QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Руководство пользователя

QSR-2830

www.qtech.ru

Оглавление

1. CONFIGURING DNS

1.1. Overview

Due to the Domain Name System (DNS), each IP address can present a host name consisting of one or more strings separated by the decimal. Then, you only need to remember the host name rather than IP address.

There are two methods of mapping the host name to the IP address: 1) Static mapping: A device maintains its host name to IP address mapping table and uses it only by itself. 2) Dynamic mapping: The host name to IP address mapping table is maintained on the DNS server. In order for a device to communicate with others by its host name, the corresponding IP address needs to be searched on the DNS server.

The domain name resolution (or host name resolution) is the process that the device obtains an IP address corresponding to the host name by the host name. Qtech switches support the host name resolution locally or by the DNS. During domain name resolution, you can firstly adopt the static method. If it fails, use the dynamic method. Some frequently used domain names can be put into the resolution list of static domain names. In this way, the efficiency of domain name resolution can be increased considerably.

1.2. Configuring Domain Name Resolution

1.2.1. Default DNS Configuration

The following table describes default configurations of DNS.

Attribute	Default value
Enable/disable the DNS resolution service	Enable
IP address of DNS server	None
Status Host List	None
Maximum number of DNS servers	Six

1.2.2. Enabling DNS Resolution Service

The following table describes how to enable the DNS resolution service.

Command	Function
Qtech(config)# **ip domain**-lookup	Enables DNS.

To disable DNS, use the **no ip domain-lookup** command.

```
Qtech(config)# ip domain-lookup
```

1.2.3. Configuring the DNS Server

This section describes how to configure the DNS server. The dynamic domain name resolution can be carried out only when the DNS Server is configured.

Use the **no ip name-server** [*ip-address*] command to remove the DNS server. In the command, the *ip-address* parameter indicates the specified DNS server to be removed. If this parameter is omitted, all the DNS servers will be removed.

Command	Function
Qtech(config)# **ip name-server** *ip-address*	Adds the IP address of the DNS Server. The switch will add a DNS Server every time this command is executed. If the domain name can’t be obtained from the first DNS Server, the switch will send the DNS request to the subsequent several servers until the correct response is received. The system can support six DNS servers at most.

1.2.4. Configuring the Host Name to IP/IPv6 Address Mapping Statically

This section describes how to configure the host name to IP/IPv6 address mapping. The switch maintains a host name to IP/IPv6 address corresponding table, which is also referred to as the host name to IP/IPv6 address mapping table. You can obtain the mapping table in two ways: manual configuration and dynamic learning. Manual configuration is required when dynamic learning is impossible.

Command	**Function**
Qtech(config)# **ip host** *host-name ip-address*	Configures the host name to IP address mapping manually.
Qtech(config)# **ipv6 host** *host-name ip-address*	Configures the host name to IPv6 address mapping manually.

To remove the mapping between the host name and IP/IPv6 address, use the **no** form of this command.

1.2.5. Clearing the Dynamic Buffer Table of Host Names

This section describes how to clear the dynamic buffer table of host names. If the **clear host** or **clear host** * command is entered, the dynamic buffer table will be cleared. Otherwise, only the entries of specified domain names will be cleared.

The following table describes related command.

Command	**Function**
Qtech# **clear host** [*word*]	Clears the dynamic buffer table of host names. The host names configured statically will not be removed.

1.2.6. Showing Domain Name Resolution Information

This section describes how to display the DNS configuration.

Command	Function
Qtech# **show hosts** [*host-name*]	Show parameters related to DNS.

```
Qtech# show hosts
Name servers are:
192.168.5.134  static
Host                  type       Address           TTL(sec)
www.163.com          static    192.168.5.243    ---
```

1.3. Typical DNS Configuration Examples

1.3.1. Example of Static DNS Configuration

1.3.1.1. Topological Diagram

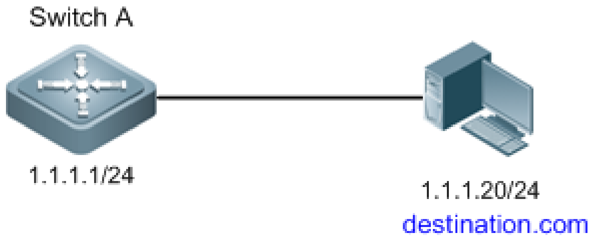


Figure1 Networking topology for static DNS configuration

1.3.2. Application Requirements

Since Switch A will frequently access the host of destination.com, you can use static DNS to access the host of IP 1.1.1.20 through the domain name of destination.com for domain resolution efficiency.

1.3.3. Configuration Tips

- Ensure that the route between device and host is reachable.
- The mapping between host name and IP address is correct.

1.3.4. Configuration Steps

Manually configure the mapping between host name and IP address. In this example, configure the host name to "destination.com" and the corresponding IP address to 1.1.1.20.

```
SwitchA(config)#ip host destination.com 1.1.1.20
```

1.3.5. Verification

Step 1: Show DNS information. Key points: the mapping between host and IP address shall be correct.

```
Qtech-A# show host
Name servers are:
Host                 type    Address                    TTL(sec)
destination.com    static  1.1.1.20                   ---
```

Step 2: Use the **ping destination.com** command to verify the result.

```
Qtech-A# ping destination.com
Translating "destination.com"...[OK]
Sending 5, 100-byte ICMP Echoes to 1.1.1.20, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The output shows that Qtech-A has successfully accessed the host with IP address being 1.1.1.20 through the host name of destination.com by means of static DNS.

1.3.6. Example of Dynamic DNS Configuration

1.3.6.1. Topological Diagram

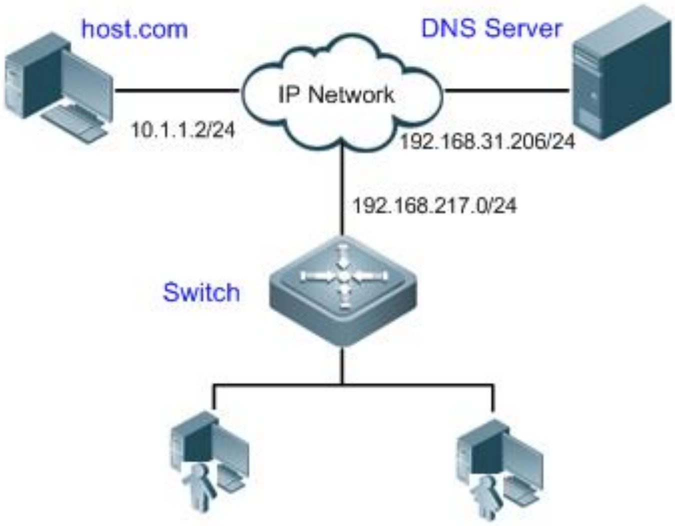


Figure2 Networking topology for dynamic DNS configuration

1.3.7. Application Requirements

- The IP address of DNS server is 192.168.31.206/24.
- The switch is the DNS client that can access the host of 10.1.1.2 through the host name of host.com by means of dynamic DNS.

1.3.8. Configuration Tips

- The route between DNS client, DNS server, and access PC shall be reachable.
- DNS shall be enabled. DNS is enabled by default.
- The IP address of the DNS server has been correctly configured.

1.3.9. Configuration Steps

Step 1: Configure the DNS server

Configure different DNS servers according to the actual conditions.

Configure the mapping between host and IP address on DNS server. This example configures the host name as "host.com" and the IP address as 10.1.1.2/24.

Step 2: Configure the DNS client

The route between DNS client, DNS server, and access PC shall be reachable. The interface IP configurations are shown in the topological diagram.

! DNS shall be enabled. The DNS feature is enabled by default.

```
Qtech(config)#ip domain-lookup
```

! Configure the IP address of DNS server as 192.168.31.206

```
Qtech(config)#ip name-server 192.168.31.206
```

1.3.10. Verification

Step 1: Use the **ping host.com** command to verify the result.

```
Qtech#ping host.com

Translating " host.com "...[OK]
Sending 5, 100-byte ICMP Echoes to 10.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The preceding information shows that the client can ping the host, and the destination IP is 10.1.1.2. Through dynamic DNS, the host with the IP address 10.1.1.2 can be accessed through the host name of host.com.

Step 2: Show DNS information. Key points: the host name and IP address.

```
Qtech#show host
Name servers are:
192.168.31.206 static

Host                  type       Address           TTL(sec)
host.com            dynamic     10.1.1.2           3503
```

The output shows that the mapping between host name and host IP is correct.

2. CONFIGURING DHCP

2.1. Understanding DHCP

The Dynamic Host Configuration Protocol (DHCP), as specified in RFC 2131, provides configuration parameters for hosts over the Internet. DHCP works in client/server mode. The DHCP server assigns IP addresses for the hosts dynamically and provides configuration parameters.

DHCP assigns IP address in three ways:

- Assigning IP addresses automatically. The DHCP server assigns permanent IP addresses to the clients;
- Assigning IP addresses dynamically. The DHCP server assigns temporary IP addresses to the clients (or the clients can release the addresses by themselves);

- Configuring IP addresses manually. Network administrators specify IP addresses and send the specified IP addresses to the clients through DHCP.

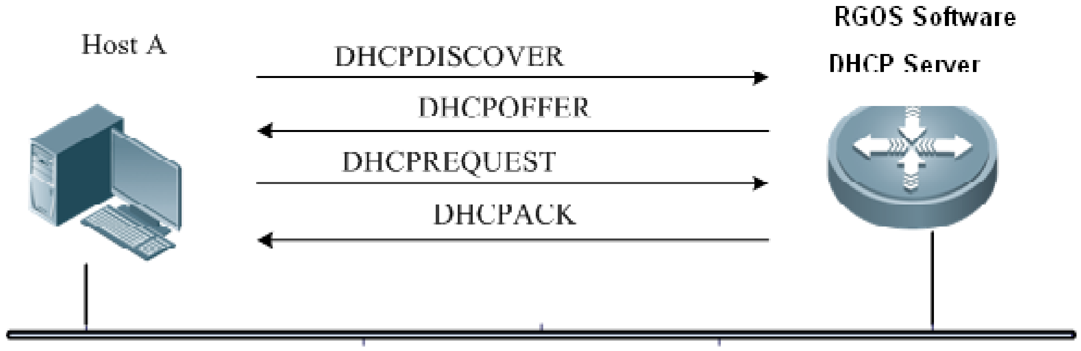
Among the mentioned three methods, only dynamic assignment allows reuse of the IP address that the client does not need any more.

The format of a DHCP message is based on that of a Bootstrap Protocol (BOOTP) message. Hence, the device must act as the BOOTP relay agent and interact with the BOOTP client and the DHCP server. The BOOTP relay agent eliminates the need of deploying a DHCP server in every physical network. DHCP is detailed in RFC 2131 and RFC 2132.

2.1.1. Understanding the DHCP Server

As specified in RFC2131, the DHCP server of Qtech Networks is implemented to assign and manage IP addresses for the DHCP clients. The DHCP operation process is shown in the following figure.

Fig 1-1 DHCP process



Process of requesting an IP address:

The host broadcasts a DHCPDISCOVER packet in the network to locate the DHCP server;
The DHCP server sends a DHCPOFFER packet in unicast form to the host, including IP address, MAC address, domain name and address lease period;
The host sends a DHCPREQUEST packet in broadcast form to formally request the server to assign the provided IP address;
The DHCP server sends a DHCPACK packet in unicast form to the host to confirm the request.

Note

The DHCP client may receive the DHCPOFFER packets from multiple DHCP servers, and accept all received DHCPOFFER packet. However, the DHCP client usually accepts the first received DHCPOFFER packet only.

Note

The address specified in the DHCPOFFER packet from the DHCP server is unnecessarily the finally assigned address. Generally, the DHCP server reserves this address until the client sends a formal request.

The DHCPREQUEST that requests the DHCP server to assign an address is a broadcast packet with the server address to enable all other DHCP servers that send DHCPOFFER response packets to receive the packet. Other DHCP servers are unable to find that the client has received the DHCPOFFER packet from just the DHCPREQUEST packet, so they will not release the IP addresses provided (pre-assigned) to the clients and will enable the IP addresses corresponding to the unaccepted OFFER lease to be reused through the timing mechanism.

If the DHCPOFFER packet sent to the DHCP client contains invalid parameters, the DHCP client sends the DHCPDECLINE packet to refuse the assigned configuration.

The following are advantages of using the DHCP server of Qtech Networks for network construction:

- Decreases network access cost. Generally, dynamic address assignment costs less than static address assignment.
- Simplifies configuration tasks and reduce network construction cost. Dynamic address assignment significantly simplifies equipment configuration, and even reduces deployment cost if devices are deployed in the places where there are no professionals.
- Centralizes management. During configuration management on several subnets, each configuration parameter can be changed simply by modifying and updating configurations in the DHCP server.

2.1.2. Understanding the DHCP Client

The DHCP client can obtain IP addresses and other configuration parameters from the DHCP server automatically. The DHCP client brings the following advantages:

- Saves device configuration and deployment time.
- Reduces the possibility of configuration errors.
- Centrally manages IP address assignment.

☑ The DHCP client is supported on the Ethernet interface, FR, PPP, and HDLC interfaces.

2.1.3. Understanding the DHCP Relay Agent

The DHCP relay agent forwards DHCP packets between the DHCP server and the DHCP clients. When the DHCP clients and the server are not located in the same subnet, the DHCP relay agent must be available for forwarding the DHCP request and response messages. Data forwarded by the DHCP relay agent is different from general forwarding. In general forwarding, IP packets are unaltered and the transmission is transparent. However, upon receiving a DHCP message, the DHCP relay agent regenerates a DHCP message before forwarding it.

For the DHCP client, the DHCP relay agent works like a DHCP server. For the DHCP server, the DHCP relay agent works like a DHCP client.

2.2. Configuring DHCP

To configure DHCP, perform the following tasks, of which the first three tasks are mandatory.

2.2.1. Enabling the DHCP Server and Relay Agent

Use the following commands to enable the DHCP server and relay agent in global configuration mode.

Command	Function
Qtech(config)# **service dhcp**	Enables the DHCP server and the DHCP relay agent.
Qtech(config)# **no service dhcp**	Disables the DHCP server and the DHCP relay agent.

☑ By default, in v10.1 and later, the **service dhcp** command can be used for both the DHCP server and DHCP relay, which are two mutually-exclusive functions. The switchover of those two functions depends on whether the DHCP address pool is configured.

☑ However, for the product in the version earlier than v10.1 (excluding v10.1), the **service dhcp** command is not supported by both DHCP server and DHCP relay. You can use the **service dhcp** command to enable the DHCP service or the DHCP server.

☑ For some products in v10.1 and later, DHCP may conflict with some functions. For more information, see the prompting message of a specific product.

2.2.2. Configuring DHCP Excluded Addresses

Unless configured particularly, the DHCP server tries to assign all the subnet addresses defined in the address pool to the DHCP clients. To reserve some addresses, such as those addresses that have been assigned, you must define those addresses as excluded.

Use the following commands to configure the excluded addresses in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp excluded-address** *low-ip-address [high-ip-address]*	Defines excluded addresses.
Qtech(config)# **no ip dhcp excluded-address** *low-ip-address [high-ip-address]*	Removes the configuration.

Note

A good practice in configuring the DHCP server is to prohibit the DHCP server from assigning any address that has been assigned specifically. This provides two advantages: 1) No address conflict will occur; 2) When DHCP assigns addresses, the time for detection is shortened and DHCP will perform assignment more efficiently.

2.2.3. Configuring DHCP Address Pool

DHCP Address assignment and DHCP parameters sent to the client should be defined in the DHCP address pool. If no DHCP address pool is configured, addresses cannot be assigned to the DHCP clients even though the DHCP server has been enabled. However, if the DHCP server has been enabled, the DHCP relay agent is always working regardless of the DHCP address pool.

You can give a meaningful name that can be memorized easily to the DHCP address pool. The name of address pool contains characters and digits. Qtech product allows you to define multiple address pools. The IP address of the DHCP relay agent in the DHCP request packet is used to determine which address pool is used for address assignment.

- If a DHCP request packet contains no IP address of the relay agent, the address will be assigned according to the segment range of the interface receiving request packets. The logic of assignment is that, if an address pool of a large segment scope is configured, addresses can be assigned for the request packets received by the small segment interfaces within the large address pool segment scope. For example, if the large address pool configured is 192.168.0.0/16, it can be used to assign addresses to the DHCP requests arriving at the small segment interfaces 192.168.1.0/24, 192.168.2.0/24 and 192.168.4.0/24. If multiple address pools of small segments are configured, these pools can assign addresses to the request packets arriving at the large segment interface covering the small segments. For example, the two small address pools 192.168.1.0/24 and 192.168.3.0/24 can assign addresses to the DHCP requests arriving at the interface of 192.168.0.0/16. If the minimum match between the segment range of the interface receiving request packets and the segment range of the address pool is unsuccessful, the address assignment fails.
- If the DHCP request packet contains the IP address of the DHCP relay agent, the address that is in the same subnet or network as this address is assigned to the DHCP client. If no address pool is defined for this network segment, address assignment fails.

To configure a DHCP address pool, perform the following tasks as appropriate, of which the first three tasks are mandatory:

-

2.2.3.1. *Configuring an Address Pool Name and Enter Configuration Mode*

Use the following command to configure an address pool name and enter address pool configuration mode in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp pool** *dhcp-pool*	Configures an address pool name and enter address pool configuration mode.

To display address pool configuration mode, use the **Qtech(dhcp-config)** command.

Configuring the Address Pool Network Number and Mask

To configure dynamic address binding, the subnet and its mask of the new address pool must be configured to provide the DHCP server with an address space that can be assigned to clients. Unless there is address exclusion configuration, the addresses in all the address pools can be assigned to clients. DHCP assigns addresses in the address pool in order. If an address exists in the DHCP binding table or is detected to have existed in the segment, the next address will be checked until a valid address is assigned.

Use the following command to configure the subnet and mask of an address pool in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **network** *network-number mask*	Configures the network number and mask of a DHCP address pool

2.2.4. Configuring the Client Boot File

The client boot file is the boot mapping file required when the client boots up. The boot mapping file is usually the operating system to be downloaded to the DHCP client.

Use the following commands to configure the client boot file in address pool configuration mode.

Command	Function
Qtech (dhcp-config)# **bootfile** *filename*	Configures the client boot file.

2.2.5. Configures the Default Gateway of the Client

The default gateway of the client is configured to function as the default gateway parameter that the server assigns to the client. The IP address of the default gateway must be in the same network as the IP address of the DHCP client.

Use the following commands to configure the default gateway of the client in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **default-router** *address* [*address2…address8*]	Configures the default gateway.

2.2.6. Configuring the Default Gateway for the DHCP Client

When Qtech devices assign DHCP addresses, default gateways to be assigned to clients can be either specified manually or assigned dynamically.

- If the default gateway of the address pool is specified manually, the gateway address manually specified is the default gateway of the client when a lease is obtained from the corresponding address pool.
- If no default gateway is configured, the default address type dynamically assigned is determined based on whether the VRRP address is configured to the interface that receives packets. If the VRRP address has been configured, the gateway is selected based on whether the request packets carry the field “relay”. If the request packet is forwarded by the relay, the segment of the field “relay” is used as the default gateway to issue; otherwise, the interface address selected by the longest match principle is the gateway to be issued.

Use the following command to configure the default gateway for the DHCP client in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **default-router** *address* [*address2…address8*]	Configures the default gateway.

2.2.6.1. Configuring the Address Lease Period

The lease period of the addresses assigned to clients by the DHCP server is infinite for static address pools, and 1 day for other address pools, by default. The client should request to update when the lease period is going to expire. Otherwise, it cannot use this address when the lease period expires.

Use the following command to configure the address lease period in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **lease** {*days* [*hours*] [*minutes*] | **infinite**}	Configures the address lease period.

Configure the startup server and boot file of the client. The client startup file is the boot image file that is used for client startup. Usually, after obtaining an IP address from the DHCP server, the DHCP client will download the boot image file from the startup server (usually the TFTP server) and initialize the device using the obtained configuration file. If no configuration file information is obtained, the device will be started up with the empty configuration.

Use the following commands to configure the download server and boot file of a client in address pool configuration mode.

Command	Function
Qtech (dhcp-config)# **next-server** *address* [*address2…address8*]	Configures the download server address for client startup
Qtech (dhcp-config)# **bootfile** *filename*	Configures the client boot file name

2.2.6.2. Configuring the Domain Name of the DHCP Client

The domain name of the DHCP client can be specified. In this way, the domain name suffix will be automatically added to the incomplete host name to form a complete host name when the DHCP client accesses the network resources using the host name.

Use the following command to configure the domain name of the DHCP client in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **domain-name** *domain*	Configures the domain name.

2.2.6.3. Configuring the Domain Name Server

A domain name server (DNS) should be specified for domain name resolution when the DHCP client accesses the network resources using a host name.

Use the following command to configure a domain name server for the DHCP client in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **dns-server** *address* [*address2…address8*]	Configures a DNS server.

2.2.6.4. Configuring the NetBIOS WINS Server

Windows Internet Naming Server (WINS) is a domain name resolution service from Microsoft used by the TCP/IP network to resolve a NetNBIOS name to an IP address. The WINS server runs in Windows NT. After started, the WINS server will receive a registration request from the WINS client. When the WINS client is being shut down, it will send a name release message to the WINS server to guarantee the consistency of available computers between the WINS database and the network.

Use the following command to configure a NetBIOS WINS server for the DHCP client in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **netbios-name-server** *address* [*address2…address8*]	Configures a DNS server.

2.2.6.5. Configuring the NetBIOS Node Type for the DHCP Client

There are four types of NetBIOS nodes for Microsoft DHCP client: 1) Broadcast. The NetBIOS name is resolved in broadcast mode; 2) Peer-to-peer. The WINS server is asked directly to resolve the NetBIOS name; 3) Mixed. First, the name is resolved in broadcast mode, and then the WINS server is connected to resolve the name; 4) Hybrid. First the WINS server is asked directly to resolve the NetBIOS name. If there is no response, the NetBIOS name is resolved in broadcast mode.

By default, the Windows operation systems support the broadcast or hybrid type NetBIOS nodes. If no WINS server is configured, the node is of the broadcast type. If a WINS server is configured, the node is of the hybrid type.

Use the following command to configure the NetBIOS node type for the DHCP client in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **netbios-node-type** *type*	Configures the NetBIOS node type.

2.2.7. Configuring the 6RD Parameters

The IPv6 rapid development (6RD) parameter includes the generic IPv4 prefix and suffix length, 6RD prefix length, 6RD prefix, and IPv4 address of the 6RD border relay (BR) for a given 6RD domain. If the DHCP client wants to create a 6RD tunnel, it can obtain the 6RD parameter via DHCP option 212.

Use the following command in DHCP address pool configuration mode to configure the 6RD parameter available for the DHCP client.

Command	Function
Qtech(dhcp-config)# **option 6rd ipv4masklen** *<mask-length>* **ipv6prefixlen** *<prefix-length>* **ipv6prefix** *<ipv6-prefix>* **br-addr** *<ipv4-address>*	Configures the 6RD parameter.

2.2.8. Configuring the Network ID and Mask of the DHCP Address Pool

You must configure the subnet and its mask to provide the DHCP server with a client address assignment range when binding dynamic addresses. All address in this range can be allocated to clients if no excluded address is configured. DHCP assigns addresses in the range one by one. If an address exists in the DHCP binding table or is detected in the network segment, the DHCP proceeds to the next address until finding an effective allocable address.

Use the following commands to configure the subnet and its mask of the address pool in address configuration mode.

Command	Function
Qtech(dhcp-config)# **network** *network-number mask*	Configures the network ID and mask of the DHCP address pool.

⚠ Caution

Address assignment is indexed by the physical address and ID of the client in the DHCP dynamic address pool of Qtech products. In this case, the DHCP address pool cannot have two leases of the same client. Then, address assignment of the server becomes faulty and may result in failure to assign addresses if path redundancy occurs in the network topology between the server and the client (the client can connect to the server through both the direct path and the relay path).

⚠ Caution

To avoid the preceding problem, the network administrator can avoid path redundancy between the server and the client using methods such as adjusting the physical link or network link.

2.2.8.1. Configuring DHCP Address Pool to Allocate Address as per Option82

Generally, the DHCP relay agent will insert Option 82 to carry relevant information about the client during the process of packet forwarding (such as the VLAN to which the client belongs, slot number, port number or user's 1X class). Upon receipt of such packets, the DHCP server will allocate addresses according to the specific information about clients by analyzing Option 82 information. For example, Option 82 can be used to allocate an IP address range to clients belonging to a VLAN or user class. This feature can be used when required to allocate a specific range of IP addresses according to user's network allocation information (such as VLAN, slot number or port number) or user's priority.

Each DHCP address pool can allocate addresses using Option 82 information. Option 82 information will be matched and classified, and we can specify the allocable address range for the corresponding class. One DHCP address pool can be associated with multiple classes, and different network segment ranges can be specified for each class.

During the process of address allocation, we can first determine the allocable address pool according to the network segment to which the client belongs, and then further determine its CLASS according to Option 82 information, so as to allocate IP address from the network segment range corresponding to the CLASS. When a request packet matches multiple classes in the address pool, address will be assigned from the address ranges corresponding to these classes so that the classes are configured in the address pool. If the class has no allocable address, the network segment range for the next matching class will be used, and the like. Each class corresponds to one address range, and the addresses must be assigned from low to high. Multiple classes can be configured with the same address range. If the CLASS associated with the address pool is specified, but the segment range of the CLASS is not configured, the DHCP clients of this CLASS cannot be assigned addresses.

Use the following commands to configure the CLASS associated with address pool and the address range corresponding to the class in address pool configuration mode.

Command	Function
Qtech(dhcp-config)# **class** *class-name*	Configures the name of associated class, and enter class configuration mode of address pool.
Qtech(config-dhcp-pool-class)# **address range** *low-ip-address high-ip-address*	Configures the corresponding network segment range.

Note

1. When the global class cannot be found, it will be created automatically.
2. The associated class configured in the address pool may conflict with the static manual binding, and therefore they cannot be configured at the same time.
3. Up to five classes can be configured for each address pool

2.2.9. Configuring Class

Configuring Option82 Matching Information for the CLASS

The specific Option82 matching information corresponding to each CLASS can be configured after entering CLASS configuration mode in global mode. One CLASS can match multiple pieces of Option 82 information, and it is considered matched if the packet matches any information. If no matching information is configured for CLASS, then this CLASS can match any request packets carrying Option 82 information. The address can only be assigned from the corresponding address pool after the request packet matches a specific CLASS.

Use the following commands to configure global CLASS and the Option 82 information corresponding to the CLASS in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp class** *class-name*	Configures CLASS name and enters global CLASS configuration mode.
Qtech(config-dhcp-class)# **relay agent information**	Enters Option 82 matching information configuration mode.
Qtech(config-dhcp-class-relayinfo)# **relay-information hex** *aabb.ccdd.eeff…* [*****]	Configures specific Option 82 matching information: 1. The parameter *aabb.ccdd.eeff..* is a hexadecimal number. The asterisk (*) indicates imperfect matching mode. It is considered matched if the information before * is matched.

Note

The Global CLASS can have up to 20 matches.

Configuring Remark Information for the CLASS

Use the following commands to configure remark information to describe the meaning of CLASS in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp class** *class-name*	Configures CLASS name and enters CLASS configuration mode.
Qtech(config-dhcp-class)#**remark** *used in #1 building*	Configures remark information.

Configuring whether to Use CLASS Allocation

Use the following command to configure address allocation using CLASS in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp use class**	Configures address allocation using CLASS.

Caution

This command is enabled by default. Execute NO command to disable address allocation using CLASS.

2.2.10. Configuring Binding Database Storage

Configuring to Periodically Save Binding Database into FLASH

To avoid the loss of binding database (lease information) on DHCP server due to power failure or reboot of the device, you can configure the delay time to write the database into FLASH. The time is **0** by default, namely the database will be written into FLASH at variable intervals.

Use the following command to periodically write the binding database into the FLASH in global configuration mode.

Command	Function
Qtech(config)# [**no**] **ip dhcp database write-delay** [*time*]	Configures DHCP delay time to write into FLASH. *The range of the time* parameter is from 600—to 86400 in seconds. The default is 0.

Caution

Since frequent FLASH reading and writing will shorten the service life of FLASH, we shall pay attention to the delay time configured. Short delay will enable efficient storage of device information, while long delay can reduce the frequency of FLASH reading and writing, thus prolonging the service life.

Configuring to Manually Save the Binding Database into FLASH

To avoid the loss of DHCP binding database (lease information) due to power failure or reboot of the device, you can also manually write the existing binding database information into the FLASH as needed besides configuring the delay time for FLASH writing.

Use the following command to manually write the binding database into the FLASH in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp database write-to-flash**	Writes DHCP binding database information into the FLASH

2.2.11. Manual Address Binding

Address binding refers to mapping the IP address to the MAC address for the DHCP clients. You can bind addresses in two ways. 1) Manual binding: Configure the static IP address to MAC address mapping for the DHCP client on the DHCP server manually. Manual binding actually offers a special address pool; 2) Dynamic binding: Upon receiving a DHCP request from the DHCP client, the DHCP server dynamically assigns an IP address from the DHCP address pool to the DHCP client, and thus mapping the IP address to the MAC address for the DHCP client.

To define manual address binding, you first need to define a host address pool for each manual binding, and then define the IP address and hardware address (MAC address) or ID for the DHCP client. Generally, a client ID, instead of a MAC address, is defined for the Microsoft clients. The client ID contains media type and MAC address. For the codes of media types, see the section "Address Resolution Protocol Parameters" in RFC 1700. The code of Ethernet type is “01”.

Use the following commands to configure the manual address binding in address pool configuration mode.

Command	Function
Qtech(config)# **ip dhcp pool** *name*	Defines the name of the DHCP address pool and enters DHCP configuration mode.
Qtech(dhcp-config)# **host** *address* [*netmask*]	Defines an IP address for the DHCP client.
Qtech(dhcp-config)# **hardware-address** *hardware-address type* *or:* Qtech(dhcp-config)# **client-identifier** unique-identifier	Defines a hardware address for the DHCP client, such as aabb.bbbb.bb88. Defines an ID for the DHCP client, such as 01aa.bbbb.bbbb.88.
Qtech(dhcp-config)# **client-name** *name*	(Optional) Defines the client name using standard characters of American Standard Code for Information Interchange (ASCII). Exclude the domain name in the client name. For example, if you define the host name as *mary*, do not define the client name as *mary.rg.com*.

2.2.12. Configuring Ping Times

By default, when trying to assign an IP address from the DHCP address pool to a DHCP client, the DHCP server will ping the IP address twice (one packet for each time). If there is no response, the DHCP server considers this address an idle address and assigns it to the DHCP client. If there is a response, the DHCP server considers that this address is in use and tries to assign another address to the DHCP client until an address is assigned successfully.

Use the following command to configure the number of Ping packets in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp ping** *packets number*	Configures the number of Ping packets before the DHCP server assigns an address. If it is set to **0**, the Ping operation is not performed. The default value is **2**.

2.2.13. Configuring Ping Packet Timeout

By default, the DHCP server considers an IP address nonexistent if no response is received within 500 milliseconds after pinging the IP address. You can adjust the Ping packet timeout.

Use the following command to configure the Ping packet timeout in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp ping timeout** *milliseconds*	Configures the Ping packet timeout for the DHCP server. The default value is 500ms.

2.2.14. Configuring the DHCP Client on the Ethernet Interface

☑ Qtech products support the function of dynamically obtaining the IP address that is assigned by the DHCP server on an Ethernet interface.

Use the following command to configure the DHCP client on the Ethernet port, execute the following command in interface configuration mode.

Command	Function
Qtech(config-if)# **ip address dhcp** [**6rd**]	Obtains an IP address through DHCP. The **6rd** parameter indicates that the device applies for the 6RD parameter configuration while requesting the IP address.

2.2.15. Configuring the DHCP Client in the PPP Encapsulation Link

Qtech products support the function of dynamically obtaining the IP addresses that is assigned by the DHCP server on a PPP encapsulation interface.

Use the following command to configure the DHCP client, execute the following command in interface configuration mode.

Command	Function
Qtech(config-if)# **ip address dhcp**	Obtains an IP address through DHCP.

2.2.16. Configuring the DHCP Client in the FR Encapsulation Link

☑ Qtech products support obtaining the IP addresses dynamically assigned by the DHCP server on an FR encapsulation interface.

Use the following command to configure the DHCP client, execute the following command in interface configuration mode.

Command	Function
Qtech(config-if)# **ip address dhcp**	Obtains an IP address through DHCP.

2.2.17. Configuring the DHCP Client in the HDLC Encapsulation Link

☑ Qtech products support obtaining the IP address dynamically assigned by the DHCP server on an HDLC encapsulation interface.

Use the following command to configure the DHCP client, execute the following command in interface configuration mode.

Command	Function
Qtech(config-if)# **ip address dhcp**	Obtains an IP address through DHCP.

☑ For some product of v10.1 and later versions, DHCP client supports obtaining the IP address assigned by the DHCP server in the point-to-point link of PPP, HDLC, and FR encapsulation.

2.3. Monitoring and Maintaining Information

2.3.1. Monitoring and Maintaining the DHCP Server

Three types of commands are available for monitoring and maintaining the DHCP server:

Clear commands, used to clear such information as DHCP address binding, address conflict and server statistics;
Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and fix faults;
Show commands, used to show information about DHCP.

Qtech products provide three clear commands. Use the following commands to clear information in command execution mode.

Command	Function
Qtech# **clear ip dhcp binding** { *address* | *****}	Clears the DHCP address binding information.
Qtech# **clear ip dhcp conflict** { *address* | *}	Clears the DHCP address conflict information.
Qtech# **clear ip dhcp server statistics**	Clears the DHCP server statistics.

Use the following command to debug the DHCP server in command execution mode.

Command	Function
Qtech# **debug ip dhcp server** [**events | packet**]	Debugs the DHCP server.

Use the following commands to show the working status of the DHCP server in command execution mode.

Command	Function
Qtech# **show ip dhcp binding** [*address*]	Shows the DHCP address binding information.
Qtech# **show ip dhcp conflict**	Shows the DHCP address conflict information.
Qtech# **show ip dhcp server statistics**	Shows the DHCP server statistics.

2.3.2. Monitoring and Maintaining the DHCP Client

There are two types of commands for monitoring and maintaining the DHCP client. The following operations can be performed on the DHCP client:

Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and clear faults.
Show commands, used to show information about DHCP.

Use the following command to debug the DHCP client, execute the following command in command execution mode.

Command	Function
Qtech# **debug ip dhcp client**	Debugs the DHCP client.

Use the following command to show information about the lease of the DHCP client in command execution mode.

Command	Function
show dhcp lease	Shows the information about DHCP lease.

2.4. Example of Configuring the Address Pool to Support Option82

In the following example, an address pool of "net82" is defined; the address pool is in the network segment of 172.16.1.0/24, and the associated classes include class1, class2, class3 and class4. Class1 will allocate addresses from the range of 172.16.1.1-172.16.1.8; class2 will allocate addresses from the range of 172.16.1.9-172.16.1.18; class3 will allocate addresses from the range of 172.16.1.19-172.16.1.28; class4 has no defined address range, and will allocate addresses from the range of entire network segment. Configure class1 to match Option 82 information of 0100002120, class2 to match 0106020145, class3 to match 06020506*, and class4 to match any information.

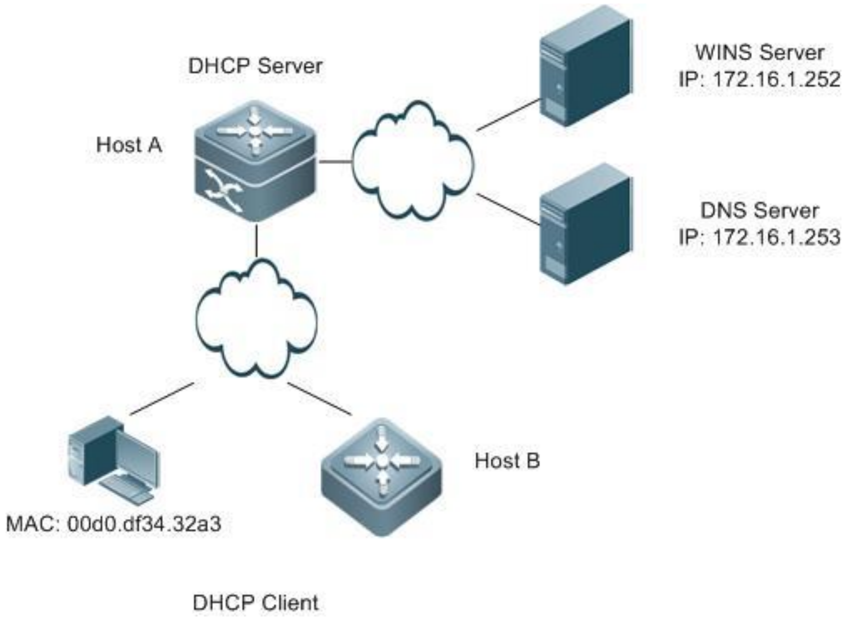
```
!
ip dhcp class class1
 relay agent information
    relay-information hex 0100002120
!
ip dhcp class class2
 relay agent information
```

```
    relay-information hex 0106020145
!
ip dhcp class class3
 relay agent information
    relay-information hex 06020506*
!
ip dhcp class class4
!
ip dhcp pool net82
network 172.16.1.0 255.255.255.0
class class1
address range 172.16.1.1 172.16.1.8
class class2
address range 172.16.1.9 172.16.1.18
class class3
address range 172.16.1.19 172.16.1.28
class class4
```

2.5. Typical DHCP Configuration Examples

Topological Diagram

Fig 1-6 Diagram of DHCP example



Application Requirements

- Host A can serve as the DHCP server to assign dynamic IP addresses to some client users. The network segment for IP address assignment is 172.16.1.0/24; the default gateway is 172.16.1.254; the domain name is Qtech.com; the domain name server is 172.16.1.253; the WINS server is 172.16.1.252; the NetBIOS node type is compound; and the address lease period is 1 day. Except the addresses from 172.16.1.2 to 172.16.1.100 in the address segment, all the other addresses can be assigned.
- □Host A assigns fixed IP addresses to some client users. The IP address assigned to the fit AP (DHCP client) with the MAC address 00d0.df34.32a3 is 172.16.1.101; the mask is 255.255.255.0; the domain name is admin; the default gateway is 172.16.1.254; the domain name server is 172.16.1.253; the WINS server is 172.16.1.252; and the NetBIOS node type is compound.
- Host B configures the DHCO automatically assigned address to the device interface FastEthernet 0/0.

Configuration Tips

- Enable the function of DHCP server on Host A and create an address pool to dynamically assign IP addresses. And create another address pool to manually bind IP addresses. Specify the address of the domain name server in the corresponding address pool (in this example, the addresses of the DNS server and WINS server) and the domain name of the client.

- Enable the function of the DHCP client on Host B to obtain the IP address automatically.

Configuration Steps

Step 1: Create a new DHCP address pool and configure dynamic IP address allocation on the Host A.

! Configure the name of address pool as "dynamic" and enter DHCP configuration mode.

```
HostA# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HostA(config)# ip dhcp pool dynamic
```

! In DHCP configuration mode, configure an IP address network allocable to clients, configure the default gateway of this network segment, and set the lease period to 1 day.

```
HostA(dhcp-config)# network 172.16.1.0 255.255.255.0
HostA(dhcp-config)# default-router 172.16.1.254
HostA(dhcp-config)# lease 1
```

Step 2: Specify the DNS Server of "dynamic" address pool and configure the domain name of client.

! Assuming that the IP address of DNS Server is 172.16.1.253, configure Domain Name Server in the address pool and configure the domain name of client as Qtech.com.

```
HostA(dhcp-config)# dns-server 172.16.1.253
HostA(dhcp-config)# domain-name Qtech.com
```

Step 3: Specify the WINS Server of "dynamic" address pool and configure the NetBIOS node type of client.

! Assuming that the IP address of WIN Server is 172.16.1.252, configure NetBIOS WINS server in the address pool and configure the NetBIOS node type as Hybrid.

```
HostA(dhcp-config)# netbios-name-server 172.16.1.252
HostA(dhcp-config)# netbios-node-type h-node
```

Step 4: Configure excluded addresses in global mode.

! As shown in the preceding information, IP addresses of 172.16.1.254, 172.16.1.253 and 172.16.1.252 have been assigned to the gateway, the DNS server and the WINS server, and the addresses from 172.16.1.2 to 172.16.1.100 are excluded addresses. The excluded addresses won't be assigned to clients.

```
HostA(dhcp-config)# exit
HostA(config)# ip dhcp excluded-address 172.16.1.252 172.16.1.254
HostA(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100
```

Step 5: Create another address pool and manually bind the IP address.

! Configure the name of address pool as "static" and enter DHCP configuration mode.

```
HostA(config)# ip dhcp pool static
```

! Manually bind the IP address of 172.16.1.101/24 to the MAC address of 00d0.df34.32a3, with client name being "admin". Note: The identifier for identifying the client shall indicate the network media type ("01" for Ethernet), namely the identifier of the client corresponding to the manually bound MAC address shall be 00d0.df34.32a3.14.

```
HostA(dhcp-config)# host 172.16.1.101 255.255.255.0
HostA(dhcp-config)# client-identifier 00d0.df34.32a3.14
HostA(dhcp-config)# client-name admin
```

Step 6: Specify the gateway address corresponding to the "static" address pool.

! Configure gateway address as 172.16.1.254.

```
HostA(dhcp-config)# default-router 172.16.1.254
```

Step 7: Specify the DNS Server of "static" address pool and configure the domain name of client.

! Assuming that the IP address of the DNS server is 172.16.1.253,configure the DNS in the address pool and configure the domain name of client as Qtech.com.

```
HostA(dhcp-config)# dns-server 172.16.1.253
```

HostA(dhcp-config)# domain-name Qtech.com Step 8: Specify the WINS Server of "static" address pool and configure the NetBIOS node type of client.

! Assuming that the IP address of WIN Server is 172.16.1.252, configure NetBIOS WINS server in the address pool and configure the NetBIOS node type as Hybrid.

```
HostA(dhcp-config)# netbios-name-server 172.16.1.252
HostA(dhcp-config)# netbios-node-type h-node
```

HostA(dhcp-config)# exit Step 9: Enable the DHCP server on HOST A.

```
HostA(dhcp-config)# exit
```

HostA(config)# service dhcp Step 10: Enable the DHCP client on Host B.

!The following example shows how to enable the DHCP client, assuming that the client uses a layer 3 interface by default.

```
HostB(config)# interface fastEthernet 0/1
HostB(config-if-fastEthernet 0/1)# ip address dhcp
```

Verification

Step 1: View the configuration information on Host A.

```
HostA# show running-config
!
service dhcp
!
ip dhcp excluded-address 172.16.1.252 172.16.1.254
ip dhcp excluded-address 172.16.1.2 172.16.1.100
!
!
ip dhcp pool dynamic
 netbios-node-type n-node
 netbios-name-server 172.16.1.252
 domain-name Qtech.com
 lease 1 0 0
 network 172.16.1.0 255.255.255.0
 dns-server 172.16.1.253
 default-router 172.16.1.254
!
ip dhcp pool static
 client-name admin
 client-identifier 00d0.df34.32a3.14
 host 172.16.1.101 255.255.255.0
 netbios-node-type n-node
 netbios-name-server 172.16.1.252
 domain-name Qtech.com
 dns-server 172.16.1.253
 default-router 172.16.1.254
!
```

Step 2: View the configuration information on Host B.

```
HostB# show running-config
!
interface fastEthernet 0/1
 // Note: For switches, the no switchport command is also required, and the interface is configured as a layer 3 interface.
ip address dhcp
```

Step 3: Connect a PC with the MAC address 0013.2049.9014, and view the IP address information assigned by the DHCP server on the Host A.

```
Qtech#show ip dhcp binding
```

```
IP address    Client-Identifier/     Lease expiration        Type
                Hardware address
172.16.1.101  00d0.df34.32a3.14      IDLE                      Manual 172.16.1.102
0100.e04c.70b7.e2 000 days 23 hours 48 mins Automatic
```

3. CONFIGURING DHCP RELAY

3.1. Overview

3.1.1. Understanding DHCP

The Dynamic Host Configuration Protocol (DHCP) is widely used to dynamically allocate reusable network resources such as IP addresses.

The DHCP client sends the DHCP DISCOVER broadcast packet to the DHCP server. After receiving the DHCP DISCOVER broadcast packet, the DHCP server allocates resources such as IP addresses to the DHCP client according to the appropriate policy, and sends the DHCP OFFER packet. After receiving the DHCP OFFER packet, the DHCP client checks if the resources are available. If yes, the DHCP client sends the DHCP REQUEST packet. If no, the DHCP client sends the DHCP DISCOVER packet. After receiving the DHCP REQUEST packet, the DHCP server checks if the IP addresses (or other limited resources) can be allocated. If yes, the DHCP server sends the DHCP ACK packet. If no, the DHCP server sends the DHCP NAK packet. After receiving the DHCP ACK packet, the DHCP client starts to use the resources allocated by the DHCP server. Upon receiving the DHCP NAK packet, the DHCP client may re-send the DHCP DISCOVER packet to request another IP address.

3.1.2. Understanding DHCP Relay

The destination IP address of DHCP REQUEST packet is 255.255.255.255. Such packets are only forwarded inside a subnet. To allocate IP addresses dynamically across network segments, the DHCP relay agent comes into being. It encapsulates the received DHCP REQUEST packet into unicast IP packets and forwards it to the DHCP server. Meanwhile, it forwards the received DHCP response packet to the DHCP client. In this way, the DHCP Relay Agent works as a transit station responsible for communicating with the DHCP clients and the DHCP server on different network segments. In this case, one DHCP server in a LAN can implement the dynamic IP management for all network segments, that is, a dynamic DHCP IP management in Client - Relay Agent - Server mode, as shown in Figure 1.

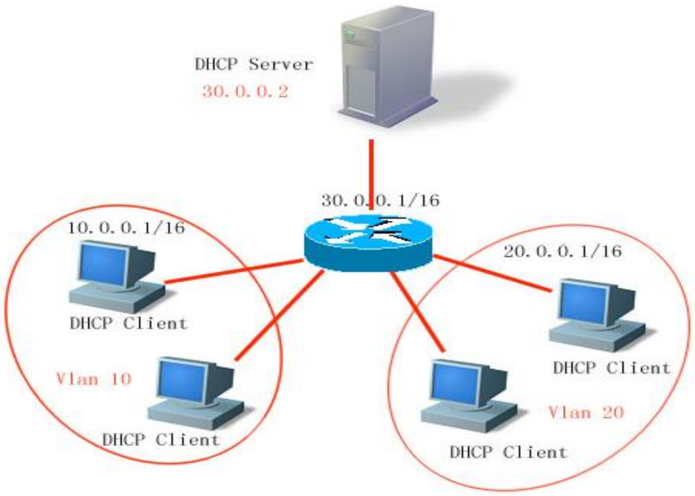


Figure 1

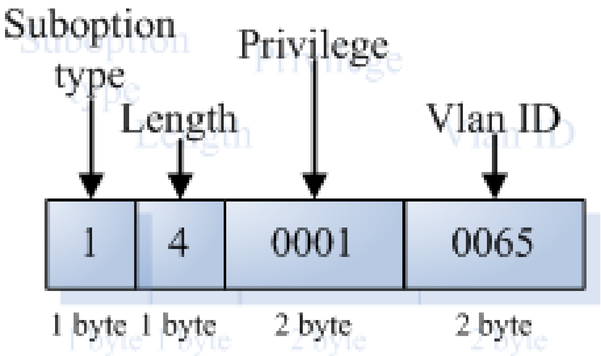
VLAN 10 and VLAN 20 correspond with the 10.0.0.1/16 and 20.0.0.1/16 networks respectively, while the DHCP server is located on the 30.0.0.1/16 network. To have a dynamic IP management on the 10.0.0.1/16 and 20.0.0.1/16 networks through the DHCP server at 30.0.0.2, just enable the DHCP Relay Agent on the device that functions as the gateway, and specify the IP address of the DHCP server to 30.0.0.2.

3.1.3. Understanding DHCP Relay Agent Information (option82)

As specified in RFC3046, when a relay device performs DHCP relay, an option can be added to identify the network information of the DHCP client, so that the DHCP server can assign users with IP addresses of different privileges. RFC3046 specifies that the option is numbered 82, so it is also called option82. This option can be divided into several sub-options. Currently, the sub-options frequently used are Circuit ID and Remote ID. Qtech Networks provides threetwo schemes for relay agent information, which are described as follows.

relay agent information option dot1x: This requires the combination of 802.1x authentication and Qtech RG-SAM.

DHCP relay forms the Circuit ID sub-option by combining the IP priority assigned to RG-SAM in 802.1x authentication with VID of the DHCP client. Figure 2 shows the option format.



relay agent information option82: This can be used without running other protocol modules. During DHCP relay, the device forms option82 information according to the port that receives the DHCP request message and the physical IP address of the device, and uploads the option82 information to the DHCP server.

Figure 3 and Figure 4 show the option formats.

Agent Circuit ID

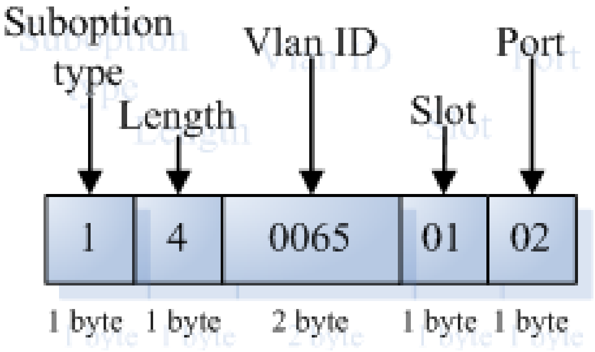


Figure 3

Agent Remote ID

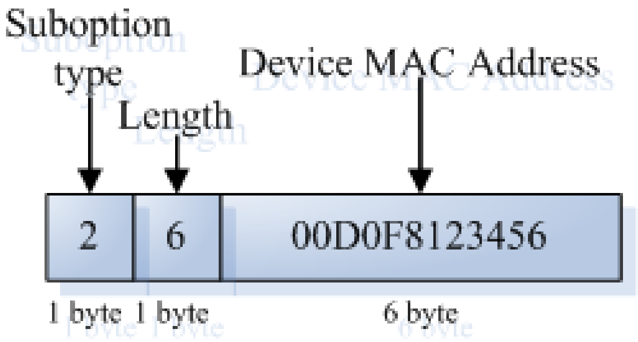


Figure 4

3.1.4. Understanding the DHCP Relay Check Server-id Function

This section describes the DHCP relay check server-id function. When DHCP is used, multiple DHCP servers are configured for a network for backup, so that the network will continue to work even if a server fails. During the four interaction processes of DHCP acquisition, a DHCP server has been selected when the DHCP client sends the DHCP request message. The DHCP request message includes the optional server-id. In particular application circumstances, you need to enable this option for relay to reduce loads on the network server. In this way, the DHCP request message is only sent to the specified DHCP server.

3.2. Configuring DHCP

3.2.1. Configuring the DHCP Relay Agent

Use the following commands to configure the DHCP relay agent in global configuration mode.

Command	Function
Qtech (config)# **service dhcp**	Enables the DHCP agent.
Qtech(config)# **no service dhcp**	Disables the DHCP agent.

3.2.2. Configuring the IP Address of the DHCP Server

After you have configured the IP address of the DHCP server, the DHCP request message received by the device will be forwarded to the DHCP server. Meanwhile, the DHCP response message from the DHCP server will be forwarded to the DHCP client.

The IP address of the DHCP server can either be configured globally or on the layer 3 interface. Up to 20 IP addresses can be configured for the DHCP server in each mode. When the DHCP request message is received from an interface, the DHCP server list on the interface is at first. If no DHCP server list is configured on the interface, the DHCP server list globally configured will be used.

DHCP supports vrf-based relay by adding the *vrf* parameter to the IP address of the DHCP server.

Use the following commands to configure the IP address of the DHCP server in global configuration mode.

Command	Function
Qtech(config)# **ip helper-address** [**vrf** { *vrf-name*} **|** **global**] *A.B.C.D*	Adds the IP address of the DHCP server globally. The VPN or global space of the specified server can be displayed.
Qtech(config-if)# **ip helper-address** [**vrf** {*vrf-name*} **|** **global**] *A.B.C.D*	Adds the IP address of the DHCP server on the interface. This command must be set on the layer 3 interface. The VPN or global space of the specified server can be displayed. The server is of the same VPN or global space as the current interface by default.

Command	Function
Qtech(config)# **no IP helper-address** [**vrf** { *vrf-name*} **|** **global**] *A.B.C.D*	Deletes the globally configured IP address of the DHCP server.
Qtech(config-if)# **no IP helper-address** [**vrf** { *vrf-name* } **| global**] *A.B.C.D*	Deletes the IP address of the DHCP server configured on the interface.

3.2.3. Configuring DHCP option dot1x

The section "Understanding the DHCP Relay Agent Information" shows that you can configure the **ip dhcp relay information option dot1x** command to enable the **option dot1x** function of DHCP relay when you need to assign the IP addresses with different privileges to the users of different privileges. When this function is enabled, the device will work with 802.1x to add corresponding option information to the DHCP server when it relays. This function should be used with the dot1x function.

Use the following commands to configure DHCP option dot1x in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp relay information option dot1x**	Enables the DHCP option dot1x function.
Qtech(config)# **no ip dhcp relay information option dot1x**	Disables the DHCP option dot1x function.

3.2.4. Configuring DHCP option dot1x access-group

In the option dot1x application scheme, the device needs to restrict the unauthorized IP address or the IP address with low privilege to access certain IP addresses, and restrict the access between users with low privileges. To do so, configure the **ip dhcp relay information option dot1x access-group** *acl-name* command. The Access Control List (ACL) defined by *acl-name* must be configured in advance. It is used to filter some contents and prohibit unauthorized users from accessing each other. In addition, the ACL associated here is applied to all the ports on the device. This ACL has no default Access Control Entry (ACE) and does not conflict with ACLs associated with other interfaces. For example:

Assign a type of IP addresses for all the unauthorized users, namely 192.168.3.2-192.168.3.254, 192.168.4.2-192.168.4.254, and 192.168.5.2-192.168.5.254. Do not assign gateway addresses 192.168.3.1, 192.168.4.1, and 192.168.5.1 to users. In this way, an unauthorized user uses one of the 192.168.3.x-5.x addresses to access the web portal for downloading the client software. The device should be configured as follows:

```
Qtech# configure terminal
Qtech(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
Qtech(config-ext-nacl)# permit ip any host 192.168.3.1
```

//Permit the packet to be transmitted to the gateway.

```
Qtech(config-ext-nacl)# permit ip any host 192.168.4.1
Qtech(config-ext-nacl)# permit ip any host 192.168.5.1
Qtech(config-ext-nacl)# permit ip host 192.168.3.1 any
```

//Permit the packet communication with the source IP address being the gateway.

```
Qtech(config-ext-nacl)# permit ip host 192.168.4.1 any
Qtech(config-ext-nacl)# permit ip host 192.168.5.1 any
Qtech(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
```

//Prohibit mutual accesses of unauthorized users.

```
Qtech(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.4.0  0.0.0.255
Qtech(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.5.0  0.0.0.255
Qtech(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.4.0  0.0.0.255
Qtech(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.5.0  0.0.0.255
Qtech(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.5.0  0.0.0.255
Qtech(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.3.0  0.0.0.255
Qtech(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.4.0  0.0.0.255
Qtech(config-ext-nacl)# exit
```

Then, apply the command to the global interfaces using the **ip dhcp relay information option dot1x access-group** *DenyAccessEachOtherOfUnauthrize* command.

Use the following commands to configure **DHCP option dot1x access-group** in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp relay information option dot1x access-group** *acl-name*	Enables DHCP option dot1x acl.
Qtech(config)# **no ip dhcp relay information option dot1x access-group** *acl-name*	Disables DHCP option dot1x acl.

3.2.5. Configuring DHCP option82

When the **ip dhcp relay information option82** command is configured, the device, as DHCP relay, adds option information in the DHCP request packet to the DHCP server during forwarding the request packet.

Use the following commands to configure DHCP option82 in global configuration mode:

Command	Function
Qtech(config)# ip dhcp relay information option82	Enables the DHCP option82 function.
Qtech(config)# no ip dhcp relay information option82	Disables the DHCP option82 function.

3.2.6. Configuring DHCP relay check server-id

After the **ip dhcp relay check** *server-id* command is configured, the device resolves the *dhcp server-id* option upon receiving DHCP relay. If this option is set, the DHCP request message is sent to this server only.

Use the following commands to configure **DHCP relay check** *server-id* function in global configuration mode.

Command	Function
Qtech(config)# **ip dhcp relay check** *server-id*	Enables the DHCP relay check server-di function.
Qtech(config)# **no ip dhcp relay check** *server-id*	Disables the DHCP relay check server-id function.

3.2.7. Configuring DHCP Relay Suppression

After the **ip dhcp relay suppression** command is configured, the port will not relay the DHCP request broadcast packet by transforming it into the unicast form. However, it will not suppress the normal forwarding of broadcast packets received.

Use the following commands to configure DHCP relay suppression in interface configuration mode.

Command	Function
Qtech(config-if)# **ip dhcp relay Suppression**	Enables the DHCP relay suppression function.
Qtech(config-if)# **no ip dhcp relay Suppression**	Disables the DHCP relay suppression function.

3.2.8. DHCP Relay Configuration Example

The following commands enable the DHCP relay function and add two groups of IP addresses of the DHCP server:

```
Qtech# configure  terminal
Qtech(config)# service dhcp            //Enable the dhcp relay function
Qtech(config)# service dhcp              //Enable the DHCP option vpn function.
Qtech(config)# ip helper-address 192.18.100.1
Qtech(config)# ip helper-address 192.18.100.2
  //Add the IP address of the server at the interface.
Qtech(config)# interface gigabitEthernet 0/3
Qtech(config-if-gigabitEthernet 0/3)# ip helper-address 192.18.200.1
Qtech(config-if-gigabitEthernet 0/3)# ip helper-address 192.18.200.2
Qtech(config-if-gigabitEthernet 0/3)# end
```

3.3. Other Precautions on DHCP Relay Configuration

For layer 2 network devices, you must enable at least one of the option dot1x, dynamic address binding, and option82 functions when the cross network segment management vlan relay function is required. Otherwise, only the relay function of management VLAN can be enabled for the layer 2 device.

3.3.1. Precautions on DHCP option dot1x Configuration

This command works only when the configuration related to AAA/802.1x is correct.

When this scheme is adopted, the IP authorization of the DHCP mode of 802.1x should be enabled.

This command cannot be used together with the **dhcp option82** command because they are conflicted.

When the IP authorization of the DHCP mode of 802.1x is enabled, the MAC address and the IP address will also be bound. Therefore, IP authorization and DHCP dynamic binding function cannot be enabled at the same time.

3.3.2. Precautions on DHCP option82 Configuration

The DHCP option82 function and the **dhcp option dot1x** function cannot be used at the same time because they are conflicted.

3.4. Showing the DHCP Configuration

Use the **show running-config** command to show the DHCP configuration in privileged mode.

```
Qtech# show running-config
Building configuration...
Current configuration : 1464 bytes
version RGOS 10.1.00(1), Release(11758)(Fri Mar 30 12:53:11 CST 2007 -nprd
hostname Qtech
vlan 1
ip helper-address 192.18.100.1
ip helper-address 192.18.100.2
ip dhcp relay information option dot1x
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
no switchport
ip helper-address 192.168.200.1
ip helper-address 192.168.200.2
interface VLAN 1
ip address 192.168.193.91 255.255.255.0
line con 0
exec-timeout 0 0
line vty 0
exec-timeout 0 0
login
password 7 0137
line vty 1 2
login
password 7 0137
line vty 3 4
login
end
```

3.5. Typical DHCP Relay Configuration Examples (for Switches)

3.5.1. Topological Diagram

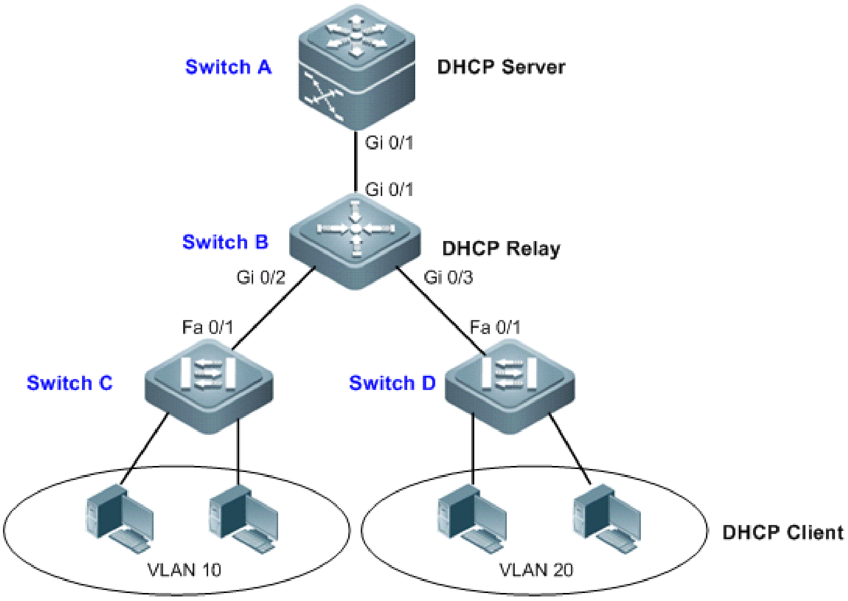


Diagram for DHCP relay configuration

3.5.2. Application Requirements

As shown in the preceding diagram, Switch C and Switch D are access devices connecting with PC users belonging to VLAN 10 and VLAN 20. Switch B is the gateway device, while Switch A is the core routing device. The following requirements must be met:

- Switch A can serve as DHCP server allocating dynamic IP addresses to VLAN users.
- The users connecting to Switch C and Switch D can acquire dynamic IP addresses across the network segment.

3.5.3. Configuration Tips

- **Configuring the DHCP server:** On Switch A, create DHCP address pools for users from VLAN 10 and VLAN 20 respectively, and enable the DHCP server (relevant configurations of the DHCP server can be found in the section "DHCP Configuration").
- **Configuring DHCP Relay:** On Switch B, configure the address of the DHCP server (configure the address of the DHCP server as 10.1.1.2/24) and enable the DHCP server.

Note

On Switch C and Switch D, configure the VLAN to which the corresponding ports belong, and the access PC can dynamically acquire IP address once connected.

3.5.4. Configuration Steps

Configure the DHCP server.

! In global mode, create a DHCP address pool named "vlan10" on Switch A, with corresponding IP network segment being 192.168.1.0/24 and the address of network gateway being 192.168.1.1.

```
SwitchA(config)#ip dhcp pool vlan10
SwitchA(dhcp-config)#network 192.168.1.0 255.255.255.0
SwitchA(dhcp-config)#default-router 192.168.1.1
SwitchA(dhcp-config)#exit
```

! Create an address pool named "vlan20", with IP network segment being 192.168.2.0/24 and gateway address being 192.168.2.1.

```
SwitchA(config)#ip dhcp pool vlan20
SwitchA(dhcp-config)#network 192.168.2.0 255.255.255.0
SwitchA(dhcp-config)#default-router 192.168.2.1
SwitchA(dhcp-config)#exit
```

! In global configuration mode, configure 192.168.1.1 and 192.168.2.1 as the excluded addresses, so as to avoid the conflict between allocated IP address and gateway address.

```
SwitchA(config)#ip dhcp excluded-address 192.168.1.1
SwitchA(config)#ip dhcp excluded-address 192.168.2.1
```

! Enable the DHCP server.

```
SwitchA(config)#service dhcp
```

Step 2: Configure layer-3 communication between Switch A and Switch B.

! On Switch A, configure port Gi 0/1 as the Route Port, with the corresponding IP address being 10.1.1.2/24.

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

! On Switch B, configure port Gi 0/1 as the Route Port, with the corresponding IP address being 10.1.1.3/24.

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if)#no switchport
SwitchB(config-if)#ip address 10.1.1.3 255.255.255.0
SwitchB(config-if)#exit
```

! Configure default route on Switch A

```
SwitchA(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.3
```

Step 3: Configure the gateway for access users.

! On Switch B, configure the Switch Virtual Interface (SVI) of VLAN 10 to 192.168.1.1/24.

```
SwitchB(config)#vlan 10
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 10
SwitchB(config-if)#ip address 192.168.1.1 255.255.255.0
SwitchB(config-if)#exit
```

! Configure the SVI of VLAN 20 to 192.168.2.1/24.

```
SwitchB(config)#vlan 20
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if)#ip address 192.168.2.1 255.255.255.0
SwitchB(config-if)#exit
```

Step 4: Configure DHCP Relay.

! On Switch B, globally configure the address of DHCP server as 10.1.1.2 and enable the DHCP server.

```
SwitchB(config)#ip helper-address 10.1.1.2
SwitchB(config)#service dhcp
```

Step 5: Configure layer-2 communication between Switch B and Switch C/D.

! On Switch B, configure ports Gi 0/2 and Gi 0/3 as the Trunk Port.

```
SwitchB(config)#interface range gigabitEthernet 0/2-3
SwitchB(config-if-range)#switchport mode trunk
```

! Configure port Fa 0/1 of Switch C and Switch D as the Trunk Port.

3.5.5. Verification

Step 1: Show configurations of devices.

! Configurations of Switch A

```
SwitchA#show running-config
!
```

```
service dhcp
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool vlan10
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool vlan20
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
!
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.1.3
!
! Configurations of Switch B
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
service dhcp
ip helper-address 10.1.1.2
!
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.3 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.2.1 255.255.255.0
!
```

Step 2: Connect two PCs with the ports belonging to VLAN 10 and VLAN 20 and verify dynamic IP address allocation.

```
SwitchA#show ip dhcp binding
IP address Client-Identifier/ Lease expiration  Type Hardware address
192.168.1.2 0100.1320.4990.14 000 days 23 hours 59 mins  Automatic
192.168.2.2 0100.e04c.70b7.e2 000 days 23 hours 59 mins  Automatic
```

3.6. Typical DHCP Relay Configuration Examples (for Routers)

3.6.1. Topological Diagram

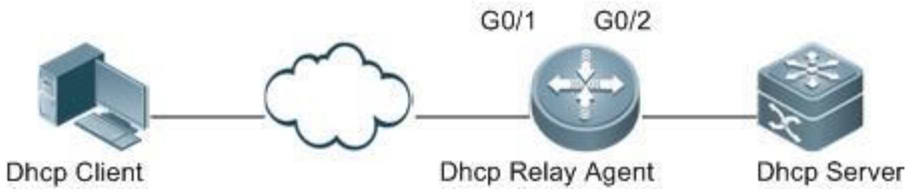


Diagram for DHCP Relay configuration

3.6.2. Application Requirements

As shown in the preceding diagram, obtaining the IP address and surfing the Internet by the user in different network segment shall be implemented when the DHCP Relay function is enabled.

3.6.3. Configuration Tips

- Enable the function of acquiring IP addresses through DHCP.
- Enable the DHCP Relay function on the DHCP Relay Agent.
- Configure the DHCP server.

3.6.4. Configuration Steps

Enable DHCP to acquire IP addresses.

Configure DHCP Relay:

# Enable the DHCP Relay Agent.

```
Qtech(config)# server dhcp
```

# Add an IP address of DHCP server globally.

```
Qtech(config)# ip helper-address 172.2.2.1
```

# Configure an IP address of the port connecting the user device.

```
Qtech(config)# interface gigabitEthernet 0/1
Qtech(config-if)# ip address 192.1.1.1 255.255.255.0
```

# Configure an IP address for the port connecting the user device.

```
Qtech(config)# interface gigabitEthernet 0/1
Qtech(config-if)# ip address 192.1.1.1 255.255.255.0
```

# Configure an IP address for the port connecting the Server device.

```
Qtech(config)# interface gigabitEthernet 0/2
Qtech(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
```

Configure the DHCP server.

3.6.5. Verification

Verify configurations of the DHCP Relay Agent device.

# Log in to the DHCP Relay Agent device, and use the **show running-config** command in privileged mode to show the DHCP Relay configuration.

```
Qtech# show running-config
service dhcp
ip helper-address 172.2.2.1
!
interface GigabitEthernet 0/1
ip address 192.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
ip address 172.2.2.2 255.255.255.0
!
```

3.7. Typical Option dot1x Configuration Example (for Switches)

3.7.1. Topological Diagram

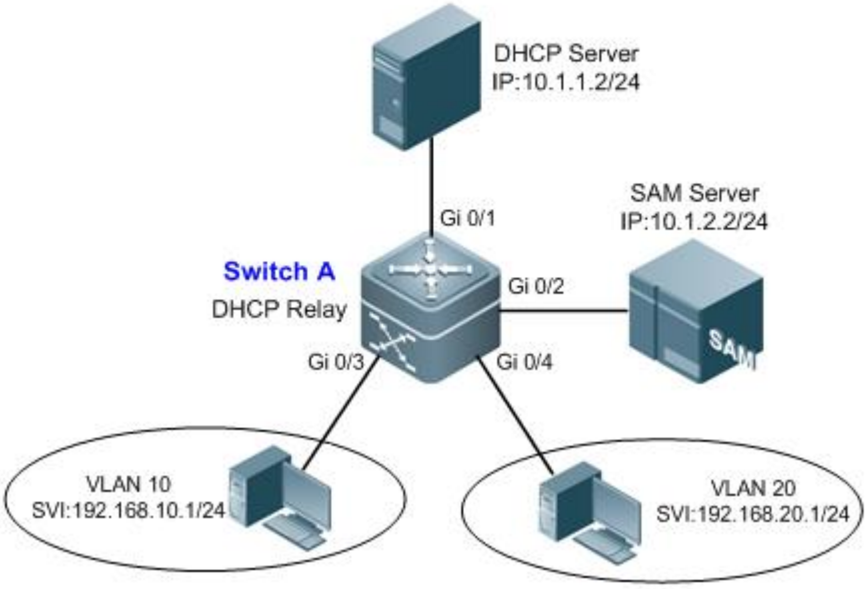


Diagram for DHCP Option Dot1x

3.7.2. Application Requirements

- Switch A is a layer 3 device allowing route communication cross different network segments.
- Access users belonging to different VLANs access Internet after Dot1x authentication, and SAM Server assigns different access privileges to different users.
- The DHCP server can allocate IP addresses to users according to the privilege of an authenticated user.

3.7.3. Configuration Tips

- **Configure basic DHCP Relay:** On Switch A, configure the address of the DHCP server (10.1.1.2/24) and enable the DHCP server. After configuration, the user can acquire dynamic IP address across the network segment.
- **Configure 802.1X authentication:** On Switch A, enable 802.1X authentication and set the user ports to controlled ports (Gi 0/3 and Gi 0/4). After configuration, the user will need to pass Dot1x authentication before accessing the Internet.
- **Configure the assignment of privilege-based IP address:** On Switch A, enable DHCP Option dot1x and configure IP authorization mode as DHCP server mode. After configuration, the DHCP server can allocate IP addresses according to user's privilege.

Note

1. Relevant configurations of 802.1X are detailed in the *802.1X Configuration*.

Note

2. The implementation of this example also needs the configuration of SAM Server and the DHCP server. For relevant details, see the relevant documents.

3.7.4. Configuration Steps

Configuring Switch A

Configure the address of the user gateway and the address of server interface.

! Configure the VLANs corresponding to Gi 0/3 and Gi 0/4 and configure the SVI corresponding to each VLAN.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#interface gigabitEthernet 0/3
Qtech(config-if-GigabitEthernet 0/3)#switchport access vlan 10
Qtech(config-if-GigabitEthernet 0/3)#exit
Qtech(config)#interface gigabitEthernet 0/4
Qtech(config-if-GigabitEthernet 0/4)#switchport access vlan 20
Qtech(config-if-GigabitEthernet 0/4)#exit
Qtech(config)#interface vlan 10
Qtech(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0
Qtech(config-if-VLAN 10)#exit
Qtech(config)#interface vlan 20
Qtech(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0
Qtech(config-if-VLAN 20)#exit
```

! Configure the interface address of the DHCP server and SAM Server.

```
Qtech(config)#interface gigabitEthernet 0/1
Qtech(config-if-GigabitEthernet 0/1)#no switchport
Qtech(config-if-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
Qtech(config-if-GigabitEthernet 0/1)#exit
Qtech(config)#interface gigabitEthernet 0/2
Qtech(config-if-GigabitEthernet 0/2)#no switchport
Qtech(config-if-GigabitEthernet 0/2)#ip address 10.1.2.1 255.255.255.0
Qtech(config-if-GigabitEthernet 0/2)#exit
```

Configure relevant features of DHCP Relay.

! Configure the address of DHCP server as 10.1.1.2/24 and enable DHCP service.

```
Qtech(config)#ip helper-address 10.1.1.2
Qtech(config)#service dhcp
```

! Enable DHCP Option dot1x.

```
Qtech(config)#ip dhcp relay information option dot1x
```

Configure 802.1X relevant features.

! Enable AAA and configure the address of Radius Server as 10.1.2.2/24; configure Radius Key as "Qtech".

```
Qtech(config)#aaa new-model
Qtech(config)#radius-server host 10.1.2.2
Qtech(config)#radius-server key Qtech
```

! Create Dot1x authentication method list named "d1x" and configure Dot1x to apply such authentication method list.

```
Qtech(config)#aaa authentication dot1x d1x group radius
Qtech(config)#dot1x authentication d1x
```

! Configure ports Gi 0/3 and Gi 0/4 as controlled ports.

```
Qtech(config)#interface range gigabitEthernet 0/3-4
Qtech(config-if-range)#dot1x port-control auto
Qtech(config-if-range)#exit
```

! Configure IP authorization mode as DHCP server mode.

```
Qtech(config)#aaa authorization ip-auth-mode dhcp-server
```

3.7.5. Verification

Verify configurations of devices.

! Configurations of Switch A

```
Qtech#show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode dhcp-server
aaa authentication dot1x d1x group radius
```

```
!
vlan 10
!
vlan 20
!
service dhcp
ip helper-address 10.1.1.2
!
ip dhcp relay information option dot1x
!
radius-server host 10.1.2.2
radius-server key Qtech
!
dot1x authentication d1x
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 no ip proxy-arp
 ip address 10.1.2.1 255.255.255.0
!
interface GigabitEthernet 0/3
 switchport access vlan 10
 dot1x port-control auto
!
interface GigabitEthernet 0/4
 switchport access vlan 20
 dot1x port-control auto
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.1 255.255.255.0
!
```

4. CONFIGURING NTP

4.1. Understanding NTP

Network Time Protocol (NTP) is designed for time synchronization on network devices. With its clock source or the server. Moreover, NTP can provide time correction (the time difference is less than one millisecond on the LAN and dozens of milliseconds on the WAN, compared with the standard time) and prevent attacks using encryption and confirmation.

To provide accurate Coordinated Universal Time (UTC), NTP needs an accurate clock source from the atom clock, observatory, satellite or Internet.

To prevent the time server from malicious attacks, NTP uses an authentication mechanism is used to check whether the time synchronization request really comes from the declared server, and check the return path, thus providing the protection of anti-interference.

Qtech switches support the NTP client and server. That is, the switch can synchronize the time from the time server and work as the time server (only in unicast server mode) to synchronize the time of other switches.

4.2. Configuring NTP

This chapter describes how to configure the NTP client and server.

4.2.1. Configuring the Global NTP Authentication Mechanism

Qtech NTP client supports encrypted communication with the NTP server using key encryption.

Configure the encrypted communication between the NTP client and the NTP server as follows: Step 1, Authenticate the NTP client and configure the key globally; Step 2, Configure the trusted key for the NTP server. To initiate the encrypted communication with the NTP server, you need to set the authentication key for the NTP server in addition to performing Step 1.

By default, the NTP client does not use the global security authentication mechanism and the communication will not be encrypted. To enable encrypted communication, you need to enable the global security authentication, configure other global keys and set an encryption key for the server.

Use the following commands in global configuration mode to configure the global security authentication mechanism.

Command	Function
ntp authenticate	Configures the global NTP security authentication mechanism.
no ntp authenticate	Disables the global NTP security authentication mechanism.

To verify the packet, use the trusted key specified by the **ntp authentication-key** or **ntp trusted-key** command.

4.2.2. Configuring the Global NTP Authentication Key

The next step to configure the global security authentication for the NTP is to set the global authentication key.

Each key is identified by a globally unique key-id. You can use the **ntp trusted-key** command to set the key corresponding to the key-id as a global trusted key.

Use the following commands in global configuration mode to specify a global authentication key.

Command	Function
ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	Specifies a global authentication key. *key-id*: sets the parameter in the range 1 to 4294967295. *key-string*: sets the parameter to any values. *enc-type*: sets the parameter to **0** or **7**.
no ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	Removes a global authentication key.

The global authentication key takes effect after being configured as a global trusted key.

⚠ Caution

Qtech's current NTP version supports up to 1024 authentication keys, but only one key can be set for each server for encrypted communication.

4.2.3. Configuring the Global NTP Trusted key ID

The last step is to set a global authentication key as a global trusted key. Only by this trusted key you can send encrypted data and check the validity of the packet.

Use the following commands to specify a global trusted key in global configuration mode.

Command	Function
ntp trusted-key *key-id*	Specifies a global trusted key ID.

Command	Function
no ntp trusted-key *key-id*	Removes a global trusted key ID.

The three steps are the basis of implementing the security authentication mechanism. To initiate encrypted communication between the NTP client and the NTP server, a trusted key must be set for the corresponding server.

⚠ Caution When a global authentication key is removed, its trusted information is also removed.

4.2.4. Configuring the NTP Server

No NTP server is configured by default. Qtech's client can simultaneously interact with up to 20 NTP servers, and one authentication key can be set for each server to initiate encrypted communication with the NTP server after relevant settings of global authentication and keys are completed.

NTP version 3 is used in communication with the NTP server by default. NTP version 3 enables you to specify the source interface for sending the NTP packet and configure that the NTP packet from the relevant server can only be received on the sending interface at the same time.

Use the following commands to configure the NTP server in global configuration mode.

Command	Function
ntp server ip-addr [**version** *version*] [**source** *if-name number*] [**key** *keyid*] [**prefer**]	Configures the NTP server. version (NTP version number): sets the parameter in the range 1 to 3 if-name (interface type): sets the parameter to **Aggregateport, Dialer GigabitEthernet**, **Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template,** or **VLAN.** keyid: sets the parameter in the range 1 to 4294967295.
no ntp server *ip-addr*	Removes the NTP server.

The NTP client can initiate the encrypted communication with the NTP server only when the global security authentication and key setting mechanisms are completed and the trusted key for communicating with the server is set. To this end, the NTP server should have the same trusted key.

4.2.5. Disabling the Function of Receiving the NTP Packet on the Interface

Use this command to disable the function of receiving the NTP packet on the interface for time synchronization, which is available to the NTP client by default.

⚠ Caution This command takes effect only for the interface whose IP address can be configured to receive and send packets.

Use the following commands to disable the interface to receive the NTP packet in interface configuration mode.

Command	Function
interface interface-type number	Enters interface configuration mode.
ntp disable	Disables the function of receiving NTP packets on the interface.

To enable the function of receiving NTP packets on the interface, use the **no ntp disable** command in interface configuration mode.

4.2.6. Enabling or Disabling NTP

Use the **no ntp** command to disable the NTP synchronization service, stop the time synchronization, and clear relevant information of NTP configuration.

The NTP function is disabled by default, but may be enabled as long as the NTP server is configured.

Use the following commands to disable or enable the NTP in global configuration mode:

Command	Function
ntp authenticate or ntp server *ip-addr* [version *version*] [source *if-name number*] [*key keyid*] [*prefer*]	Enables NTP.
no ntp	Disables NTP.

4.2.7. Configuring the NTP Real-time Synchronization

To improve accuracy, eight consecutive packets are synchronized for the first synchronization between the client and the server. Follow-up NTP synchronization occurs automatically every one minute. To manually implement real-time synchronization during the auto-synchronization interval, you can use this command.

Use the following commands to configure the NTP real-time synchronization in global configuration mode.

Command	Function
ntp synchronization	Enables the NTP real-time synchronization.
no ntp synchronization	Disables the NTP real-time synchronization.

The synchronization is set to be implemented every 30 minutes on Qtech's client system. New servers will trigger the real-time synchronization, which is also be implemented when this command is used during the synchronization interval. However, the command is invalid during the auto-synchronization.

The command of disabling the real-time synchronization and the one that disables NTP can be used to end the time synchronization (during the synchronization) or disable the synchronization function (between the synchronization interval). The difference lies in that the NTP-disabling command disables the NTP synchronization as well as clears related NTP configuration.

Note

The NTP real-time synchronization is supported only by some products. The **ntp synchronize** command cannot be executed on products that do not support this function.

4.2.8. Configuring the NTP Update-Calendar

Use this command to enable the NTP client to update the calendar using the clock time synchronized from an external clock source.

Use the following commands to configure the NTP update-calendar in global configuration mode.

Command	Function
ntp update-calendar	Configures the update-calendar.
no ntp update-calendar	Disables the update-calendar.

The update-calendar is not configured by default. After configuration, the NTP client updates the calendar when the time synchronization of external clock source is successful. It is recommended to enable this function for keeping the accurate calendar.

4.2.9. Setting the NTP Master

Use this command to set the local clock as the NTP master (the reference source of the local clock is reliable), providing the synchronized time for other devices.

Generally, the local system synchronizes the time from the external clock source directly or indirectly. However, if the time synchronization of the local system fails for the network connection trouble, use the command to set the reliable reference source of the local time, providing the synchronized time for other devices.

Once set, the system time can not be synchronized to the clock source with higher stratum.

Note

NTP uses stratum to describe the hops between the device and the authorization clock. A time server with 1 stratum shall have a directly connected atomic clock or radio wave clock. A time server with the 2 stratums obtains time from the stratum 1 server and a time server with 3 stratums obtains time from the stratum 2 server and so on. Therefore, the clock source with the lowest stratum value is more precise than others.

Use the following commands to configure the NTP master in global configuration mode:

Command	Function
ntp master [*stratum*]	Sets the local time as the NTP master and specifies the corresponding stratum. The time stratum is in the range 1 to 15. The default value is 8.
no ntp master	Cancels the NTP master setting.

The following example shows how to set the reliable reference source of the local time and set the time stratum to 12:

```
Qtech(config)# ntp master 12
```

Caution

Be careful when using this command. Using this command to set the local time as the master (in particular, specify a lower stratum value), is likely to cover the effective clock source. If multiple devices in the same network use this command, time synchronization instability may occur due to time difference between the devices.

Caution

In addition, before using this command, if the system has never been synchronized with an external clock source, it is necessary to manually calibrate the system clock to prevent too much bias. (For more information, see the section about system time configuration in the *Basic Host management Configuration Guide*.)

4.2.10. Configuring the Access Control Privilege of NTP Service

The NTP service access control function provides a minimal security measure (a more secure way is to use the NTP authentication mechanism). By default, no NTP access control rules are configured in the system.

Use the following commands to set the NTP services access control privilege in global configuration mode.

Command	Function
ntp access-group { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*	Sets the access control privilege of the local service.
no ntp access-group { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*	Cancels the settings of access control privilege of the local service.

peer: allows the time requests and control queries for the local NTP service as well as the time synchronization between the local device and the remote system (full access privilege).

serve: allows the time requests and control queries for the local NTP service, not the time synchronization between the local device and the remote system.

serve-only: allows the time requests for the local NTP service.

query-only: allows the control queries for the local NTP service.

access-list-number: indicates the IP access control list label in the range of 1 to 99 and 1300 to 1999. For how to create IP access control list, see the *Access Control List Configuration Guide*.

access-list-name: indicates the IP access control list name. For how to create IP access control list , see the *Access Control List Configuration Guide*.

When an access request arrives, the NTP service matches the rules from the smallest to the largest access restriction, and the first matched rule shall prevail. The matching order is *peer*, *serve*, *serve-only*, and *query-only*.

Caution

The control query function (used by the network management device to control the NTP server, such as setting the leap second mark or monitoring the working state) is not supported in the current system. Although it matches with the order in accordance with the preceding rules, requests related to the control query function are not supported.

If you do not configure any access control rules, all accesses are allowed. Once the access control rules are configured, only the rule that allows access can be carried out.

The following example shows how to allow the peer device in acl1 to control the query, request for and synchronize the time with the local device; and limit the peer device in acl2 to request the time for the local device.

```
Qtech(config)# ntp access-group peer 1
Qtech(config)# ntp access-group serve-only 2
```

4.3. Showing NTP Information

4.3.1. Debugging NTP

Use this command to debug NTP for diagnosis and troubleshooting,.

Use the following commands to enable or disable the function of debugging NTP in privilege mode.

Command	Function
debug ntp	Enables the debugging function.
no debug ntp	Disables the debugging function.

4.3.2. Showing NTP Information

Use the **show ntp status** command in privilege mode to show the current NTP information.

Use the following command to show the NTP status information in privilege mode.

Command	Function
show ntp status	Shows the current NTP information.

This command be used to print the shown information only when the relevant communication server is configured.

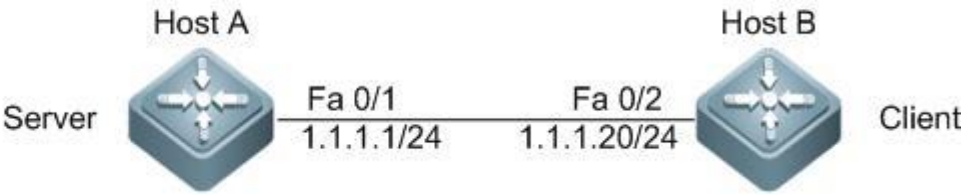
```
Qtech# show ntp status
Clock is synchronized, stratum 9, reference is 192.168.217.100
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is AF3CF6AE.3BF8CB56 (20:55:10.000 UTC Mon Mar 1 1993)
clock offset is 32.97540 sec, root delay is 0.00000 sec
root dispersion is 0.00003 msec, peer dispersion is 0.00003 msec
```

Note *stratum* indicates the level of current clock;
reference indicates the address of the server used for synchronization;
freq indicates the clock frequency of current system;
precision indicates the precision of current system clock;
reference time indicates the UTC time of reference clock on the synchronization server;
clock offset indicates the offset of current clock;
root delay indicates the delay of current clock,
root dispersion indicates the precision of top server;
peer dispersion indicates the precision of synchronization server.

4.4. Typical NTP Configuration Examples

4.4.1. Configuring NTP Client or Server Mode

4.4.1.1. Topological Diagram



NTP client or server model

4.4.1.2. Application Requirements

On Host A, the local clock is configured as the NTP master clock, with the clock stratum being 12;
Host B is configured as the NTP client and Host A is specified as the NTP server;
The hardware clock of Host B shall be synchronized as well.

4.4.1.3. Configuration Tips

NTP server

Generally, the local system will directly or indirectly synchronize with the external clock sources. However, the local system may not be able to synchronize with the external clock sources due to the network connection failure. In this case, you can use the **ntp master** command to configure the local clock as NPT master to synchronize time to other devices.

NTP client

Configure the NTP server

By configuring the NTP update-calendar, the NTP client can use the clock value synchronized from external clock sources to update its calendar for accuracy.

4.4.1.4. Configuration Steps

Configuration of the NTP server

! Configure the NTP master. Configure local clock as the trusted reference clock source, with the clock stratum being 12.

```
HostA(config)# ntp master 12
```

Configuration of the NTP client

! Configure Host A as the NTP server.

```
HostB(config)#ntp server 1.1.1.1
```

! Configure NTP hardware clock update

```
HostB(config)# ntp update-calendar
```

4.4.1.5. Verification

Verify the time before configuring NTP synchronization.

! Verify the time of reference clock source.

```
HostA#show clock
17:12:48 UTC Tue, Sep 8, 2009
```

! Verify the time of client before synchronization.

```
HostB#show clock
12:01:10 UTC Sat, Jan 1, 2000
```

! Verify the NTP status of client before synchronization.

```
HostB(config)#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**0
reference time is 0.0 (00:00:00.000 UTC Thu, Jan 1, 1970)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00000 msec, peer dispersion is 0.00000 msec
```

The output shows that the time hasn't been synchronized.

After configuring NTP synchronization, show NTP configurations. Key points: the NTP server address and stratum.

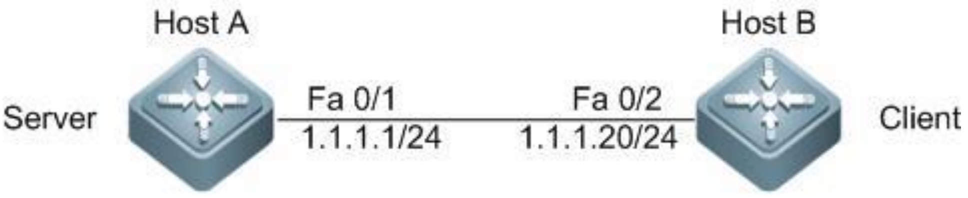
The following log information will be displayed on CLI interface:

```
*Sep  8 18:10:37: %SYS-6-CLOCKUPDATE: System clock has been updated to 18:10:37 UTC
Tue Sep  8 2009.
HostB#show ntp status
Clock is synchronized, stratum 13, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE511CC9.37EB5B2D (18:11:21.000 UTC Tue, Sep 8, 2009)
clock offset is -0.00107 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

The output shows that the NTP client has connected to the server and the time of Host B has been synchronized with the time of Host A, with the stratum level being higher than that of Host A by 1 (i.e., 13).

4.4.2. Configuring NTP Client or Server Mode with Authentication

4.4.2.1. Topological Diagram



NTP client/server model

4.4.2.2. Application Requirements

On Host A, the local clock is confiugred as the NTP master clock, with the clock stratum being 12;
Host B is configured as the NTP client and Host A is specified as the NTP server;
The authentication mechanism is enabled to prevent illegal users from maliciously attacking the clock server.

4.4.2.3. Configuration Tips

Configuring NTP server/client authentication will involve the following steps:

Enable NTP global authentication.
Configure the key for NTP global authentication and the corresponding key ID.
Specify NTP global trusted key ID.

The authentication key used by NTP client to communicate with NTP server must be consistent with the corresponding Key ID.

4.4.2.4. Configuration Steps

Configuration of the NTP server

Step 1: Configure the NTP master. Configure the local clock as the trusted reference clock source, with the clock stratum being 12;

```
HostA(config)#ntp master 12
```

Step 2: Configure NTP authentication;

! Enable NTP global authentication.

```
HostA(config)# ntp authenticate
```

! Configure the NTP global authentication key as **helloworld** and the corresponding key ID as **6**.

```
HostA(config)# ntp authentication-key 6 md5 helloworld
```

! Specify **6** as the NTP global trusted key ID

```
HostA(config)# ntp trusted-key 6
```

Configuration of the NTP client

Step 1: Configure NTP authentication;

! Enable NTP global authentication.

```
HostB(config)# ntp authenticate
```

! Configure NTP global authentication key as **helloworld** and the corresponding key ID as **6**.

```
HostB(config)# ntp authentication-key 6 md5 helloworld
```

! Specify **6** as the NTP global trusted key ID.

```
HostB(config)# ntp trusted-key 6
```

! Configure Host A as the NTP server and set the key ID for communicating with this server as **6**.

```
HostB(config)# ntp server 1.1.1.1 key 6
```

4.4.2.5. Verification

Verify the configurations of NTP server. Key points: the NTP master clock configuration, NTP server's IP address, and authentication related configurations.

```
HostA#show run
!
interface fastEthernet 0/1
ip address 1.1.1.1 255.255.255.0
!
ntp authentication-key 6 md5 07360623191d300a004609 7
ntp authenticate
ntp trusted-key 6
ntp master 12
!
```

Verify the configurations of NTP client. Key points: the IP address and key ID of NTP server, and authentication related configurations.

```
HostB #show run
!
interface fastEthernet 0/2
 ip address 1.1.1.20 255.255.255.0
!
ntp authentication-key 6 md5 141a4f012d1d3c23174905 7
ntp authenticate
ntp trusted-key 6
ntp server 1.1.1.1 key 6
!
```

After proper configurations, the following log information will be displayed on the CLI:

```
*Sep  9 11:31:29: %SYS-6-CLOCKUPDATE: System clock has been updated to 11:31:29 UTC
Wed Sep  9 2009.
```

The log information indicates that the clock of HostB (NTP client) has been updated.

Verify NTP server status.

```
HostA #show ntp status
Clock is synchronized, stratum 12, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE521261.E52DECA2 (11:39:13.000 UTC Wed, Sep 9, 2009)
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

Verify NTP client status. Key points: the NTP server address and stratum.

```
HostB# show ntp status
Clock is synchronized, stratum 13, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is CE5212A1.E5D712A0 (11:40:17.000 UTC Wed, Sep 9, 2009)
clock offset is -0.00005 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

The output shows that the NTP client has successfully connected to the server and the time of Host B has been synchronized with that of Host A, with the stratum level being higher than that of Host A by 1 level (i.e., 13).

5. CONFIGURING SNTP

5.1. Overview

Network Time Protocol (NTP) is designed for time synchronization on network devices. Another protocol, the Simple Network Time Protocol (SNTP) can also be used to synchronize the network time.

NTP can be used across various platforms and operating systems, provide precise time calculation (1-50 ms precision), and prevent from latency and jitter in the network. NTP also provides the authentication mechanism with a high security level. However, the NTP algorithm is complicated and demands delicate systems.

As a simplified version of NTP, SNTP simplifies the algorithm of time calculation while maintains great performance, with the precision about 1s.

The SNTP client is totally compatible with the NTP server due to the consistency between the SNTP and NTP packets.

5.1.1. Understanding SNTP

SNTP works in client/server mode. The standard server system time is set by receiving the GPS signal or the atomic clock. The client obtains its accurate time from the service time accessing the server regularly, and adjusts its system clock to synchronize the time.

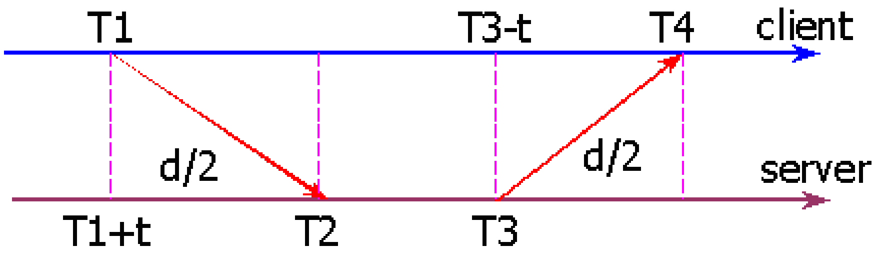


Figure-1

Originate Timestamp	T1	Time request sent by client

Receive Timestamp	T2	Time request received at server
Transmit Timestamp	T3	Time reply sent by server
Destination Timestamp	T4	Time reply received at client

T1: Time request sent by client (refer to the client time) with the mark “Originate Timestamp”;

T2: Time request received at server (refer to the server time) with the mark “Receive Timestamp”;

T3: Time reply by server (refer to the server time) with the mark “Transmit Timestamp”;

T4: Time reply received at client (refer to the client time) with the mark “Destination Timestamp”.

T: Time offset between the server and the client

d: Round-tour time between the server and the client

The following formula calculates the time:

```
∵ T2 = T1 + t + d / 2;
∴ T2 - T1 = t + d / 2;
∵ T4 = T3 - t + d / 2;
∴ T3 - T4 = t - d / 2;
∴ d = (T4 - T1) - (T3 - T2);
t = ((T2 - T1) + (T3 - T4)) / 2;
```

Then, according to the value of *t* and *d*, the SNTP client gets the current time: T4 + t.

5.2. Configuring SNTP

This chapter describes how to configure SNTP.

5.2.1. Default Configuration

The following table describes the default SNTP configurations.

Function	**Default**
SNTP state	Disabled
IP address for the NTP server	0
SNTP Sync Interval	1800 seconds
Local Time-zone	GMT + 3

5.2.2. Enabling SNTP

Enter privileged mode and perform the following steps to enable the SNTP:

Enter global configuration mode:

```
Qtech# config
```

Enable the SNTP and synchronize the time once immediately. The time will be immediately synchronized if this command is entered and regular synchronization is unnecessary. (in order to prevent frequent time synchronization, the sync-interval must not be less than 5 seconds)

```
Qtech(config)# sntp enable
Return to privileged mode:
Qtech(config)# End
```

Show the current configuration:

```
Qtech# show running-config
```

Save the configuration:

```
Qtech# copy running-config startup-config
```

To disable the SNTP, use the **no sntp enable** command.

5.2.3. Configuring the IP address of the SNTP Server

The SNTPclient is totally compatible with the NTP server due to the consistency between SNTP and NTP packets. There are many NTP servers in the network, and you can choose one with less latency.

For the detailed NTP server ip addresses, please log on to http://www.ntp.org/. For example, 192.43.244.18 (time.nist.gov).

Enter privileged mode and perform the following steps to specify an IP address for the SNTP server:

Enter global configuration mode:

```
Qtech# config
```

Specify the IP address for the SNTP server.

```
Qtech(config)# sntp server <ip-addr>
```

Return to privileged mode:

```
Qtech(config)# End
```

Show the current configuration:

```
Qtech# show running-config
```

Save the configuration:

```
Qtech# copy running-config startup-config
```

5.2.4. Configuring the SNTP Synchronization Interval

To adjust the time regularly, you need to set the synchronization interval for SNTP client to access the NTP server SNTP client regularly. Perform the following steps to set the sync interval for the device and the NTP server:

Enter global configuration mode:

```
Qtech# config
```

Configure the SNTP sync interval, in second.

Interval range: 60-65535s; Default value: 1800s.

```
Qtech(config)# sntp interval <seconds>
```

Return to privileged mode:

```
Qtech(config)# End
```

Show the current configuration:

```
Qtech# show running-config
```

Save the configuration:

```
Qtech# copy running-config startup-config
```

⚠ Caution

The synchronization interval configuration cannot take effect immediately unless you execute the **sntp enable** command immediately after configuring the synchronization interval.

5.2.5. Configuring the Local Time Zone

Greenwich Mean Time (GMT) is obtained through the SNTP communication. To obtain the accurate local time, you need to set the local time to adjust the mean time.

Enter global configuration mode:

```
Qtech# config
```

Configure the time-zone, ranging from GMT-23 to GMT+23, wherein “-” indicates western area, “+” indicates eastern area. For example "3" indicates the 3th eastern time zone, "-3" indicates the 3th western time zone and “0” indicates Greenwich mean time. Universal Time Coordinated (UTC) is the default time zone name and the default value is **0**.

```
Qtech(config)# clock timezone <time-zone>
```

Return to privileged mode:

```
Qtech(config)# end
```

Show the current configuration:

```
Qtech# show running-config
```

Save the configuration:

```
Qtech# copy running-config startup-config
```

To restore the local time-zone to the default, use the command **no clock time-zone**.

5.3. Showing SNTP Information

The procedure is as follows:

Show related SNTP parameters:

```
Qtech# show sntp
```

Use the **show sntp** command to show configured SNTP parameters:

```
Qtech# show sntp
SNTP state                   : ENABLE           //to view whether SNTP is enabled or
not
SNTP server                  : 192.168.4.12   //NTP Server
SNTP sync interval         : 60             //SNTP sync interval
Time zone                : +3                 //Local Time-zone
```

6. CONFIGURING UDP-HELPER

6.1. Understanding UDP-Helper

6.1.1. Overview

UDP-Helper relays and forwards User Datagram Protocol (UDP) broadcast packets. As a relay, UDP-Helper can convert the UDP broadcast packets into the unicast packets and then forward them to the specified destination server by configuring the destination server for the UDP broadcast packets to be forwarded.

Once enabled, UDP-Helper checks whether the destination UDP port number of the received packet matches the port number to be forwarded to. If yes, it modifies the destination IP address of packets as the IP address of the specified destination server, and sends the packet to the destination server in unicast form.

When UDP-Helper is enabled, the broadcast packets from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

Note

The BOOTP/DHCP broadcast packet is relayed through the UDP Port 67 and 68 by the DHCP Relay module; therefore, the two ports cannot be configured as the relay port of UDP-Helper.

6.2. Configuring UDP-Helper

6.2.1. Default Configuration

The following table describes the default configuration.

Attribute	Default value
Relay and forwarding	Disabled
UDP port for relay and forwarding	Indicates that the UDP broadcast packets from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default when UDP-Helper is enabled.
Destination server for delay and forward	None

6.2.2. Enable the Relay and Forward Function of UDP-Helper

Command	**Function**
Qtech(config)# **udp-helper Enable**	Enables the relay and forward function of UDP broadcast packets. This function is disabled by default.

To disable this function ,sue the **no udp-helper enable** command.

Note This function is disabled by default.

Note When UDP-Helper is enabled, the broadcast packets from UDP Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

Note When UDP-Helper is disabled, all of the configured UDP ports including the default ports are cancelled.

6.2.3. Configuring the Destination Server for Relay and Forwarding

Command	**Function**
Qtech(config-if)# **ip helper-address** *IP-address*	Configures the destination server to which the UDP broadcast packets are relayed and forwarded. By default, it is not configured.

To remove the destination server for relay and forwarding, use the **no ip helper-address** command.

Note At most 20 destination servers can be configured for an interface.

Note If the destination server for relay and forwarding is configured on a specified interface and UDP-Helper is enabled, the broadcast packets of the specified UDP port received from this interface will be sent to the destination server configured for this interface in unicast form.

6.2.4. Configuring the UDP Port for Relay and Forwarding

Command	**Function**
Qtech(config)# **ip forward-protocol udp** [*port*]	Configures the UDP port for relay and forwarding. If only the UDP parameter is specified, the default port will be used for relay and forwarding; otherwise, the port can be configured if necessary. When UDP-Helper is enabled, the broadcast packets from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

To disable the UDP port for relay and forwarding, use the **no ip forward-protocol udp** [*port*] command.

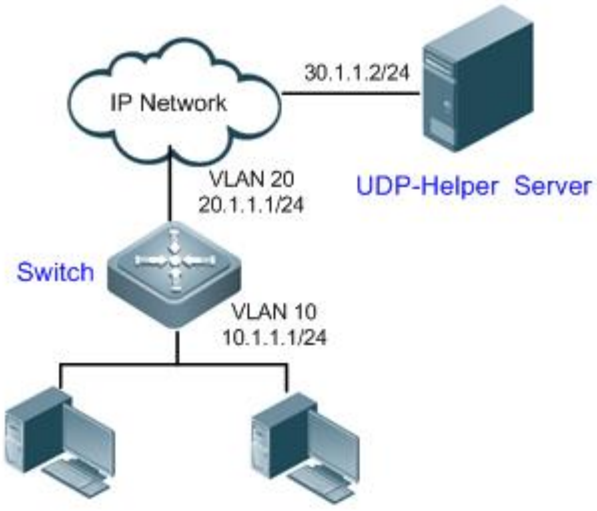
Note The UDP port can be configured for relay and forwarding. Otherwise, the error prompts will appear only when the function of delay and forwarding is enabled for UDP-Helper and the destination server is configured for the relay and forwarding.

Note

When the relay and forwarding function of UDP-Helper is enabled, the function of forwarding the broadcast UDP packets from the default ports 69, 53, 37, 137, 138 and 49 will be enabled immediately without any configuration.
At most 256 UDP ports are supported for relay and forwarding by the switch.
You can use both the **ip forward-protocol udp domain** and **ip forward-protocol udp** *53* commands to configure default ports.

6.3. Configuration Examples

6.3.1. Topology Diagram



Topology diagram for UDP-Helper configuration

6.3.2. Application Requirements

The network device can forward UDP broadcast packets with destination port being 1000 to the specified UDP-Helper server (with server IP being 30.1.1.2/24).

6.3.3. Configuration Tips

Configure UDP-Helper relay and forwarding as follows:

Enable UDP-Helper relay forwarding.

Configure the destination server of UDP-Helper relay forwarding.

Configure the destination port number of UDP broadcast packets for relay forwarding (in this example, UDP broadcast packets with destination port being 1000 are subject to relay forwarding; meanwhile, the device will by default forward UDP broadcast packets containing destination port numbers of 69, 53, 37, 137, 138 and 49).

Note

The UDP port for relay forwarding can only be configured after UDP-Helper relay forwarding is enabled and the destination server is configured; otherwise, error messages will be displayed.
After UDP relay forwarding is enabled, the device will immediately forward UDP broadcast packets containing the default port numbers of 69, 53, 37, 137, 138 and 49 without further configuration.

6.3.4. Configuration Steps

Before configuring relevant features of UDP-Helper, make sure that the route from the switch to the network segment of UDP-Helper server is reachable. The IP addresses configured on respective interfaces are shown in the topological diagram. Here we will introduce how to configure relevant features of UDP-Helper.

Step 1: Enable UDP-Helper relay forwarding on the network device

```
Qtech(config)#udp-helper enable
```

Step 2: Configure the IP address for the destination server of UDP-Helper relay forwarding as 30.1.1.2 on fastEthernet 1/1.

```
Qtech(config)# interface fastEthernet 1/1
Qtech(config-if-VLAN 10)#ip address 10.1.1.1 255.255.255.0
Qtech(config-if-VLAN 10)# ip helper-address 30.1.1.2
Qtech(config-if-VLAN 10)#exit
```

Step 3: Configure the Switch to forward UDP broadcast packets carrying the destination port number 1000.

```
Qtech(config)#ip forward-protocol udp 1000
```

6.3.5. Verification

Verify configurations of the switch. Key points: whether relay forwarding is enabled or not; IP address of relay server; destination port number carried in UPD broadcast packets requiring relay forwarding.

```
Qtech#show run
!
udp-helper enable
!
ip forward-protocol udp 1000
!
interface fastEthernet 0/1
 ip address 10.1.1.1 255.255.255.0
!
interface fastEthernet 1/1
ip helper-address 30.1.1.2
 ip address 20.1.1.1 255.255.255.0
!
```

Verify whether relay forwarding has taken effect.

Step 1: Send UDP broadcast packets carrying the destination port number 999.

PC1 sends a UDP broadcast packet of the following format:

```
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
Dst_ip:255.255.255.255
Dst_port:999
PC2 acts as UDP-Helper server. Such packet is not received on PC2.
Step 2: Send UDP broadcast packets carrying the destination port number of 1000.
PC1 sends a UDP broadcast packet of the following format:
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
Dst_ip:255.255.255.255
Dst_port:1000
PC2 acts as UDP-Helper server. Such packet is received on PC2. The destination
IP address of packet is 30.1.1.2, and the data contained are the same as the
packets sent.
```

Step 3: Send UDP broadcast packets with destination port number 69, 53, 37, 137, 138 or 49.

PC1 sends a UDP broadcast packet of the following format (taking destination port number of 69 as the example):

```
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
```

```
Dst_ip:255.255.255.255
Dst_port:69
```

PC2 acts as UDP-Helper. Such packet is received on PC2. The destination IP address of packet is 30.1.1.2, and the data contained are the same as the packets sent.

From the verification output, we can learn that the switch has successfully forwarded UDP broadcast packets with the user-defined destination port number (destination port number 1000 and default numbers of 69, 53, 37, 137, 138, and 49) to the specified UDP-Helper server.

7. CONFIGURING IPFIX

7.1. Overview

IP Flow Information eXport (IPFIX), is a standard protocol published by the Internet Engineering Task Force (IETF) for the netflow measurement. It standardizes the format of the network traffic statistics. IPFIX is applicable to network devices and management system platforms of any manufacturers, and is used to export the flow statistics by network device. On one hand, IPFIX allows an administrator to easily extract and view the important flow information stored in the network device. On the other hand, it is unnecessary for the administrator to upgrade the network device software or management tools if the flow monitoring requirement changes as the export format is extensible.

IP flow information is transmitted from an export device (router, switch, or network sniffer device) to the collector. Different data formats are defined to meet different requirements, because IPFIX is a highly-scalable template-based format for the data export.

To export the complete data, seven key fields are adopted to represent each network flow: source IP address, destination IP address, source port, destination port, Layer-3 protocol type, byte of Type-of-service, and input logical interface. If all those seven key fields of different IP packets are matched, then all the IP packets belong to the same flow. Network optimization, security detection and traffic accounting can be performed according to the current network application information about recorded features of the netflow, such as flow duration, and the average length of the packet in the flow.

7.1.1. Basic Concept

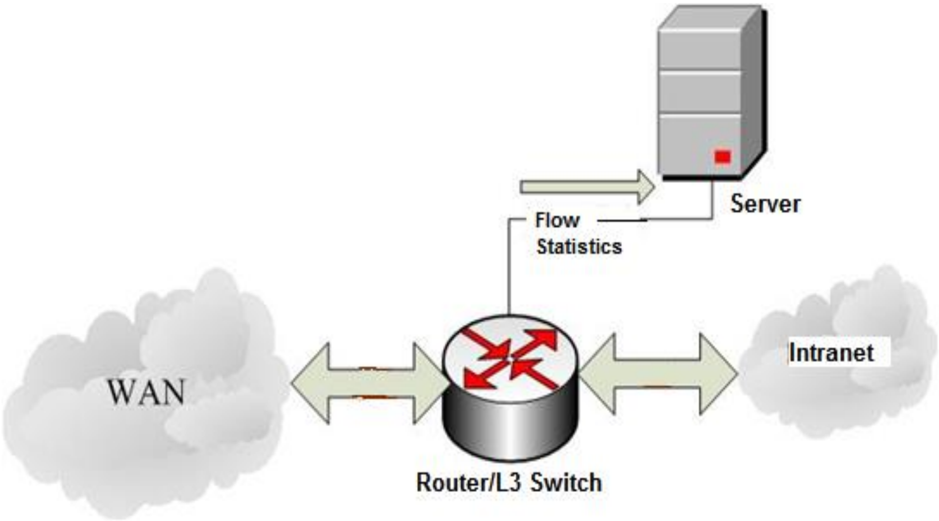
Template: Defines the recorded data format, including a series of data bit domain fields, each of which contains the data type of the data bit domain and the data length. You can parse the recorded data according to the template. If you want to add a data field you are interested in to the data record, you only need to add the corresponding data bit domain field to this template, without modifying the management software.

Collector: Receives the IP flow information generated from the network device. The collector analysis is based on the received data template and data records, and it clearly shows flow information in graphics or tables and saves the information to the database for further use.

7.1.2. IPFIX Application

The router/switch enabled with the IPFIX flow statistics function can collect the statistics on lots of information of packets, including the Layer-3 protocol type, the transport layer port, source/destination address, and service type. The information can be widely used in application scenarios such as user detection, network analysis and planning, security analysis, traffic accounting, and network traffic engineering. Figure-1 shows a typical application topology.

Figure-1



7.1.3. Network Application and User Detection

The IPFIX traffic statistics feature allows you to view detailed, real-time, application-based, and current network usage. It allows you to reasonably allocate and optimize the network resources, and provides the capability of real-time detection of the network capacity. With the IPFIX flow detection function, you can easily understand the network usage and plan to limit the usage combined with other functions such as the Access Control List (ACL). IPFIX can also help effectively and quickly solve some potential security problems.

7.1.4. Network Planning

The IPFIX flow statistics function can detect netflow information over a long period and track network trends. The data enables you to predict network changes and optimize upgrade plans of various networks effectively. It minimizes network costs, but maximizes network performance, capacity and stability. IPFIX can also detect unwanted traffic in Wide Area Network (WAN) and redundant bandwidth and quality of service (QoS) usage. The IPFIX flow statistics function offers valuable information for reducing the cost of operating the network. For example, when the traffic over a WAN link increases, generally you will increase the investment to upgrade the link. However, the traffic increase is possibly attributed to some illegal usage such as BT download. IPFIX enables you to find out the real reason, modify the network usage policy and solve the problem, and thus preventing unnecessary network upgrade.

7.1.5. Security Analysis and Attack Detection

You can use the export flow record of the IPFIX flow statistics to identify denial of service (DoS) attacks, viruses and worms in real-time. Anomalistic changes in network behaviors are clearly reflected in flow records. Take DoS attack for example, its feature is to send a bulk of IP packets (different from the ordinary ones) in the network from untrusted source addresses to the same destination address. Combined with other network control methods (ACL and QoS), the IPFIX flow statistics function can prevent malicious network attack effectively by collecting the source address, destination address, protocol number, port number and size of these packets and sending the information to the collector for network security experts or software analysis.

7.1.6. Flow Accounting

The IPFIX flow statistics function measures the flows in a network in a fine granularity way, including the source/destination IP address, number of packets, total bytes, timestamp, QoS and application ports. Internet Service Providers (ISPs) can utilize the information for accounting based on time, bandwidth, application or network service quality.

7.2. IPFIX Function

Note Qtech IPFIX function is implemented based on the multi-service card only.

7.2.1. Understanding the IP Packet Flow

A packet flow is a series of consecutive packets of the same attributes and pass a same detection point in a period. The packets belong to a same flow have some same attributes, which can be some fields in the head of the IP packets, such as source IP address, Tos field and any combination of those fields. The key fields defining the packet flow are not fixed. For Qtech switches, a netflow is defined as the unidirectional packet flow with the same source and destination. To be precise, a netflow is determined by the combination of the following key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer-3 protocol type
- Tos
- Input logical interface
- VRF

Those eight key fields determine a unique flow. If one key field of a packet is different from that of another packet, they belong to different flows. A flow record also includes other statistical fields, such as the packet number, the next-hop IP address, total flow byte number, etc. For each probe packet, ascertain the flow records first, and record the corresponding information stored in the main cache. The flow record cache is used to store the IP flow information, including the main cache and the flow aggregation cache.

7.2.2. Understanding the Main Cache

The main cache is used to store the raw IP flow information, using seven keywords to match the flow statistics. The IPFIX export mechanism records the flow information and sends it to the configured collector. For an IP packet, first search for the corresponding flow record from its keyword in the main cache: if no flow record exists, create a new one; and if the flow record exists, then update the flow statistical information, such as the packet number, flow bytes, etc. The cache capacity is limited; therefore, the aging mechanism of the flow record is set. The following conditions are used to determine whether a flow is aged out or not:

If no packets belong to the flow are detected in a certain period of time (the non-active time), this flow has been aged and shall be exported.
The flow information cannot be recored indefinitely for it persists for a too long time, which exceeds the set active time, then this flow shall be aged.

When it needs to export the aged flow record, the flow information shall be encapsulated as User Datagram Protocol (UDP) packets and sent to the set collector on the server for processing. The collector is the software tool for processing the flow record, and can display the visualized current network status and analyze the netflow according to the received flow record information.

7.2.3. Understanding the Format of the Flow Export Packet

The format of the flow record export packet is the IPFIX standard format. The IPFIX standard format is based on the template, and easy to extend. When encapsulating the data record, first create the format template of the data record, which defines the filed type and length of the data record. For each data record, use the template to identify and explain the analytical format. To add a new field to the date record, you only need to re-create the corresponding data template rather than to upgrade the software, which greatly improves the scalability.

On Qtech routers, IPFIX supports the exporting of netflow packet formats of version 9 and version 10, and supports the netflow software versions ManageEngine_NetFlowAnalyzer_7001 and ManageEngine_NetFlowAnalyzer_8000. However, the netflow software version ManageEngine_NetFlowAnalyzer_9100 may be problematic on Qtech routers, because the deployed template is different from Cisco's template.

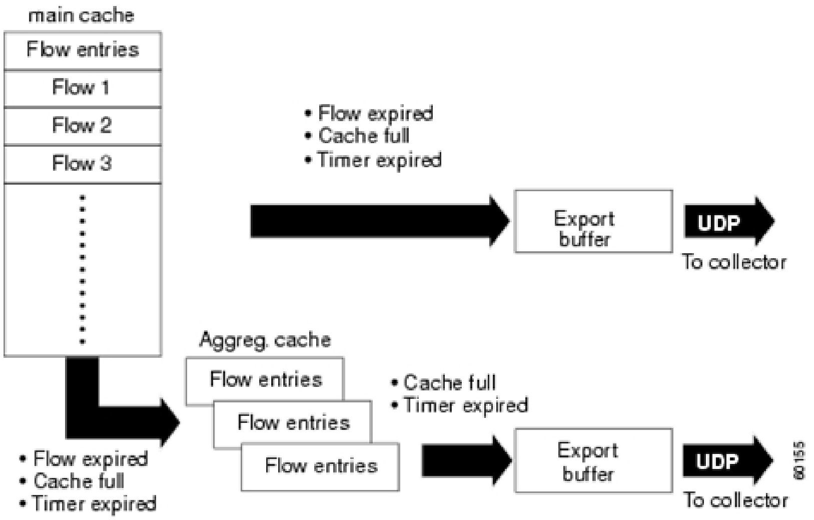
7.2.4. Understanding Flow Aggregation Mode

Similar to main mode, flow aggregation mode also deals with the netflow statistics. The only difference is that the main mode acquires the original packet to generate and export the flow record, while flow aggregation mode reprocesses the flow record to generate and export the new record of the flow aggregation.

Such processing meets requirements of using different key fields to reprocess flow records and generate the required flow records in different flow aggregation modes. As described in the preceding sections, a flow consists of packets of the same attributes, and the attributes can be the combination of any fields in packet headers. In the software, seven keywords differentiate flows, and you can select any seven fields in packet headers to reprocess flow records. For example, to know Layer-3 packet distribution, you can use Layer-3 protocol ID as the key field to aggregate flow records exported in main mode and obtain the required flow information.

Similar to the main mode, flow aggregation mode requires the cache to store the current statistical flow information. The flow aggregation function maps the export flow record in the main cache to the corresponding flow record in the flow aggregation cache, updates the flow aggregation record and regularly checks whether the flow aggregation record expires. Once expired, the flow aggregation record must be exported. Figure-2 shows the principle..

Figure-2:



7.2.5. Configuring the Flow Record Export in Main Mode

When a flow record in the main cache expires, the software uses the export mechanism to encapsulate the expired flow record to a UDP packet and sends the UDP packet to the configured server. Meanwhile, to prevent the loss of the template carrying the flow record because of unrelizable transmission over UDP, it requires for the regular template retransmission to ensure the successful receiving of the data template.

7.2.6. Configuring the Export Destination IP Address and Port

Up to two export servers can be set at the same time to improve the reliability of flow information transmission.

Use the following commands to configure the export server.

Command	Function
Qtech> **enable**	Enters privileged command mode.
Qtech# **config terminal**	Enters global configuration mode.
Qtech(config)# **ip flow-export destination** *ip-address udp-port* [**vrf** [*vrf-name*]]	Configures the destination IP address and destination port of the flow export, and VRF.
Re-execute the third command	Configures the destination IP addresses and destination ports of multiple flow exports.
Qtech(config)# **end**	Returns to privileged command mode.
Qtech# copy running-config startup-config	Saves the configuration.

To remove the flow export, use the **no ip flow-export destination** *ip-address udp-port* [**vrf** [*vrf-name*]] command.

Configuration example

```
Qtech# config terminal
Qtech(config)#ip flow-export destination 192.168.217.76 1111
Qtech(config)#ip flow-export destination 192.168.217.76 2222
%Warning: Second destination address is the same as previous address 192.168.217.76
Qtech(config)#ip flow-export destination 192.168.217.76 3333
%Exceeded maximum export destinations
Qtech(config)# end
Qtech products display error information when the third export destination is
configured.
```

⚠ Caution

By default, no flow export is set in the system. The flow record will be saved in the device for checking instead of being exported.

7.2.7. Configuring the Export Source IP Address

A device can have multiple IP addresses, so the IP address on one port can be specified as the source IP address for the sent packet when exporting the flow record.

Use the following commands to configure the source IP address.

Command	Function
Qtech> **enable**	Enters privileged command mode.
Qtech# **config terminal**	Enters global configuration mode.
Qtech(config)# **ip flow-export source** *interface-number*	Configures the export source IP address as the IP address for an interface.
Qtech(config)# **end**	Returns to privileged command mode.
Qtech# copy running-config startup-config	Saves the configuration.

Configuration example

```
Qtech# config terminal
Qtech(config)# ip flow-export source gigabitEthernet 6/2
Qtech(config)# end
Qtech#
```

The example uses the IP address of g 6/2 as the source address.

⚠ Caution

By default, the default system IP address is used as the source IP address when sending the packets in the system.

⚠ Caution

An IP address must have been configured for the port designated as the source address.

7.2.8. Configuring the Related Parameters of the Export Template

Before exporting the netflow data, the corresponding data template shall be sent to the server. UDP, an unreliable protocol, may result in the template loss and cause that the server fails to analyze the flow data correctly. Therefore, the retransmission mechanism is adopted to send the template. There are two RGOS retransmission mechanisms: 1. In the unit of packets, retransmit the template once each time sending *n* data packets; 2. In the unit of minutes, retransmit the template at every certain interval.

Use the following configuration commands.

Command	Function
Qtech> **enable**	Enters privileged command mode.

Qtech# **config terminal**	Enters global configuration mode.
Qtech(config)# **ip flow-export template refresh-rate** *packets*	Configures the retransmission packet number. The range is from 1 to 600. The default value is 20.
Qtech(config)# **ip flow-export template timeout-rate** *minutes*	Configures the retransmission interval, in minutes. The range is from 1 to 1000 minutes. The default value is 30 minutes.
Qtech(config)# **end**	Returns to privileged command mode.
Qtech(config)# **copy running-config startup-config**	Saves configurations.

Configuration example

```
Qtech# config terminal
Qtech(config)#ip flow-export template refresh-rate 30
Qtech(config)#ip flow-export template timeout-rate 40
Qtech(config)# end
Qtech#
```

In the example, *refresh-rate 30* indicates that the template is retransmitted every 30 packets, and *timeout-rate 40* indicates that the template is retransmitted every 40 minutes.

Caution By default, the retransmission packet refresh rate is 20, the time interval is 10 minutes.

7.2.9. Showing the Export Configurations in Main Mode

Use the **show ip flow export** command to display the current export configurations, including the export enable, export destination, the format of the flow record export packet, etc.

7.2.10. Configuring the Main Cache

The main cache is used to save the raw flow record information, and each flow entry size is fixed. A flow entry is created for each active flow in the system, with the record of flow characteristic and statistical information. All flow entries will be regularly checked for determining whether they have expired based on the following conditions:

1. The cache is full and no available space for the flow entries, so some entries shall expire.

2. A flow is inactive. By default, if a flow is not updated within 15 seconds, it becomes inactive.

3. A flow keeps active for too long time. By default, a flow shall expire if it has been active for 30 minutes.

The following introduces those configurable parameters.

7.2.11. Configuring the Flow Cache Entry Number

With the IPFIX flow statistics function enabled on a port, certain storage space is reserved for saving the flow entry in the main cache, which meets the user network demands generally. By default, 64K flow entries (with each entry size 64 bytes) are reserved, so it needs 4M memory space for the main cache. You can increase or decrease the entry number according to your needs to improve the performance or reduce the memory usage, which depends on your device memory size. Use the **ip flow-cache entries** *number* command to set the entry number in the cache.The range of *number* is from 1024 to 524288. The detailed configuration is described as follows.

Use the following configuration commands.

Command	**Function**
Qtech> **enable**	Enters privileged command mode.
Qtech# **config terminal**	Enters global configuration mode.
Qtech(config)# **ip flow-cache entries** *number*	Configures the entry number in the cache. The range is from 1024 to 524288.
Qtech(config)# **end**	Returns to privileged command mode.

Command	Function
Qtech# **copy running-config startup-config**	Saves the configuration.

To restore the entry number to the default value, use the **no ip flow-cache entries** command.

Configuration example

```
Qtech# config terminal
Qtech(config)#ip flow-cache entries 32768
Qtech(config)# end
```

Caution

By default, 65536 entries are in the main cache. With IPFIX enabled, the entry number configuration in the cache will take effect only after you re-enabling the IPFIX function. It is not recommended to change the entry number in the cache casually and inappropriately, which may result in abnormal system working.

7.2.11.1. Configuring the Flow Cache Timeout

Use the following command to set the flow cache timeout parameters.

Command	Function
Qtech> **enable**	Enters privileged command mode.
Qtech# **config terminal**	Enters global configuration mode.
Qtech(config)# **ip flow-cache timeout active** *minutes*	Configures the active aging time in minutes. The range is from 1 to 60 minutes.
Qtech(config)# **ip flow-cache timeout inactive** *seconds*	Configures the inactive aging time in seconds. The range is from 10 to 600 seconds.
Qtech(config)# **end**	Returns to privileged command mode.
Qtech# **copy running-config startup-config**	Saves the configuration.

By default, the active aging time is 30 minutes and the inactive aging time is 15 seconds. To restore the default value, use the **no ip flow-cache timeout active** command and the **no ip flow-cache timeout inactive** command.

Configuration example

```
Qtech# config terminal
Qtech(config)#ip flow-cache entries 32768
Qtech(config)#ip flow-cache timeout active 20
Qtech(config)#ip flow-cache timeout inactive 20
Qtech(config)# end
```

7.2.11.2. Showing Information About the Main Cache

Use the **show ip flow cache** command to show the packet flow statistical information in the current main mode, including the packet size distribution, the cache entry usage, etc.

The output is as follows:

```
Qtech# sh ip flow cache
Ipfix collect data from CM-CARD
ip flow switching cache, 250000 entries
    10 active, 249990 inactive
    active flows timeout in 1 minutes
    inactive flows timeout in 15 seconds
Protocol       Total Flows    Total packets  Total bytes    Active time
udp-other      3              13             834            151
ospf           12             72             5284           622
gre            2              76             1900           114
udp            3              13             834            151
Total:         17             161            8018           887
```

```
Display entries in main cache :
SrcIf               SrcIPAddress      DstIf               DstIPAddress      Pr   Tos
SrcPort DstPort Pkts        ActiveTime  Vrf
Vi1                 111.1.1.200       Null0               224.0.0.5         89   0
0       0       0           16          0
Ipfix collect data from device 3
ip flow switching cache, 250000 entries
    17 active, 249983 inactive
    active flows timeout in 1 minutes
    inactive flows timeout in 15 seconds
Protocol       Total Flows    Total packets  Total bytes    Active time
udp-other      8              144            10436          468
ospf           14             82             6144           791
gre            4              253            16182          246
udp            8              144            10436          468
Total:         26             479            32762          1505
Display entries in main cache :
SrcIf               SrcIPAddress      DstIf               DstIPAddress      Pr   Tos
SrcPort DstPort Pkts        ActiveTime  Vrf
Lo1                 22.2.2.2          Gi1/0/1             55.1.1.55         17   0
32768   99      2           12          0
Lo0                 20.1.1.1          Gi1/0/1             20.1.1.2          17   0
10000   10000   1           12          0
```

7.3. Enabling Flow Statistics

The preceding configurations are performed when the IPFIX flow statistics function is disabled. This section describes how to enable the IPFIX flow statistics function which is to measure the ingress or egress packets. Therefore, to enable the IPFIX flow statics function, you need to set the observation point, flow types, and ports where flows are measured. To enable the IPFIX flow statistics function for ingress or egress flows, you need to enter interface configuration mode.

Use the following configuration commands.

Command	Function
Qtech> **enable**	Enters privileged command mode.
Qtech# **config terminal**	Enters global configuration mode.
Qtech(config)# **interface** *interface-type interface-number*	Enters interface configuration mode.
Qtech(config)# **ip flow { ingress | egress }**	Enables the IPFIX flow statistics function on the interface.
Qtech(config)# **end**	Returns to privileged command mode.
Qtech# **copy running-config startup-config**	Saves the configuration.

To disable the IPFIX flow statistics function, use the **no ip flow { ingress | egress }** command interface configuration modein interface configuration mode.

Configuration example

```
Qtech# config terminal
Qtech(config)# interface gigabitEthernet 6/2
Qtech(config-if)# ip flow ingress            //Enable IPFIX on port 6/2 for statistics of
ingress flows.
Qtech(config-if)# exit
Qtech(config)# interface gigabitEthernet 6/3
Qtech(config-if)# ip flow ingress            //Enable IPFIX on port 6/3 for statistics of
ingress flows.
Qtech(config-if)# exit
Qtech(config)# interface gigabitEthernet 6/4
Qtech(config-if)# ip flow ingress            //Enable IPFIX on port 6/4 for statistics of
ingress flows.
Qtech(config-if)# exit
Qtech(config)# interface gigabitEthernet 6/5
Qtech(config-if)# ip flow ingress           //Enable IPFIX on port 6/5 for statistics of
ingress flows.
Qtech(config-if)# exit
Qtech(config)#
```

Use the **show ip flow interface** command to show the IPFIX state on the interface.

Configuration example

```
Qtech# show ip flow interface
interface gigabitEthernet 6/2
Ip flow ingress
interface gigabitEthernet 6/3
Ip flow ingress
interface gigabitEthernet 6/4
Ip flow ingress
interface gigabitEthernet 6/5
Ip flow ingress
```

⚠ Caution

By default, IPFIX is disabled on all interfaces. Once the IPFIX flow statistics function is enabled on an interface, the global IPFIX function is enabled, and the corresponding cache and timer are created. The settings of the main cache will take effect when the IPFIX function is re-enabled. Use the **no** form to disable all interface with IPFIX enabled, and then the global IPFIX takes no effect.

The IPFIX captured data flow is sent to the data flow analysis software (Such as NewFlow,RILL) and then be converted into a visible report for the user. Because the IPFIX flow statistics function is enabled on an interface.When the system restarted, the interface index might change and the IPFIX is unable to capture the data flow on the original designated interface. To avoid this consequence, use the command snmp-server if-index persist to bind the function on a interface.

7.4. Configuring Flow Aggregation Mode

7.4.1. Flow Aggregation Mode Overview

Flow aggregation mode re-aggregates the main mode flow and generates a new flow through the defined specified key field. The system reserves certain cache, which is similar to the main cache and here called the flow aggregation cache, for aggregation mode. When a flow entry comes out of the main cache, the flow information is used to refresh the flow aggregation record in each enabled flow aggregation cache. You could set the entry number in the aggregation cache, entry aging parameter, export destination IP address and export destination UDP port separately. Meanwhile, the entry aging mechanism in the flow aggregation mode, which supports the forcible aging according to the user requirements, is the same as the one in main mode. By default, the entry number in the flow aggregation cache is 4096.

The following flow aggregation modes are supported:

- Destination Prefix aggregation mode
- Prefix aggregation mode
- Protocol Port aggregation mode
- Source Prefix aggregation mode
- Destination Prefix-ToS aggregation mode
- Prefix-port aggregation mode
- Prefix-ToS aggregation mode
- Protocol-port-ToS aggregation mode
- Source Prefix-ToS aggregation mode

Aggregation Mode	Key Field
destination-prefix	Destination AS number, destination address mask length, destination prefix and egress interface index

Aggregation Mode	Key Field
prefix	Source AS number, destination AS number, source address mask length, destination address mask length, source prefix, destination prefix and egress interface index.
prefix-port	Source prefix, destination prefix, source port, egress interface index and ToS value.
protocol-port	Protocol number, source port and destination port.
source-prefix	Source AS number, source address mask length, source prefix.
destination-prefix-tos	Destination AS number, destination mask length, destination prefix and egress interface index.
prefix-tos	ToS, source AS number, source prefix, source mask length, destination AS number, destination mask length, destination prefix.
protocol-port-tos	ToS, protocol type, source port and destination port.
source-prefix-tos	ToS, source prefix, source mask length and source interface index.

The nine modes are independent and can be configured concurrently.

7.4.1.1. Configuring Flow Aggregation Mode

7.4.1.2. IPv4 Aggregation Mode

Configuration example

```
enable
configure terminal
ip flow-aggregation cache { destination-prefix | destination-prefix-tos | prefix |
prefix-port | prefix-tos | protocol-port | protocol-port-tos | source-prefix | source-
prefix-tos}
cache entries number
cache timeout active minutes
cache timeout inactive seconds
export destination ip-address udp-port
Repeat the step7, set the second export destination.
enabled
exit
interface interface-type interface-number
ip flow {ingress | egress}
exit
Repeat the step11-13, set the IPFIX function on other interfaces.
end
```

The following table describes the configuration commands in detail.

Command	Function
Qtech> **enable**	Enters user execution mode.
Qtech# config terminal	Enters global configuration mode.

Command	Function
Qtech(config)# ip flow-aggregation cache { destination-prefix | destination-prefix-tos | prefix | **prefix-port | prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** }	Enters corresponding flow aggregation mode. destination-prefix: enters destination-prefix aggregation configuration mode. destination-prefix-tos: enters destination-prefix-tos aggregation configuration mode. prefix: enters prefix aggregation configuration mode. prefix-port: enters prefix-port aggregation configuration mode. prefix-tos: enters prefix-tos aggregation configuration mode. protocol-port: enters protocol-port aggregation configuration mode. protocol-port-tos: enters protocol-port-tos aggregation configuration mode. source-prefix: enters source-prefix aggregation configuration mode. source-prefix-tos: enters source-prefix-tos aggregation configuration mode.
Qtech(config-flow-cache)# **cache entries number**	Configures the cache entry number. number: indicates the allowed cache entry number in this aggregation mode. The range is from 1024 to 524288. The default value is 4096.
Qtech(config-flow-cache)# **cache timeout active minutes**	(Optional) Configures the cache entry active timeout time. minutes: indicates the active timeout time. The range is from 1 to 60 minutes. The default value is 30 minutes.
Qtech(config-flow-cache)# **cache timeout inactive seconds**	(Optional) Configures the cache entry inactive timeout time. seconds: indicates the inactive timeout time. The range is from 10 to 600 seconds. The default value is 15 seconds.
Qtech(config-flow-cache)# **export destination ip-address udp-port**	(Optional) Configures the flow aggregation export destination. ip-address: indicates the export destination IP address. udp-port: indicates the destination UDP port number.
Repeat the previous step, set the second export destination.	(Optional) Configures up to two export destination for each aggregation mode.
Qtech(config-flow-cache)# **enabled**	
Qtech(config-flow-cache)# exit	Exits flow aggregation configuration mode and enters global configuration mode.
Qtech(config)# **interface ethernet** 0/0	Enters interface configuration mode.
Qtech(config-if)# ip flowegress	Enables the IPFIX function on the interface. Ingress: detects the ingress flow to the interface; Egress: detects the egress flow from the interface.
Qtech(config-if)# **end**	Exits interface configuration mode.

Configuration example

```
Qtech> enable
Qtech# configure terminal
Qtech(config)# ip flow-aggregation cache destination-prefix
Qtech(config-flow-cache)# cache entries 2048
Qtech(config-flow-cache)# cache timeout active 15
Qtech(config-flow-cache)# cache timeout inactive 300
Qtech(config-flow-cache)# export destination 172.30.0.1 991
Qtech(config-flow-cache)# enabled
Qtech(config-flow-cache)# exit
Qtech(config)# interface ethernet 0/0
Qtech(config-if)# ip flow egress
Qtech(config-if)# end
```

7.4.1.3. *Showing Flow Aggregation Information*

IPv4 configuration commands

show ip flow cache aggregation { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** } [vrf *vrf-name*]

Use this command to show the cache information in each flow aggregation mode, including the cache size, effective flow entry number, idle flow entry number, etc.

Configuration example

```
Qtech# sh ip flow cache aggregation protocol-port
IP Flow Switching Cache, 278544 bytes
2 active, 4094 inactive, 12523 added
239947 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17160 bytes
0 active, 1024 inactive, 0 added, 0 added to flow
0 alloc failures, 0 force free
1 chunk, 1 chunk added
Protocol  Source Port  Dest Port  Flows  Packets  Bytes/Packet  Active
0x11       0x007B      0x007B      1        1        76
0.0
0x01       0x0000      0x0303      1        5       132
5.0
Qtech#
```

show ip flow export

Use this command to show the export information in main mode, and the export configuration information about enabled aggregation modes, such as the format of the ouput packet, export destination, etc.

Configuration example

```
Qtech# sh ip flow export
Ipfix collect data from CM-CARD
cache for main metering process:
        flow export is enabled
        Exporting flows to 55.1.1.55 (99)
        Exporting using source interface Loopback 1
        Template export information:
           Template timeout = 10 minutes
           Template refresh rate = 20 packets
        total 400 packets metering
        total 0 packets dropped for no memory
        total 42 flows exported in 5 udp datagrams
        0 ipfix message export failed

Ipfix export information from device 3
cache for main metering process:
        flow export is enabled
        Exporting flows to 55.1.1.55 (99)
        Exporting using source interface Loopback 1
        Template export information:
           Template timeout = 10 minutes
           Template refresh rate = 20 packets
        total 1124 packets metering
        total 0 packets dropped for no memory
        total 62 flows exported in 9 udp datagrams
        0 ipfix message export failed
```

7.4.2. Configuring the Flow Filtering and Sampling Mechanism

With the netflow growth, concurrent netflows set in, affecting the performance of the IPFIX flow measurement. Then the flow filtering and sampling mechanism comes into being. The flow filtering analyzes the flows which the users are interested in, decreasing the IPFIX flow and network device loads sharply. The sampling mechanism analyzes some netflows randomly according to a certain sampling rate, decreasing the IPFIX flow greatly.

7.4.2.1. Configuring Sampling for the Specified Flow

The sampling for the specified flow uses the ACL to match the packets, and only the matched packet flow is recorded.

Use the following configuration commands.

Command	Function
Qtech> **enable**	Enters privileged command mode.
Qtech# **config terminal**	Enters global configuration mode.
Qtech(config)# **interface** *interface-name*	Enters interface configuration mode.
Qtech(config-if)# **flow-sample** *packet-num* filter *acl-name*	Applies the ACL to the interface to filter the input flow. *acl-name* is the existed ACL ID or name, it can also be 0, which means all flows are permitted. The matched packets are sampled by the ratio of 1/*packet-num*, and then flow statistics are collected.
Qtech(config)# **end**	Returns to privileged command mode.
Qtech# **copy running-config startup-config**	Saves the configuration.

To restore the default configuration of an interface, use the **no** form of this command in interface configuration mode.

All packets of ports are sampled and measured by the ratio 1/255 by default.

Caution

If the IPFIX flow measurement is disabled on the configured interface, this configuration will be saved. Once IPFIX is enabled on the port, this configuration takes effect. The corresponding ACL must exist when you configure this command. If the ACL is deleted, this configuration will be deleted automatically.

For example:

```
Qtech# config terminal
Qtech(config)# interface gi 2/2
Qtech(config-if)# flow-sample 100 filter acl1
Qtech(config-if)# end
```

8. CONFIGURING RLOG

8.1. Overview

The device side is responsible for log collection and uploading, while RLOG will send all Internet access information and user connection information to the server. The server-side software will analyze the logs and then write the logs into the database, and the user can then find the corresponding connection records through log query system.

RLOG contains NAT logs and the number of bytes received/sent, as well as connection establishment/deletion and other relevant information.

To enable logging function, you need to complete the following configurations:

- Configure logging service on device side and enable flow log;
- Enable background service program on the service side;

- Configure web server.

8.2. Log configuration

8.2.1. Log Server Configuration

Configure log server to enable logging function. If no log server is configured, the device will not send any log to the log server.

When the log server is configured, the device will enable the logging module and send out log information in UDP packets.

To configure log server, execute the following commands in global configuration mode:

Command	Function
Qtech(config)# **rlog server** *server-ip* [**vrf** *vrf-name*]	Specify the IP address and VRF name of log server and enable log service;
Qtech(config)# **no rlog server**	Remove log server configuration, disable logging service and clear relevant statistics.

Note

The command to configure log server will only enable log service, and the log output function is not enabled at the same time. Executing this command along will not output any log. The command to enable flow log is "**ip session log-on**", which must be executed separately.

8.2.2. Log Service Parameter Configuration

Log service related parameters include the maximum length of log packets, number of service port.

By executing these commands, the user can modify the configurations of log server and avoid the conflict between log service and other network services.

To configure log service parameters, execute the following commands in global configuration mode:

Command	Function
Qtech(config)# **rlog mtu** *number* Qtech(config)# **no rlog mtu**	Configure maximum length of log packets Remove the configuration of maximum length of log packets and restore to the default 1500
Qtech(config)# **rlog port** *number* Qtech(config)# **no rlog port**	Specify the log service port number Remove the configuration of log service port number and restore to the default 10000.
Qtech(config)# **rlog export-rate** *number* Qtech(config)# **no rlog export-rate**	Specify the log service export rate (maximum number of logs sent per second) Remove the configuration of log service export rate and restore to the default 1000

Note

Any change to the log service parameters will not take effect immediately. You need to restart log service to apply the configurations. You can reconfigure log server to reboot the server.

Note

The default value for log export rate is on the low side. You can configure to the maximum value if the performance of log server allows.

8.2.3. Log Service Testing

You can execute log service testing command to check whether the logging function is normal. This command is used to check free buffer and send test packets to the log server. If the log server receives the test packets and replies with the corresponding prompting messages, we can then determine that whether the log service is properly configured and whether the network is accessible.

To test the log server, execute the following command in global configuration mode:

Command	Function
Qtech(config)# **rlog test**	Test log server and check free buffer; send test packets to the log server.

Note

Checking free buffer may occupy full log buffer and result in the loss of logs. Please don't use this function unless it is necessary.

8.2.4. Log Service Statistics

Log service statistics also includes the current configuration information, the number of logs received, the number of logs sent, the number of errors sent, and the cause of the latest error.

To display log service statistics, execute the following command in global configuration mode:

Command	Function
Qtech(config)# **show rlog**	Display log service statistics.

8.3. Log Database

The log server supports MySQL, SQLSever, Oracle and etc.

Log data are long-term and continuous records. The storage of long-term data will require sufficient storage space. Different on-site service conditions will have different requirements on database.

The following is a simple example for explaining the size of database required.

Approximate 4,000 users in one school access Internet through router. Assuming that there are averagely 8k new connections and each connection contains 50 bytes of data.

Data per second: 8k*50 = 400k

Daily data: 400k*60*60*24 = 34.5G

Monthly data: 34.5*30 = about 1T

If there are more users or if the storage time is longer, then the storage space shall be increased accordingly.

Caution

The device will only send logs ceaselessly, while the log server will only analyze the logs and write into the database. The user shall be responsible for data maintenance.

⚠ Caution

For example, logs to be kept for only 15 days can be deleted by adding a trigger configured to delete data exceeding 15 days at 12:00pm of everyday.

⚠ Caution

The logs will keep all connection information, as well as some attack attempts or invalid connections. If these data are considered unnecessary, you can add a trigger configured to periodically records with 0 received byte in order to optimize the data.

⚠ Caution

These actions cannot be achieved by programs on the device or log server.

Web pages are directly related to database. Any change to the database (address, username, password and other configuration items) will need to change the corresponding web page.

8.4. Log Server

Please refer to the enclosed CD for content and web configurations of the server.

9. CONFIGURING WAN-TA

9.1. Understanding WAN-TA

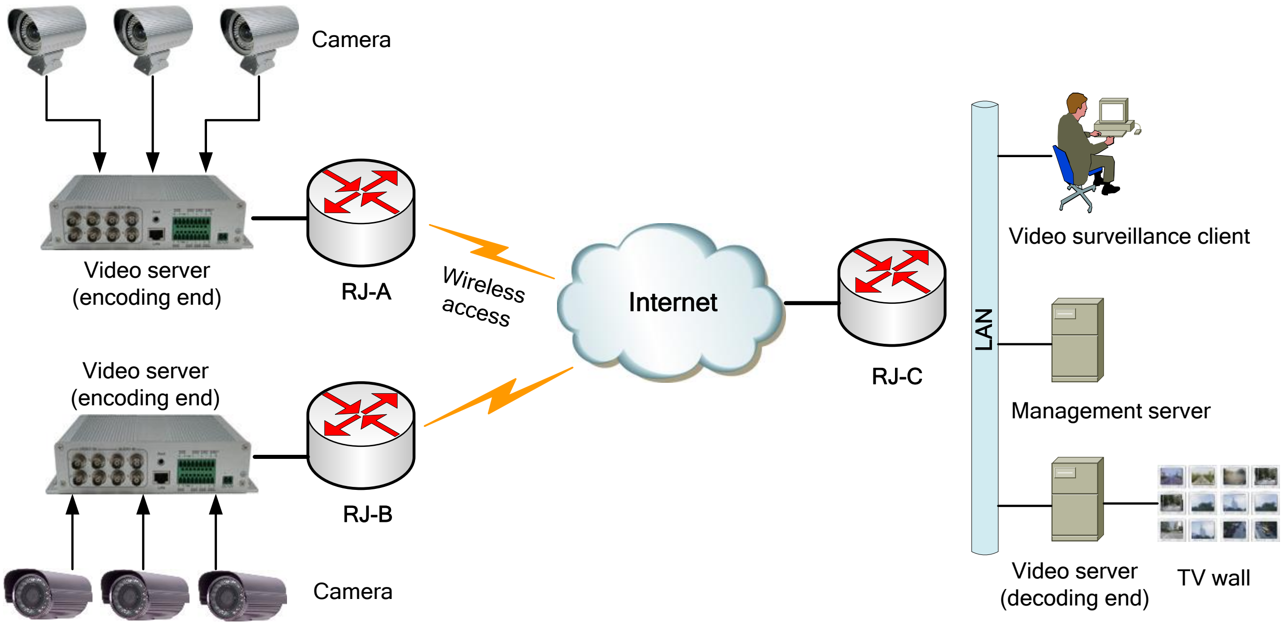
9.1.1. Overview

The video transmission optimization solution is mainly used in network video surveillance scenarios. This document briefly introduces the network video surveillance system and the video transmission optimization solution.

9.1.1.1. Network Video Surveillance System

The network video surveillance system is generally a real-time remote video surveillance system based on an IP network. It involves the processes of video collection, digital video encoding, data transmission, video decoding, and video playing. A typical video surveillance system consists of front-end surveillance devices (such as a camera, a microphone, and a video server), an IP network, and display devices (video clients). After the camera collects image signals and the microphone collects voice signals, the signals access the video server. The video server performs analog-to-digital conversion, H.264-based video compression and other digital processing, and releases the data to the network. The data reaches the video client after traversing a LAN, a wireless network, and the Internet. Then the video client decodes the data and plays the data on a screen. Figure 9-1 shows the typical structure of the wireless network video surveillance system.

Figure 9-1 Wireless Network Video Video data has two characteristics during transmission:



1) Mass data: A large volume of video data and information is involved.

2) Irregular traffic: The video data volume changes over time.

The characteristics, however, result in many challenges when video data is transmitted on a wireless network. It is well known that the wireless network has poor stability, such as instable bandwidths, high delay, high jitter, and high packet loss rates. The video server at the sending end sends video frames at a fixed interval (a video frame is composed of one or more packets). If video packets are transmitted through an unstable network, the video packets may reach the receiving end after an irregular delay. As a result, video played after being decoded may pause or stutter, or even that the video connection is interrupted and needs to be set up again.

9.1.1.2. Video Transmission Optimization Solution

The video transmission optimization solution shown in Figure 1-1 is implemented as follows: Firstly, enable WAN-TA on the sending end (RJ-A or RJ-B) to enhance video transmission quality; secondly, enable WAN-TA and RTP shaping on the receiving end (RJ-C) to eliminate video pause and stutter caused by network jitter. This solution enables videos transmitted through networks to be more smoothly played, reduces video pause and stutter, and enhances the video effect.

9.1.2. Basic Concepts

9.1.2.1. Main Protocols

The network video surveillance system mainly involves the protocols TCP, RTSP, and RTP/RTCP.

The Transmission Control Protocol (TCP) provides a mechanism that allows applications to reliably exchange data on a network. Although TCP provides a connection-oriented and reliable transmission environment, the network where applications are deployed has been greatly changed over the past two decades. In many cases, TCP has become a bottleneck for WAN application performance. The low transmission efficiency of TCP is outstanding on a wireless network (3G/4G), and therefore is urgent to be solved.

The Real Time Streaming Protocol (RTSP) defines a process for one-to-multiple applications to efficiently transmit multimedia data through an IP network, and provides the stop, fast forward, fast backward, and positioning functions for video and audio streams. RTSP is also an application-layer protocol and works with RTP and other lower-layer protocols to provide complete sets of services based on the Internet. Generally, RTSP uses TCP to complete control information transmission and uses RTP to complete media data transmission. The TCP port 554 is used by RTSP.

The Realtime Transport Protocol (RTP) is a protocol for transmitting multimedia data streams on the Internet. RTP is mainly used to transmit real-time streams in network video surveillance applications. It is defined to work in one-to-one or one-to-many transmission scenarios, aiming to provide time information and synchronize streams. RTP only ensures transmission of real-time data, but cannot provide a mechanism for transmitting data packets in order. It does not provide the traffic control or congestion control function, either. RTP provides services based on the Realtime Transport Control Protocol (RTCP).

9.1.2.2. WAN-TA

WAN Transmission Acceleration (WAN-TA) is a generic name of technologies for enhancing TCP transmission efficiency on WAN links. To enhance the TCP transmission efficiency in a video network transmission environment (in the network video surveillance system, video packets are encapsulated in TCP packets), Qtech routers have ushered in new TCP features through WAN-TA and applied the features to data streams to be forwarded so as to improve TCP transmission performance on WAN links. WAN-TA splits a TCP connection that is set up through a Qtech router into two connections, so that the router can serve as a client to participate in TCP sessions, and control TCP data streams through a WAN-TA optimization policy on the router. WAN-TA can eliminate nearly all TCP barriers without changing the client, the server, or network features.

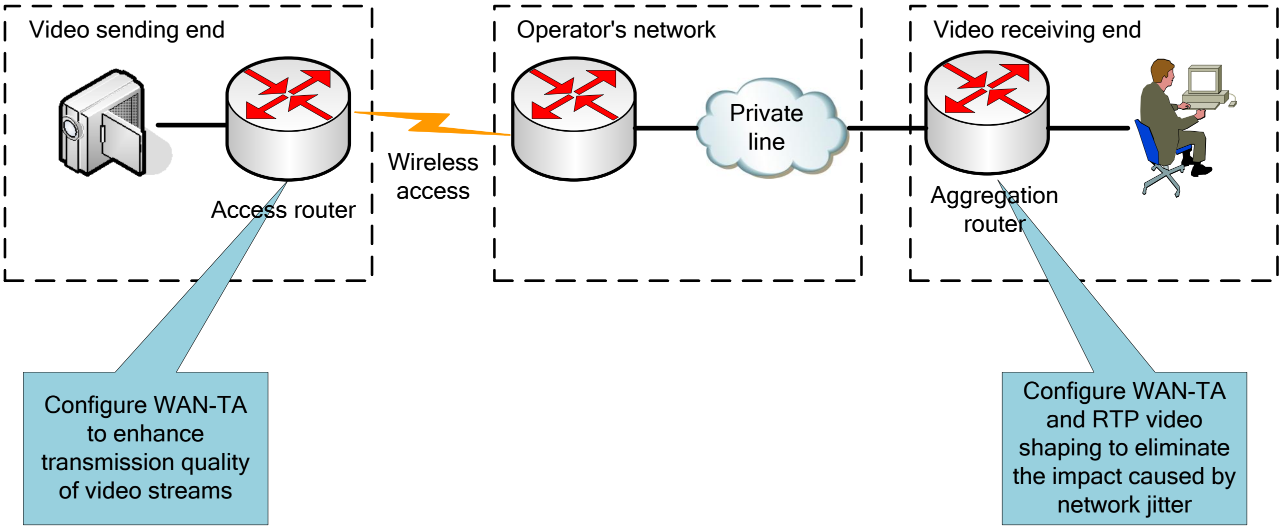
9.1.2.3. RTP Shaping

RTP shaping mainly uses the delay technology to ensure that RTP service packets reach the peer end at a fixed interval. Based on WAN-TA, RTP shaping fetches packets from a WAN-TA receiving queue, and caches video frames in an RTP queue. After a specific period of time (generally hundreds of milliseconds to several seconds), video frames are sent one after another according to the original time sequence at a fixed interval. This allows the video client to receive stable video streams.

9.1.3. Working Principle

As shown in the wireless network video transmission system in Figure 9-2, the video server is connected with the access router through a wired line, and the access router is connected with the video client through a wireless link. When WAN-TA is configured on the access router, the access router can use the air interface bandwidth to the utmost, thereby accelerating traffic transmission from the server to the client (in the outbound direction). Configured with WAN-TA and RTP shaping, the aggregation router can receive and cache video packets and send them to the video client at a fixed interval, allowing the client to obtain stable video streams. WAN-TA on the receiving router and RTP shaping on the aggregation router work together to ensure the best video effect. If WAN-TA is not configured on the access router to ensure video data transmission, videos played on the client may stutter frequently, or even that the connection is interrupted and needs to be set up again. If RTP shaping is not configured on the aggregation router for caching and shaping video packets, videos played on the client may pause frequently.

Figure 9-2 Deployment Mode of the Video Transmission Optimization Solution


Video sending end
Operator's network
Video receiving end
Private line
Wireless access
Access router
Aggregation router
Configure WAN-TA to enhance transmission quality of video streams
Configure WAN-TA and RTP video shaping to eliminate the impact caused by network jitter

9.1.4. Protocol Specification

The video transmission optimization solution involves the following RFC specifications:

- RFC793: TCP
- RFC2326: RTSP
- RFC3550: RTP

9.2. Configuring WAN-TA

9.2.1. Default Configuration

Feature	Default Setting
Globally enabling WAN-TA	WAN-TA is disabled by default.
Configuring a WAN-TA policy	No WAN-TA policy is configured.
Configuring the congestion control algorithm of the WAN-TA policy	The default algorithm is low-bandwidth-delay.
Configuring the WAN-TA policy to support SACK	The SACK option of the WAN-TA policy is enabled.
Configuring whether the WAN-TA policy supports the timestamp option	The timestamp option of the WAN-TA policy is enabled.
Configuring whether the WAN-TA policy supports the window scaling option	The window scaling option of the WAN-TA policy is enabled.
Configuring the send queue depth of the WAN-TA policy	The send queue depth is 1024 by default.
Configuring the window compensation of the WAN-TA policy	The window compensation is 0 by default. That is, no window compensation is added.
Configuring the initial window of the WAN-TA policy	The initial window size is 10 MSS by default.
Configuring the MSS of the WAN-TA policy	The MSS is 1420 by default.
Configuring the keepalive packet sending interval and the maximum number of retries of the WAN-TA policy	The keepalive packet sending interval is 120 minutes, and the maximum number of retries is 9 by default.
Applying the WAN-TA policy to an interface	WAN-TA is disabled on an interface.
Configuring the matching port of the WAN-TA policy	The default matching port number is 554.

9.2.2. Configuration Guide

- The inbound interface and the outbound interface of data flows to which WAN-TA is applied must be express-forwarding interfaces.
- All TCP data flows optimized by WAN-TA are forwarded by the device running WAN-TA.

9. 2. 3. Globally Enabling WAN-TA

Command	Function
Qtech(config)# **wan-ta enable**	Globally enables the WAN-TA function. The WAN-TA function takes effect on an interface only when the WAN-TA function is globally enabled and a WAN-TA policy is applied to the interface.

To disable the WAN-TA function, use the **no wan-ta enable** command in global configuration mode.

Configuration example:

The following example enables the global WAN-TA function:

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# wan-ta enable
```

Note

After the WAN-TA function is enabled, it takes effect for only new flows instead of existing flows. If you hope that the WAN-TA function takes effect for an existing connection, you need to disconnect and then re-create the connection after enabling the WAN-TA function.

Note

After the global WAN-TA function is disabled, the existing TCP sessions to which WAN-TA is applied will continue to be effective.

9. 2. 4. Creating a WAN-TA Policy

Command	Function
Qtech(config)# **wan-ta policy { video |** *policy-name* } [**cong-algorithm** *cong-value* | **init-cwnd** *cwnd-value* | **sack { enable | disable} | mss** *mss-value* | **keepalive interval** *interval-value* **retry** *retry-count* **]**	Creates a WAN-TA policy and specifies the parameters of the WAN-TA policy. This command can be configured in the following two ways: 3) Directly specify parameters behind the command. Then the command does not enter the following WAN-TA policy configuration mode. 4) Do not specify any parameter behind the command. Then the command enters the following WAN-TA policy configuration mode, and you can specify the parameters of the WAN-TA policy one by one.
Qtech(config-wan-ta-policy)#**cong-algorithm { default | high-delay-1 | high-delay-2 | high-lost | low-bandwidth-delay }**	Configures the congestion algorithm of the WAN-TA policy. This command has the same function as the cong-algorithm *cong-value* parameter of the wan-ta policy command.
Qtech(config-wan-ta-policy)# **sack { enable | disable }**	Enables or disables the SACK function of the WAN-TA policy. This command has the same function as the sack parameter of the wan-ta policy command.
Qtech(config-wan-ta-policy)# **init-cwnd** *cwnd-value*	Configures the initial window size of the WAN-TA policy. The value range is 2 to 10. This command has the same function as the init-cwnd *cwnd-value* parameter of the wan-ta policy command.
Qtech(config-wan-ta-policy)#**mss** *mss-value*	Configures the MSS of the WAN-TA policy. The value range is 68 to 1460. This command has the same function as the mss *mss-value* parameter of the wan-ta policy command.
Qtech(config-wan-ta-policy)#**keepalive interval** *interval-value* retry *retry-count*	Configures the keepalive packet sending interval of the WAN-TA policy within the range from 2 to 300 minutes and the maximum number of retries of the keepalive packet within the range from 1 to 9. This command has the same function as the keepalive interval *interval-value* retry *retry-count* parameter of the wan-ta policy command.
Qtech(config-wan-ta-policy)#**peer window-compensation** *cmp-value*	Configures the peer window compensation of the WAN-TA policy. The value range is 0 to 655350.
Qtech(config-wan-ta-policy)#**queue-send-depth** *dep-value*	Configures the send queue depth of the WAN-TA policy. The value range is 8 to 4096.
Qtech(config-wan-ta-policy)#**timestamp disable**	Disables the timestamp option of the WAN-TA policy. Use the no form of this command to enable the timestamp option.
Qtech(config-wan-ta-policy)#**window-scale disable**	Disables the window scaling option of the WAN-TA policy. Use the no form of this command to enable the window scaling option.
Qtech(config-wan-ta-policy)#**match-port** *port-number [port-number…]*	Configures the matching port of the WAN-TA policy. The port number range is 1 to 65535 (554, by default). Use the **no** form of this command to delete all matching ports.

To delete the configured WAN-TA policy, use the **no wan-ta policy video** command in global configuration mode.

Configuration example 1:

The following example creates a system-defined WAN-TA policy named "video":

```
Qtech(config)#wan-ta policy video
```

Configuration example 2:

The following example creates a user-defined WAN-TA policy named "ftp" and specifies parameters behind the command:

```
Qtech#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# wan-ta policy ftp init-cwnd 8 cong-algorithm low-bandwidth-delay
```

Configuration example 3:

The following example creates a user-defined WAN-TA policy named "ftp" and enters the policy mode to specify parameters:

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#wan-ta policy ftp
Qtech(config-wan-ta-policy)#init-cwnd 8
Qtech(config-wan-ta-policy)#cong-algorithm low-bandwidth-delay
```

⚠ Caution

It is not recommended that you specify parameters when creating a system-defined policy, such as the policy in configuration example 1. The system automatically generates the parameters. It is not recommended that you modify the settings of the parameters.

⚠ Caution

When creating a user-defined policy, you can directly use the **wan-ta policy** command with parameters or enter the WAN-TA policy configuration mode to specify parameters one by one. For details, see configuration examples 2 and 3.

⚠ Caution

In WAN-TA policy configuration mode (**wan-ta-policy**), you can configure the peer window compensation and send queue depth, disable the timestamp option, and disable the window scaling option. However, it is recommended that generally you keep the default settings of these parameters instead of manually configuring them.

⚠ Caution

Before deleting a WAN-TA policy, you need to remove the WAN-TA policy from interfaces on which the WAN-TA policy has been applied. If you modify the configuration after a policy is applied on an interface, the changes do not take effect for the existing connections to which WAN-TA is applied.

9.2.5. Enabling a WAN-TA Policy on an Interface

Command	Function
Qtech(config-if-gigaethernet0/0)# **wan-ta-policy video list** { *acl-id* | *acl-name*}	Applies a WAN-TA policy to an interface. The *acl-id* or *acl-name* parameter specifies the ACL that matches the flow to be optimized.

To delete the configured WAN-TA policy from an interface, use the **no wan-ta-policy** { *policy-name* | **video** } command in interface configuration mode.

Configuration example:

The following example applies a WAN-TA policy named "video" to an interface, so that all flows matching ACL 101 will be accelerated according to the WAN-TA policy named "video":

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#interface gigaethernet0/0
Qtech(config-if-gigaethernet0/0)# wan-ta-policy video  list 101
```

⚠ Caution

When there is a TCP connection to which a WAN-TA policy is applied on an interface, the WAN-TA function still takes effect on the interface even after the WAN-TA policy is deleted from the interface.

9.3. Monitoring and Maintaining WAN-TA

Command	Function
Qtech# **show wan-ta policy session**	Shows summary information about TCP sessions to which WAN-TA has been applied.
Qtech# **show wan-ta policy session** *session_id*	Shows statistics about the session with the specified session ID.
Qtech# **show wan-ta policy video**	Shows configuration information about a WAN-TA policy.

9.4. Configuration Examples

9.4.1. Configuration Example of Video Transmission Optimization

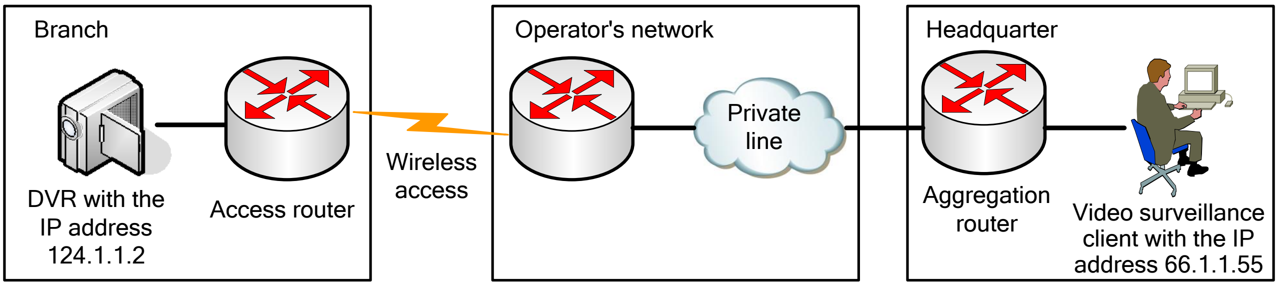
Networking Requirements

As shown in the wireless video surveillance scenario in Figure 9-3, the access router in the branch is connected to the video server (DVR); the aggregation router in the headquarter is connected to the video client.

- The access router is connected to the headquarters through a 3G/4G link.
- The video surveillance connection between the branch and the headquarter is set up based on TCP.
- Before reaching the router to which an optimization policy applies, data streams are not encrypted or encapsulated in other tunnels.

Networking Topology

Figure 9-3 WAN-TA Application Topology



Configuration Tips

On the access router:

- Globally enable WAN-TA.
- Identify the features of data streams to which WAN-TA applies.
- Create a WAN-TA optimization policy.
- Enable the WAN-TA optimization policy on the interfaces that data streams pass through.

On the aggregation router, configure WAN-TA and RTP shaping:

- Identify the features of data streams to which RTP applies.
- Configure RTP shaping.

Configuration Steps

1. Configure and enable WAN-TA on the access router.

1) Configure an ACL for matching data streams that need to be optimized.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#ip access-list extended 101
Qtech(config-ext-nacl)#10 permit ip any any
```

2) Globally enable WAN-TA.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#wan-ta enable
```

3) Create a WAN-TA optimization policy. For example, create an optimization policy named "video" to optimize the video surveillance connection between the branch and the headquarter. Video surveillance data is generally encapsulated through RTSP on the TCP port 554.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# wan-ta policy video
Qtech(config-wan-ta-policy)#match-port 554 37777
```

4) Enable the optimization policy on a port. You can enable the WAN-TA optimization policy on either the inbound interface gigaethernet0/1 or the outbound port on the access router.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#int gigabitEthernet 0/1
Qtech(config-if-GigabitEthernet 0/1)#wan-ta-policy video list 101
```

2. Configure WAN-TA and enable RTP shaping on the aggregation router.

5) Configure and enable WAN-TA on the aggregation router, because RTP shaping is based on WAN-TA.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#ip access-list extended 111
Qtech(config-ext-nacl)#10 permit ip any any
Qtech(config-ext-nacl)#exit
Qtech(config)#wan-ta enable
Qtech(config)#wan-ta policy video
Qtech(config-wan-ta-policy)#match-port 554 37777
Qtech(config-wan-ta-policy)#exit
Qtech(config)#interface gigabitEthernet 2/1/0
Qtech(config-if-GigabitEthernet 2/1/1)#wan-ta-policy video list 111
```

6) Configure RTP shaping on either the inbound port or the outbound port on the aggregation router.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#
Qtech(config)#traffic classifier tc1 or
Qtech(config-traffic-classifier)# if-match acl 111
Qtech(config-traffic-classifier)#
Qtech(config-traffic-classifier)#traffic behavior tb1
Qtech(config-traffic-behavior)# rtp-shaping delay 1000 clock-rate 90000
Qtech(config)#traffic policy tp1
Qtech(config-traffic-policy)# classifier tc1 behavior tb1 precedence 1
Qtech(config-if-GigabitEthernet 2/1/0)#traffic-policy tp1 inbound
```

Verification

7) Check WAN-TA optimization policy configuration.

```
Qtech#show wan-ta policy video
wan-ta policy: video
    Congestion Control : low-bandwidth-delay
    SACK Support: TRUE
    Initial Congest Window: 10 MSS
    Maxitum Segment Size: 1460
Keepalvie Interval(retry): 120(9)
Match Port: 554 37777

apply on interfaces:
```

```
interface name                          list
GigabitEthernet 2/1/0                     101
```

8) Check the current session.

```
Qtech#sh wan-ta  policy session  vtty 2/1
session_id  pair     flow                                tcp_state          uptime
service
391         392      [124.1.1.2:554->66.1.1.55:1776]     TCP_ESTABLISHED    0:00:06
RTSP
392         391      [66.1.1.55:1776->124.1.1.2:554]     TCP_ESTABLISHED    0:00:06
RTSP
```

The session proxy with the session ID 392 deals with LAN communication with the off-bank ATM end. The session proxy with the session ID 391 deals with WAN communication with the headquarter end. Qtech focuses on WAN communication.

9) Check the running status of a session on a link.

```
Qtech#sh wan-ta  policy session vtty 2/1 391

[124.1.1.2:554->66.1.1.55:1776]
(timer notify: 7898, handle: 2177, signal handle: 4205245876, while: 1702656051)
efb_total_num: 50115, efb_avbuf_num: 48476
sock state: TCP_ESTABLISHED        ref_cnt: 2
Congestion Control:
  algorithm      : low-bandwidth-delay
  icsk_ca_state : Disorder         icsk_retransmits: 11
  icsk_rto       : 6720 ms         icsk_timeout     : 4180 ms
  icsk_backoff   : 5               icsk_probes_out : 0
  disorder_num   : 12              cwr_num          : 0
  recovery_num   : 1               loss_num         : 0
TCP Options:
  is_tstamp      : no
  is_sack        : yes
  is_wscale      : yes         snd_wscale: 0             rcv_wscale: 0
Statistics:
  unacked        : 1               sacked           : 0
  lost           : 0               retrans          : 1
  in flight      : 2               fackets          : 0
  total retans   : 32
Times:
  last_data_sent: 2540 ms  last_data_recv: 12160 ms  last_ack_recv: 10300 ms
Keepalive:
  interval       : 7200 s          retry            : 9
Metrics:
  usable_wnd     : 65215           bw               : 9800 B/s
  snd_ssthresh   : 2               rcv_ssthresh     : 25560
  snd_cwnd       : 2               rtt              : 10 ms
  snd_wnd        : 65535           rttvar           : 50 ms
  reordering     : 3               rcv_rtt          : 0 ms
  mss_cache      : 1420            advmss           : 1420
  in_pkt_num     : 4               out_pkt_num      : 54
Queue length:
  recv_queue_len: 0          write_queue_len: 64        ofo_queue_len: 0
```

Major parameters are described as follows:

- **write_queue_len**: Specifies the length of the sending queue. Packets can be sent to a specific link only when the parameter value is not null.
- **out_pkt_num**: Specifies the number of sent packets.
- **snd_cwnd**: Specifies the sending congestion window, which defines the number of packets allowed to be sent to a link. It is an important parameter to control congestion.
- **total retans**: Specifies the number of retransmitted packets.

- **srtt**: Specifies the current delay of the link.

10) Enter line card mode to check RTP shaping statistics.

```
[LC2/1]#show rtp-shaping statistics
ref_count[1], sch_count[10671], free_count[1022]
rtp-que[4dd54cf0]:
        delay[1000],clock_rate[90000]
        flow[124.1.1.2,66.1.1.55,6,554,1776]
        que-
pkts[179],pass_pkts[113],video_frames[26],audio_frames[0],disorder_frames[0]
        rtp_time[991451572],sys_time[585873838],reply_cseq[3]
```

10. CONFIGURING HTTP SERVICE

10.1. Understanding HTTP

10.1.1. Overview

The Hypertext Transfer Protocol (HTTP) is used to transmit web page information over the Internet. HTTP resides at the application layer of the TCP/IP protocol stack. The transmission layer uses connection-oriented TCP.

Hypertext Transfer Protocol Secure (HTTPS) is the HTTP supporting the Secure Sockets Layer (SSL). HTTPS sets up a secure channel on an insecure network to ensure that information can hardly be intercepted and to defend against man-in-the-middle attacks to some extent. Currently, HTTPS has been widely used among security-sensitive communication services, such as electronic payment.

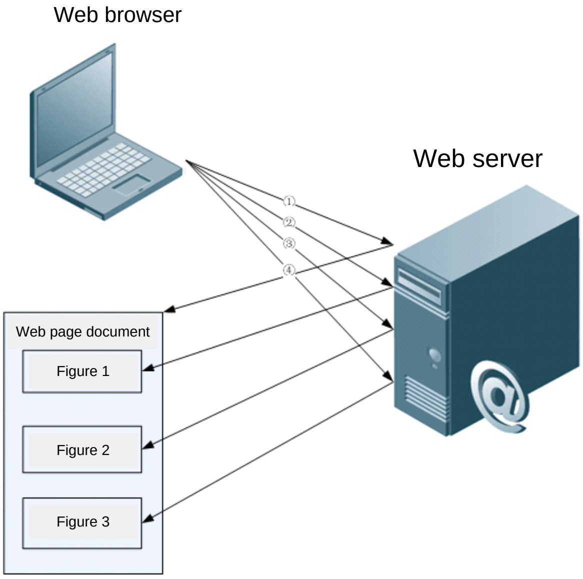
10.1.2. Basic Concept

HTTP Service

The HTTP service facilitates HTTP to transmit web page information over the Internet. HTTP/1.0 is the most popular HTTP version in the industry. HTTP/1.0 uses the short connection mode to simplify connection management, as a web server may be accessed for tens of thousands or even a million times each day. When receiving a connection request, the server sets up a TCP connection and releases it after the request is completed. The server does not record or trace previous requests. Although HTTP/1.0 simplifies connection management, it introduces certain performance defects.

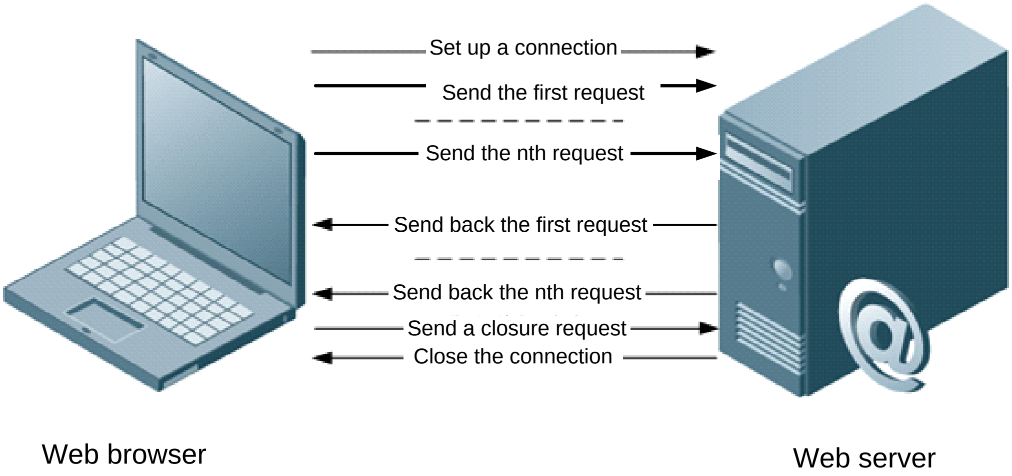
For example, a web page may contain URLs of multiple images, so that the browser sends multiple requests in the access process. When receiving a request, the server sets up an independent connection which is completely isolated from other connections. The process of setting up and releasing a connection consumes plenty of resources, and therefore has serious severe impact on the performance of the client and the server, as shown in Figure 10-1.

Figure 10-1 HTTP/1.0 Protocol Packet Exchange



HTTP/1.1, however, has solved this defect. HTTP/1.1 supports a persistent connection, through which multiple requests and responses can be transmitted. The client can send the next request before the previous request is completed, thereby reducing network delay and enhancing performance, as shown in Figure 10-2.

Figure 10-2 HTTP/1.1 Protocol Packet Exchange



Currently, Qtechdevices support HTTP/1.0 and HTTP/1.1.

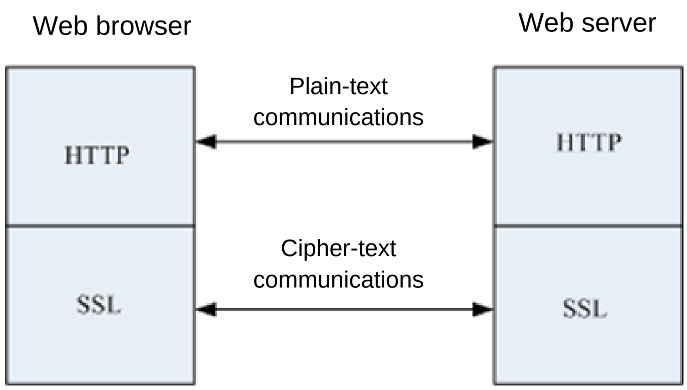
Note The protocol version used by a device depends on the specific web browser.

HTTPS Service

HTTPS adds the security base of SSL to HTTP. To enable HTTPS to run normally, the server must have a Public Key Infrastructure (PKI) certificate, which is not necessary for the client. SSL provides the following services:

- Authenticating users and servers to ensure that data is sent to correct clients and servers
- Encrypting data to prevent data interception during transmission
- Keeping data integrity to ensure that data is not changed during transmission

Figure 10-3 HTTPS Service



HTTP Upgrade Service

The HTTP upgrade service includes local and remote HTTP upgrade services.

- During local upgrade, the device works as an HTTP server. Users can log in to the device through the web browser and upload the upgrade files to the device so as to upgrade files on the device.
- During remote upgrade, the device works as a client connected to a remote HTTP server. It obtains the upgrade files from the server so as to upgrade local files.

10.1.3. Working Principle

HTTP Working Process

HTTP is used for web management. Users log in to the device through the web interface for configuration and management. Web management involves the web client and web server. The HTTP service adopts the client/server mode accordingly. The HTTP client is embedded in the web browser of the web management client and can send HTTP packets, receive HTTP response packets, and handle HTTP response packets. The web server (HTTP server) is embedded in the device. The client and the server exchanges information with each other according to the following process:

- The client sets up a TCP connection with the server. The default HTTP port number is 80, and the default HTTPS port number is 443.
- The client sends a request to the server.
- After processing the request, the server sends a response to the client.
- After processing a request, the HTTP service directly closes the TCP connection between the client and the server; while HTTPS can handle multiple requests until the client sends a TCP connection closure request or until the connection is closed due to server timeout.

The HTTP remote upgrade process is summarized as follows:

- The device connects to the server. In this process, the user-configured server address is preferentially used. If the connection fails, the server address in the local upgrade record file is used to establish the connection.
- The device sends the version numbers of local programs to the server.
- After resolution, the server returns a download file list.
- The device connects to file servers according to the list and downloads the upgrade files as necessary.
- The device can connect to different file servers according to the different files to be downloaded.
- The device upgrades its local files.

10.1.4. Protocol Specification

RFC1945 - Hypertext Transfer Protocol -- HTTP/1.0

RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1

RFC2818 - Hypertext Transfer Protocol Over TLS -- HTTPS

10.1.5. Typical Application

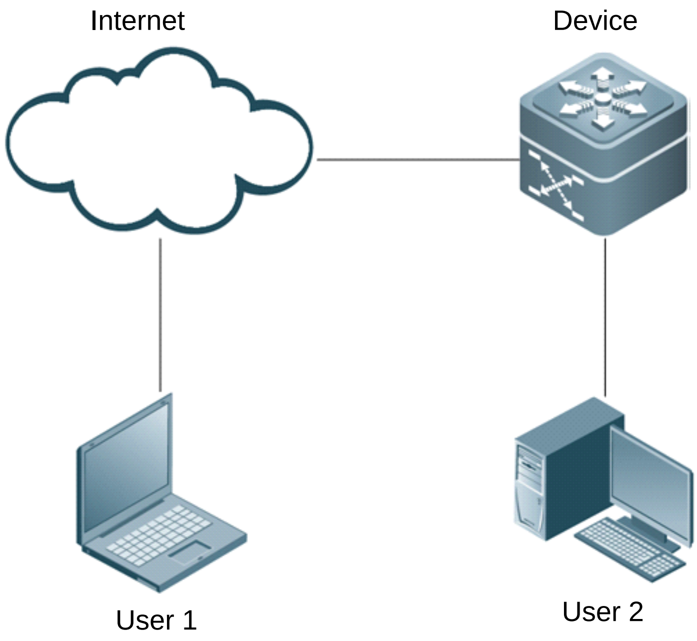
HTTP Application Service

Currently, the web NMS is still a major method for users to maintain and manage devices. Qtech network devices also provide the web management function. When HTTP is enabled, users can log in to the web management interface after entering "http://+device IP address" on the PC browser and passing the authentication. Through the web interface, users can perform various operations, such as monitoring device states, configuring devices, uploading files, and downloading files.

The common HTTP-based service is actually insecure. For security-sensitive communications, Qtech devices also provide the more secure HTTPS service, which encrypts the information transmitted between users and the device, so that third-party devices cannot intercept or modify the information. Users can perform web management simply after entering "https://+device IP address" on the web browser and passing the authentication.

Figure 10-4 illustrates a typical web management scenario. Users can remotely access and manage the device through the Internet or log in to the web server through a LAN to perform configuration management for the device. Users can enable either HTTPS or HTTP, or both as necessary on the device.Users can also specify HTTP/1.0 or HTTP/1.1 on the web browser for accessing the HTTP service of the device.

Figure 10-4 HTTP Application Scenario



HTTP Remote Upgrade Service

The HTTP Remote Upgrade Service means that a device serving as a client connects the remote HTTP server and obtains files from the server to upgrade local files.

10.2. Configuring HTTP

Default Configuration

The following table describes the default configuration of HTTP.

Feature	Default Setting
Enabling the HTTP service	The HTTP service is disabled by default.
HTTP authentication method	Usernames: **admin** and **guest**
HTTP service port	Common HTTP port number: 80 HTTPS port number: 443

HTTP upgrade server	Server address: 0.0.0.0 Port number: 80
HTTP upgrade mode	Manual
HTTP upgrade auto-detection time	Random

Prerequisites

Before configuring the domain name of the HTTP upgrade server, enable the DNS function on the device and configure the address of the DNS server.

Configuration Steps

Step	Configuration Task	Description
1	Enable the HTTP service.	Mandatory
2	Configure HTTP authentication information.	(Optional) This step is performed when authentication information needs to be modified.
3	Configure the HTTP port.	(Optional) This step is performed when the HTTP port needs to be changed.
4	Configure the HTTP upgrade server.	(Optional) This step is performed when the server address needs to be specified.
5	Configure the HTTP upgrade mode.	(Optional) This step is performed when the upgrade mode needs to be changed.
6	Configure HTTP upgrade auto-detection time.	(Optional) This step is performed when the HTTP upgrade auto-detection time needs to be changed.
7	Manually upgrade files with HTTP.	Mandatory

10.2.1. Enabling the HTTP Service

The HTTP service includes the commonly used HTTP service and the HTTPS service. HTTPS adds SSL on the basis of HTTP to enhance information security.

Use the following commands to enable the HTTP service in configuration mode.

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)#**enable service web-server http**	(Mandatory) Enables the HTTP service.
Qtech(config)#**enable service web-server https**	(Mandatory) Enables the HTTPS service.
Qtech(config)#**enable service web-server [all]**	(Mandatory) Enables both HTTP and HTTPS services.

Configuration example:

The following example enables both HTTP and HTTPS services on a Qtech device.

```
Qtech# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# enable service web-server
```

10.2.2. Configuring HTTP Authentication Information

When HTTP is enabled, users can log in to the web interface only after being authenticated. Use the **webmaster level** command to configure HTTP authentication information.

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(confing)# **webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password* }	(Mandatory) Configures the login authentication mode, which is not configured by default.

Note

Usernames and passwords come with three permission levels, each of which includes at most 20 usernames and passwords.

Configuration example:

The following example uses the username **admin** and plain-text password **Qtech** at level 0 to perform web authentication on a Qtech device.

```
Qtech# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# webmaster level 0 username admin password Qtech
```

10.2.3. Configuring the HTTP Port

Configuring the HTTP port can reduce attacks from unauthorized users to HTTP. Qtech devices support the HTTP and HTTPS service modes.

- Use the following commands to configure the HTTP port number.

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **ip http port** *port-number*	(Optional) Configures the HTTP port number, which is 80 by default.

Configuration example:

The following example configures the HTTP port number as 8080 on a Qtech device.

```
Qtech# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# ip http port 8080
```

- Use the following commands to configure the HTTPS port.

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **ip http secure-port** *port-number*	(Optional) Configures the HTTPS port number, which is 443 by default.

Configuration example:

The following example configures the HTTPS port number as 4430 on a Qtech device.

```
Qtech# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# ip http secure-port 4430
```

10.2.4. Configuring the HTTP Upgrade Server

The address of the HTTP remote upgrade server is 0.0.0.0 and the port number is 80 by default. Use the following commands to change the server address.

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **http update server** { *host-name* | *ip-address* } [**port** *port-number*]	(Optional) Configures the address of the HTTP upgrade server.

Note

The HTTP upgrade server address does not need to be configured because the local upgrade record file records available upgrade server addresses.

Caution

If the server domain needs to be configured, enable the DNS function on the device and configure the DNS server address.

Caution

The server address cannot be an IPv6 address.

Configuration example:

The following example configures the domain name of the HTTP upgrade server as **rgos.Qtech.ru** and the port number as 85 on a Qtech device.

```
Qtech# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# http update server rgos.Qtech.ru port 85
```

10.2.5. Configuring an HTTP Upgrade Mode

The manual upgrade mode applies for HTTP by default. Use the following commands to enter global configuration mode and configure HTTP to automatically detect the files available for upgrade on the server.

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **http update mode auto-detect**	(Optional) Configures the HTTP upgrade mode as auto-detection. If this step is not performed or the **no** form of this command is executed, the manual upgrade mode is used by default.

In auto-detection mode, the device detects the files on the server during upgrade. Users can find the web versions to be upgraded through the web interface.

Configuration example:

The following example configures the HTTP upgrade mode as auto-detection on a Qtech device.

```
Qtech# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# http update mode auto-detect
```

10.2.6. Configuring HTTP Upgrade Auto-Detection Time

In auto-detection mode, the remote HTTP auto-detection time is random. Use the following commands to change the auto-detection time in global configuration mode.

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **http update time daily** *hh*:*mm*	(Optional) Configures HTTP auto-detection time, which is random by default.

Note

The HTTP auto-detection time is a specific time point with the accuracy of minutes each day.

Caution

This configuration command takes effect only when the HTTP upgrade mode is auto-detection.

Configuration example:

The following example configures the HTTP auto-detection time as 3:00 am on a Qtech device.

```
Qtech# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# http update time daily 03:00
```

10.2.7. Manually Upgrading Files with HTTP

- Remote Upgrade

HTTP provides only the remote auto-detection function by default, and the system does not automatically perform upgrade. Use the following commands to upgrade the system in privileged EXEC mode.

Command	Function
Qtech# **http check-version**	(Optional) Checks the upgrade version.
Qtech# **http update web** [**version** *string*]	Updates the web package.

Configuration example:

The following example performs remote file upgrade for a Qtech device through HTTP.

```
Qtech# http check-version
app name:web
sn               version                     filename
-- -------------------- -------------------------
0          1.2.1(82381)       web1.2.1(145680).upd
1          1.2.1(82380)       web1.2.1(145680).upd
2          1.2.1(82379)       web1.2.1(145680).upd
3          1.2.1(82378)       web1.2.1(145680).upd
```

- Local Upgrade

You can use the **copy tftp** command to download latest web files to a Qtech device and then use the following command to upgrade the web package.

Command	Function
Qtech# **http web-file update**	Updates the web package.

⚠ Caution To enable the new web package to take effect, log in to the web interface again.

The following example locally upgrades the web package for a Qtech device.

```
Qtech#copy tftp://10.10.10.13/web_management_pack.upd flash:web_management_pack.upd
Qtech#http web-file update
```

10.3. Monitoring and Maintaining HTTP

10.3.1. Displaying HTTP Configuration Information

Command	Function
show web-server status	Displays the configuration information and status of the web service.

Configuration example:

The following example displays the HTTP configuration information of a Qtech device.

```
Qtech# show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
http(s) use memory block: 768, create task num: 0
```

10.4. Configuration Examples

10.4.1. HTTP Configuration Example

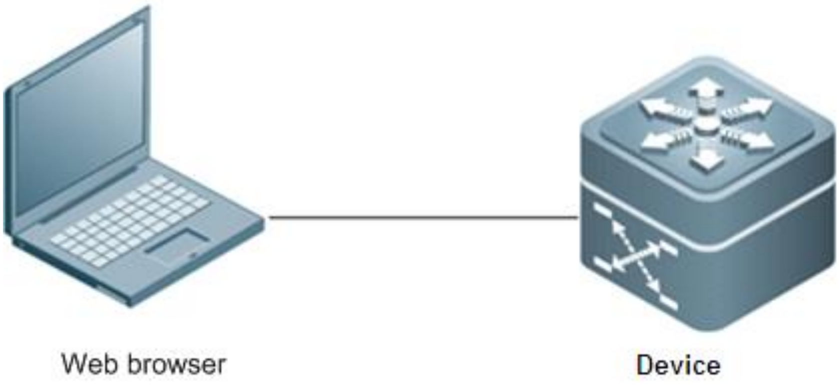
Networking Requirements

Network administrators hope to manage a device through web, and therefore log in to the device through the web browser to configure the switch.

- Log in with the user-configured authentication information.
- Ensure that the web browser can be accessed through HTTP or HTTPS so as to enhance security.
- Configure the HTTP port to reduce attacks from unauthorized users to HTTP.

Networking Topology

Figure 10-5 HTTP Application Topology



Configuration Tips

To meet the customer's requirements, focus on the following points:

- Use the **webmaster level** command to configure authentication information.
- Enable HTTP and HTTPS at the same time to meet the customer's security requirements.
- Configure the HTTP port number as 8080 and the HTTPS port number as 4430.

Configuration Steps

11) Configure the username as admin and the password as Qtech.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# webmaster level 0 username admin password Qtech
```

12) Enable the HTTP and HTTPS services.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#enable service web-server
```

13) Configure the HTTP port number as 8080.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#ip http port 8080
```

14) Configure the HTTPS port number as 4430.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#ip http secure-port 4430
```

Verification

15) Check HTTP configuration information.

```
Qtech#show web-server status
http server status : enabled
http server port : 8080
https server status: enabled
https server port: 4430
http(s) use memory block: 768, create task num: 0
```

10.4.2. Configuration Example of HTTP Remote Upgrade

Networking Requirements

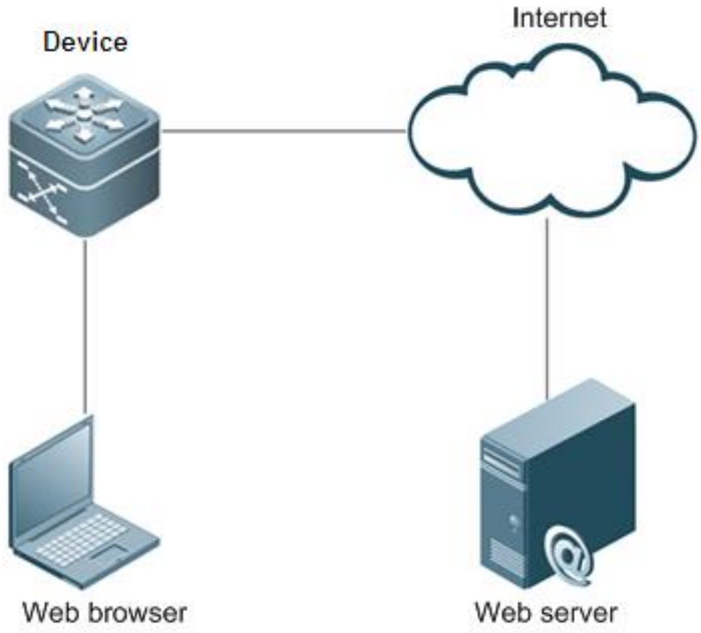
An enterprise purchasing a Qtech device hopes to use the HTTP upgrade function to upgrade files.

- Ensure that the device can periodically and remotely obtain information about the files available for upgrade from a Qtech server.

- Check the files currently available for upgrade.
- Download the latest files from the Qtech server and update the device to be upgraded.

Networking Topology

Figure 10-6 Networking Topology of HTTP Remote Upgrade



Configuration Tips

To meet the customer's requirements, focus on the following point:

- Configure the device to remotely obtain information about the latest files at 2:00 am each day.

Configuration Steps

16) Configure DNS information.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#ip domain-lookup                                //Enable the DNS
function on the device.
Qtech(config)#ip name-server 192.168.5.134                    //Configure the IP
address of the DNS server.
```

17) Configure the address of the upgrade server.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)# http update server rgos.Qtech.ru
```

18) Enable the auto-detection mode and configure the remote detection time of the device as 2:00 am.

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#http update mode auto-detect
Qtech(config)#http update time daily 02:00
```

19) Obtain information about the files available for upgrade from the remote server.

```
Qtech#http check-version
app name:web
sn             version                  filename
-- -------------------- -------------------------
```

```
0          1.2.1(82381)       web1.2.1(145680).upd
1          1.2.1(82380)       web1.2.1(145680).upd
2          1.2.1(82379)       web1.2.1(145680).upd
3          1.2.1(82378)       web1.2.1(145680).upd
```

20) Download the files from the server and update the device.

```
Qtech#http update web
```

Verification

Check server version information on the online upgrade interface of web.

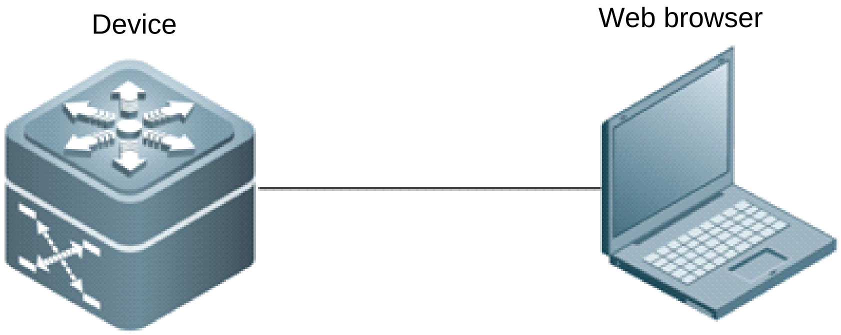
10.4.3. Configuration Example of HTTP Local Upgrade

Networking Requirements

- Users hope to run the latest web package, which is obtained from an official website, on a device.

Networking Topology

Figure 10-7 Networking Topology of HTTP Local Upgrade



Configuration Tips

To meet the customer's requirements, focus on the following points:

- Connect the device to a local PC whose IP address is 10.10.10.13, and configure the device with an IP address 10.10.10.131 in the same network segment.
- Download the latest web package to the device.
- Update the web package on the device.

Configuration Steps

21) Create VLAN1 and configure an IP address for the device

```
Qtech#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Qtech(config)#vlan 1
Qtech(config-vlan)#exit
Qtech(config)#interface vlan 1
Qtech(config-VLAN 1)#ip address 10.10.10.131 255.255.255.0
```

22) Enable the TFTP server function on the PC and run the copy tftp command on the device to download the web package.

```
Qtech#copy tftp://10.10.10.13/web_management_pack.upd flash:web_management_pack.upd
```

23) Update the web package on the device.

```
Qtech#http web-file update
```

Verification

On the PC, log in with web authentication once again to check whether the latest web interface is displayed.

11. CONFIGURING RADIUS DYNAMIC AUTHORIZATION EXTENSION

11.1. Understanding RADIUS Dynamic Authorization Extension

11.1.1. Overview

The Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS) protocol is defined in RFC 3576 by IETF. This protocol defines a user offline management method, that is, the device communicates with a RADIUS server through Disconnect-Messages (DMs) to log out authenticated users. This protocol enables devices from different vendors to communicate with a RADIUS server and log out users of these devices.

The DM mechanism is as follows: A RADIUS sends user logout requests to the device. The device logs out the users that match the session IDs in the request packets, and sends response packets that contain processing results to the server. This mechanism allows the RADIUS server to manage user logout.

11.1.2. Working Principle

Figure 1-1 DM exchange for RADIUS dynamic authorization extension

```
+----------+   Disconnect-Request     +----------+
|          |   <--------------------   |          |
|    NAS   |                           |  RADIUS  |
|          |   Disconnect-Response     |  Server  |
|          |   --------------------->  |          |
+----------+                           +----------+
```

The above figure shows the DM exchange between the RADIUS server and device. When the RADIUS server sends a Disconnect-Request packet to the UDP port numbered 3799, the device processes the packet and sends a Disconnect-Response packet containing the processing results to the server.

11.1.3. Protocol Specification

RADIUS is defined in RFC 3576.

11.2. Default Configuration

The default configuration about RADIUS dynamic authorization extension is shown in the table below.

Feature	Default Setting
RADIUS dynamic authorization extension	Disabled
The number of a UDP port for intercepting DMs	3799

11.3. Configuring RADIUS Dynamic Authorization Extension

11.3.1. Enabling RADIUS Dynamic Authorization Extension

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)#**radius dynamic-authorization-extension enable**	Enables RADIUS dynamic authorization extension.
Qtech(config)# **show running-config**	Shows configuration.

Use the **no radius dynamic-authorization-extension enable** command to disable RADIUS dynamic authorization extension in global configuration mode.

The example below shows how to configure RADIUS dynamic authorization extension:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# radius dynamic-authorization-extension enable
Qtech(config)# show run
```

Note

By default, RADIUS dynamic authorization extension is disabled.

11.3.2. Viewing the Configuration

Command	Function
Qtech# **show radius dynamic-authorization-extension statistics**	Shows statistics about RADIUS dynamic authorization extension.
Qtech# **clear radius dynamic-authorization-extension statistics**	Clears statistics about RADIUS dynamic authorization extension.

The example below shows how to show statistics about RADIUS dynamic authorization extension.

```
Qtech# show radius dynamic-authorization-extension statistics
Disconnect-Request Received:                             50
Incorrect Disconnect-Request Received:                  1
Disconnect-Request Dropped for Queue Full:              0
Disconnect-Request Process Timeout:                      0
Disconnect-Request Process Success:                      49
Disconnect-ACK Sent:                                        25
Disconnect-ACK Sent Failed:                                 0
Disconnect-NAK Sent:                                        24
Disconnect-NAK Sent Failed:                                 0
```

11.4. Configuring Optional Features of RADIUS Dynamic Authorization Extension

11.4.1. Configuring a UDP Port

Command	Function
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)#**radius dynamic-authorization-extension port** *num*	Sets a UDP port for intercepting the packets about RADIUS dynamic authorization extension. The value ranges from 1024 to 65535. The default value is 3799.
Qtech(config)# **show running-config**	Shows configuration.

Use the **no radius dynamic-authorization-extension port** command to restore the default interception port in global configuration mode.

The example below shows how to configure a UDP port intercepting the packets about RADIUS dynamic authorization extension.

# Set the port numbered 8080 to intercept RADIUS requests:

```
Qtech#  configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# radius dynamic-authorization-extension port 8080
Qtech(config)#  show running-config
```

# Reset the configuration:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# no radius dynamic-authorization-extension port
Qtech(config)# show running-config
```

11.5. Examples for Configuring RADIUS Dynamic Authorization Extension

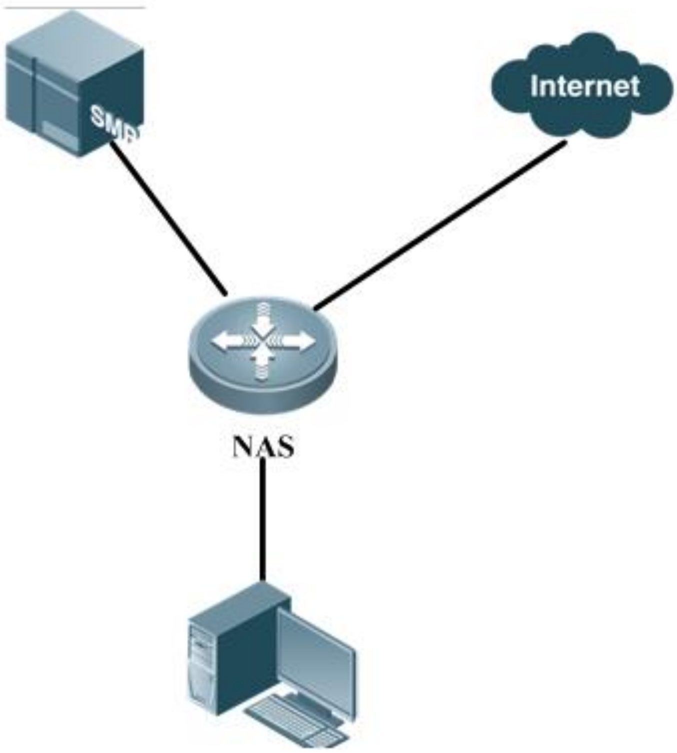
Networking Requirements

RADIUS dynamic authorization extension must work with the authentication mechanism. The network comprises SAM servers, Qtech access devices, and PCs of users.

Qtech access devices must support RADIUS dynamic authorization extension.

Networking Topology

Figure 4-1 Network topology of RADIUS dynamic authorization extension



11.5.1. Configuration Procedure

1. Configure AAA on the access authentication device.

```
aaa new-model
aaa accounting update periodic 1
aaa accounting update
aaa accounting network default start-stop group radius
aaa authentication ppp default local group radius
```

2. Configure the PPP authentication on the access device.

```
vpdn enable
vpdn-group 1
accept-dialin
protocol l2tp
  virtual-template 1
```

```
interface Virtual-Template 1
ppp authentication chap
 ip unnumbered Loopback 1
interface Loopback 1
 ip address 110.1.1.254 255.255.255.0
interface GigabitEthernet 8/1/1
ip address 100.1.1.2 255.255.255.0
duplex auto
      speed auto
```

3. Enable RADIUS dynamic authorization extension.

```
radius dynamic-authorization-extension enable
```

4. After the user logs in, the administrator uses RADIUS dynamic authorization extension on the SAM to log out the user.
5. The user is logged out and needs to be authenticated again to access the network.

12. CONFIGURING SMART STATUS MONITORING

12.1. Overview

12. 1. 1. Introduction

A network egress generally provides two or more operator links. For example, in a campus network of a university, a network egress provides an education network link and an operator link; in a government network, a network egress provides links. When links in a wide area network (WAN) have different bandwidths and the number of links is no less than three, there can be 2^n adjustment policies, and, it is impossible to manually perform adjustment at any time. In view of this, the smart status monitoring module can sense network changes, and can perform complex logical operation, to obtain the final policy and implement the corresponding control script.

For example, in an aggregate port (AP) scenario where all AP members operate properly, the HQoS (Hierarchical Quality of Service) traffic policy needs to limit the traffic rate based on the sum of bandwidth of all AP members and guarantee user services based on priorities. When the link of a certain AP member is down, the HQoS traffic policy changes accordingly. In this case, the total bandwidth to be guaranteed is the sum of bandwidth of all AP members subtracted by the bandwidth of the failed member link.

12.1.2. Working Principle

The smart status monitoring module loads and runs different scripts to control the device according to different preset status detection situations of scheduling instances.

Detection events mainly involve the BDF session status, interface link status, the selected, unselected, and track the status of Link Aggregation Control Protocol (LACP) on the AP members. According to the configured smart status monitoring instances, unary operation or binary operation between multiple detection events are performed starting from the predetermined operation sequence. If the operation result meets the detection quantity, the smart status monitoring module loads and runs the script copied by TFTP to control the device.

Different scripts are executed according to different detection results. In this way, the device can be flexibly controlled, thereby reducing the maintenance workload.

12.2. Defaults

Feature	Default Value
Smart Status Monitoring Scheduling Instance	N/A
Smart Status Monitoring Operation Sequence	N/A

Smart Status Monitoring Detection Events	N/A
Smart Status Monitoring Heartbeat Period	5 seconds

12.3. Smart Status Monitoring Heartbeat Period

12.3.1. Configuring Heartbeat Period

Command	Function
config	Enters the global configuration mode.
smart-monitor tick *seconds*	Sets the scheduling heartbeat period for smart status monitoring in seconds. The value range is from **1** to **60**.
exit	Exits the global configuration mode and enters the privileged EXEC mode.

Run the **no smart-monitor tick** command to restore the default scheduling heartbeat period.

Configuration Example

#Configure the smart status monitoring heartbeat period to 2 seconds.

```
Qtech#configure
Qtech(config)# smart-monitor status tick 2
Qtech(config)#exit
Qtech#
```

12.4. Smart Status Monitoring Detection Events

12.4.1. Configuring Detection Event

Command	Function
config	Enters the global configuration mode.
smart-monitor status *status-id* { bfd ***peer-address*** {down **|** up**}** } [member-interface ***interface-name***]} | { **interface** *interface-name* **{ line {down | up}** | **lacp {selected** | **unselected}**| **link-quality { enable | disable}** *link-quality -value* } } | { **track** *track-id* {**up** | **down**} | { **time-range** *time-range-name* {**active** | **inactive** } }	Configures smart status monitoring detection events. The event ID range is from **1** to **64**. bfd *peer-address*: Indicates the peer address of the detected BFD session. down: Indicates that the detected BFD session is in the down state. up: Indicates that the detected BFD session is in the up state. *interface-name*: Indicates the name of an AP member that supports BFD session detection. *interface-name*: Indicates the name of the detected interface. down: Indicates that the line of the detected interface is down. up: Indicates that the line of the detected interface is up. selected: LACP of the detected interface is selected. unselected: LACP of the detected interface is not selected. *link-quality–value*: Indicates the link quality value of the detected interface. The value range is from **0** to **100**.

	track-id: Indicates detected track ID. The value range is from **1** to **700**. *time-range-name*: Indicates the name of the detected time range. active: Indicates that the detected time range is in the active state. inactive: Indicates that the detected time range is in the inactive state.
exit	Exits the global configuration mode and enters the privileged EXEC mode.

Run the **no smart-monitor status** *status-id* command to delete a smart status monitoring detection event.

Configuration Example

#Create Smart Status Detection Event 1 to detect the event that the BFD session with the peer IP address being 19.19.19.1 is up.

```
Qtech#configure
Qtech(config)# smart-monitor status 1 bfd 19.19.19.1 up
Qtech(config)#exit
Qtech#
```

#Create Smart Status Detection Event 3 to detect the event that the link of GigabitEthernet 0/0 is up.

```
Qtech#configure
Qtech(config)# smart-monitor status 3 interface gigabitEthernet0/0 line up
Qtech(config)#exit
Qtech#
```

#Create Smart Status Detection Event 4 to detect the event with the track ID being 1 and the state being up.

```
Qtech#configure
Qtech(config)# smart-monitor status 4 track 1 up
Qtech(config)#exit
Qtech#
```

#Create Smart Status Detection Event 5 to detect the event that the BFD session of the AP member Gi0/0 with the peer address being 19.19.19.1 is up.

```
Qtech#configure
Qtech(config)#interface Route-aggregateport 1
Qtech(config-if-Route-aggregateport 1)# ip address 19.19.19.1 255.255.255.252
Qtech(config-if-Route-aggregateport 1)# bfd interval 50 min_rx 50 multiplier 3
Qtech(config-if-Route-aggregateport 1)# member interface GigabitEthernet 0/0 bind bfd
peer-ip 192.168.1.10
Qtech(config-if-Route-aggregateport 1)# member interface GigabitEthernet 0/1 bind bfd
peer-ip 192.168.1.10
Qtech(config-if-Route-aggregateport 1)#end
Qtech#configure
Qtech(config)# smart-monitor status 5 bfd 19.19.19.1 up member-interface
GigabitEthernet 0/0
Qtech(config)#
```

#Create Smart Status Detection Event 6 to detect the event that the weekdays time range is active.

```
Qtech(config)# smart-monitor status 6 time-range check active
```

#Create Smart Status Detection Event 7 to detect the event that the weekdays time range is inactive.

```
Qtech(config)# smart-monitor status 7 time-range check inactive
```

#Create a time range named weekdays.

```
Qtech(config)# time-range check
Qtech(config-time-range)# periodic weekdays 8:30 to 17:30
```

To configure a time range, perform the following commands in privileged EXEC mode:

Command	Function
configure terminal	Enters the global configuration mode.
time-range *time-range-name*	Names a time range using a significant string.
Qtech(config-time-range)# **absolute** [start time date] end time date	(Optional) Configures an absolute time range. For more information, see time range configuration manual.
Qtech(config-time-range)# **periodic day-of-the-week** time to [day-of-the-week] time	(Optional) Configures a periodical time range. For details, see the time range configuration guide.
exit	Exits the global configuration mode and enters the privileged EXEC mode.

12.4.2. Displaying

Run the following command to display information about smart status monitoring detection events.

Command	Function
show smart-monitor status [status-id]	Displays information about smart status monitoring detection events. The result of a smart status monitoring detection event may be **True**, **False**, or **Fail**. **True** indicates a match, **False** indicates a mismatch, and **Fail** indicates that the configuration is incorrect and does not meet the detection target.

The displayed information is as follow:

```
Qtech(config)# show smart-monitor status 3
Smart-monitor status 3 : final-status True
smart-monitor status 3 interface GigabitEthernet 0/0 line up
Qtech(config)# show smart-monitor status 5
Smart-monitor status 5 : final-status False
smart-monitor status 5 bfd 19.19.19.1 up member-interface GigabitEthernet 0/0
```

12.5. Smart Status Monitoring Operation Sequence

12.5.1. Configuring Detection Event

Command	Function
config	Enters the global configuration mode.
smart-monitor status *status-id* { bfd ***peer-address*** {down **|** up} } | { **interface** *interface-name* { **line {down | up}** | **lacp {selected** | **unselected} | link-quality { enable** | **disable}** *link-quality -value* } } | { **track** *track-id* {**up | down**} **|** { **time-range** *time-range-name* {**active** | in**active** } }	Configures smart status monitoring detection events.

exit	Exits the global configuration mode and enters the privileged EXEC mode.

Run the **no smart-monitor** status ***status-id*** command to delete smart status monitoring detection events.

12.5.2. Configuring Operation Sequence

Command	Function
config	Enters the global configuration mode.
smart-monitor seq *seq-id* {**seq [not]** *seq-id*} **|** {**status [not]** *status-id*} **[** {**and | or**} {**seq [not]** *seq-id*} **|** {**status [not]** *status-id*} **]**	Configures the operation sequence for smart status detection. The operation sequence ID range is from **1** to **100**. (Optional) not: Performs the NOT operation via operators. *status-id*: Indicates the ID of a smart status monitoring detection event. The value range is from **1** to **64**. and: Indicates binary operation. The AND operation is performed via the left and right operators. or: Indicates binary operation. The OR operation is performed via the left and right operators.
exit	Exits the global configuration mode and enters the privileged EXEC mode.
show smart-monitor seq [*seq-id*]	Displays the smart status monitoring operation sequence.

Run the **no smart-monitor seq** *seq-id* command to delete a smart status monitoring operation sequence.

Configuration Example

#Configure the operation rule of Operation Sequence 1: perform negation operation on the result of Event 1 that the link of the detected interface GigabitEthernet1/1/0 is up.

```
Qtech(config)# smart-monitor status 1 interface GigabitEthernet 0/0 line up
Qtech(config)# smart-monitor seq 1 status not 1
```

#Configure the operation rule of Operation Sequence 2: perform binary operation, that is, perform AND operation on the statuses of Instance 2 and Instance 1 of smart status monitoring detection events.

```
Qtech#configure
Qtech(config)# smart-monitor status 2 interface GigabitEthernet 0/1 line up
Qtech(config)# smart-monitor seq 2 status  2 and seq  1
```

12.5.3. Displaying

Run the following command to display the smart status monitoring operation sequence.

Command	Function
show smart-monitor seq *[seq-id]]*	Displays the smart status monitoring operation sequence.

The displayed information is as follow:

Run the **show smart-monitor seq** command to display all operation sequence information.

```
Qtech#show smart-monitor schedule
smart-monitor seq 1 status not 1
smart-monitor seq 2 status  1 and seq  1
```

12. 6. Smart Status Monitoring Scheduling Instance

12.6.1. Configuring Detection Event

Command	**Function**
config	Enters the global configuration mode.
smart-monitor status *status-id* { bfd ***peer-address*** {down **|** up**}** } } | { **interface** *interface-name* { **line** {**down | up**} | **lacp {selected** | **unselected}** | **link-quality { enable | disable}** *link-quality -value* } } | { **track** *track-id* {**up | down**} | { **time-range** *time-range-name* {**active** | **inactive** } }	Configures smart status monitoring detection events. The event ID range is from **1** to **64**. bfd *peer-address*: Indicates the peer address of the detected BFD session. down: Indicates that the detected BFD session is in the down state. up: Indicates that the detected BFD session is in the up state. *interface-name*: Indicates the name of the detected interface. down: Indicates that the line of the detected interface is down. up: Indicates that the line of the detected interface is up. selected: LACP of the detected interface is selected. unselected: LACP of the detected interface is not selected. *link-quality–value*: Indicates the link quality value of the detected interface. The value range is from **0** to **100**. *track-id*: Indicates detected track ID. The value range is from **1** to **700**. *time-range-name*: Indicates the name of the detected time range. active: Indicates that the detected time range is in the active state. inactive: indicates that the detected time range is in the inactive state.
exit	Exits the global configuration mode and enters the privileged EXEC mode.

Run the **no smart-monitor status** *status-id* command to delete a smart status monitoring detection event.

12.6.2. Configuring Operation Sequence

Command	**Function**
config	Enters the global configuration mode.

smart-monitor seq *seq-id* {**seq [not]** *seq-id*} **|** {**status [not]** *status-id*} **[** {**and | or**} {**seq [not]** *seq-id*} **|** {**status [not]** *status-id*} **]**	Configures the operation sequence for smart status detection. The operation sequence ID range is from **1** to **100**. (Optional) not: Performs the NOT operation via operators. *status-id*: Indicates the ID of a smart status monitoring detection event. The value range is from **1** to **64**. and: Indicates binary operation. The AND operation is performed via the left and right operators. or: Indicates binary operation. The OR operation is performed via the left and right operators.
exit	Exits the global configuration mode and enters the privileged EXEC mode.
show smart-monitor seq [*seq-id*]	Displays the smart status monitoring operation sequence.

Run the **no smart-monitor seq** *seq-id* command to delete a smart status monitoring operation sequence.

12.6.3. Configuring Scheduling Instance

Command	Function
config	Enters the global configuration mode.
smart-monitor schedule *schedule-id* **final-seq** *seq-id* **action load** *file-name tag_infor* [**times** *times-number*]	Configures a smart status monitoring scheduling instance. *schedule-id*: Indicates the serial number of a smart status monitoring scheduling instance. The value range is from **1** to **8**. *seq-id*: Indicates the serial number of an operator. The value range is from **1** to **100**.*file-name*: Indicates the name of a to-be-loaded script file. The file name contains 1 to 63 characters. *tag_infor*: Executes tagged information in the script. (Optional) times-number: Loads and runs the script labeled by **file-name** when the number of detection times reaches the value of **times-number**. The value range is from **1** to **20**. The default value is **1**.
exit	Exits the global configuration mode and enters the privileged EXEC mode.
show smart-monitor schedule [*schedule-id* [**do**]]	Displays information about smart status monitoring scheduling instances.

Run the **no smart-monitor schedule** *schedule-id* command to delete a smart status monitoring scheduling instance.

Configuration Example

#Create a smart status monitoring scheduling instance with the ID 1, perform operation starting from Operation Sequence 2, and load content of the switch_to_pos section in the configuration script ah-wh-pos-mstp-chg.text if the number of detection times reaches 3.

```
Qtech#configure
```

```
Qtech (config)# smart-monitor schedule 1 final-seq 2 action load ah-wh-pos-mstp-
chg.text switch_to_pos times 3
```

Syntax of the configuration file ah-wh-pos-mstp-chg.text:

```
@@@@@start
switch_to_pos:
enable
config
interface GigabitEthernet 1/4/2/7
shutdown
end
@@@@@end
```

1. Each execution section starts with @@@@@start and ends with @@@@@end.Content to be loaded is identified the section identifier in the **smart-monitor schedule 1** command.

It should be noted that the colon behind the section identifier is an English character.

12.6.4. Displaying

Run the following command to display information about smart status monitoring scheduling instances.

Command	Function
show smart-monitor schedule [schedule-id [do]]	Displays the smart status monitoring configuration information, automatic loading and execution information, and operation result.

The displayed information is as follow:

Example 1: Run the **show smart-monitor schedule** command to display information about all operation scheduling instances.

```
Qtech#show smart-monitor schedule
smart-monitor schedule 1 final-seq 2 action load ah-wh-pos-mstp-chg.text switch_to_pos
times 3
smart-monitor schedule 2 final-seq 1 action load ah-wh-pos-mstp-chg.text pos_to_switch
times 1
smart-monitor schedule 3 final-seq 1 action load 3.text times 2
```

Example 2: Run the **show smart-monitor schedule** 2 command to display information about a specified operation scheduling instance.

```
Qtech#show smart-monitor schedule 2
smart-monitor schedule 2 final-seq 1 action load ah-wh-pos-mstp-chg.text pos_to_switch
times 1
```

Example 3: Run the **show smart-monitor schedule** 2 **do** command to display information about a specified operation scheduling instance.

```
Qtech#show smart-monitor schedule 2 do
smart-monitor schedule 2 final-seq 1 action load ah-wh-pos-mstp-chg.text pos_to_switch
times 1
```

12.7. Smart Status Monitoring Configuration Example

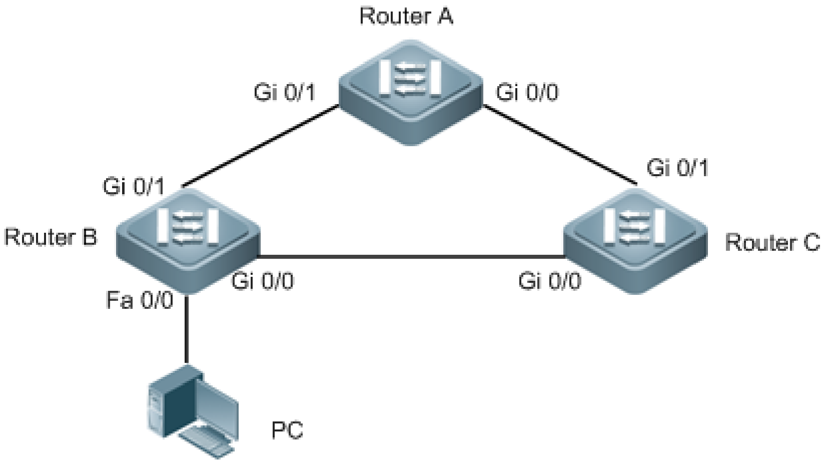
12.7.1. Configuration Example 1

12.7.1.1. Networking Requirements

Three routers are deployed.

12.7.1.2. Network Topology

Figure 12-1 Smart Status Monitoring



12.7.1.3. Configuration Key Points

1. Configure the flow queue, user queue, and user group queue.
2. Configure the traffic classifier, traffic behavior, and traffic policy.
3. Apply the HQoS policy.
4. Configure an AP and use LACP for detection on the AP.
5. Configure the smart status monitoring detection and dynamically adjust the HQoS policy.

12.7.1.4. Configuration Steps

#Configure the flow queue of the production service.

```
flow-queue sc_0/0
 queue be wfq weight 10
 queue af1 wfq weight 20
 queue af2 pq shaping 2666
 queue af3 wfq weight 15
 queue af4 wfq weight 15
 queue ef pq
 queue cs6 pq
 queue cs7 pq

flow-queue sc_0/1
 queue be wfq weight 10
 queue af1 wfq weight 20
 queue af2 pq shaping 5333
 queue af3 wfq weight 15
 queue af4 wfq weight 15
 queue ef pq
 queue cs6 pq
 queue cs7 pq
```

#Configure the flow queue of the office service.

```
flow-queue bg_0/1
 queue be wfq weight 10
 queue af1 wfq weight 20
 queue af2 pq shaping 2666
 queue af3 wfq weight 15
 queue af4 wfq weight 15
 queue ef pq
 queue cs6 pq
 queue cs7 pq

flow-queue bg_0/0
 queue be wfq weight 10
 queue af1 wfq weight 20
 queue af2 pq shaping 1333
 queue af3 wfq weight 15
 queue af4 wfq weight 15
 queue ef pq
 queue cs6 pq
 queue cs7 pq
```

#Configure the user queue of the production service.

```
user-queue sc_0/0 outbound
 cir 6666 pir 10000
 flow-queue sc_0/0
 user-group-queue sc_bg_0/0

user-queue sc_0/1 outbound
 cir 13333 pir 20000
 flow-queue sc_0/1
 user-group-queue sc_bg_0/1
```

#Configure the user queue of the office service.

```
user-queue bg_0/0 outbound
 cir 3333 pir 10000
 flow-queue bg_0/0
 user-group-queue sc_bg_0/0

user-queue bg_0/1 outbound
 cir 6666 pir 20000
 flow-queue bg_0/1
 user-group-queue sc_bg_0/1
```

#Configure the user group queue.

```
user-group-queue sc_bg_0/0 outbound
 shaping 10000
user-group-queue sc_bg_0/1 outbound
 shaping 20000
```

#Configure the traffic classifier of the production service.

```
traffic classifier sc_111_cos or
 if-match acl sc_111
traffic classifier sc_222_cos or
 if-match acl sc_222
traffic classifier sc_333_cos or
 if-match acl sc_333

traffic classifier sc_0/0 and
 if-match dst-if GigabitEthernet 0/0
 if-match src-if VLAN 2
traffic classifier sc_0/1 and
 if-match dst-if GigabitEthernet 0/1
 if-match src-if VLAN 2
```

#Configure the traffic classifier of the office service.

```
traffic classifier bg_bg_cos or
 if-match acl bg_bg
traffic classifier bg_voip_cos or
```

```
 if-match acl bg_voip
traffic classifier bg_777_cos or
 if-match acl bg_777

traffic classifier bg_0/0 and
 if-match dst-if GigabitEthernet 0/0
 if-match src-if VLAN 3
traffic classifier bg_0/1 and
 if-match dst-if GigabitEthernet 0/1
 if-match src-if VLAN 3
```

#Configure traffic behaviors of three sub services of the production service.

```
traffic behavior sc_222_cos
 service-class be color green
traffic behavior sc_333_cos
 service-class af1 color green
traffic behavior sc_111_cos
 service-class af2 color green
```

#Configure traffic behaviors of three sub services of the office services.

```
traffic behavior bg_777_cos
 service-class be color green
traffic behavior bg_voip_cos
 service-class af1 color green
traffic behavior bg_bg_cos
 service-class af2 color green
```

#Configure traffic behaviors of the production service.

```
traffic behavior sc_0/0
 user-queue sc_0/0 outbound
traffic behavior sc_0/1
 user-queue sc_0/1 outbound
```

#Configure traffic behaviors of the office service.

```
traffic behavior bg_0/0
 user-queue bg_0/0 outbound
traffic behavior bg_0/1
 user-queue bg_0/1 outbound
```

#Configure traffic policies of all services.

```
traffic policy sc_bg_out
 classifier sc_0/0 behavior sc_0/0 precedence 1
 classifier sc_0/1 behavior sc_0/1 precedence 2
 classifier bg_0/0 behavior bg_0/0 precedence 3
 classifier bg_0/1 behavior bg_0/1 precedence 4
```

#Configure traffic policies of three sub services of the production service.

```
traffic policy district-1_in
 classifier sc_111_cos behavior sc_111_cos precedence 1
 classifier sc_222_cos behavior sc_222_cos precedence 2
 classifier sc_333_cos behavior sc_333_cos precedence 3
```

#Configure traffic policies of three sub services of the office service.

```
traffic policy disctrict-2_in
 classifier bg_bg_cos behavior bg_bg_cos precedence 1
 classifier bg_voip_cos behavior bg_voip_cos precedence 2
 classifier bg_777_cos behavior bg_777_cos precedence 3
```

#Apply the HQoS policy to the AP.

```
interface AggregatePort 1
 port-user-key dst-ip
 traffic-policy sc_bg_out outbound
```

#Apply the HQoS policy to AP members and configure LACP detection.

```
interface GigabitEthernet 0/0
 port-bandwidth 10000
 port-group 1 mode active

interface GigabitEthernet 0/1
 port-bandwidth 20000
 port-group 1 mode active
```

#Configure the smart status monitoring function to detect the event that LACP of the AP member Gi0/0 is selected or not selected.

```
smart-monitor status 1 interface GigabitEthernet 0/0 lacp unselected
smart-monitor seq 1 status  1
smart-monitor seq 2 status not 1
smart-monitor schedule 1 final-seq 1 action load hqos.txt  up2down times 10
smart-monitor schedule 2 final-seq 2 action load hqos.txt down2up times 10
smart-monitor tick 10
```

#Compile the corresponding script for configuring the smart status monitoring function to detect the event that LACP of the AP member Gi0/0 is selected or not selected.

//Smart status monitoring script

```
@@@@@start
up2down:
enable
config
interface GigabitEthernet 0/0
shutdown
end
@@@@@end
@@@@@start
Down2up:
enable
config
interface GigabitEthernet 0/0
no shutdown
end
```

12.7.1.5. Verification

1. Display the smart status monitoring information on the device.

```
Qtech# show smart-monitor status 1
Smart-monitor status 1 : final-status True
smart-monitor status 1 interface GigabitEthernet 0/0 line up

Qtech#show smart-monitor schedule 1
smart-monitor schedule 1 final-seq 1 action load hqos.txt up2down times 3
```

13. CONFIGURING DOMAIN NAME POLICY

13.1. Overview

13.1.1. Introduction

On current routers, policy functions such as routing and flow control are implemented based on IP addresses. Although such processing is quick and accurate, an IP address involved in the processing is abstract to users and it is inconvenient to record IP addresses.

Policy routing provides a new bridge between service modules and users. Original configurations and logics of the service modules are retained and users only need to record domain names (URLs) that are easy to memorize.

13. 1. 2. Basic Concepts

URL Library

The URL library is generated in the device memory based on the URL library file and the URLs configured by the user in URL classes. The URL library includes specific domain names and domain name classification information.

URL Class

A URL class is a group of URLs with the same attribute.

URL Group

A URL group is a policy that combines a URL class and a user group.

DNS Parser

The DNS parser parses DNS response packets in depth, to obtain the domain names and corresponding IP addresses from the packets.

13.1.3. Working Principle

A URL group is configured on the router to specify the association between a URL class and a user group. After receiving a DNS response packet, the router searches the URL library to obtain the URL class and URL group that are corresponding to the URL in the DNS response packet, so as to further obtain the corresponding user group. The router can fill the answer IP address in the DNS response packet into the user group, and apply the user group to policy-based routing (PBR), thereby implementing routing based on the domain name.

The ultimate effect of the domain name policy function is to fill IP addresses corresponding to a type of domain names into a user group. For details about how to user this user group, refer to related configurations of other functional modules.

13.1.4. Application

The domain name policy module is a public module that must operate in combination with other modules to meet requirements of corresponding scenarios. For example, the domain name policy module can cooperate with HQoS to provide domain name-based service guarantee, or can associate with PBR to provide domain name-based policy routing.

13.2. Domain Name Policy Configuration

Defaults

No domain name policy is configured by default.

Configuration Prerequisites

Configuration Steps

Step	Task	Description
1	Enable the URL library.	Mandatory.
2	Configure the URL class.	Optional.
3	Configure the user group.	Mandatory.
4	Configure the URL group.	Mandatory.
5	Enable the DNS parser.	Mandatory.

13.2.1. Enabling URL Library

Enable the URL library by running the **lib.dat** file in the **flash:/urlib/lib.dat** path on the device. If the URL library file does not exist on the device, obtain this file and save it to the corresponding path.

Similar to other files, the library file can be downloaded to the device in TFTP or FTP mode, for example, copy the file from the **tftp://101.101.101.155/lib.dat** path or the **flash:/urlib/lib.dat** path.

Command	Function
Qtech(config)#url-lib enable	Enables the URL library.

13.2.2. Configuring URL Class (Optional)

Run the following commands to configure a URL class. Because the system presets several URL classes in the URL library, this function is optional.

Command	Function
Qtech(config)#url-class *class_name*	Enters the URL class configuration mode.
Qtech(config-url-class)#url *url*	Adds a URL class.

Example: Configure URL redirection rules on physical interfaces.

```
Qtech#configure terminal
Qtech(config)# url-class test_class
Qtech(config-url-class)#url www.Qtech.ru
Qtech(config-url-class)#url *.edu.ru
```

13.2.3. Configuring User Group

Run the following command to configure a user group.

Command	Function
Qtech(config)#user-group *groupname*	Configures a user group.

13.2.4. Example: Configure URL redirection rules on physical interfaces.

13.2.5. Configuring URL Group

Run the following command to configure a URL group:

Command	Function
Qtech(config)#url-group *num*	Enters the URL group configuration mode.
Qtech(config-url-group)#class *class_name*	Configures forward proxy mapping.
Qtech(config-url-group)#relate user-group *group_name*	Configures a user group associated with the URL group.

Example: Configure URL redirection rules on physical interfaces.

```
Qtech#configure terminal
Qtech(config)# url-group 3
Qtech(config-url-group)#class test_class
Qtech(config-url-group)#relate user-group test_group
Qtech(config-url-group)#exit
Qtech(config)#
```

13.2.6. Enabling DNS Parser

Run the following command to enable the DNS parser on an interface:

Command	Function
Qtech(config-if)# dns-parser enable	Enables DNS forward proxy on an interface.

Example: Configure URL redirection rules on physical interfaces.

```
Qtech#configure terminal
Qtech(config)#interface gigabitEthernet 1/1/1
Qtech(config-if-GigabitEthernet 1/1/1)#dns-parser enable
Qtech(config-if-GigabitEthernet 1/1/1)#exit
Qtech(config)#
```

13.3. Monitoring

Run the following command to display the current URL group list.

Command	Function
Qtech# show url-group	Displays the current URL group list.

13.4. Configuration Example

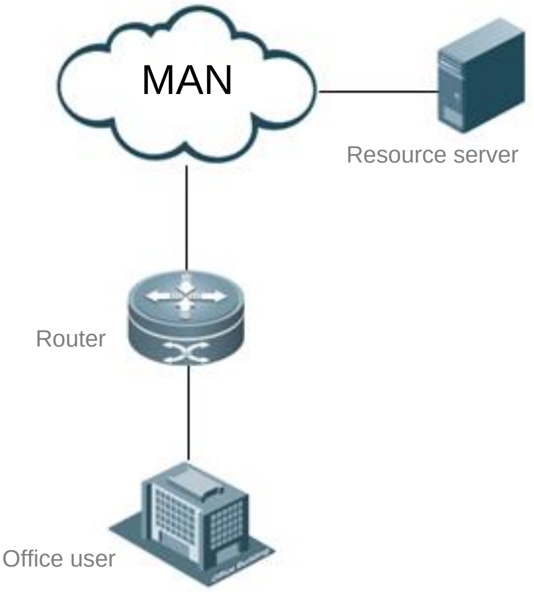
13.4.1. Domain Name-based Service Guarantee

Networking Requirements

A resource server is deployed in a MAN and can be accessed at www.XXX.net. The network quality of office users must be guaranteed when they access (for example, video resources in) the resource server in the MAN.

Network Topology

Figure 2-1



The office network is connected to the MAN via a router. The router is connected to the office network via GigabitEthernet0/0.

Configuration Steps

1) Configure the basic network connection.

Configure basic egresses and routes on the router based on different routing requirements and scenarios.

2) Configure the domain name policy.

```
Qtech(config)#user-group user_url1
Qtech(config-user-group)#exit
Qtech(config)#
Qtech(config)#url-lib enable
Qtech(config)#url-class user_url1
Qtech(config-url-class)#url *.XXX.net
Qtech(config-url-class)#exit
Qtech(config)#
Qtech(config)# url-group 5
Qtech(config-url-group)#class user_url1
Qtech(config-url-group)#relate user-group user_url1
Qtech(config-url-group)#exit
Qtech(config)#
Qtech(config)#url-group ttl 60
```

3) Configure the HQoS

The HQoS configuration is flexible. For details, see the configuration guides of router-related products and the HQoS chapter in the command reference document. In this document, HQoS is applied to the outbound direction of the inside interface of the port queue is used as an examples.

```
Qtech(config)# ip access-list extended 100
Qtech(config-ext-nacl)# permit ip user-group user_url1 any
Qtech(config-ext-nacl)#exit
Qtech(config)#
Qtech(config)#traffic classifier aaa
Qtech(config-traffic-classifier)#if-match acl 100
Qtech(config-traffic-classifier)#exit
Qtech(config)#
Qtech(config)#traffic behavior aaa
Qtech(config-traffic-behavior)#service-class cs6 color green
Qtech(config-traffic-behavior)#exit
Qtech(config)#
Qtech(config)#traffic policy aaa
Qtech(config-traffic-policy)#classifier aaa behavior aaa
Qtech(config-traffic-policy)#exit
Qtech(config)#
Qtech(config)#port-queue test
Qtech(config-port-queue)#exit
Qtech(config)#
Qtech(config)#interface gigabitEthernet 0/0
Qtech(config-if-GigabitEthernet 0/0)#traffic-policy aaa outbound
Qtech(config-if-GigabitEthernet 0/0)#port-queue test shaping 2000
Qtech(config-if-GigabitEthernet 0/0)#exit
Qtech(config)#
```

4) Enable the DNS parser and DNS proxy on the interface.

```
Qtech(config)#interface GigabitEthernet 0/0
Qtech(config-if-GigabitEthernet 0/0)#dns-parser enable
Qtech(config-if-GigabitEthernet 0/0)#exit
Qtech(config)#
```

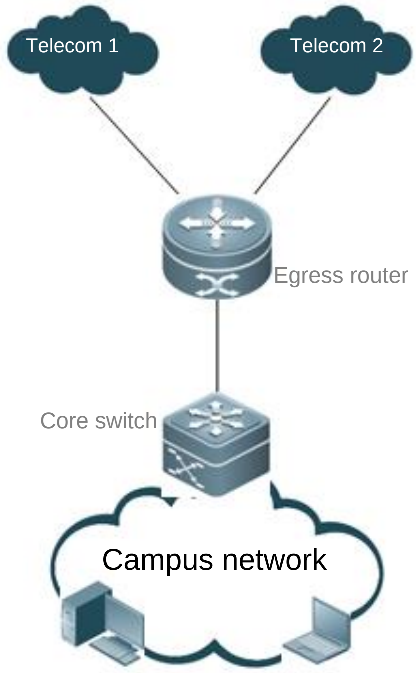
13.4.2. URL Routing

Networking Requirements

A campus network provides two Telecom egresses: Telecom 1 and Telecom 2. All services are connected to the public network via Telecom 2. In this example, it is required to connect the NKI service to the public network via Telecom 1.

Network Topology

Figure 2-2



Connection Between Interface TenGi1/1/1 and Core Switch of Campus Network

Configuration Steps

(1). Configure outbound routes for operators.

According to different routing requirements, intranet user packets are forwarded on different operator links based on operator routes, PBR routes, user routes, and the like. DNS packets as user packets are also routed based on the same policy.

(2). Configure the domain name policy.

```
Qtech(config)#url-lib enable
Qtech(config)#user-group nki
Qtech(config-user-group)#exit
Qtech(config)#
Qtech(config-url-class)#url *.nki.net
Qtech(config-url-class)#url nki.*
Qtech(config-url-class)#uexit
Qtech(config)#
Qtech(config)# url-group 3
Qtech(config-url-group)#class nki
Qtech(config-url-group)#relate user-group nki
Qtech(config-url-group)#exit
Qtech(config)#
```

(3). Enable the DNS parser on the interface.

```
Qtech(config)#interface tenGigabitEthernet 1/1/1
Qtech(config-if-TenGigabitEthernet 1/1/1)#dns-parser enable
Qtech(config-if-TenGigabitEthernet 1/1/1)#exit
Qtech(config)#
```

(4). Configure PBR.

The gateway address of Telecom 1 is 177.136.69.1.

```
Qtech(config)# ip access-list extended 100
Qtech(config-ext-nacl)# permit ip any user-group nki
Qtech(config-ext-nacl)#exit
Qtech(config)#
Qtech(config)# route-map nki_policy
Qtech(config-route-map)# match ip address 100
Qtech(config-route-map)# set ip next-hop 177.136.69.1
Qtech(config-route-map)#exit
Qtech(config)#
```

14. CONFIGURING DDNS

14.1. Overview

Dynamic Domain Name Server (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information.

14.2. Configuring DDNS

Default Configuration

Feature	Default Settings
Oray client	Disabled by default.

14.2.1. Configuring Oray Client

Command	Description
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **peanut username** *test* **password** *test*	Configures the username and password for the oray client.
Qtech(config)#**end**	Returns the privileged EXEC mode.
Qtech#**show running**	Verifies the configuration.

To remove the oray client configuration, run the **no** form of this command.

The following example configures an oray client.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# peanut username test password test
Qtech(config)#
```