Contents

1 Configuring the HTTP Service........1

1.1 Introduction........1

1.1.1 Overview........1

1.1.2 Principles........1

1.1.3 Protocols and Standards........3

1.2 Configuration Task Summary........3

1.3 Configuring Basic Features........3

1.3.1 Overview........3

1.3.2 Configuration Tasks........3

1.3.3 Configuring HTTP Service........3

1.3.4 Configuring HTTP Redirection to HTTPS........4

1.3.5 Configuring an HTTPS Service Certificate........5

1.4 Configuring Remote HTTP Upgrade........6

1.4.1 Overview........6

1.4.2 Restrictions and Guidelines........6

1.5 Monitoring........7

1.6 Configuration Examples........7

1.6.1 Configuring Basic Features of HTTP Service........7

1.6.2 Configuring Remote HTTP Upgrade........10

1 Configuring the HTTP Service

1.1 Introduction

1.1.1 Overview

The Hypertext Transfer Protocol (HTTP) is used to transmit Web page information on the Internet. It is at the application layer of the TCP/IP protocol stack. The transport layer adopts the connection-oriented Transmission Control Protocol (TCP).

The Hypertext Transfer Protocol Secure (HTTPS) is an HTTP protocol supporting the Secure Sockets Layer (SSL) protocol. HTTPS is used to create a secure channel on an insecure network, to prevent information from being monitored and protect against man-in-the-middle attacks. HTTPS is widely used in secure and sensitive communication on the Internet, for example, electronic transaction payments.

1.1.2 Principles

1. HTTP Service

HTTP is a service provided for Web management. Users log in to devices through Web pages to configure and manage the devices.

Web management covers Web clients and Web servers. Similarly, the HTTP service adopts the client/server mode. The HTTP client is embedded in the Web browser of the Web management client. It sends HTTP packets and receives and processes HTTP response packets. The Web server (HTTP server) is embedded in devices. The information exchange between the client and the server is as follows:

- A TCP connection is established between the client and the server. The default port number of the HTTP service is 80 and the default port number of the HTTPS service is 443.
- A TCP connection is established between the client and the server. The default port number of the HTTP service is 80 and the default port number of the HTTPS service is 4430.
- The client sends a request to the server.
- The server parses the request sent by the client. The request content includes obtaining a Web page, running a CLI command, and uploading a file.
- After executing the request content, the server sends a response to the client.
- The TCP connection between the server and the client is closed.

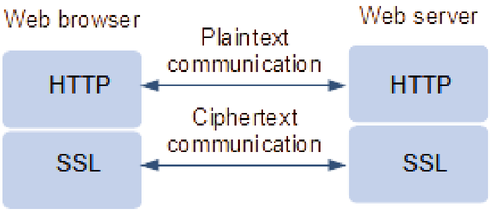
2. HTTPS Service

The HTTPS service is an SSL-based HTTP service, as shown in Figure 1-1. The HTTPS service improves the device security through the following services provided by the SSL protocol:

- Mutual authentication is needed between the client and the server to ensure that data is sent to the correct client and server, and unauthorized users are prevented from attacking the device.

- The communication data between the client and the server is encrypted to prevent the data from being stolen midway, ensuring security and integrity of the data transmission and achieving security management of the device.

Figure 1-1Principle of HTTPS Service



⚠ **Caution**

To run HTTPS properly, a server must have a Public Key Infrastructure (PKI) certificate while a client may not.

3. HTTPS Service Certificate

An HTTPS Service certificate is used to authenticate a server and encrypt data transmission. Users can enable the device to generate a new self-signed certificate or install a trust certificate issued by the certificate authority. If the HTTPS service certificate is not trusted by the browser, the browser displays a security prompt, asking for user's confirmation before the user accesses the Web management system of the device through HTTPS. Principles are as follows:

(1) The device generates a self-signed certificate as the HTTPS service certificate upon its first startup. Users can enable the device to generate a new self-signed certificate again or install a trust certificate issued by the certificate authority.

(2) The server delivers the certificate to the browser after the browser connects to the server via HTTPS.

(3) The browser checks the certificate delivered by the server to see whether the certificate user matches the address accessed, whether the certificate is in the validity period, and whether the certificate issuer is trusted by the browser. If not, the browser displays a security prompt, asking for user's confirmation before the user accesses the server.

4. HTTP Redirection to HTTPS

HTTP redirection to HTTPS means that the device redirects the browser access request to HTTPS when a user accesses the Web management service through the HTTP. Principles are as follows:

(1) A user enters the URL of HTTP into the address bar of the browser, for example, http://192.168.1.1. The browser sends an HTTP access request to the device.

(2) The device returns an HTTP access response packet containing a redirection URL, for example, https://192.168.1.1.

(3) The browser sends an HTTPS access request to the device to access the Web management page.

5. Remote HTTP Upgrade

The device is connected to a remote HTTP server as a client and upgrades local files by obtaining files from the server. Principles are as follows:

a Connect the device to the server. Connect to the server address configured by users first.

b The device sends the version numbers of its service modules to the server.

c The server parses the version numbers and provides a file download list.

d Based on the file download list, the device connects to the file server and downloads the upgrade file. The device can connect to different servers to download different upgrade files.

e The device upgrades itself by using the upgrade file.

1.1.3 Protocols and Standards

- RFC1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616: Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818: Hypertext Transfer Protocol Over TLS -- HTTPS

1.2 Configuration Task Summary

HTTP service configuration includes the following tasks:

(1) Configuring Basic Features

- Configuring HTTP Service
- (Optional) Configuring HTTP Redirection to HTTPS
- (Optional) Configuring an HTTPS Service Certificate

(2) Configuring Remote HTTP Upgrade

1.3 Configuring Basic Features

1.3.1 Overview

After the HTTP service is enabled on a device, users can log in to the Web management page after they pass authentication, and can monitor the device status, configure the device, upload and download files.

1.3.2 Configuration Tasks

The basic HTTP service includes the following tasks:

- Configuring HTTP Service
- (Optional) Configuring HTTP Redirection to HTTPS
- (Optional) Configuring an HTTPS Service Certificate

1.3.3 Configuring HTTP Service

1. Overview

After the HTTP service is enabled on a device, users can log in to the Web management page to manage the device after they pass authentication, and can monitor the device status, configure the device, upload and download files.

2. Restrictions and Guidelines

- Usernames and passwords involve three permission levels: Up to 10 usernames and passwords are configured for each permission level.
- By default, the system creates the account **admin**. The account cannot be deleted and only the password of the account can be changed. The administrator account **admin** corresponds to the level 0 privilege. Account **admin** owns all function privileges on the Web client and can edit other management accounts and authorize the accounts to access pages. All new accounts correspond to the level 1 privilege.
- To change an HTTPS service port, configure the HTTPS service port.
- Users can configure an HTTPS service port number to reduce attacks initiated by unauthorized users on HTTPS service.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the HTTP service.

enable service web-server [**http** | **https** | **all**]

The HTTP and HTTPS service features are disabled by default.

(4) Configure the HTTP authentication information.

webmaster level *privilege-level* **username** *username* { **password** [**0** | **7**] *password* | **secret** [**0** | **8**] *secret* }

The permission level bound to a user is 0, username is **admin**, and plaintext password is **admin** by default.

(5) Configures an HTTP service port.

http port *port-number*

The default port number of the HTTP service is 80.

(6) Configures an HTTPS service port.

http secure-port *port-number*

The default port number of the HTTPS service is 443.

1.3.4 Configuring HTTP Redirection to HTTPS

1. Overview

After HTTP and HTTPS are enabled in the device, HTTP can automatically redirect to HTTPS to improve security when users access the Web management page of the device through HTTP.

2. Restrictions and Guidelines

- Only after the HTTP and HTTPS services are enabled, HTTP automatically redirects to HTTPS.

- If an IP address to be accessed is a Network Address and Port Translation (NAPT) address, the redirection function may fail. To access the device through HTTP, disable the NAPT feature; to access the device through HTTPS, use HTTPS directly.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure HTTP redirection to HTTPS.

web-server http redirect-to-https

Automatic HTTP redirection to HTTPS is disabled by default.

1.3.5 Configuring an HTTPS Service Certificate

1. Overview

Orion_B26Q devices use an automatically generated self-signed certificate as the HTTPS service certificate by default. By configuring an HTTPS service certificate, the device generates a self-signed certificate again or uses the certificate assigned by Certificate Authority.

2. Restrictions and Guidelines

- The **web-server https generate self-signed-certificate** command is an interactive command. After running this command, enter the information to generate a self-signed certificate as prompted, or press **Ctrl+C** to cancel the operation.
- If the device is installed with a third-party HTTPS service certificate is installed, it uses the HTTPS certificate preferentially. The re-generated self-signed certificate does not replace the current HTTPS service certificate.
- After the HTTPS service certificate is generated again, the browser may require you to add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.
- After the HTTPS service certificate is installed, the browser may require you to add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the device to generate an HTTPS self-signed certificate again.

web-server https generate self-signed-certificate

The HTTPS service uses the self-signed certificate by default.

This command is not displayed in the configuration.

(4) (Optional) Install the HTTPS certificate.

web-server https certificate { **pem** *cert-filename* **private-key** *key-filename* } | { **pfx** *cert-filename* } [**password** *password-text*]

No HTTPS service certificate is installed by default.

This command is not displayed when the **show running-config** command is run.

1.4 Configuring Remote HTTP Upgrade

1.4.1 Overview

The device is connected to a remote HTTP server as a client and upgrades local files by obtaining files from the server.

1.4.2 Restrictions and Guidelines

- Before configuring the domain name of an HTTP upgrade server, enable the Domain Name System (DNS) on the device and configure the DNS server address.
- The server address does not support IPv6.
- Run the **http update server** command to configure the server address and port number for HTTP upgrade.
- During an HTTP upgrade, the device first connects to the server address configured by this command. If the server address is not connected, the device attempts to connect to server addresses recorded in the local file in turn. If none of the servers are connected, the upgrade cannot be performed.
- The system records the address or addresses of one or more upgrade servers. These addresses cannot be modified.
- If there is no special requirement, the HTTP upgrade time does not need to be configured by default.
- The **http update time** command can be used to change the automatic upgrade time, but can only configure a time point in each day. The time is accurate to minutes.
- In automatic upgrade mode, the device checks the file versions on the server as scheduled every day and upgrades itself by using the upgrade file.

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the HTTP upgrade server.

http update server { *host-name* | *ip-address* } [**port** *port-number*]

The default server address for HTTP upgrade is 0.0.0.0 and the default port number is 80.

(4) (Optional) Configure the HTTP upgrade mode.

http update mode manual

The default HTTP upgrade mode is automatic upgrade.

(5) (Optional) Configure the HTTP automatic detection time.

http update time daily *hh*:*mm*

The automatic detection time is random in the range from 00:00 to 23:59 by default.

(6) (Optional) Configure upgrade using the MGMT port.

http update set oob

The upgrade using a common port instead of a MGMT port is configured by default.

(7) Exit to the privileged EXEC mode.

end

(8) (Optional) Configure the device to detect upgrade files on the HTTP server.

http check-version [**extend**]

The function of detecting the version information of upgrade files on an HTTP server is enabled by default.

(9) Use the upgrade file to manually upgrade the specified service module.

http update { **all** | *string* }

No file for manual upgrade is configured by default.

1.5 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1HTTP Service Monitoring

Command	Purpose
show web-server status	Displays the configuration and status of the Web service.
show web-server https certificate information	Displays the HTTPS certificate of the Web server.

1.6 Configuration Examples

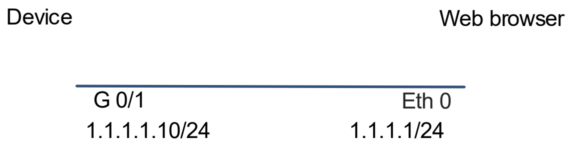
1.6.1 Configuring Basic Features of HTTP Service

1. Requirements

To manage a Orion_B26Q device in Web mode, log in to the device through a Web browser and configure related features.

2. Topology

Figure 1-1Topology for Basic Features of HTTP Service



3. Notes

- Configure L3 route reachable between the server and the device.
- To improve security, change the authentication username, HTTP service port, and HTTPS service port for login to the device. Moreover, configure redirection to HTTPS when accessing through HTTP. Thus, the Web browser can access the Web server through either HTTP or HTTPS.

4. Procedure

Configure the management IP address on the device to make the device reachable to the server via L3 routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 1.1.1.1 255.255.255.0
```

Enable both the HTTP and HTTPS services.

```
Hostname(config)# enable service web-server
```

Set the HTTP service port number to 8080.

```
Hostname(config)# http port 8080
```

Set the HTTPS service port number to 4430.

```
Hostname(config)# http secure-port 4430
```

Configure the HTTP authentication information.

```
Hostname(config)# webmaster level 1 username test1 password 0 test_password1
```

Configure HTTP redirection to HTTPS.

```
Hostname(config)# web-server http redirect-to-https
```

Configure the device to generate a self-signed certificate again.

```
Hostname# configure terminal
Hostname(config)# web-server https generate self-signed-certificate
RSA key modulus bits (1024~4096) [2048]:
Common Name (e.g. server IP) [Self-Signed-600B16C2]:
% Generate self-signed certificate successfully
```

5. Verification

Run the **ping** command to check whether the L3 route between the server and the server is reachable.

```
Hostname# ping 1.1.1.10
Sending 5, 100-byte ICMP Echoes to 1.1.1.10, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms.
```

Run the **show web-server status** command to display the configuration of the HTTP service.

```
Hostname# show web-server status
http server status: enabled
http server port: 8080
https server status:enabled
https server port: 4430
```

Run the **show web-server status** command to check whether HTTP redirection to HTTPS is enabled. When **http redirect to https** is **true**, the feature is enabled.

```
Hostname# show web-server status
http server status : enabled
http server port: 8080
https server status: enabled
https server port: 4343
http redirect to https: true
```

Run the **show web-server https certificate information** command to display the certificate information.

```
Hostname# show web-server https certificate information
Source: Default
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Self-Signed-93610DFD
        Validity
            Not Before: Apr  7 02:05:02 2020 GMT
            Not After : Apr  5 02:05:02 2030 GMT
        Subject: CN=Self-Signed-93610DFD
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:fb:de:8e:c0:f8:0d:53:ff:c1:57:a0:82:32:23:
                    41:d9:1c:c3:95:8e:02:a7:d7:5d:20:86:bb:bc:8f:
                    42:40:22:ef:9b:03:53:40:bf:16:fd:b7:ec:07:61:
                    78:8a:21:6c:4b:27:91:43:c4:5c:72:e5:df:bc:0e:
                    8a:d7:8f:e9:61:9b:77:22:4c:6e:e1:bf:cd:d6:9b:
                    f6:0d:ce:4e:32:b4:e4:e7:74:9b:fc:1d:45:a4:41:
                    5a:0f:6b:2e:b7:a3:ff:93:2e:f3:6b:67:b0:9e:89:
                    55:eb:ac:a2:ab:1f:b1:bc:24:4a:c2:87:ba:db:06:
                    09:22:b2:51:ae:6e:79:6b:c7:cb:16:25:d3:9a:6f:
                    41:99:b3:da:51:5d:39:21:aa:d2:45:44:79:40:78:
                    76:aa:1d:e0:3f:b3:ee:7a:ac:5b:8a:c6:96:c2:01:
```

```
                    57:60:83:16:b6:5c:55:d6:38:20:28:26:28:60:8c:
                    51:7b:3f:08:c1:f1:1b:1e:8d:58:b9:e9:c3:00:0c:
                    9d:6f:12:6a:97:67:70:61:1b:64:48:c3:2d:22:43:
                    15:51:3c:6c:24:15:66:bd:85:3b:4b:f0:bc:94:eb:
                    ef:f6:c0:5c:d1:54:1e:1f:84:72:9c:45:82:8f:e3:
                    83:26:a6:fe:72:d6:5f:32:27:93:ac:ae:a6:f4:d0:
                    d4:77
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
    Signature Algorithm: sha256WithRSAEncryption
         df:d2:8a:81:bf:d7:6b:23:1e:d9:a2:2c:48:35:ee:82:b0:33:
         c2:eb:a3:be:3f:78:57:39:6a:f1:ce:f2:ce:85:60:22:22:5c:
         94:b9:f2:d3:07:8e:f2:6b:7e:8f:b6:7b:5b:08:20:7a:73:e3:
         96:42:9d:9d:b9:11:39:2c:41:eb:fb:c7:57:87:6e:85:67:b5:
         35:a4:9b:04:43:8b:97:f5:66:80:e1:31:fb:ef:3c:74:59:2b:
         5b:77:6c:9d:9e:59:a8:3e:95:28:f8:76:97:b6:5a:d0:8e:4e:
         d0:e2:69:89:df:ba:a0:c3:12:39:f3:77:92:66:f6:d0:49:4a:
         e1:d2:df:01:d3:90:03:57:8d:2a:ef:ff:5c:b0:8a:6b:32:e0:
         84:bb:54:99:5f:0a:c5:6f:ff:4d:7d:8f:52:a7:ed:b2:f5:79:
         bd:20:f8:13:2a:05:d0:10:49:48:3d:72:b2:b1:f5:89:32:aa:
         f8:bd:76:f3:af:d9:59:8c:06:fe:4d:0d:d4:66:47:d2:c2:f4:
         bd:16:93:6c:31:1e:3a:8e:2c:3c:bc:af:81:3f:50:7f:8c:74:
         a1:90:a8:ea:34:29:7f:53:32:57:a9:cb:c3:a1:c7:0f:4a:97:
         c1:18:88:ab:cf:0c:c9:60:64:4e:42:25:dc:9d:e7:d0:5b:35:
         e8:23:30:dd
```

6. Configuration Files

```
hostname Device
!
ip name-server 1.1.1.1
!
http port 8080
http secure-port 4430
enable service web-server http
enable service web-server https
web-server http redirect-to-https
webmaster level 0 username admin secret 8 $1c$7eyy23uMQk$!
b(`dhh`n<nxlvxn&tp8$.<h!dfp46#2rlzj>x#h$
!
interface GigabitEthernet 0/1
 no switchport
 ip address 1.1.1. 255.255.255.0
```

7. Common Errors

If the HTTP service port is not the default port 80 or 443, you must enter a specific configured service port in the browser. Otherwise, you cannot access the device in Web mode.

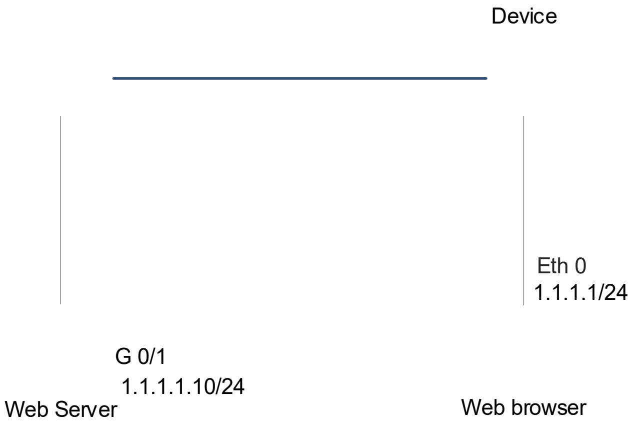
1.6.2 Configuring Remote HTTP Upgrade

1. Requirements

To reduce the impact on network communications, perform upgrade early in the morning. Therefore, you can use the remote HTTP upgrade feature to upgrade the device using files.

2. Topology

Figure 1-1Topology for Remote HTTP Upgrade



3. Notes

- Configure L3 route reachable between the server and the device.
- Enable the HTTP service.
- Before configuring the domain name of an HTTP upgrade server, enable DNS on the device and configure the DNS server address.
- The device obtains upgrade files from the Web server at 02:00 every day, and downloads the latest upgrade files to upgrade itself.

4. Procedure

Configure the management IP address on the device to make the device reachable to the server via L3 routes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 1.1.1.1 255.255.255.0
```

Configure the DNS.

```
Hostname(config)# ip domain-lookup
Hostname(config)# ip name-server 192.168.58.110
```

Enable the HTTP service.

```
Hostname(config)# enable service web-server
```

Set the scheduled time for the device to start remote monitoring to 02:00.

```
Hostname(config)# http update time daily 02:00
```

Configure the device to obtain upgrade files from the remote server.

```
Hostname# http check-version
```

Configure the device to download upgrade files from the server and update the device.

```
Hostname# http update all
```

5. Verification

Run the **ping** command to check whether the L3 route between the server and the server is reachable.

```
Hostname# ping 1.1.1.1
Sending 5, 100-byte ICMP Echoes to 1.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms.
```

6. Configuration Files

```
hostname Device
!
ip name-server 1.1.1.1
!
enable service web-server http
enable service web-server https
webmaster level 0 username admin secret 8 $1c$7eyy23uMQk$!
b(`dhh`n<nxlvxn&tp8$.<h!dfp46#2rlzj>x#h$
http update time daily 02:00
!
interface GigabitEthernet 0/1
 no switchport
 ip address 1.1.1. 255.255.255.0
```

7. Common Errors

DNS is disabled, so the device cannot establish a connection with the server.