H3C SecPath UTM Series-CMW520-F5123P34 Release Notes

Contents

List of Tables

This document describes the features, restrictions and guidelines, open problems, and workarounds for version F5123P34. Before you use this version in a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Version information

Version number

List the version number with the command display version.

For example:

H3C SecPath U200-S Comware Software, Version 5.20, Feature 5123P34

H3C SecPath U200-A Comware Software, Version 5.20, Feature 5123P34

Note: You can see the version number with the command display version in any view. Please see Note①.

Version history

Table 1 Version history

Version number	Last version	Release date	Release type	Remarks
F5123P34	F5123P33	2016-11-28	Release version	Fixes bugs
F5123P33	F5123P32	2016-1-28	Release version	CVE-2015-1788/ CVE-2015-3195
F5123P32	F5123P31	2015-8-20	Release version	CVE-2015-0287
F5123P31	F5123P30	2015-4-16	Release version	CVE-2014-3571/CVE-2014-9295
F5123P30	F5123P29	2015-1-22	Release version	CVE-2014-3566
F5123P29	F5123P27	2014-11-26	Release version	Fixes bugs
F5123P27	F5123P24	2014-7-8	Release version	Fixes bugs
F5123P24	F5123P22	2013-09-25	Release version	Fixes bugs
F5123P22	F5123P19	2013-06-19	Release version	Fixes bugs
F5123P19	F5123P18	2013-02-04	Release version	Fixes bugs
F5123P18	F5123P15	2013-01-18	Release version	Fixes bugs

Version number	Last version	Release date	Release type	Remarks
F5123P15	F5123P11	2012-5-16	Release version	Fixes bugs
F5123P11	F5123P10	2011-11-25	Release version	Fixes bugs
F5123P10	F5123P08	2011-10-28	Release version	Fixes bugs
F5123P08	F5123P07	2011-7-22	Release version	Fixes bugs
F5123P07	F5118	2011-5-12	Release version	Fixes bugs
F5118	R5116P04	2009-9-7	Release version	Fixes bugs
R5116P04	R5116	2009-9-7	Release version	Fixes bugs
R5116P02	R5116	2009-9-7	Release version	Fixes bugs
R5116	E5114	2009-8-13	Release version	Fixes bugs
E5114	First Release	2009-6-13	Release version	Fixes bugs

Hardware and software compatibility matrix

CAUTION:

To avoid an upgrade failure, use Table 2 to verify the hardware and software compatibility before performing an upgrade.

Table 2 Hardware and software compatibility matrix

Item	Specifications	
Product family	SecPath U200-A	SecPath U200-S
Minimum memory requirements	1024M	512M
Minimum Flash requirements	32M	
Host software	SECPATH200UA-CMW520-F5123P34.bin SECPATH200US-CMW520-F5123P34.bin	
iMC version	iMC PLAT 7.2 (E0403P04) iMC EIA 7.2 (E0402) iMC IVM 7.2 (E0402) iMC UBA 7.2 (E0401)	
iNode version	iNode PC 7.2 (E0401)	

Item	Specifications
Remarks	

Display the system software and Boot ROM versions of the SecPath series:

```
<Sysname>dis version
H3C Comware Platform Software
Comware Software, Version 5.20, Feature 5123P34----------Note①
Copyright (c) 2004-2011 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C SecPath U200-A uptime is 0 week, 0 day, 8 hours, 47 minutes
 CPU type: RMI XLS208 750MHz CPU
 1024M bytes DDR2 SDRAM Memory
 32M bytes Flash Memory
 PCB             Version:Ver.A
 Logic           Version:  3.0
 Basic  BootWare  Version:  1.35
 Extend BootWare  Version:  1.35
 [FIXED PORT] CON       (Hardware)Ver.A, (Driver)1.0,    (Cpld)1.0
 [FIXED PORT] GE0/0     (Hardware)Ver.A, (Driver)1.0,    (Cpld)1.0
 [FIXED PORT] GE0/1     (Hardware)Ver.A, (Driver)1.0,    (Cpld)1.0
 [FIXED PORT] GE0/2     (Hardware)Ver.A, (Driver)1.0,    (Cpld)1.0
 [FIXED PORT] GE0/3     (Hardware)Ver.A, (Driver)1.0,    (Cpld)1.0
 [FIXED PORT] GE0/4     (Hardware)Ver.A, (Driver)1.0,    (Cpld)1.0
 [FIXED PORT] GE0/5     (Hardware)Ver.A, (Driver)1.0,    (Cpld)1.0
 [SUBSLOT  1] The SubCard is not present
 [SUBSLOT  2] The SubCard is not present
```

Upgrading restrictions and guidelines

None

Hardware feature updates

None

Software feature and command updates

For more information about the software feature and command update history, see F5123P34 *Release Notes (Software Feature Changes)*.

MIB updates

Table 3 MIB updates

Version number	Item	MIB file	Module	Description
F5123P34	New			None

Version number	Item	MIB file	Module	Description
	Modified			None
F5123P33	New			None
	Modified			None
F5123P29	New			None
	Modified			None
F5123P27	New			None
	Modified			None
F5123P24	New			None
	Modified			None
F5123P22	New			None
	Modified			None
F5123P19	New			None
	Modified			None
F5123P18	New			None
	Modified			None
F5123P15	New			None
	Modified			None
F5123P11	New			None
	Modified			None
F5123P10	New			None
	Modified			None
F5123P08	New			None
	Modified			None
F5123P07	New			None
	Modified			None
F5118	New			None
	Modified			None
R5116P04	New			None
	Modified			None
R5116P02	New			None
	Modified			None
R5116	New			None
	Modified			None
E5114	New			None
	Modified			None

Operation changes

None

Open problems and workarounds

Problem 1(HSD110295)

- Symptom: The interfaceGigabitEthernet0/4and 0/5 each can only support 3 groups of VRRP.
- Condition: When more VRRP groups need to be used.
- Workaround: If there are more than 3 groups of VRRP needed choose other interface.

List of Resolved Problems

Resolved Problems in F5123P34

Problem ID (201606010065)

- Symptom: The iMC did not respond to the ICMP message.
- Condition: Do same set operation for the nodes of ipForwarding and ipDefaultTTL.

Problem ID (201610180402)

- Symptom: CVE-2016-1409
- Condition: The Neighbor Discovery (ND) protocol implementation in the IPv6 stack in Cisco IOS XE 2.1 through 3.17S, IOS XR 2.0.0 through 5.3.2, and NX-OS allows remote at tackers to cause a denial of service (packet-processing outage) via crafted ND mess ages, aka Bug ID CSCuz66542, as exploited in the wild in May 2016.

Resolved Problems in F5123P33

Problem ID (201508040100)

- Symptom:CVE-2015-1788
- Condition: When processing an ECParameters structure OpenSSL enters an infinite loop. This can be used to perform denial of service against any system which processes public keys, certificate requests or certificates.

Problem ID (201512280257)

- Symptom: CVE-2015-3195
- Condition: When presented with a malformed X509_ATTRIBUTE structure OpenSSL will leak memory. This structure is used by the PKCS#7 and CMS routines so any application which reads PKCS#7 or CMS data from untrusted sources is affected.

Resolved Problems in F5123P32

Problem ID (201505070251)

- Symptoms: CVE-2015-0287
- Condition: Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write. Applications that parse structures containing CHOICE or ANY DEFINED BY components may be affected.

Resolved Problems in F5123P31

Problem ID (201501050340)

- Symptom: CVE-2014-9295
- Condition: Stack-based buffer overflows in ntpd in NTP before 4.2.8 allows remote attackers to execute arbitrary code via a crafted packet.

Problem ID(201502050080)

- Symptom: CVE-2014-3571
- Condition: A carefully crafted DTLS message can cause a segmentation fault in OpenSSL due to a NULL pointer dereference. This could lead to a Denial Of Service attack.

Resolved Problems in F5123P30

Problem ID (201410230582)

- Symptom: SSL 3.0 Fallback protection
- Condition: OpenSSL has added support for TLS_FALLBACK_SCSV to allow applications to block the ability for a MITM attacker to force a protocol downgrade. Some client applications (such as browsers) will reconnect using a downgraded protocol to work around interoperability bugs in older servers. This could be exploited by an active man-in-the-middle to downgrade connections to SSL 3.0 even if both sides of the connection support higher protocols. SSL 3.0 contains a number of weaknesses including POODLE (CVE-2014-3566).

Resolved Problems in F5123P29

Problem ID (201409050466)

- Symptom: CVE-2014-3508
- Condition: A flaw in OBJ_obj2txt may cause pretty printing functions such as X509_name_oneline, X509_name_print_ex et al. to leak some information from the stack. Applications may be affected if they echo pretty printing output to the attacker.

Problem ID (201407250564)

- Symptom: CVE-2008-5161
- Description: Error handling in the SSH protocol in several SSH servers/clients, including OpenSSH 4.7p1 and possibly other versions, when using Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data.

Resolved Problems in F5123P27

Problem ID(201407020278)

- Symptom:CVE-2014-0224
- Condition:When Open SSL Server or Client is used.

Resolved Problems in F5123P24

Problem ID (201308210139)

- Symptom: Using the Nessus test tool can find that the firewall has an SSL security vulnerability that reduces negotiated key strength.
- Condition: This symptom can be seen using the Nessus test tool and SSL VPN should be enabled.

Problem ID(201307310145)

- Symptom: URL filter was not functioning and IPS/AV advanced control stopped working.
- Condition: Functionality of URL Classified Filter had been running for a long time before the symptom occurred.

Resolved Problems in F5123P22

Problem ID(HSD113441)

- Symptom: If URL filtering has been enabled for a long time, the device unexpectedly reboots.
- Condition: This symptom might be seen if URL filtering has been enabled for a long time.

Problem ID(HSD113385)

- Symptom: Upon receiving a DHCP packet in which the length of Option 82 is incorrect, the device unexpectedly reboots.
- Condition: This symptom occurs if the device receives a DHCP packet in which the length of Option 82 is incorrect.

Problem ID (HSD106217)

- Symptom: If the userlog function has been enabled for a long time, the device unexpectedly reboots.
- Condition: This symptom occurs after the userlog function has been enabled for a long time.

Problem ID(HSD113735)

- Symptom: After the signature databases are updated, the IPS and AV modules might fail to work.
- Condition: This symptom might occur after the signature databases are updated.

Problem ID(HSD111388)

- Symptom: When the device operates in UTM mode, upgrading the software through Web fails.

- Condition: This symptom occurs if you upgrade the software through Web when the device operates in UTM mode.

Problem ID(HSD113426)

- Symptom: After the configuration file is saved and then the device is rebooted, the undo alg h323 command gets lost.
- Condition: This symptom occurs after you save the configuration file and then reboot the device.

Problem ID(HSD112889)

- Symptom: After the flash is formatted and then the F5123P19 version is upgraded, upgrading the signature databases for IPS and AV fails.
- Condition: This symptom occurs if you upgrade the signature databases for IPS and AV after you format the flash and then upgrade the software to F5123P19

Resolved Problems in F5123P19

Problem ID(HSD111389)

- Symptom: when enabling category-based URL filtering, the device showed “Service is being set”.
- Condition: after the device registered successfully, the device can’t connect to the server for a long time.

Problem ID(HSD111508)

- Symptom: URL’s task abnormally exited.
- Condition: when a URL address received by device was longer than 1024 bytes.

Resolved Problems in F5123P18

Problem ID(HSD108882)

- Symptom: When access the hh3cUserPassword node of hh3cUserInfoTable by SNMP, the device return the user's password.
- Condition: Access the hh3cUserPassword node of hh3cUserInfoTable by SNMP.

Resolved Problems in F5123P15

Problem 1 (HSD104519)

- First found-in version: SECPATH200US-CMW520-F5123P11
- Condition: long-time visiting HTTP while opening the URL filtering function on the device.
- Description: The URL filtering function is disabled/not available.

Problem 2 (HSD104069)

- First found-in version: SECPATH200US-CMW520-F5123P11
- Condition: plug two 4GE Optical cards in each of the two slots on U200-A.
- Description: The last interface of the 4GE card of the second slot cannot up physically.

Problem 3 (HSD103564)

- First found-in version: SECPATH200US-CMW520-F5123P11
- Condition: Open the flow log function of session log on the device.
- Description: While UTM configuring strategies like IPS, AV, bandwidth management, content monitor/control, the device will corrupt.

Resolved Problems in F5123P11

Problem 1

- First found-in version: F5123P10
- Condition: Configure the configuration content audit and application control functions on a U200-A device, and then inject 10M HTTP/SMTP/P2P traffic to the device.
- Description: The U200-A corrupt.

Resolved Problems in F5123P10

Problem 1

- First found-in version: F5123P08
- Condition: The UTM device can work as a NAT gateway to allow conference devices to access conference servers on external networks.
- Description: UTM cannot translate H323 addresses to support normal communication.

Resolved Problems in F5123P08

Problem 1

- First found-in version: R5116
- Condition: Configure IPSec on the U200A as the IPSec center device and configure NAT on another device at the egress. Packets for IKE negotiation pass the NAT device. Then, a branch device initiates IKE negotiation.
- Description: IPSec communication fails.

Resolved Problems in F5123P07

Noney

Resolved Problems in F5118

Problem 1

- First found-in version: R5116
- Condition: Configure the U200-S block the BT application software.
- Description: the system can not identify the encrypted BT application correctly.

Resolved Problems in R5116P04

Problem 1

- First found-in version: R5116
- Condition: Power down the U200 device and then power up for 20 times.
- Description: The system corrupt for some times.

Resolved Problems in R5116P02

Problem 1

- First found-in version: E5114
- Condition: Configure the U200 URL filter.
- Description: the system corrupt.

Resolved Problems in R5116

Problem 1

- First found-in version: E5114
- Condition: Configure the U200 snmp.
- Description: None of U200 snmp trap can be sent.

Problem 2

- First found-in version: R1627
- Condition: Configure the U200 interface 4 or 5 as HA interface, get high throughput.
- Description: the system corrupt and reboot.

Resolved Problems in E5114

First Version

Related documentation

Documentation set

- H3C UTM License Registration and Activation Guide-5PW100
- H3C SecPath UTM Products User Manual(F5123)-5PW100
- H3C SecPath U200-A_U200-M_U200-S Unified Threat Management Products Installation Guide-6PW106
- H3C SecPath U200-CA_U200-CM_U200-CS New Generation Multi-Functional Firewalls Installation Guide-6PW106

Obtaining documentation

Take the following steps to get related documents from the H3C website at www.h3c.com.

1. Go to http://www.h3c.com/portal/Technical_Documents.
2. Choose the desired product category and model.

Technical support

service@h3c.com

http://www.h3c.com

Appendix A Feature list

Hardware features

Table 4 UTM200 series hardware features

Item	U200-A	U200S
Dimensions (H × W × D)	44.2×442×400mm	43.6×300×260mm
Weight	5.9KG	2.2KG
Interface	1*Console	
	6*10/100/1000M ETH	5*10/100M ETH
Interface module	2*slot 2GBE/4GEF	1*slot 2GBE/4GEF/WLAN
Flash	32MB	32MB
SDRAM	Default 1GB	Default 512M
Power(AC)	100-240V a.c., 50/60Hz, 1.6A	100-240V a.c., 50/60Hz, 1.5A
Temperature	0 to 40 ℃	
Humidity	10 to 95%	

Software features

Table 5 Software features of the UTM 200 series

Category		Features
Network Security	AAA	RADIUS HWTACACS CHAP validate PAP validate radius domain Authentication
	Firewall	Packet Filter ACL ASPF DoS/DDoS (Land, Smurf, Fraggle, WinNuke, Ping of Death, Tear Drop, IP Spoofing, SYN Flood, ICMP Flood, UDP Flood, ARP Flood etc.) Static and Dynamic Black List MAC and IP Address Binding ARP Reverse Query ARP Cheat Check

Category		Features
	Mail/Web Filter	Mail Filter
		SMTP Mail Address Fileter
		SMTP Mail Title Filter
		SMTP Mail Content Filter
		SMTP Mail Attachment Filter
		Support SQL/Java Applet/ActiveX Filter
		Web Filter
		HTTPURL Filter
		HTTP Content Filter
	Security Management	DoS/DDoS Log
		Black List Log
		Address Binding Log
		Flow Alarm Log
		Flow Statistic and Analysis
	Data Security	IPSec
		IKE
	NAT	Address Pool NAT
		ACL NAT
		Easy IP
		NAT Server
		NAT Static
		Some ALGs, include FTP, H323, DNS etc.
VPN	L2TP VPN	LNS
		LAC
	IPSec/IKE	AH/ESP/AH-ESP
		SA
		ESP Support DES/3DES/AES
		MD5/SHA-1
		Aggressive/Main exchange-mode
		NAT through
	GRE VPN	
	DVPN	
Network Connection	LAN Protocol	Ethernet_II
		Ethernet_SNAP
		VLAN
	Link Protocol	PPP
		PPPoE
IPS	Target network attack types	Worms, viruses, Trojan horses, backdoor programs, DoS/DDoS attacks, probing/scanning, spyware, Phishings, attacks exploiting vulnerabilities, SQL injection attacks, Buffer overflow attacks, protocol abnormities, and IDS/IPS bypass attacks

Category		Features
	Response actions	Block, limit, TCP Reset, capture original packets, redirect, quarantine, record logs locally, send Email alarms, and report to syslog
	Signature database	Unique integrated signature database, which combines the attack signature database, and protocol signature database Supporting both automatic upgrade and manual upgrade
AV	Target network Virus types	Backdoor Constructor DoS Email-Worm Exploit IM-Flooder IM-Worm IRC-Worm Net-Worm P2P-Worm Packed Rootkit SMS-Flooder SpamTool StringFrom Trojan Trojan-Clicker Trojan-DDoS Trojan-Downloader Trojan-Dropper Trojan-Proxy Trojan-PSW Trojan-Spy Virus Worm AdWare Dialer Downloader FraudTool BadJoke Hoax
	Response actions	Block, TCP Reset, capture original packets, redirect, quarantine, record logs locally, send Email alarms, and report to syslog
	Signature database	Supporting both automatic upgrade and manual upgrade

Appendix B Upgrading software

This chapter describes how to upgrade software while the device is operating normally or when the device cannot correctly start up.

Software upgrade overview

Upgrading software includes upgrading the BootWare image, system software images, and configuration files.

The default storage medium of the device depends on the software version. The examples in this chapter use the Flash as the default storage medium.

BootWare images

Each time the device is powered on, it runs the BootWare image to initialize hardware and locates and loads the system software image.

The BootWare image comprises a basic section and an extended section:

- The basic section is the minimum code that bootstraps the system.
- The extended section performs hardware initialization and provides system management menus. You can use the menus to load system software and the startup configuration file.

The basic section is executed at first. Then, you can load the extended section on the menu.

The BootWare image is saved in a file with the extension btw, such as main.btw.

System software images

System software images are used at device startup. The U200-CA supports three types of system software images:

- Main system software image—Used by default.
- Backup system software image—Used when the main system software image is invalid.
- Secure system software image—Used when the backup system software image is invalid. If the secure system software image is also invalid, the switch displays a failure prompt.

A system software image is a .bin file such as main.bin.

Configuration file

A configuration file saves the configuration you make on the device. You can save the running configuration to a configuration file so the configuration takes effect after the device reboots and you can view the configuration anytime. You can also back up the configuration file to a server and download the file to other devices to configure devices in bulk.

Upgrade methods

To upgrade the system software image, use one of the following methods:

Upgrade method	Remarks
Upgrading the system software image at the CLI	You must reboot the device to make the new image take effect. Rebooting the device interrupts ongoing network services.
Upgrading the system software image in the Web interface	To upgrade the system software image in the Web interface, you do not need to enable the FTP or TFTP server function on the file server.
Upgrading the system software image from BootWare menu	Use this method when the device cannot correctly start up.

To upgrade the BootWare image, use either of the following methods:

Upgrade method	Remarks
Upgrading the BootWare image at the CLI	Whichever method is used, you must reboot the device to make the new image take effect. Rebooting the device interrupts ongoing network services.
Upgrading the BootWare image from BootWare menu	

NOTE:

The upgrade methods for the H3C SecPath U200 series devices are the same. The following example was created and verified on the U200-CA, and the command outputs in this document are for reference only.

Preparing for the upgrade

IMPORTANT:

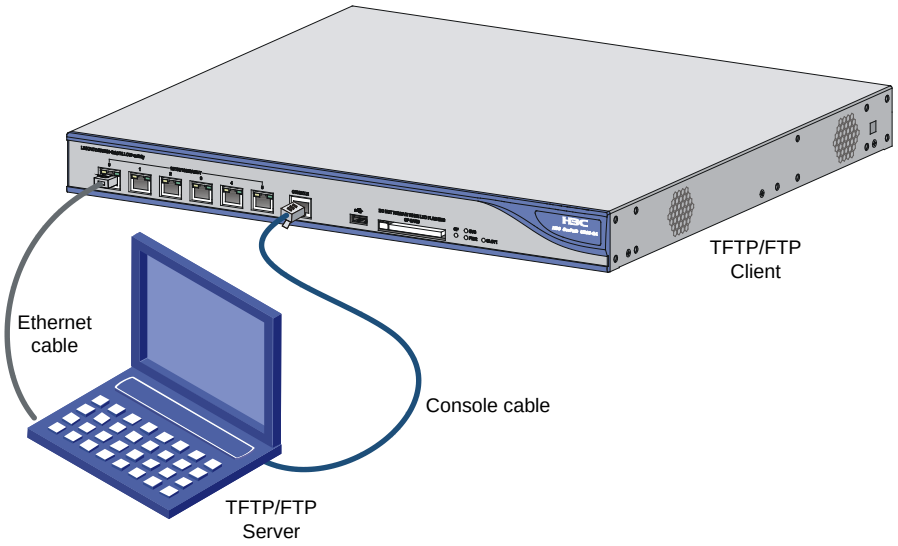
Configuration files of different versions may not be compatible. The upgrade can cause the configuration in the configured files invalid. For information about configuration file compatibility, see the release notes.

Before you upgrade system software, complete the following tasks:

- Prepare the TFTP or FTP server software by yourself. The devices are not shipped with the software.
- Set up the upgrade environment as shown in Figure 1.
- Run a TFTP or FTP server on the file server. (Skip this task if you upgrade the system software from Web.)
- The U200-CA can function as the TFTP client, FTP client, or FTP server. In the following examples that use FTP, the U200-CA functions as the FTP client.
- Assign an IP address to the file server to make sure that the U200-CA and the file server can reach each other.
- Log in to the CLI of the U200-CA through the console port. (Skip this task if you upgrade the system software in the Web interface.)

- Copy the upgrade file to the file server and correctly set the working directory on the TFTP or FTP server.

Figure 1 Setting up the upgrade environment



Upgrading the system software image

This chapter describes only how to upgrade the main system software image. The procedures for upgrading the other types of system software images are similar.

Upgrading the system software image at the CLI

You can use the TFTP or FTP commands on the U200-CA to access the TFTP or FTP server to back up or download files.

The Flash is 32 M and can save only one system software image file. Use one of the methods to upgrade the software:

- Method 1—Use a new image file to overwrite the one in the Flash. The new image file must have the same name as the one in the Flash.
- Method 2—Delete the existing system software image file from the Flash and download the new image file. Before deleting the file, make sure the Flash has sufficient space for the new image file.

This section describes method 2 to upgrade the system software.

Using TFTP for the upgrade

This section describes how to upgrade system software by using TFTP.

1. Back up the running system software image and configuration files
   a. Perform the save command in any view to save the current configuration.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
```

```
 Validating file. Please wait....
 Configuration is saved to device successfully.
<Sysname>
```

b. Perform the dir command in user view to identify the system software image and configuration file names and verify that the Flash has sufficient space for the new system software image.

```
<Sysname> dir
Directory of flash:/

   0     -rw-       891  May 08 2012 07:45:49   default_ca.cer
   1     -rw-      1411  May 08 2012 07:45:50   default_local.cer
   2     -rw-      1159  May 31 2012 16:54:43   startup.cfg
   3     -rw-     10260  May 31 2012 16:54:38   system.xml
   4     -rw-  30617340  May 31 2012 16:55:41   main.bin

30353 KB total (433 KB free)

<Sysname>
```

This example uses the default system software image file name main.bin and the default configuration file names startup.cfg and system.xml. The startup.cfg file saves configuration that can be made in CLI and Web. The system.xml file saves configuration that can be made only in Web.

c. Perform the tftp put command in user view to upload the main.bin file to the TFTP server.

```
<Sysname> tftp 192.168.0.2 put main.bin

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... /
  TFTP: 30617340 bytes sent in 38 second(s).
  File uploaded successfully.

<Sysname>
```

d. Perform the tftp put command in user view to upload the startup.cfg file and system.xml file to the TFTP server.

```
<Sysname> tftp 192.168.0.2 put startup.cfg

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... \
  TFTP:     1159 bytes sent in 0 second(s).
  File uploaded successfully.
<Sysname> tftp 192.168.0.2 put system.xml

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... |
  TFTP:    10260 bytes sent in 0 second(s).
  File uploaded successfully.

<Sysname>
```

2. Upgrade the system software image:

This configuration example was created and verified on Feature 5123P17 for the system software image file u200-ca.bin.

a. Delete the existing main image file from the Flash.

```
<Sysname>delete /unreserved flash:/main.bin
The contents cannot be restored!!! Delete flash:/main.bin?[Y/N]:y
Deleting a file permanently will take a long time. Please wait...
.....................................................................
.....................................................................
.....................................................................
%Delete file flash:/main.bin...Done.
<Sysname>
```

b. Perform the tftp get command in user view to download the system software image file, for example, u200-ca.bin, to the Flash on the device.

```
<Sysname> tftp 192.168.0.2 get u200-ca.bin

  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...\
  TFTP: 30617340 bytes received in 89 second(s)
  File downloaded successfully.

<Sysname>
```

c. Perform the boot-loader command in user view to load the file u200-ca.bin and specify the file as the main image file at the next reboot.

```
<Sysname> boot-loader file u200-ca.bin main
  This command will set the boot file. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on
slot 0!
<Sysname>
```

d. Perform the display boot-loader command in user view to verify that the file has been loaded.

```
<Sysname> display boot-loader
 Failed to get the boot file used this time!
 The boot file used next time:flash:/u200-ca.bin attribute: main
 Failed to get the backup boot file used next time!
 Failed to get the secure boot file used next time!
<Sysname>
```

e. Perform the reboot command in user view to reboot the device.

```
<Sysname> reboot
 tart to check configuration with next startup configuration file, please wait.
........DONE!
 This command will reboot the device. Continue? [Y/N]:y
#Jun  1 11:50:00:690 2012 Sysname DEVM/1/REBOOT:
 Reboot device by command.

%Jun  1 11:50:00:691 2012 Sysname DEVM/5/SYSTEM_REBOOT: System is rebooting now.
System start booting...
…
```

f. After the reboot is complete, perform the display version command to verify that the system software image is correct.

```
<Sysname> display version
H3C Comware Platform Software
Comware Software, Version 5.20, Feature 5123P17
Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C SecPath U200-CA uptime is 0 week, 0 day, 1 hour, 23 minutes

 CPU type: XXX
 1024M bytes DDR2 SDRAM Memory
 32M bytes Flash Memory
 495M bytes CF0 Card
 PCB             Version:Ver.A
 Logic           Version:  3.0
 Basic  BootWare  Version:  1.34
 Extend BootWare  Version:  1.34
 [FIXED PORT] CON       (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
 [FIXED PORT] GE0/0     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
 [FIXED PORT] GE0/1     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
 [FIXED PORT] GE0/2     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
 [FIXED PORT] GE0/3     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
 [FIXED PORT] GE0/4     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
 [FIXED PORT] GE0/5     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
 [SUBCARD  1] The SubCard is not present

<Sysname>
```

Using FTP for the upgrade

This section describes how to upgrade the system software image by using FTP.

1. Back up the running system software image and configuration files:
   a. Perform the save command in any view to save the current configuration.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait....
 Configuration is saved to device successfully.
<Sysname>
```

   b. Perform the dir command in user view to identify the system software image and configuration file names and verify that the Flash has sufficient space for the new system software image.

```
<Sysname> dir
Directory of flash:/

   0     -rw-       891  May 08 2012 07:45:49   default_ca.cer
   1     -rw-      1411  May 08 2012 07:45:50   default_local.cer
   2     -rw-      1159  May 31 2012 17:16:03   startup.cfg
   3     -rw-     10260  May 31 2012 17:15:58   system.xml
```

```
   4     -rw-  30617340  May 31 2012 16:55:41   main.bin

30353 KB total (433 KB free)

<Sysname>
```

This example uses the default system software image file name main.bin and the default configuration file names startup.cfg and system.xml.

c. Perform the ftp command in user view to access the FTP server.

```
<Sysname> ftp 192.168.0.2
Trying 192.168.0.2 ...
Press CTRL+K to abort
Connected to 192.168.0.2.
220 3Com 3CDaemon FTP Server Version 2.0
User(192.168.0.2:(none)):user123
331 User name ok, need password
Password:
230 User logged in
```

d. Perform the put command in FTP client view to upload the main.bin file to the FTP server.

```
[ftp] put main.bin
227 Entering passive mode (192,168,0,2,26,0)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 306173406 byte(s) sent in 14.605 second(s), 1355.00Kbyte(s)/sec.

[ftp]
```

e. Perform the put command in FTP client view to upload the startup.cfg file and the system.xml file to the FTP server.

```
[ftp] put startup.cfg
227 Entering passive mode (192,168,0,2,26,3)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 1159 byte(s) sent in 0.187 second(s), 6.00Kbyte(s)/sec.

[ftp] put system.xml
227 Entering passive mode (192,168,0,2,26,6)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 10260 byte(s) sent in 0.203 second(s), 50.00Kbyte(s)/sec.

[ftp]
```

2. Upgrade the system software image:

This configuration example was created and verified on Release 3166P13 for the system software image file u200-ca.bin.

a. Perform the get command in FTP client view to download the system software image file main.bin to the Flash on the device.

```
[ftp] get main.bin
flash:/main.bin has been existing. Overwrite it? [Y/N]:y
```

```
227 Entering passive mode (192,168,0,201,8,13)
125 Using existing data connection
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.........226 Closing data connection; File transfer successful.
FTP: 30617340 byte(s) received in 437.634 second(s), 69.00K byte(s)/sec.

[ftp]
```

b. Perform the quit command in FTP client view to return to user view.

```
[ftp] quit
221 Service closing control connection

<Sysname>
```

c. Perform the boot-loader command in user view to load the file main.bin and specify the file as the main image file at the next reboot.

```
<Sysname> boot-loader file main.bin main
  This command will set the boot file. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot
0!
<Sysname>
```

d. Perform the display boot-loader command in user view to verify that the file has been loaded.

```
<Sysname> display boot-loader
 The boot file used this time:flash:/main.bin attribute: main
 The boot file used next time:flash:/main.bin attribute: main
 Failed to get the backup boot file used next time!
 Failed to get the secure boot file used next time!
<Sysname>
```

e. Perform the reboot command in user view to reboot the device.

```
<Sysname> reboot
 Start to check configuration with next startup configuration file, please wait.
........DONE!
 This command will reboot the device. Continue? [Y/N]:y
System start booting...
…
```

f. After the reboot is complete, perform the display version command to verify that the system software image is correct.

```
<Sysname> display version
H3C Comware Platform Software
Comware Software, Version 5.20, Feature 5123P17
Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C SecPath U200-CA uptime is 0 week, 0 day, 0 hour, 15 minutes

 CPU type: XXX
 1024M bytes DDR2 SDRAM Memory
 32M bytes Flash Memory
```

```
495M bytes CF0 Card
PCB             Version:Ver.A
Logic           Version:  3.0
Basic  BootWare  Version:  1.34
Extend BootWare  Version:  1.34
[FIXED PORT] CON       (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
[FIXED PORT] GE0/0     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
[FIXED PORT] GE0/1     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
[FIXED PORT] GE0/2     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
[FIXED PORT] GE0/3     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
[FIXED PORT] GE0/4     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
[FIXED PORT] GE0/5     (Hardware)Ver.A, (Driver)1.0,    (Cpld)3.0
[SUBCARD  1] The SubCard is not present

<Sysname>
```

Upgrading the system software image in the Web interface

CAUTION:

Do not perform any operation in the Web when the upgrading is in process.

The U200-CA provides the Web-based management function.

Use the default login information (see Table 6) to log in to the Web interface of the U200-CA.

Table 6 Default login information

Login information	Default setting
Username	admin
Password	admin
IP address of GigabitEthernet 0/0	192.168.0.1/24

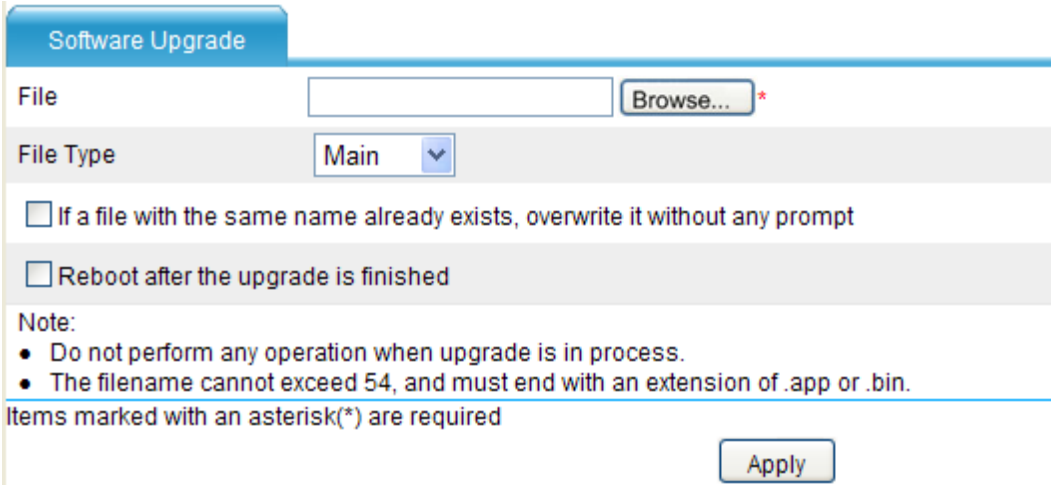
To upgrade the system software from the Web:

1. Use an Ethernet cable to connect the U200-CA to the PC.
2. Assign an IP address on subnet 192.168.0.0/24 (except 192.168.0.1) to the PC.

   In this example, assign 192.168.0.2 to the PC.
3. Run the IE, and enter 192.168.0.1 in the address bar.

   The Web login page appears.
4. Type the default username and password, and click Login.
5. Select Device Management > Software Upgrade from the navigation tree.

Figure 2 Upgrading the software



6. Specify the software upgrading configuration items as described in Table 7.

Table 7 Configuration items

Item	Description
File	Click Browse to set the path to the system software image file. The file name must end with .bin.
File Type	Set the file type. • Main—Used at the next startup • Backup—Used when the main system software image is invalid.
If a file with the same name already exists, overwrite it without any prompt	If you do not select the option, the message "The file already exists." appears when a file with the same name is on the device. You cannot continue the upgrading.
Reboot after the upgrade is finished	If you select this option, the device reboots after the upgrade is finished to validate the new system software image.

7. Click Apply.

Upgrading the system software image from BootWare menu

You can use FTP/TFTP (through an Ethernet port) or XMODEM (through the console port) for system software image upgrade from the BootWare menu. An upgrade through an Ethernet port is faster than that through the console port.

Accessing the BootWare menu

1. Power on the device, and you can see the following information:

```
System start booting...
Booting Normal Extend BootWare........

**************************************************************************
```

```
*                                                                              *
*               H3C SecPath U200-CA BootWare, Version 1.34                     *
*                                                                              *
********************************************************************************
Copyright (c) 2004-2012 Hangzhou H3C Technologies Co., Ltd.

Compiled Date       : Mar 29 2012
CPU Type            : XXX
CPU L1 Cache        : 32KB
CPU Clock Speed     : 750MHz
Memory Type         : DDR2 SDRAM
Memory Size         : 1024MB
Memory Speed        : 533MHz
BootWare Size       : 512KB
Flash Size          : 32MB
cfa0 Size           : 480MB
CPLD Version        : 3.0
PCB Version         : Ver.A


BootWare Validating...
Press Ctrl+B to enter extended boot menu...
…
```

2. Press Ctrl + B at the prompt.

```
Please input BootWare password:
```

3. Enter the BootWare password at the prompt to access the BootWare menu.

   By default, no password is required.

   If three password attempts are failed, the system reboots.

```
Note: The current operating device is flash
Enter < Storage Device Operation > to select device.

==========================<EXTEND-BOOTWARE MENU>==========================
|<1> Boot System                                                         |
|<2> Enter Serial SubMenu                                                |
|<3> Enter Ethernet SubMenu                                              |
|<4> File Control                                                        |
|<5> Modify BootWare Password                                            |
|<6> Skip Current System Configuration                                   |
|<7> BootWare Operation Menu                                             |
|<8> Clear Super Password                                                |
|<9> Storage Device Operation                                            |
|<0> Reboot                                                              |
==========================================================================
Enter your choice(0-9):
```

Table 8 BootWare menu options

Item	Description
<1> Boot System	Boot the system software image.
<2> Enter Serial SubMenu	Access the Serial submenu (see Table 11) for upgrading system software through the console port or changing the serial port settings.
<3> Enter Ethernet SubMenu	Access the Ethernet submenu (see Table 9) for upgrading system software through an Ethernet port or changing Ethernet settings.
<4> File Control	Access the File Control submenu (see Table 15) to retrieve and manage the files stored on the device.
<5> Modify BootWare Password	Modify the BootWare password.
<6> Skip Current System Configuration	Start the device with the factory default configuration. This is a one-time operation and does not take effect at the next reboot. You use this option when you forget the console login password.
<7> BootWare Operation Menu	Access the BootWare Operation menu for backing up, restoring, or upgrading BootWare.
<8> Clear Super Password	Clear all super passwords used for switching to higher user privilege levels. By default, no super password is required for switching to a higher user privilege level.
<9> Storage Device Operation	Access the Storage Device Operation menu to manage storage devices.
<0> Reboot	Restart the device.

Using TFTP/FTP to upgrade software through an Ethernet port

1. Enter 3 in the BootWare menu to access the Ethernet submenu.

```
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                        |
|<1> Download Application Program To SDRAM And Run                         |
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
============================================================================
Enter your choice(0-5):
```

Table 9 Ethernet submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download a system software image to the SDRAM and run the image.
<2> Update Main Application File	Upgrade the main system software image.
<3> Update Backup Application File	Upgrade the backup system software image.

Item	Description
<4> Update Secure Application File	Upgrade the secure system software image.
<5> Modify Ethernet Parameter	Modify network settings.
<0> Exit To Main Menu	Return to the BootWare menu.

2. Enter 5 to configure the network settings.

```
=========================<ETHERNET PARAMETER SET>=========================
|Note:       '.' = Clear field.                                           |
|            '-' = Go to previous field.                                  |
|          Ctrl+D = Quit.                                                 |
==========================================================================
Protocol (FTP or TFTP) :tftp
Load File Name         :main.bin
                       :
Target File Name       :main.bin
                       :
Server IP Address      :192.168.0.2
Local IP Address       :192.168.0.1
Gateway IP Address     :0.0.0.0
FTP User Name          :user
FTP User Password      :password
```

Table 10 Network parameter fields and shortcut keys

Field	Description
'.' = Clear field	Press a dot (.) and then Enter to clear the setting for a field.
'-' = Go to previous field	Press a hyphen (-) and then Enter to return to the previous field.
Ctrl+D = Quit	Press Ctrl + D to exit the Ethernet Parameter Set menu.
Protocol (FTP or TFTP)	Set the file transfer protocol to FTP or TFTP.
Load File Name	Set the name of the file to be downloaded.
Target File Name	Set a file name for saving the file on the device. By default, the target file name is the same as the source file name.
Server IP Address	Set the IP address of the FTP or TFTP server. If a mask must be set, use a colon (:) to separate the mask length from the IP address. For example, 192.168.80.10:24.
Local IP Address	Set the IP address of the Ethernet interface that connects to the TFTP or FTP server.
Gateway IP Address	Set a gateway IP address if the device is on a different network from the server.
FTP User Name	Set the username for accessing the FTP server. This username must be the same as configured on the FTP server. This field is not available for TFTP.
FTP User Password	Set the password for accessing the FTP server. This password must be the same as configured on the FTP server. This field is not available for TFTP.

3. Select an option in the Ethernet submenu to upgrade a system software image. For example, enter 2 to upgrade the main system software image.

```
Loading.....................................................................
.....................................................................
.....................Done!
30617340 bytes downloaded!
Updating File flash:/main.bin.....................................
The file already exists,Overwrite it? [Y/N]Y.....................
.................................................Done!
=========================<Enter Ethernet SubMenu>=========================
|Note:the operating device is flash                                       |
|<1> Download Application Program To SDRAM And Run                        |
|<2> Update Main Application File                                         |
|<3> Update Backup Application File                                       |
|<4> Update Secure Application File                                       |
|<5> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
|<Ensure The Parameter Be Modified Before Downloading!>                   |
===========================================================================
Enter your choice(0-5):
```

When you enter a number in the range of 1 to 4 and the system detects that a file with the same name exists on the device, the system gives you a message and asks you whether to overwrite the existing file.

- Enter Y, and the file is updated.
- Enter N, and the existing file is not changed. The upgrading fails.

4. Enter 0 to return to the BootWare menu, and then enter 1 to boot the system.

Using XMODEM to upgrade software through the console port

1. Enter 2 in the BootWare menu to access the Serial submenu.

```
=========================<Enter Serial SubMenu>=========================
|Note:the operating device is flash                                     |
|<1> Download Application Program To SDRAM And Run                      |
|<2> Update Main Application File                                       |
|<3> Update Backup Application File                                     |
|<4> Update Secure Application File                                     |
|<5> Modify Serial Interface Parameter                                  |
|<0> Exit To Main Menu                                                  |
=========================================================================
Enter your choice(0-5):
```

Table 11 Serial submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download an application to SDRAM through the serial port and run the program.
<2> Update Main Application File	Upgrade the main system software image.
<3> Update Backup Application File	Upgrade the backup system software image.
<4> Update Secure Application File	Upgrade the secure system software image.

Item	Description
<5> Modify Serial Interface Parameter	Modify serial port parameters
<0> Exit To Main Menu	Return to the BootWare menu.

NOTE:

If you use the baud rate of 9600 bps, jump to step 10.

2. Enter 5 to enter the baud rate setting menu.

```
==============================<BAUDRATE SET>==============================
|Note:'*'indicates the current baudrate                                   |
|     Change The HyperTerminal's Baudrate Accordingly                     |
|-------------------------<Baudrate Available>-------------------------|
|<1> 9600(Default)*                                                       |
|<2> 19200                                                                |
|<3> 38400                                                                |
|<4> 57600                                                                |
|<5> 115200                                                               |
|<0> Exit                                                                 |
==========================================================================
Enter your choice(0-5):
```

3. Select an appropriate baud rate for the console port. For example, enter 5 to select 115200 bps.

   The following messages appear:

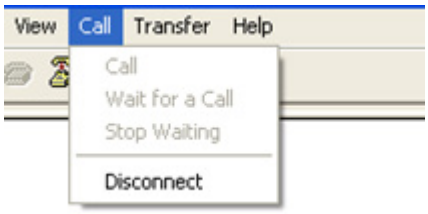
```
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
```

NOTE:

Typically the size of a .bin file is over 10 MB. Even at 115200 bps, the download takes about 30 minutes.

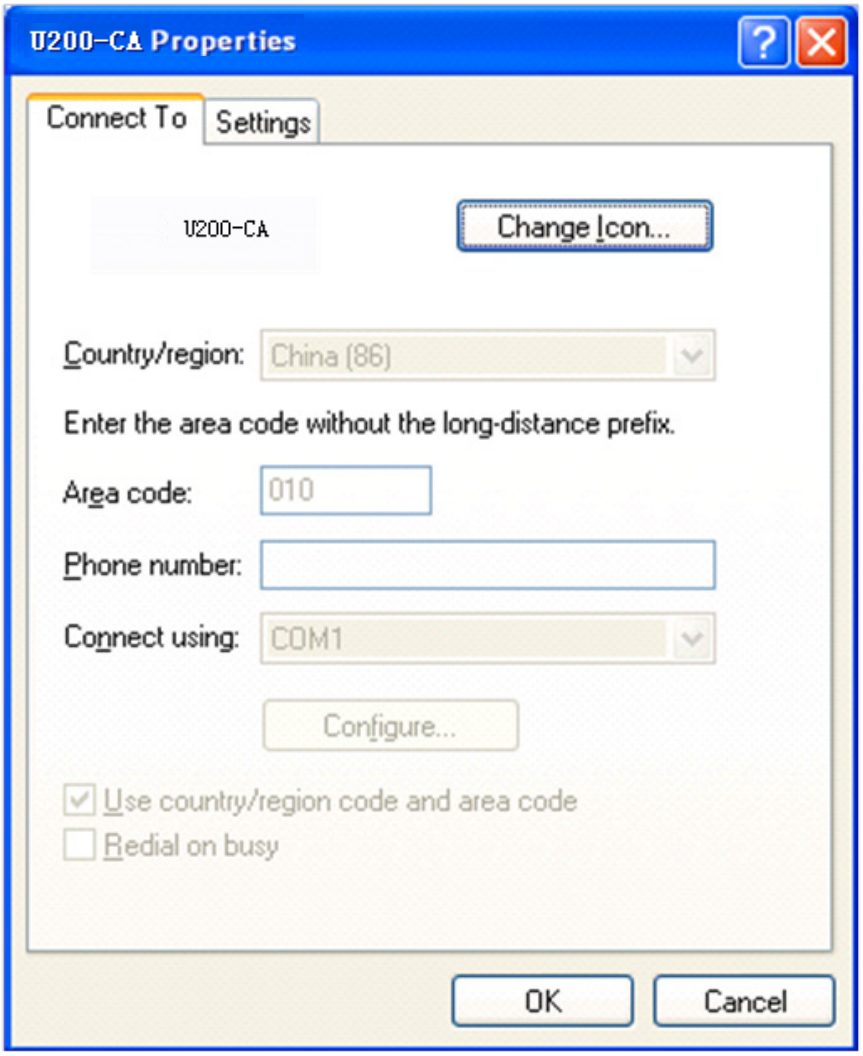
4. Select Call > Disconnect in the HyperTerminal window to disconnect the terminal from the device.

Figure 3 Disconnecting the terminal connection



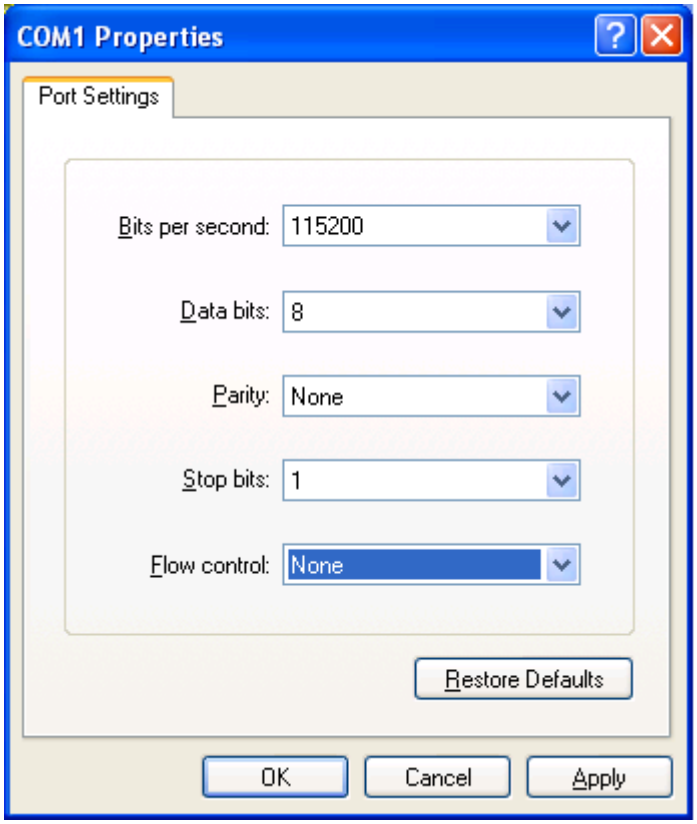
5. Select File > Properties, and in the Properties dialog box, click Configure.

Figure 4 Properties dialog box



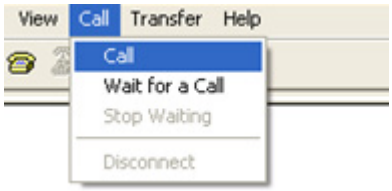
6. Select 115200 from the Bits per second list and click OK.

Figure 5 Modifying the baud rate



7. Select Call > Call to reestablish the connection.

Figure 6 Reestablishing the connection



8. Press Enter.

   The following menu appears:

```
The current baudrate is 115200 bps
==============================<BAUDRATE SET>==============================
|Note:'*'indicates the current baudrate                                  |
|     Change The HyperTerminal's Baudrate Accordingly                    |
|-------------------------<Baudrate Available>-------------------------|
|<1> 9600(Default)                                                       |
|<2> 19200*                                                              |
|<3> 38400                                                               |
|<4> 57600                                                               |
|<5> 115200                                                              |
|<0> Exit                                                                |
==========================================================================
Enter your choice(0-5):
```

9. Enter 0 to return to the Serial submenu.

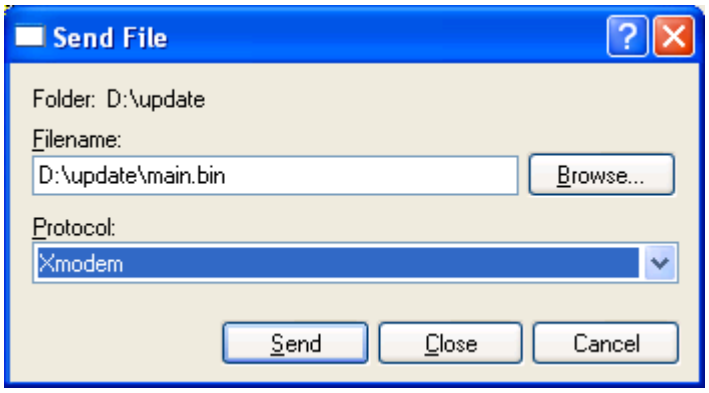
```
==========================<Enter Serial SubMenu>==========================
|Note:the operating device is flash                                      |
|<1> Download Application Program To SDRAM And Run                       |
|<2> Update Main Application File                                        |
|<3> Update Backup Application File                                      |
|<4> Update Secure Application File                                      |
|<5> Modify Serial Interface Parameter                                   |
|<0> Exit To Main Menu                                                   |
================================================================================
Enter your choice(0-5):
```

10. Select an option from options 2 to 4 to upgrade a system software image. For example, enter 2 to upgrade the main system software image.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCC
```

11. Select Transfer > Send File in the HyperTerminal window. In the dialog box that appears, click Browse to select the source file, and select Xmodem from the Protocol list.

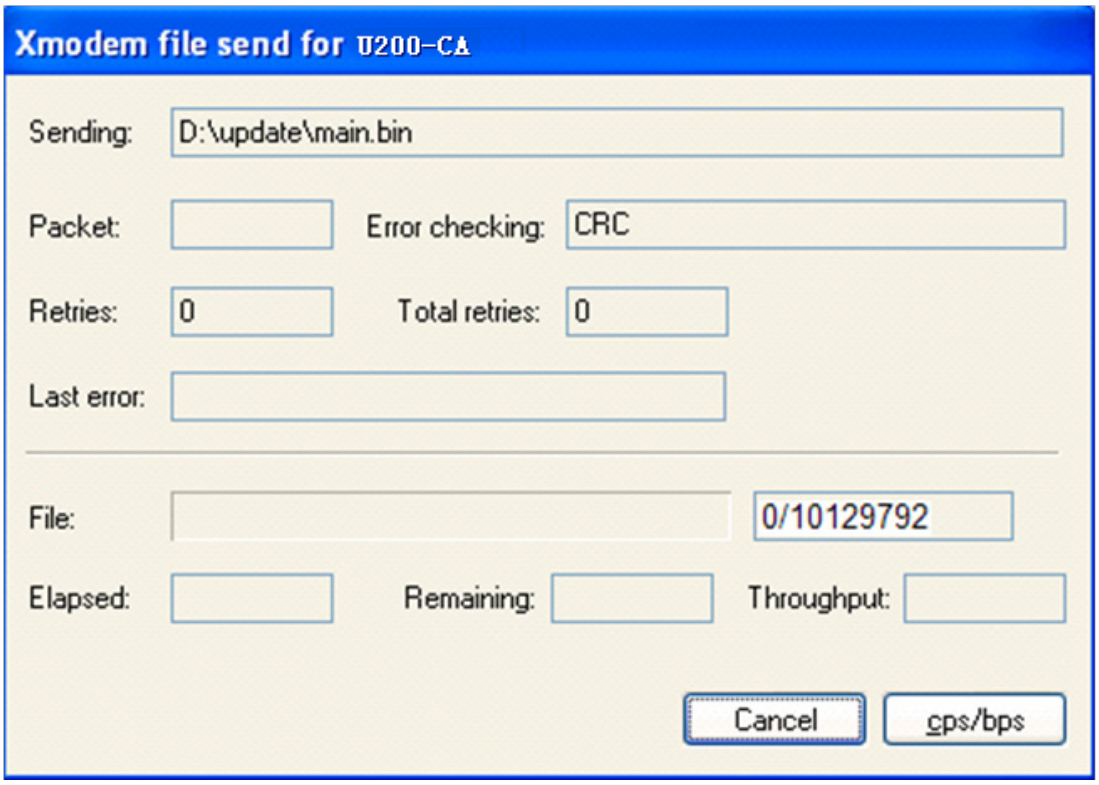
Figure 7 File transmission dialog box



12. Click Send.

The following dialog box appears:

Figure 8 File transfer progress



13. When the Serial submenu appears after the file transfer is complete, enter 0 at the prompt to return to the BootWare menu.

```
Download successfully!
30617340 bytes downloaded!
Input the File Name:main.bin
Updating File flash:/main.bin
The file already exists,Overwrite it? [Y/N]Y.....................
.................................................Done!

==========================<Enter Serial SubMenu>==========================
|Note:the operating device is flash                                      |
|<1> Download Application Program To SDRAM And Run                       |
|<2> Update Main Application File                                        |
|<3> Update Backup Application File                                      |
|<4> Update Secure Application File                                      |
|<5> Modify Serial Interface Parameter                                   |
|<0> Exit To Main Menu                                                   |
==========================================================================
Enter your choice(0-5):
```

14. Enter 1 in the BootWare menu to boot the system.
15. If you are using a download rate other than 9600 bps, change the baud rate of the terminal to 9600 bps. If the baud rate has been set to 9600 bps, skip this step.

Upgrading the BootWare image

Whether a .btw file is compressed together with a .bin file depends on the software release. Please check it with H3C technical support. This section describes how to upgrade the BootWare image separately at the CLI or from BootWare menus.

Upgrading the BootWare image at the CLI

To upgrade the BootWare image at the CLI:

1. Use FTP or TFTP to download or upload the new BootWare image file to the root directory of the storage medium on the device.
2. Execute the bootrom upgrade command to upgrade the BootWare image.

```
<System> bootrom update file flash:/main.btw
  This command will update bootrom file, Continue? [Y/N]:y
  Now updating bootrom, please wait...

 Updating basic bootrom!

 Update basic bootrom success!
 Updating extended bootrom!

 Update extended bootrom success!
 Update bootrom success!
<System>
```

3. Execute the reboot command to reboot the device.

```
<Sysname> reboot
 tart to check configuration with next startup configuration file, please wait.
........DONE!
 This command will reboot the device. Continue? [Y/N]:y
#Jun  1 11:50:00:690 2012 Sysname DEVM/1/REBOOT:
 Reboot device by command.

%Jun  1 11:50:00:691 2012 Sysname DEVM/5/SYSTEM_REBOOT: System is rebooting now.
System start booting...
…
```

Upgrading the BootWare image from BootWare menu

Accessing the BootWare menu

See "Accessing the BootWare menu."

Using TFTP/FTP to upgrade the BootWare through an Ethernet port

1. Enter 7 in the BootWare menu to access the BootWare operation submenu.

```
=========================<BootWare Operation Menu>==========================
|Note:the operating device is flash                                        |
|<1> Backup Full BootWare                                                  |
|<2> Restore Full BootWare                                                 |
|<3> Update BootWare By Serial                                             |
```

```
|<4> Update BootWare By Ethernet                                              |
|<0> Exit To Main Menu                                                        |
==============================================================================
Enter your choice(0-4):
```

Table 12 BootWare operation submenu options

Item	Description
<1> Backup Full BootWare	Back up the entire BootWare image.
<2> Restore Full BootWare	Restore the entire BootWare image.
<3> Update BootWare By Serial	Upgrade the BootWare image through the serial port.
<4> Update BootWare By Ethernet	Upgrade the BootWare image through the Ethernet port.
<0> Exit To Main Menu	Return to the BootWare menu.

2. Enter 4 to enter the Ethernet submenu.

```
==================<BOOTWARE OPERATION ETHERNET SUB-MENU>==================
|<1> Update Full BootWare                                                   |
|<2> Update Extend BootWare                                                 |
|<3> Update Basic BootWare                                                  |
|<4> Modify Ethernet Parameter                                              |
|<0> Exit To Main Menu                                                      |
==============================================================================
Enter your choice(0-4):
```

Table 13 Ethernet submenu options

Item	Description
<1> Update Full BootWare	Upgrade the entire BootWare image.
<2> Update Extend BootWare	Upgrade the extended section of the BootWare image.
<3> Update Basic BootWare	Upgrade the basic section of the BootWare image.
<4> Modify Ethernet Parameter	Modify Ethernet settings.
<0> Exit To Main Menu	Return to the BootWare menu.

3. Enter 4 to configure the network settings.

```
=========================<ETHERNET PARAMETER SET>=========================
|Note:       '.' = Clear field.                                           |
|            '-' = Go to previous field.                                  |
|          Ctrl+D = Quit.                                                 |
==============================================================================
Protocol (FTP or TFTP) :TFTP
Load File Name         :main.btw
                           :
Target File Name       :main.btw
                           :
Server IP Address      :192.168.0.2
Local IP Address       :192.168.0.1
Gateway IP Address     :0.0.0.0
```

For more information about the fields, see Table 10.

4. To upgrade the entire BootWare image, enter 1 on the Ethernet submenu.

```
==================<BOOTWARE OPERATION ETHERNET SUB-MENU>==================
|<1> Update Full BootWare                                                 |
|<2> Update Extend BootWare                                               |
|<3> Update Basic BootWare                                                |
|<4> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
==========================================================================
Enter your choice(0-4): 1
Loading............Done!
351388 bytes downloaded!
Updating Basic BootWare? [Y/N]Y
Updating Basic BootWare...........Done!
Updating Extend BootWare? [Y/N]Y
Updating Extend BootWare...........Done!
```

5. Enter 0 twice to return to the BootWare menu, and then enter 1 to reboot the system.

Using XMODEM to upgrade the BootWare image through the console port

1. Enter 7 in the BootWare menu to access the BootWare operation submenu, and then enter 3 in the BootWare menu to access the Serial submenu.

```
==================<BOOTWARE OPERATION SERIAL SUB-MENU>====================
|<1> Update Full BootWare                                                 |
|<2> Update Extend BootWare                                               |
|<3> Update Basic BootWare                                                |
|<4> Modify Serial Interface Parameter                                    |
|<0> Exit To Main Menu                                                    |
==========================================================================
Enter your choice(0-4):
```

Table 14 Serial submenu options

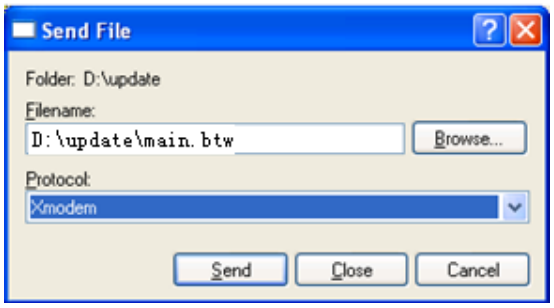
Item	Description
<1> Update Full BootWare	Upgrade the entire BootWare image.
<2> Update Extend BootWare	Upgrade the extended section of the BootWare image.
<3> Update Basic BootWare	Upgrade the basic section of the BootWare image.
<4> Modify Serial Interface Parameter	Modify Serial port settings.
<0> Exit To Main Menu	Return to the BootWare menu.

2. Enter 1 to upgrade the entire BootWare image.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCCCCCCCCCCCCCCCCCCCCCC...
```

3. In the HyperTerminal window, select Transfer > Send File. In the dialog box that appears, click Browse to select the source file, and select Xmodem from the Protocol list.

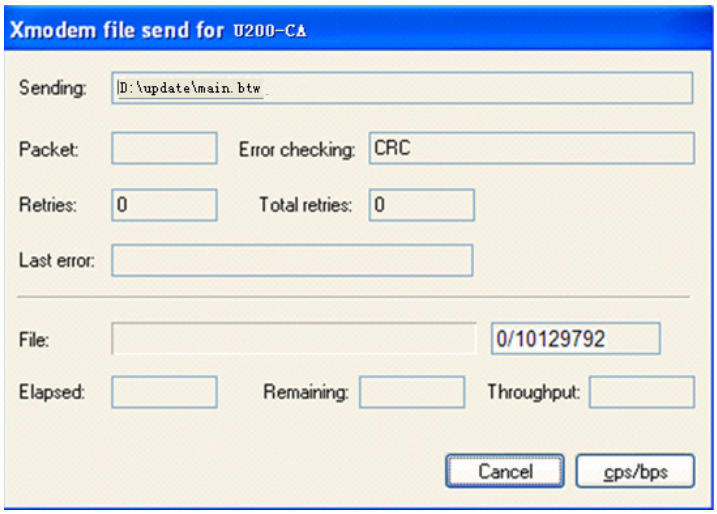
Figure 9 File transmission dialog box



4. Click Send.

   The following dialog box appears:

Figure 10 File transfer progress



After the file transfer is complete, the following messages appear:

```
Download successfully!
351488 bytes downloaded!
Updating Basic BootWare? [Y/N]Y
Updating Basic BootWare..........Done!
Updating Extend BootWare? [Y/N]Y
Updating Extend BootWare..........Done!

====================<BOOTWARE OPERATION SERIAL SUB-MENU>====================
|<1> Update Full BootWare                                                  |
|<2> Update Extend BootWare                                                |
|<3> Update Basic BootWare                                                 |
|<4> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

After the upgrade is complete, return to the BootWare menu and then enter 1 in the BootWare menu to boot the system.

Managing files from the BootWare menu

To change the type of a system software image, retrieve files, or delete files, enter 4 in the BootWare menu.

The File Control submenu appears:

```
==============================<File CONTROL>==============================
|Note:the operating device is flash                                      |
|<1> Display All File(s)                                                 |
|<2> Set Application File type                                           |
|<3> Delete File                                                         |
|<0> Exit To Main Menu                                                   |
=========================================================================
Enter your choice(0-3):
```

Table 15 File Control submenu options

Item	Description
<1> Display All File(s)	Display all files.
<2> Set Application File type	Change the type of a system software image.
<3> Delete File	Delete files.
<0> Exit To Main Menu	Return to the BootWare menu.

Displaying all files

On the File Control submenu, enter 1 to display all files:

```
Display all file(s) in flash:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
=========================================================================
|NO. Size(B)   Time                   Type   Name                       |
|1   6819      Feb/03/2012 10:39:24   N/A    flash:/system.xml          |
|2   207865    Dec/07/2011 17:43:38   N/A    flash:/logfile/~/logfile.log |
|3   1271      Feb/03/2012 10:39:26   B      flash:/startup.cfg         |
|4   30617340  Feb/02/2012 11:01:50   M      flash:/main.bin            |
=========================================================================


==============================<File CONTROL>==============================
|Note:the operating device is flash                                      |
|<1> Display All File(s)                                                 |
|<2> Set Application File type                                           |
|<3> Delete File                                                         |
|<0> Exit To Main Menu                                                   |
=========================================================================
Enter your choice(0-3):
```

Changing the type of a system software image

System software image file attributes include main (M), backup (B), and secure (S). You can store only one main image, one backup image, and one secure image on the device. A system software image can have any combination of the M, B, and S attributes. If the file attribute you are assigning has been assigned to an image, the assignment removes the attribute from that image. The image is marked as N/A if it has only that attribute. The file of the N/A type cannot be used at device startup.

For example, the file main.bin has the M attribute and the file update.bin has the S attribute. After you assign the M attribute to update.bin, the type of update.bin changes to M+S and the type of main.bin changes to N/A.

NOTE:

You cannot remove or assign the S attribute in the File Control submenu.

To change the type of a system software image:

1. Enter 2 in the File Control submenu.

```
'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
================================================================================
|NO. Size(B)   Time                    Type   Name                           |
|1   30617340  Feb/02/2012 11:01:50   M      flash:/main.bin                |
|0   Exit                                                                    |
================================================================================
Enter file No:
```

2. Enter the number of the file you are working with, and press Enter.

```
Modify the file attribute:
================================================================================
|<1> +Main                                                                    |
|<2> -Main                                                                    |
|<3> +Backup                                                                  |
|<4> -Backup                                                                  |
|<0> Exit                                                                    |
================================================================================
Enter your choice(0-4):
```

3. Enter a number in the range of 1 to 4 to add or delete a file attribute for the file.

```
Set the file attribute success!
```

Deleting files

When storage space is insufficient, you can delete obsolete files to free up storage space.

To delete files:

1. Enter 3 in the File Control submenu.

```
Deleting the file in flash:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
================================================================================
|NO. Size(B)   Time                    Type   Name                           |
|1   6819      Feb/03/2012 10:39:24    N/A    flash:/system.xml              |
|2   207865    Dec/07/2011 17:43:38    N/A    flash:/logfile/~/logfile.log |
```

```
|3   1271      Feb/03/2012 10:39:26    M+B    flash:/startup.cfg          |
|4   30617340  Feb/02/2012 11:01:50    M      flash:/main.bin             |
|0   Exit                                                                 |
==========================================================================
Enter file No:
```

2. Enter the number of the file to delete.
3. When the following prompt appears, enter Y.

```
The file you selected is flash:/logfile/~/logfile.log,Delete it? [Y/N]Y
Deleting.............Done!
```

Handling software upgrade failures

If a software upgrade fails, the system runs the old software version. To handle a software failure:

1. Check the physical ports for a loose or incorrect connection, and verify the LEDs are correctly reflecting the port status.
2. If you are using the console port for file transfer, check the HyperTerminal settings (including the baud rate and data bits) for any wrong setting.
3. Check the file transfer settings:
   - If XMODEM is used, you must set the same baud rate for the terminal as for the console port.
   - If TFTP is used, you must enter the same server IP addresses, file name, and working directory as set on the TFTP server.
   - If FTP is used, you must enter the same FTP server IP address, source file name, working directory, and FTP username and password as set on the FTP server.
4. Check the FTP or TFTP server for any incorrect setting.
5. Check that the Flash has sufficient space for the upgrade file.

If the message "Something is wrong with the file" appears, check the file for file corruption.

H3C SecPath UTM Series-CMW520-F5123P34 Release Notes

Software Feature Changes

Contents

Release F5123P34

This release has no feature changes.

Release F5123P27

This release has the following changes:

- New feature: Tiny TCP fragment attack protection

New feature: Tiny TCP fragment attack protection

Enabling tiny TCP fragment attack protection

The tiny TCP fragment attack protection function enables the device to drop tiny TCP fragments to prevent attacks that use tiny TCP fragments. As defined in RFC 1858, tiny TCP fragments refer to first fragments smaller than 20 bytes and non-first fragments with an offset no larger than 8.

To enable tiny TCP fragment attack protection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable tiny TCP fragment attack protection.	attack-defense tcp fragment enable	By default, tiny TCP fragment attack protection is enable.

Command reference

attack-defense tcp fragment enable

Use attack-defense tcp fragment enable to enable tiny TCP fragment attack protection.

Use undo attack-defense tcp fragment enable to disable tiny TCP fragment attack protection.

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

Default

Tiny TCP fragment attack protection is enable.

Views

System view

Default command level

2: System level

Usage guidelines

This command enables the device to drop tiny TCP fragments to prevent attacks that use tiny TCP fragments.

Examples

Enable tiny TCP fragment attack protection.

```
<Sysname> System-view
[Sysname] attack-defense tcp fragment enable
```

Release F5123P16

New feature: Configuring flow-based forwarding mode

Configuring flow-based forwarding mode

The UTM 200 series firewalls are multicore devices. By default, the device uses the packet-based forwarding mode and distributes packets equally to each VCPU for processing. However, frame loss may occur due to the disorder of the packets. In this case, the flow-based forwarding mode needs to be configured on firewalls to forward packets in order.

To configure the flow-based forwarding mode:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify a forwarding mode.	ip forwarding [per-flow | per-packet]	The default mode is per-packet. To make the forwarding mode modification take effect, reboot the device.
3. Display forwarding modes being used and to be used after reboot.	display ip forwarding mode [| { begin | exclude | include } *regular-expression*]	N/A

Command reference

ip forwarding

Use ip forwarding to specify a forwarding mode.

Syntax

ip forwarding { per-flow | per-packet }

Default

The mode is per-packet.

Views

System view

Default command level

2: System level

Parameters

per-flow: Specifies the flow-based mode. The device forwards flows with the same 5-tuple elements (source IP address, destination IP address, source port number, destination port number, and protocol number) to a same VCPU.

per-packet: Specifies the packet-based mode. The device distributes received packets equally to each VCPU.

Usage guidelines

To make the forwarding mode modification take effect, reboot the device.

Examples

Specify the forwarding mode as per-flow.

```
<Sysname> System-view
[Sysname] ip forwarding per-flow
 The operation succeeds, please reboot to take effect.
```

display ip forwarding mode

Use display ip forwarding mode to display forwarding modes being used and to be used after reboot.

Syntax

display ip forwarding mode [**|** { begin | exclude | include } *regular-expression*]

Views

Any view

Default command level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the user manual.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Examples

Display forwarding modes being used and to be used after reboot.

```
<Sysname> display ip forwarding  mode
  Current forwarding mode is per-packet.
  Next forwarding mode is per-flow after reboot.
```