on Client1.

```
<HUAWEI> system-view
[HUAWEI] easy-operation commander ip-address 172.31.20.10
```

Specify the Commander IP address on Client2 to Client6 in the same way.

Step 3 Configure basic functions of the Commander.

```
<HUAWEI> system-view
[HUAWEI] sysname Commander
[Commander] easy-operation commander ip-address 172.31.20.10
[Commander] easy-operation commander enable
[Commander] easy-operation
```

```
[Commander-easyoperation] sftp-server 172.31.1.90 username admin password
easyoperation
[Commander-easyoperation] backup configuration interval 2
```

Step 4 Configure clients to automatically join the management domain of the Commander.

```
[Commander-easyoperation] client auto-join enable
```

NOTE

After enabling the auto-join function, you can view information about the clients and files to be loaded on the Commander using the **display easy-operation client** command.

Step 5 Specify file information and the file activation mode on the Commander.

# Configure a group for Client1 based on the IP address, and specify the files to be loaded and file activation mode in the group.

```
[Commander-easyoperation] group custom ip-address g1
[Commander-easyoperation-group-custom-g1] match ip-address 172.31.20.100 24
[Commander-easyoperation-group-custom-g1] system-software s7700.cc V200R003C00
[Commander-easyoperation-group-custom-g1] license license.dat
[Commander-easyoperation-group-custom-g1] custom-file header1.txt
[Commander-easyoperation-group-custom-g1] activate-file in 02:00
```

# Configure a group for Client2, Client3, and Client5 based on the device type, and specify the files to be loaded and file activation mode in the group.

```
[Commander-easyoperation] group build-in s5700-hi
[Commander-easyoperation-group-build-in-S5700-HI] system-software s5700-hi.cc
V200R003C00
[Commander-easyoperation-group-build-in-S5700-HI] activate-file reload
[Commander-easyoperation-group-build-in-S5700-HI] activate-file in 02:00
```

# Configure a group for Client4 based on the IP address, and specify the files to be loaded and file activation mode in the group.

```
[Commander-easyoperation] group custom ip-address g2
[Commander-easyoperation-group-custom-g2] match ip-address 172.31.10.10 24
[Commander-easyoperation-group-custom-g2] system-software s5700-ei.cc V200R003C00
[Commander-easyoperation-group-custom-g2] activate-file reload
[Commander-easyoperation-group-custom-g2] activate-file in 02:00
```

# Configure a group for Client6 based on the MAC address. Specify the files to be loaded and set the file activation mode to the default mode in the group.

```
[Commander-easyoperation] group custom mac-address g3
[Commander-easyoperation-group-custom-g3] match mac-address 5489-9875-ea12
[Commander-easyoperation-group-custom-g3] web-file web_1.web.7z
[Commander-easyoperation-group-custom-g3] custom-file header.txt
[Commander-easyoperation-group-custom-g3] quit
[Commander-easyoperation] quit
```

Step 6 Verify the configuration.

# Check the global configuration on the Commander.

```
[Commander] display easy-operation configuration
---------------------------------------------------------------------------
 Role                           : Commander
 Commander IP address          : 172.31.20.10
 Commander UDP port             : 60000
 IP address of file server       : 172.31.1.90
 Type of file server             : SFTP
 Username of file server         : admin
 Default system-software file    : -
 Default system-software version: -
 Default configuration file      : -
 Default patch file              : -
 Default Web page file                : -
 Default license file            : -
 Default custom file 1           : -
 Default custom file 2           : -
 Default custom file 3           : -
 Auto clear up                   : Disable
 Auto join in                    : Enable
 Activating file time           : Immediately
 Activating file method          : Default
 Backup configuration file mode : Default
 Backup configuration file interval(hours): 2
----------------------------------------------------------------------------
```

# Check configuration of all groups on the Commander.

```
[Commander] display easy-operation group
The total number of group configured is : 4
The number of build-in group is         : 1
The number of custom group is           : 3

-------------------------------------------------------
 Groupname                   Type    MatchType
-------------------------------------------------------
 S5700-HI                    build-in device-type
 g1                         custom   ip-address
 g2                         custom   ip-address
 g3                         custom   mac-address
-------------------------------------------------------
```

# Check configuration of the group named **g1** on the Commander.

```
[Commander] display easy-operation group custom g1
----------------------------------------------------------------------------
 Group name              : g1
 Configuration file       : -
 System-software file     : s7700.cc
 Patch file              : -
 Web page file               : -
 License file            : license.dat
 Customs file 1           : header1.txt
 Customs file 2           : -
 Customs file 3           : -
 Activating file time     : In 02:00
 Activating file method    : Default
 Ip-address list          :
  Ip-address       Ip-mask
  172.31.1.100     255.255.255.0
----------------------------------------------------------------------------
```

Step 7 Start the batch upgrade process.

```
[Commander] easy-operation
[Commander-easyoperation] upgrade group
Warning: This command will start the upgrade processing of all groups. Continue?
[Y/N]:y
```

You can run the **display easy-operation download-status** command to check the file downloading progress on the clients.

```
[Commander] display easy-operation download-status
The total number of client in downloading files is : 6

----------------------------------------------------------------------------
  ID    Mac address    IP address     Method     Phase       Status
----------------------------------------------------------------------------
  1     0011-2233-4455 172.31.20.100   upgrade    Sys-file     UPGRADING
  2     00E0-FC34-3190 172.31.10.15   upgrade    Sys-file     UPGRADING
  3     0011-2233-4457 172.31.10.20   upgrade    Sys-file     UPGRADING
  4     70F3-950B-1A52 172.31.10.10   upgrade    Sys-file     UPGRADING
  5     0011-2233-4459 172.31.10.18   upgrade    Sys-file     UPGRADING
  6     5489-9875-ea12 172.31.10.11   upgrade    Web-file     UPGRADING
```

----End

Configuration Files

# Configuration file of the switch

```
#
 sysname Commander
#
easy-operation commander ip-address 172.31.20.10
easy-operation commander enable
#
easy-operation
 client auto-join enable
 sftp-server 172.31.1.90 username admin password %$%$"lcYC3a9)~67^c$uM%5ZQ>Uc%$%$
 backup configuration interval 2
 group build-in S5700-HI
  system-software s5700-hi.cc V200R003C00
  activate-file in 02:00
 group custom ip-address g1
  system-software S7700.cc V200R003C00
  license license.dat
  custom-file header1.txt
  activate-file in 02:00
  match ip-address 172.31.1.100 255.255.255.0
 group custom ip-address g2
  activate-file reload
  match ip-address 172.31.10.10 255.255.255.0
 group custom mac-address g3
  web-file web_1.web.7z
  custom-file header.txt
  match mac-address 5489-9875-EA12 FFFF-FFFF-FFFF
#
return
```

Configuration file of Client1 to Client6

```
#
easy-operation commander ip-address 172.31.20.10
#
return
```