IP Address & Application Configuration

Оглавление

www.qtech.ru

1 CONFIGURING IP ADDRESSES AND SERVICES

1.1 Overview

Internet Protocol (IP) sends packets to the destination from the source by using logical (or virtual) addresses, namely IP addresses. At the network layer, routers forward packets based on IP addresses.

Protocols and Standards

- RFC 1918: Address Allocation for Private Internets
- RFC 1166: Internet Numbers

1.2 Applications

Application	Description
Configuring an IP Address for Communication	Two networks communicate through one switch interface.

1.2.1 Configuring an IP Address for Communication

Scenario

A switch is connected to a Local Area Network (LAN), which is divided into two network segments, namely, 172.16.1.0/24 and 172.16.2.0/24. Computers in the two network segments can communicate with the Internet through switches and computers between the two network segments can communicate with each other.

Figure 1-1 Configuring IP Addresses

1. Configuring IP Addresses and Services
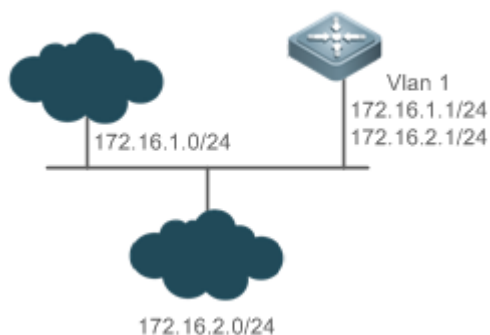
Deployment

- Configure two IP addresses on VLAN1. One is a primary IP address and the other is a secondary IP address.
- On hosts in the network segment 172.16.1.0/24, set the gateway to 172.16.1.1; on hosts in the network segment 172.16.2.0/24, set the gateway to 172.16.2.1.

1.3 Features

Basic Concepts

IP Address

An IP address consists of 32 bits in binary. To facilitate writing and description, an IP address is generally expressed in decimal. When expressed in decimal, an IP address is divided into four groups, with eight bits in each group. The value range of each group is from 0 to 255, and groups are separated by a full stop ".". For example, "192.168.1.1" is an IP address expressed in decimal.

IP addresses are used for interconnection at the IP layer. A 32-bit IP address consists of two parts, namely, the network bits and the host bits. Based on the values of the first several bits in the network part, IP addresses in use can be classified into four classes.

For a class A address, the most significant bit is 0.7 bits indicate a network ID, and 24 bits indicate a local address. There are 128 class A networks in total.

1. Configuring IP Addresses and Services

Figure 1-2

		8	16	24	32
Class A IP address	0	Network ID	Host ID		

For a class B address, the first two most significant bits are 10.14 bits indicate a network ID, and 16 bits indicate a local address. There are 16,348 class B networks in total.

Figure 1-3

			8	16	24	32
Class B IP address	1	0	Network ID	Host ID		

For a class C address, the first three most significant bits are 110.21 bits indicate a network ID, and 8 bits indicate a local address. There are 2,097,152 class C networks in total.

Figure 1-4

				8	16	24	32
Class C IP address	1	1	0	Network ID		Host ID	

For a class D address, the first four most significant bits are 1110 and other bits indicate a multicast address.

Figure 1-5

					8	16	24	32
Class D IP address	1	1	1	0	Multicast address			

The addresses with the first four most significant bits 1111 cannot be assigned. These addresses

1. Configuring IP Addresses and Services

are called class E addresses and are reserved.

When IP addresses are planned during network construction, IP addresses must be assigned based on the property of the network to be built. If the network needs to be connected to the Internet, users should apply for IP addresses to the corresponding agency. In China, you can apply to China Internet Network Information Center (CNNIC) for IP addresses. Internet Corporation for Assigned Names and Numbers (ICANN) is the final organization responsible for IP address assignment. If the network to be built is an internal private network, users do not need to apply for IP addresses. However, IP addresses cannot be assigned at random. It is recommended to assign dedicated private network addresses.

The following table lists reserved and available addresses.

Class	Address Range	Status
Class A network	0.0.0.0 - 0.255.255.255	Reserved
	1.0.0.0 - 126.255.255.255	Available
	127.0.0.0 - 127.255.255.255	Reserved
Class B network	128.0.0.0 - 191.254.255.255	Available
	191.255.0.0 - 191.255.255.255	Reserved
Class C network	192.0.0.0 - 192.0.0.255	Reserved
	192.0.1.0 - 223.255.254.255	Available
	223.255.255.0 - 223.255.255.255	Reserved
Class D network	224.0.0.0 - 239.255.255.255	Multicast address
Class E network	240.0.0.0 - 255.255.255.254	Reserved
	255.255.255.255	Broadcast address

Three address ranges are dedicated to private networks. These addresses are not used in the Internet. If the networks to which these addresses are assigned need to be connected to the

1. Configuring IP Addresses and Services

Internet, these IP addresses need to be converted into valid Internet addresses. The following table lists private address ranges. Private network addresses are defined in RFC 1918.

Class	Address Range	Status
Class A network	10.0.0.0 - 10.255.255.255	1 class A network
Class B network	172.16.0.0 - 172.31.255.255	16 class B networks
Class C network	192.168.0.0 - 192.168.255.255	256 class C networks

For assignment of IP addresses, TCP/UDP ports, and other codes, refer to RFC 1166.

Subnet Mask

A subnet mask is also a 32-bit value. The bits that identify the IP address are the network address. In a subnet mask, the IP address bits corresponding to the bits whose values are 1s are the network address, and the IP address bits corresponding to the bits whose values are 0s are the host address. For example, for class A networks, the subnet mask is 255.0.0.0. By using network masks, you can divide a network into several subnets. Subnetting means to use some bits of the host address as the network address, thus decreasing the host capacity, and increasing the number of networks. In this case, network masks are called subnet masks.

Broadcast Packet

Broadcast packets refer to the packets destined for all hosts on a physical network. QTECH products support two types of broadcast packets: (1) directed broadcast, which indicates that all hosts on the specified network are packet receivers and the host bits of a destination address are all 1s; (2) limited broadcast, which indicates that all hosts on all networks are packet receivers and the 32 bits of a destination address are all 1s.

ICMP Packet

Internet Control Message Protocol (ICMP) is a sub-protocol in the TCP/IP suite for transmitting control messages between IP hosts and network devices. It is mainly used to notify corresponding devices when the network performance becomes abnormal.

TTL

Time To Live (TTL) refers to the number of network segments where packets are allowed to pass

1. Configuring IP Addresses and Services

before the packets are discarded. The TTL is a value in an IP packet. It informs the network whether packets should be discarded as the packets stay on the network for a long time.

Features

Feature	Description
IP Address	The IP protocol can run on an interface only after the interface is configured with an IP address.
Broadcast Packet Processing	Broadcast addresses are configured and broadcast packets are forwarded and processed.
Sending ICMP Packets	ICMP packets are sent and received.
Limiting Transmission Rate of ICMP Error Packets	This function prevents Denial of Service (DoS) attacks.
IP MTU	Maximum Transmission Unit (MTU) of IP packets on an interface is configured.
IP TTL	The TTL of unicast packets and broadcast packets is configured.
IP Source Route	Source routes are checked.

1.3.1 IP Address

IP addresses are obtained on an interface in the following ways:

1. Manually configuring IP addresses
2. Obtaining IP addresses through DHCP
3. Borrowing IP addresses of other interfaces

These approaches are mutually exclusive. If you configure a new approach to obtain an IP address, the old IP address will be overwritten.

ℹ️ For details on how to obtain IP addresses through DHCP, see the "DHCP" chapter. The following describes the other three approaches for obtaining IP addresses.

Configuring the IP Address for an Interface

1. Configuring IP Addresses and Services

A device can receive and send IP packets only after the device is configured with an IP address. Only the interface configured with an IP address can run the IP protocol.

Configuring Multiple IP Addresses for an Interface

QTECH products support multiple IP address configuration on one interface, of which one is a primary IP address and the others are secondary IP addresses. Theoretically, the number of secondary IP addresses is not limited. However, secondary IP addresses must belong to different networks and secondary IP addresses must be in different networks from primary IP addresses. In network construction, secondary IP addresses are often used in the following circumstances:

- A network does not have enough host addresses. For example, a LAN now needs one class C network to allocate 254 addresses. However, when the number of hosts exceeds 254, one class C network is not enough and another class C network is needed. In this case, two networks need to be connected. Therefore, more IP addresses are needed.
- Many old networks are based on L2 bridged networks without subnetting. You can use secondary IP addresses to upgrade the network to a routing network based on IP layer. For each subnet, one device is configured with one IP address.
- When two subnets of one network are isolated by another network, you can connect the isolated subnets by creating a subnet of the isolated network and configuring a secondary address. One subnet cannot be configured on two or more interfaces of a device.

Borrowing an IP Addresses from Another Interface

One interface may not be configured with an IP address. To enable the interface, it must borrow an IP address from another interface.

- ℹ️ IP addresses of Ethernet interfaces, tunnel interfaces, and loopback interfaces can be borrowed. However, these interfaces cannot borrow IP addresses from other interfaces.
- ℹ️ The IP addresses of borrowed interfaces cannot be borrowed from other interfaces.
- ℹ️ If a borrowed interface has multiple IP addresses, only the primary IP address can be borrowed.
- ℹ️ The IP address of one interface can be lent to multiple interfaces.
- ℹ️ IP addresses of borrowing interfaces are always consistent with and vary with IP addresses of borrowed interfaces.

Related Configuration

Configuring an Interface with One or More IP Addresses

- By default, an interface is not configured with an IP address.
- The **ip address** command is used to configure an IP address for an interface.

1. Configuring IP Addresses and Services

- After an IP address is configured, the IP address can be used for communication when it passes conflict detection.
- The **ip address** *ip-address mask* **secondary** command can be used to configure multiple secondary IP addresses.

Borrowing an IP Address from Other Interfaces

- By default, an interface is not configured with an IP address.
- The **ip unnumbered** command can be used to borrow IP addresses from other interfaces.

1.3.2 Broadcast Packet Processing

**Working
Principle**

Broadcast is divided into two types. One is limited broadcast, and the IP address is 255.255.255.255. Because the broadcast is prohibited by routers, the broadcast is called local network broadcast. The other is directed broadcast. All host bits are 1s, for example, 192.168.1.255/24. The broadcast packets with these IP addresses can be forwarded.

If IP network devices forward limited broadcast packets (destination IP address is 255.255.255.255), the network may be overloaded, which severely affects network performance. This circumstance is called broadcast storm. Devices provide some approaches to confine broadcast storms within the local network and prevent continuous spread of broadcast storms. L2 network devices such as bridges and switches forward and spread broadcast storms.

The best way to avoid broadcast storm is to assign a broadcast address to each network, which is directed broadcast. This requires the IP protocol to use directed broadcast rather than limited broadcast to spread data.

For details about broadcast storms, see RFC 919 and RFC 922.

Directed broadcast packets refer to the broadcast packets destined for a subnet. For example, packets whose destination address is 172.16.16.255 are called directed broadcast packets. However, the node that generates the packets is not a member of the destination subnet.

After receiving directed broadcast packets, the devices not directly connected to the destination subnet forward the packets. After directed broadcast packets reach the devices directly connected to the subnet, the devices convert directed broadcast packets to limited broadcast packets

1. Configuring IP Addresses and Services

(destination IP address is 255.255.255.255) and broadcast the packets to all hosts on the destination subnet at the link layer.

Related Configuration

Configuring an IP Broadcast Address

- By default, the IP broadcast address of an interface is 255.255.255.255.
- To define broadcast packets of other addresses, run the **ip broadcast-address** command on the interface.

Forwarding Directed Broadcast Packets

- By default, directed broadcast packets cannot be forwarded.
- On the specified interface, you can run the **ip directed-broadcast** command to enable directed broadcast packets forwarding. In this way, the interface can forward directed broadcast packets to networks that are directly connected. Broadcast packets can be transmitted within the destination subnet without affecting forwarding of other directed broadcast packets.
- On an interface, you can define an Access Control List (ACL) to transmit certain directed broadcast packets. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.

1.3.3   Sending ICMP Packets

Working Principle

ICMP Protocol Unreachable Message

A device receives non-broadcast packets destined for itself, and he packets contain the IP protocol that cannot be processed by the device. The device sends an ICMP protocol unreachable message to the source host. Besides, if the device does not know a route to forward packets, it also sends an ICMP host unreachable message.

ICMP Redirection Message

Sometimes, a route may be less than optimal, which makes a device send packets from the interface that receives packets. If a device sends packets from an interface on which it receives the packets, the device sends an ICMP redirection message to the source, informing the source that the gateway is another device on the same subnet. In this way, the source sends subsequent packets according to the optimal path.

Error Message for TTL Timeout

1. Configuring IP Addresses and Services

When forwarding an IP packet of which TTL expires, a device responds to the source end with an error message indicating exceeded TTL. To prevent attacks after the route is traced, the functionality of sending such error messages can be disabled.

Timestamp Query

RFC 792 requires the system, after receiving an ICMP timestamp request query message, to return its current time. You can disable sending of such reply messages to avoid attacks aimed at time-based protocols. By this means, once received, ICMP timestamp request query messages are discarded.

Related
Configuration

Enabling ICMP Protocol Unreachable Message

- By default, the ICMP Protocol unreachable message function is enabled on an interface.
- You can run the [**no**] **ip unreachables** command to disable or enable the function.

Enabling ICMP Redirection Message

- By default, the ICMP redirection message function is enabled on an interface.
- You can run the [**no**] **ip redirects** command to disable or enable the function.

Enabling ICMP Mask Response Message

- By default, the ICMP mask response message function is enabled on an interface.
- You can run the [**no**] **ip mask-reply** command to disable or enable the function.

Enabling Error Message for TTL Timeout

- By default, the error message for TTL timeout function is enabled.
- You can run the [**no**] **ip ttl-expires enable** command to disable or enable the function.

Enabling Timestamp Query

- By default, the timestamp query function is enabled on an interface.
- You can run the [**no**] **ip icmp timestamp** command to disable or enable the function.

1.3.4   Limiting Transmission Rate of ICMP Error Packets

Working
Principle

This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm.

1. Configuring IP Addresses and Services

If an IP packet needs to be fragmented but the Don't Fragment (DF) bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively.

Related

Configuration

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by DF Bit in the IP Header

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval DF** command can be used to configure the transmission rate.

Configuring the Transmission Rate of Other ICMP Error Packets

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval** command can be used to configure the transmission rate.

1.3.5 IP MTU

Working

Principle

If an IP packet exceeds the IP MTU size, the RGOS software splits the packet. For all devices in the same physical network segment, the IP MTU of interconnected interfaces must be the same. You can adjust the link MTU of interfaces on QTECH products. After the link MTU of interfaces is changed, the IP MTU of interfaces will be changed. The IP MTU of interfaces automatically keeps consistent with the link MTU of interfaces. However, if the IP MTU of interfaces is adjusted, the link MTU of interfaces will not be changed.

Related

Configuration

Setting the IP MTU

- By default, the IP MTU of an interface is 1500.
- The **ip mtu** command can be used to set the IP packet MTU.

1.3.6 IP TTL

Working

Principle

1. Configuring IP Addresses and Services

An IP packet is transmitted from the source address to the destination address through routers. After a TTL value is set, the TTL value decreases by 1 every time when the IP packet passes a router. When the TTL value drops to zero, the router discards the packet. This prevents infinite transmission of useless packets and waste of bandwidth.

Related Configuration

Setting the IP TTL

- By default, the IP TTL of an interface is 64.
- The **ip ttl** command can be used to set the IP TTL of an interface.

1.3.7 Protecting IP Routed Ports

Working Principle

This command is used to forbid packets to come in and go out via the same routed port.

Related Configuration

Enabling Protection of IP Routed Ports

- By default, protection of IP routed ports is disabled.
- The **ip redirect-drop** command can be used to enable or disable the function.

1.3.8 IP Source Route

Working Principle

QTECH products support IP source routes. When a device receives an IP packet, it checks the options such as source route, loose source route, and record route in the IP packet header. These options are detailed in RFC 791. If the device detects that the packet enables one option, it responds; if the device detects an invalid option, it sends an ICMP parameter error message to the source and then discards the packet.

After the IP source route is enabled, the source route option is added to an IP packet to test the throughput of a specific network or help the packet bypasses the failed network. However, this may cause network attacks such as source address spoofing and IP spoofing.

Related Configuration

1. Configuring IP Addresses and Services

Configuring an IP Source Route

- By default, the IP source route function is enabled.
- The **ip source-route** command can be used to enable or disable the function.

1.4   Configuration

Configuration	Description and Command	
Configuring the IP Addresses of an Interface	⚠ (Mandatory) It is used to configure an IP address and allow the IP protocol to run on an interface.	
	ip address	Manually configures the IP address of an interface.
	ip unnumbered	Borrows an IP address from another interface.
Configuring Broadcast Forwarding	⚠ (Optional) It is used to set an IP broadcast address and enable directed broadcast forwarding.	
	ip broadcast-address	Configures an IP broadcast address.
	ip directed-broadcast	Enables directed broadcast forwarding.
Configuring ICMP Forwarding	⚠ (Optional) It is used to enable ICMP packet forwarding.	
	ip unreachables	Enables ICMP unreachable messages and host unreachable messages.
	ip redirects	Enables ICMP redirection messages.
	ip mask-reply	Enables ICMP mask response messages.
	ip ttl-expires enable	Enables error messages for TTL timeout.

1. Configuring IP Addresses and Services

	ip icmp timestamp	Enables ICMP timestamp query.
Configuring the Transmission Rate of ICMP Error Packets	⚠ Optional.	
	ip icmp error-interval DF	Configures the transmission rate of ICMP destination unreachable packets triggered by the DF bit in the IP header.
	ip icmp error-interval	Configures the transmission rate of ICMP error packets and ICMP redirection packets.
Setting the IP MTU	⚠ (Optional) It is used to configure the IP MTU on an interface.	
	ip mtu	Sets the MTU value.
Setting the IP TTL	⚠ (Optional) It is used to configure the TTL of unicast packets and broadcast packets.	
	ip ttl	Sets the TTL value.
Configuring an IP Source Route	⚠ (Optional) It is used to check the source routes.	
	ip source-route	Enables the IP source route function.

1.4.1   Configuring the IP Addresses of an Interface

Configuration Effect

Configure the IP address of an interface for communication.

Notes

- N/A

Configuration

1. Configuring IP Addresses and Services

Steps

Configuring the IP Address of an Interface

- Mandatory
- Perform the configuration in L3 interface configuration mode.

Borrowing an IP Addresses from Another Interface

- Optional
- If a point-to-point interface is not configured with an IP address, borrow an IP address from another interface.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

Manually Configuring the IP Address of an Interface

Command	ip address *ip-address network-mask* [secondary]
Parameter Description	*ip- address*: 32-bit IP address, with 8 bits for each group. The IP address is expressed in decimal and groups are separated by a full stop (.). *network-mask*: 32-bit network mask. Value 1 indicates the mask bit and 0 indicates the host bit. Every 8 bits form one group. The network mask is expressed in decimal and groups are separated by a full stop (.). **secondary**: Secondary IP address.
Command Mode	Interface configuration mode
Usage Guide	N/A

Borrowing an IP Addresses from Another Interface

Command	ip unnumbered*interface-type interface-number*
Parameter	*interface-type*: Interface type.

1. Configuring IP Addresses and Services

Description	*interface-number*: Interface ID.
Command Mode	Interface configuration mode
Usage Guide	An unnumbered interface indicates that the interface is enabled with the IP protocol without an IP address assigned. An unnumbered interface needs to be associated with an interface configured with an IP address. For an IP packet generated on an unnumbered interface, the source IP address of the packet is the IP address of the associated interface. In addition, the routing protocol process decides whether to send a route update packet to the unnumbered interface according to its associated IP address. If you want to use an unnumbered interface, pay attention to the following limitations:
	An Ethernet interface cannot be set to an unnumbered interface.
	When a serial interface encapsulates SLIP, HDLC, PPP, LAPB, and Frame-Relay, the serial interface can be set to an unnumbered interface. During Frame
	-Relay encapsulation, however, only a point-to-point interface can be configured as an unnumbered interface. AnX.25 interface cannot be configured as an unnumbered interface.
	The **ping** command cannot be used to check whether an unnumbered interface is working properly because an unnumbered interface is not configured with an IP address. However, you can monitor the status of an unnumbered interface remotely through SNMP.
	A device cannot be cold started through an unnumbered interface.

Configuration Example

Configuring an IP Address for an Interface

Configuration Steps	Configure IP address 192.168.23.110 255.255.255.0 on interface GigabitEthernet 0/0.
	QTECH #configure terminal
	QTECH (config)#interface gigabitEthernet 0/0
	QTECH (config-if-GigabitEthernet 0/0)# no switchport
	QTECH (config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0
Verification	Run the **show ip interface** command to check whether the configuration takes effect.

QTECH
МИР ДОСТУПНЕЕ

www.qtech.ru

1. Configuring IP Addresses and Services

QTECH # show ip interface gigabitEthernet 0/0
 	
GigabitEthernet 0/0
 	
  IP interface state is: UP
 	
  IP interface type is: BROADCAST
 	
  IP interface MTU is: 1500
 	
  IP address is:
 	
    192.168.23.110/24 (primary)

1.4.2 Configuring Broadcast Forwarding

Configuration Effect

Set the broadcast address of an interface to 0.0.0.0 and enable directed broadcast forwarding.

Notes

N/A

Configuration Steps

Configuring an IP Broadcast Address

- (Optional) Some old hosts may identify broadcast address 0.0.0.0 only. In this case, set the broadcast address of the target interface to 0.0.0.0.
- Perform the configuration in L3 interface configuration mode.

Enabling Directed Broadcast Forwarding

- (Optional) If you want to enable a host to send broadcast packets to all hosts in a domain that it is not in, enable directed broadcast forwarding.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show running-config interface** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Broadcast Address

1. Configuring IP Addresses and Services

Command	ip broadcast-address *ip-address*
Parameter Description	*ip-address*: Broadcast address of an IP network.
Command Mode	Interface configuration mode
Usage Guide	Generally, the destination address of IP broadcast packets is all 1s, which is expressed as 255.255.255.255. The RGOS software can generate broadcast packets of other IP addresses through definition and receive self-defined broadcast packets and the broadcast packets with address 255.255.255.255.

Allowing Forwarding of Directed Broadcast Packets

Command	ip directed-broadcast [*access-list-number*]
Parameter Description	*access-list-number*: Access list number, ranging from 1 to 199 and from1300 to 2699. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.
Command Mode	Interface configuration mode
Usage Guide	If the no ip directed-broadcast command is run on an interface, the RGOS software will discard directed broadcast packets received from the network that is directly connected.

Configuration Example

Configuration Steps	**On interface gigabitEthernet 0/1, set the destination address of IP broadcast packets to 0.0.0.0 and enable directed broadcast forwarding.**
	QTECH #configure terminal
	QTECH (config)#interface gigabitEthernet 0/1
	QTECH (config-if-GigabitEthernet 0/1)# no switchport
	QTECH (config-if-GigabitEthernet 0/1)#ip broadcast-address 0.0.0.0
	QTECH (config-if-GigabitEthernet 0/1)#ip directed-broadcast

1. Configuring IP Addresses and Services

Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	QTECH #show running-config interface gigabitEthernet 0/1
	ip directed-broadcast
	ip broadcast-address 0.0.0.0

1.4.3   Configuring ICMP Forwarding

Configuration Effect

Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on an interface.

Notes

N/A

Configuration Steps

Enabling ICMP Unreachable Messages

- By default, ICMP unreachable messages are enabled.
- (Optional) The **no ip unreachables** command can be used to disable ICMP unreachable messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Redirection Messages

- By default, ICMP redirection messages are enabled.
- (Optional) The **no ip redirects** command can be used to disable ICMP redirection messages.
- Perform the configuration in L3 interface configuration mode.

Enabling Error Messages for TTL Timeout

- By default, error messages for TTL timeout are enabled.
- (Optional) The **no ip ttl-expires enable** command can be used to disable error messages for TTL timeout.
- Perform the configuration in global configuration mode.

Enabling Timestamp Query

- By default, timestamp query is enabled.
- (Optional) The **no ip icmp timestamp** command can be used to disable timestamp query.

1. Configuring IP Addresses and Services

- Perform the configuration in global configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Run the **show running-config** command to check whether error messages for TTL timeout are disabled.

Run the **show running-config** command to check whether timestamp query is disabled.

Related Commands

Enabling ICMP Unreachable Messages

Command	ip unreachables
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Redirection Messages

Command	ip redirects
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Mask Response Messages

Command	ip mask-reply

1. Configuring IP Addresses and Services

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling Error Messages for TTL Timeout

Command	no ip ttl-expires enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Timestamp Query

Command	no ip icmp timestamp
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

1. Configuring IP Addresses and Services

Configuration Steps	Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on interface gigabitEthernet 0/1.
	QTECH #configure terminal QTECH (config)# no ip ttl-expires enable QTECH (config)# no ip icmp timestamp QTECH (config)#interface gigabitEthernet 0/1 QTECH (config-if-GigabitEthernet 0/1)# no switchport QTECH (config-if-GigabitEthernet 0/1)# ip unreachables QTECH (config-if-GigabitEthernet 0/1)# ip redirects QTECH (config-if-GigabitEthernet 0/1)# ip mask-reply
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	QTECH #show running-config | include ip ttl-expires enable no ip ttl-expires enable QTECH #show running-config | include ip icmp timestamp no ip icmp timestamp QTECH #show ip interface gigabitEthernet 0/1 GigabitEthernet 0/1 ICMP mask reply is: ON Send ICMP redirect is: ON Send ICMP unreachabled is: ON

1.4.4   Configuring the Transmission Rate of ICMP Error Packets

Configuration Effect

Configure the transmission rate of ICMP error packets.

Notes

N/A

1. Configuring IP Addresses and Services

Configuration Steps

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header

- ▪ Optional
- ▪ Perform the configuration in global configuration mode.

Configuring the Transmission Rate of Other ICMP Error Packets

- ▪ Optional
- ▪ Perform the configuration in global configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header

Command	ip icmp error-interval DF *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is from 0 to 2,147,483,647 and the default value is 100 milliseconds. When the value is 0, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is from 1 to 200 and the default value is 10.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. If an IP packet needs to be fragmented but the DF bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other

1. Configuring IP Addresses and Services

	ICMP error packets, the ICMP destination unreachable packet (code 4) may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively. It is recommended to set the refresh cycle to integral multiples of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10milliseconds.

Configuring the Transmission Rate of Other ICMP Error Packets

Command	ip icmp error-interval *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is 0to 2,147,483,647, and the default value is 100 (ms). When the value is 0, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is 1to 200 and the default value is 10.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. It is recommended to set the refresh cycle to integral multiples of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds.

1. Configuring IP Addresses and Services

Configuration Example

Configuration Steps	Set the transmission rate of ICMP destination unreachable packets triggered the DF bit in IP header to 100 packets per second and the transmission rate of other ICMP error packets to 10 packets per second.
	QTECH (config)# ip icmp error-interval DF 1000 100 QTECH (config)# ip icmp error-interval 1000 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	QTECH #show running-config | include ip icmp error-interval ip icmp error-interval 1000 10 ip icmp error-interval DF 1000 100

1.4.5   Setting the IP MTU

Configuration Effect

Adjust the IP packet MTU.

Notes

N/A

Configuration Steps

- ▪ (Optional) When the IP MTU of interconnected interfaces is different on devices in the same physical network segment, set the IP MTU to the same value.
- ▪ Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

1. Configuring IP Addresses and Services

Setting the IP MTU

Command	ip mtu*bytes*
Parameter Description	*bytes*: IP packet MTU. The value range is from 68 to 1,500 bytes.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	Set the IP MTU of interface gigabitEthernet 0/1 to 512 bytes.
	QTECH #configure terminal QTECH (config)#interface gigabitEthernet 0/1 QTECH (config-if-GigabitEthernet 0/1)# no switchport QTECH (config-if-GigabitEthernet 0/1)#ip mtu 512
Verification	Run the show ip interface command to check whether the configuration takes effect.
	QTECH # show ip interface gigabitEthernet 0/1 IP interface MTU is: 512

1.4.6   Setting the IP TTL

Configuration Effect

Modify the IP TTL value of an interface.

Notes

N/A

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

1. Configuring IP Addresses and Services

Configuration Steps

- ▪ Optional
- ▪ Perform the configuration in L3 interface configuration mode.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Setting the IP TTL

Command	ip ttl *value*
Parameter Description	*value*: TTL value. The value range is from 0 to 255.
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	Set the TTL of unicast packets to 100.
	QTECH #configure terminal QTECH (config)#ip ttl 100
Verification	Run the show run-config command to check whether the configuration takes effect.
	QTECH #show running-config ip ttl 100

1. Configuring IP Addresses and Services

1.4.7   Configuring Protection of IP Routed Ports

Configuration

Effect

Enable or disable protection of IP routed ports.

Notes

This configuration is supported on Layer 3 routed ports.

Configuration

Steps

- By default, protection of IP routed ports is disabled.
- (Optional) The **ip redirect-drop** command can be used to enable or disable the function.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related

Commands

Configuring Protection of IP Routed Ports

Command	ip redirect-drop
Parameter Description	N/A
Command Mode	Interface configuration mode.
Usage Guide	N/A

Configuration

Example

Configuration Steps	Requries packets coming in via the fastEthernet 0/1 interface to go out via other routed ports .

1. Configuring IP Addresses and Services

	QTECH (config)#interface gigabitEthernet 0/1 QTECH (config-if-GigabitEthernet 0/1)#ip redirect-drop
Verification	Run the show run-config command to check whether the configuration takes effect.
	QTECH #show running-config ip redirect-drop

1.4.8 Configuring an IP Source Route

Configuration Effect

Enable or disable the IP source route function.

Notes

N/A

Configuration Steps

- By default, the IP source route function is enabled.
- Optional) The **no ip source-route** command can be used to disable the IP source route function.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Source Route

Command	ip source-route
Parameter Description	N/A
Command Mode	Global configuration mode.

1. Configuring IP Addresses and Services

Usage Guide	N/A

Configuration Example

Configuration Steps	**Disable the IP source route function.**
	QTECH #configure terminal QTECH (config)#no ip source-route
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	QTECH #show running-config no ip source-route

1.5 Monitoring

Displaying

Description	Command
Displays the IP address of an interface.	**show ip interface** [*interface-type interface-number* | **brief**]
Displays IP packet statistics.	**show ip packet statistics** [**total** | *interface-name*]
Displays statistics on sent and received IP packets in the protocol stack.	**show ip packet queue**

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

2 CONFIGURING ARP

2.1 Overview

In a local area network (LAN), each IP network device has two addresses: 1) local address. Since the local address is contained in the header of the data link layer (DLL) frame, it is a DLL address. However, it is processed by the MAC sublayer at the DLL and thereby is usually called the MAC address. MAC addresses represent IP network devices on LANs. 2) network address. Network addresses on the Internet represent IP network devices and also indicate the networks where the devices reside.

In a LAN, two IP devices can communicate with each other only after they learn the 48-bit MAC address of each other. The process of obtaining the MAC address based on the IP address is called address resolution. There are two types of address resolution protocols: 1) Address Resolution Protocol (ARP); 2) Proxy ARP. ARP and Proxy ARP are described respectively in RFC 826 and RFC 1027.

ARP is used to bind the MAC address with the IP address. When you enter an IP address, you can learn the corresponding MAC address through ARP. Once the MAC address is obtained, the IP-MAC mapping will be saved to the ARP cache of the network device. With the MAC address, the IP device can encapsulate DLL frames and send them to the LAN. By default, IP and ARP packets on the Ethernet are encapsulated in Ethernet II frames.

Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol
- RFC 1027: Using ARP to implement transparent subnet gateways

2.2 Applications

Application	Description
LAN-based ARP	A user learns the MAC addresses of other users in the same network segment through ARP.
Proxy ARP-based Transparent Transmission	With Proxy ARP, a user can directly communicate with users in another network without knowing that it exists.

2. Configuring ARP

2.2.1 LAN-based ARP

Scenario

ARP is required in all IPv4 LANs.

- A user needs to learn the MAC addresses of other users through ARP to communicate with them.

Figure 2-1

C:192.168.23.3/24   D:192.168.23.4/24   E:192.168.23.5/24
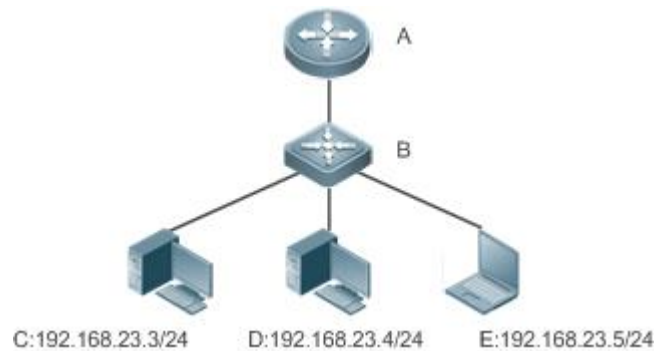
Remarks	A is a router.
	A is a router.
	B is a switch. It acts as the gateway.
	C, D, and E are hosts.

Deployment

- Enable ARP in a LAN to implement IP-MAC mapping.

2.2.2 Proxy ARP-based Transparent Transmission

Scenario

Transparent transmission across IPv4 LANs is performed.

- Enable Proxy ARP on the router to achieve direct communication between users in different network segments.

2. Configuring ARP

Figure 2-2
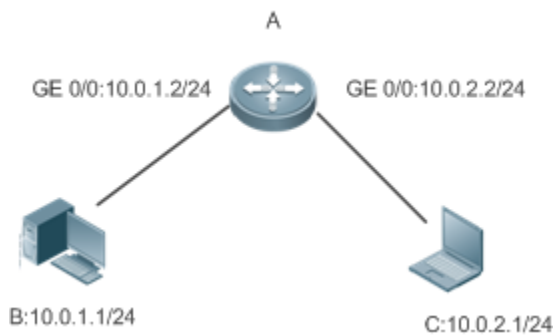
Remark s	A is a router connecting two LANs.
	B and C are hosts in different subnets. No default gateway is configured for them.

Deployment

- Enable Proxy ARP on the subnet gateway. After configuration, the gateway can act as a proxy to enable a host without any route information to obtain MAC addresses of IP users in other subnets.

2.3 Features

Overview

Feature	Description
Static ARP	Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.
ARP Attributes	Users can specify the ARP entry timeout, ARP request retransmission times and interval, and maximum number of unresolved ARP entries.

2. Configuring ARP

Gratuitous ARP	Gratuitous ARP is used to detect IP address conflicts and enable peripheral devices to update ARP entries.
Proxy ARP	A proxy replies to the ARP requests from other devices in different subnets.
Local Proxy ARP	A proxy replies to the ARP requests from other devices in the same subnet.
Any IP ARP	Users can access the network without changing the IP address and gateway.
ARP Trustworthiness Detection	Neighbor Unreachable Detection (NUD) is used to ensure that correct ARP entries are learned.
Scheduled Automatic ARP Scanning	Enable scheduled automatic ARP scanning on neighbors in the LAN.
ARP-based IP Guard	You can set the number of IP packets for triggering ARP drop to prevent a large number of unknown unicast packets from being sent to the CPU.
Refraining from Sending ARP Requests to Authentication VLANs	The device refrains from sending ARP broadcast requests to authentication VLANs to reduce the number of ARP broadcast requests in the network.
Fast Aging of ARP Entries	Enable fast aging of fast aging of ARP entries on an interface.

2.3.1   Static ARP

Static ARP entries can be configured manually or assigned by the authentication server. The manually configured ones prevail. Static ARP can prevent the device from learning incorrect ARP entries.

**Working
Principle**

If static ARP entries are configured, the device does not actively update ARP entries and these ARP entries permanently exist.

When the device forwards Layer-3 packets, the static MAC address is encapsulated in the Ethernet

2. Configuring ARP

header as the destination MAC address.

Related Configuration

Enabling Static ARP

Run the **arp** [**vrf** *name*] *ip-address mac-address type* command in global configuration mode to configure static ARP entries. By default, no static ARP entry is configured. Users can bind static ARP entries to individual VRF instances or the global VRF instance. ARP encapsulation supports only the Ethernet II type, which is represented by ARPA.

2.3.2   ARP Attributes

Users can specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on an interface.

Working Principle

ARP Timeout

The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP entry timeout expires, the device sends a unicast ARP request packet to detect whether the peer end is online. If it receives an ARP reply from the peer end, it does not delete this ARP entry. Otherwise, the device deletes this ARP entry.

When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth.

ARP Request Retransmission Interval and Times

The device consecutively sends ARP requests to resolve an IP address to a MAC address. The shorter the retransmission interval is, the faster the resolution is. The more times the ARP request is retransmitted, the more likely the resolution will succeed and the more bandwidth ARP will consume.

Maximum Number of Unresolved ARP Entries

In a LAN, ARP attacks and scanning may cause a large number of unresolved ARP entries generated on the gateway. As a result, the gateway fails to learn the MAC addresses of the users. To prevent such attacks, users can configure the maximum number of unresolved ARP entries.

Maximum Number of ARP Entries on an Interface

2. Configuring ARP

Configure the maximum number of ARP entries on a specified interface to prevent ARP entry resource waste.

Related Configuration

Configuring the ARP Timeout

Run the **arp timeout** *seconds* command in interface configuration mode to configure the ARP timeout. The default timeout is 3,600 seconds. You can change it based on actual situations.

Configuring the ARP Request Retransmission Interval and Times

- Run the **arp retry interval** *seconds* command in global configuration mode to configure the ARP request retransmission interval. The default interval is 1 second. You can change it based on actual situations.
- Run the **arp retry times** *number* command in global configuration mode to configure the ARP request retransmission times. The default number of retransmission times is 5. You can change it based on actual situations.

Configuring the Maximum Number of Unresolved ARP Entries

Run the **arp unresolve** *number* command in global configuration mode to configure the maximum number of unresolved ARP entries. The default value is the maximum number of ARP entries supported by the device. You can change it based on actual situations.

Configuring the Maximum Number of ARP Entries on an Interface

Run the **arp cache interface-limit** *limit* command in interface configuration mode to configure the maximum number of ARP entries learned on an interface. The default number is 0. You can change it based on actual situations. This command also applies to static ARP entries.

2.3.3   Gratuitous ARP

Working Principle

Gratuitous ARP packets are a special type of ARP packets. In a gratuitous ARP packet, the source and destination IP addresses are the IP address of the local device. Gratuitous ARP packets have two purposes:

1. IP address conflict detection. If the device receives a gratuitous packet and finds the IP address in

2. Configuring ARP

the packet the same as its own IP address, it sends an ARP reply to notify the peer end of the IP address conflict.

2. ARP update. When the MAC address of an interface changes, the device sends a gratuitous ARP packet to notify other devices to update ARP entries.

The device can learn gratuitous ARP packets. After receiving a gratuitous ARP packet, the device checks whether the corresponding dynamic ARP entry exists. If yes, the device updates the ARP entry based on the information carried in the gratuitous ARP packet.

Related Configuration

Enabling Gratuitous ARP

Run the **arp gratuitous-send interval** *seconds* [*number*] command in interface configuration mode to enable gratuitous ARP. This function is disabled on interfaces by default. Generally you need to enable this function on the gateway interface to periodically update the MAC address of the gateway on the downlink devices, which prevents others from faking the gateway.

2.3.4 Proxy ARP

Working Principle

The device enabled with Proxy ARP can help a host without any route information to obtain MAC addresses of IP users in other subnets. For example, if the device receiving an ARP request finds the source IP address in a different network segment from the destination IP address and knows the route to the destination address, the device sends an ARP reply containing its own Ethernet MAC address. This is how Proxy ARP works.

Related Configuration

Enabling Proxy ARP

- Run the **ip proxy-arp** command in interface configuration mode to enable Proxy ARP.
- This function is disabled by default.

2.3.5 Local Proxy ARP

Working

2. Configuring ARP

Principle

Local Proxy ARP means that a device acts as a proxy in the local VLAN (common VLAN or sub VLAN).

After local Proxy ARP is enabled, the device can help users to obtain the MAC addresses of other users in the same subnet. For example, when port protection is enabled on the device, users connected to different ports are isolated at Layer 2. After local Proxy ARP is enabled, the device receiving an ARP request acts as a proxy to send an ARP reply containing its own Ethernet MAC address. In this case, different users communicate with each other through Layer-3 routes. This is how local Proxy ARP works.

Related
Configuration

Enabling Local Proxy ARP

- Run the **local-proxy-ar** command in interface configuration mode to enable local Proxy ARP.
- This function is disabled by default.
- This command is supported only on switch virtual interfaces (SVIs).

2.3.6   Any IP ARP

Working
Principle

If any IP ARP is enabled, users can access the network with any IP address. This applies when a user is using his own laptop in a hotel and wants to access the network without changing the IP address and gateway. If the gateway receiving an ARP request finds the source IP address in a different subnet and the destination address possibly not its own address, the gateway still sends an ARP reply and creates a direct route for the user.

Related
Configuration

Enabling Any IP ARP

Run the **arp any-ip** command in interface configuration mode to enable any IP ARP. This function is disabled on interfaces by default.

2.3.7   ARP Trustworthiness Detection

Working
Principle

The **arp trust-monitor enable** command is used to enable anti-ARP spoofing to prevent excessive useless ARP entries from occupying device resources. After ARP trustworthiness detection

2. Configuring ARP

is enabled on a Layer-3 interface, the device receives ARP request packets from this interface:

1. If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs NUD after 1 to 5 seconds. That is, the device begins to age the newly learned ARP entry and sends a unicast ARP request. If the device receives an ARP update packet from the peer end within the aging time, it stores the entry. If not, it deletes the entry.
2. If the corresponding ARP entry exists, NUD is not performed.
3. If the MAC address in the existing dynamic ARP entry is updated, the device also performs NUD.

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

After this function is disabled, NUD is not required for learning and updating ARP entries.

Related Configuration

Enabling ARP Trustworthiness Detection

Run the **arp trust-monitor enable** command in interface configuration mode to enable ARP trustworthiness detection. This function is disabled by default.

2.3.8 Scheduled Automatic ARP Scanning

Working Principle

When scheduled automatic ARP scanning is enabled, the network segment configured on the interface is scanned in a scheduled manner to learn the ARP entries of neighbors. The scanning interval ranges from 1 to 30 minutes, and the default interval is 5 minutes. The scanning rate ranges from 1 to 100 pps, and the default rate is 20 pps.

Related Configuration

Configuring ARP Scanning

▪ Run the **arp scan auto** *start-ip-address end-ip-address* command in interface configuration mode to enable scheduled automatic ARP scanning. By default, this function is disabled.
▪ Run the **arp scan interval** *minutes* command in global configuration mode to configure the scanning interval.
▪ Run the **arp scan rate** *rate-value* command in global configuration mode to configure the scanning rate.

2. Configuring ARP

2.3.9   ARP-based IP Guard

Working
Principle

When receiving unresolved IP packets, the switch cannot forward them through the hardware and thereby need to send them to the CPU for address resolution. If a large number of such packets are sent to the CPU, the CPU will be congested, affecting other services on the switch.

After ARP-based IP guard is enabled, the switch receiving ARP request packets counts the number of packets in which the destination IP address hits this ARP entry. If this number is equal to the configured number, the switch sets a drop entry in the hardware so that the hardware will not send the packets with this destination IP address to the CPU. After the address resolution is complete, the switch continues to forward the packets with this destination IP address.

Related
Configuration

Enabling ARP-based IP Guard

▪ Run the **arp anti-ip-attack** command in global configuration mode to configure the number of IP packets for triggering ARP drop.
▪ By default, the switch discards the corresponding ARP entry after it receives three unknown unicast packets containing the same destination IP address.

2.3.10 Refraining from Sending ARP Requests to Authentication VLANs

Working
Principle

In gateway authentication mode, all sub VLANs in a Super VLAN are authentication VLANs by default. Users in an authentication VLAN have to pass authentication to access the network. After authentication, a static ARP entry is generated on the device. Therefore, when accessing an authenticated user, the device does not need to send ARP requests to the authentication VLAN. If the device attempts to access users in an authentication-exemption VLAN, it only needs to send ARP requests to the authentication-exemption VLAN.

In gateway authentication mode, this function is enabled on the device by default. If the device needs to access authentication-exemption users in an authentication VLAN, disable this function.

Related

2. Configuring ARP

Configuration

Refraining from Sending ARP Requests to Authentication VLANs

- Run the **arp suppress-auth-vlan-req** command in interface configuration mode to refrain from sending ARP requests to authentication VLANs.
- This function is enabled by default.

2.3.11 ARP Packet Statistics Collection

Working
Principle

The device counts the total numbers of sent/received ARP requests/responses and packets of unknown types on all interfaces from power-on.

2.3.12 ARP Packet Rate Statistics Collection

Working
Principle

The device measures, at a minimum interval of 1s, the rate of ARP requests, ARP responses, and packets of unknown types received on each interface in a period of time.

2.3.13 Enabling Fast Aging of ARP Entries

Working
Principle

ARP entries cannot be learned under unusual circumstances. After MAC addresses age, ARP entries age fast so as to achieve fast route convergence.

Related
Configuration

Enabling Fast Aging of ARP Entries

- In interface configuration mode, run the **arp fast-aging enable** command to enable fast aging of ARP entries.
- By default, this function is disabled.

2.4 Configuration

Configuration	Description and Command	
Enabling Static ARP	⚠ (Optional) It is used to enable static IP-MAC binding.	
	arp	Enables static ARP.
Configuring ARP Attributes	⚠ (Optional) It is used to specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on an interface.	
	arp timeout	Configures the ARP timeout.
	arp retry interval	Configures the ARP request retransmission interval.
	arp unresolve	Configures the maximum number of unresolved ARP entries.
	arp cache interface-limit	Configures the maximum number of ARP entries on an interface.
Enabling Trusted ARP	⚠ (Optional) It is used to enable anti-ARP spoofing.	
	service trustedarp	Enables trusted ARP.
	arp trusted user-vlan	Enables VLAN redirection when a trusted ARP entry is added.
	arp trusted aging	Enables trusted ARP aging.
	arp trusted	Configures the capacity of trusted ARP entries.

2. Configuring ARP

[Enabling Gratuitous ARP](#)	⚠️ (Optional) It is used to detect IP address conflicts and enables peripheral devices to update ARP entries.	
	arp gratuitous-send interval	Enables gratuitous ARP.
[Enabling Proxy ARP](#)	⚠️ (Optional) It is used to act as a proxy to reply to ARP requests from the devices in different subnets.	
	ip proxy-arp	Enables Proxy ARP.
[Enabling Local Proxy ARP](#)	⚠️ (Optional) It is used to act as a proxy to reply to ARP requests from other devices in the same subnet.	
	local-proxy-arp	Enables local Proxy ARP.
[Enabling Any IP ARP](#)	⚠️ (Optional) It is used to allow users to access the network without changing the IP address and gateway.	
	arp any-ip	Enables any IP ARP.
[Enabling ARP Trustworthiness Detection](#)	⚠️ (Optional) It is used to unicast ARP request packets to ensure that correct ARP entries are learned.	
	arp trusted-monitor enable	Enables ARP trustworthiness detection.
[Configuring Scheduled Automatic ARP Scanning](#)	⚠️ (Optional) It is used to enable scheduled automatic ARP scanning on an interface.	
	arp scan auto	Enables scheduled automatic ARP scanning on an interface.
	arp scan interval	Configures the scheduled automatic ARP scanning interval in global configuration mode.
	arp scan rate	Configures the scheduled automatic ARP scanning rate in global configuration mode.

2. Configuring ARP

Enabling ARP-based IP Guard	⚠ (Optional) It is used to prevent a large number of IP packets from being sent to the CPU.	
	arp anti-ip-attack	Configures the number of IP packets for triggering ARP drop.
Refraining from Sending ARP Requests to Authentication VLANs	⚠ (Optional) It is used to refrain from sending ARP requests to authentication VLANs.	
	arp suppress-auth-vlan-req	Refrains from sending ARP requests to authentication VLANs.
Configuring ARP Packet Rate Statistics Collection	⚠ (Optional) It is used to enable ARP packet rate statistics collection and configure the interval for collecting rate statistics.	
	arp rate-statistic enable	Enables ARP packet rate statistics collection.
	arp rate-statistic compute interval	Configures the interval for collecting ARP packet rate statistics.
Enabling Fast Aging of ARP Entries	⚠ (Optional) It is used to enable fast aging of ARP entries.	
	arp fast-aging enable	Enables fast aging of ARP entries.

2.4.1 Enabling Static ARP

Configuration Effect

Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.

Notes

After a static ARP entry is configured, the Layer-3 switch learns the physical port corresponding to the MAC address in the static ARP entry before it performs Layer-3 routing.

Configuration Steps

2. Configuring ARP

Configuring Static ARP Entries

- ▪ Optional.
- ▪ You can configure a static ARP entry to bind the IP address of the uplink device with its MAC address to prevent MAC change caused by ARP attacks.
- ▪ Configure static ARP entries in global configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect. Or run the **show arp static** command to check whether a static ARP cache table is created.

Related Commands

Configuring Static ARP Entries

Command	arp [vrf *name* | oob] *ip-address mac-address type*
Parameter Description	**vrf** *name*: Specifies a VRF instance. The **name** parameter indicates the name of the VRF instance. **oob**: Configures a static ARP entry for a management port. *ip-address*: Indicates the IP address mapped to a MAC address, which is in four-part dotted-decimal format. *mac-address*: Indicates the DLL address, consisting of 48 bits. *type*: Indicates the ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.
Command Mode	Global configuration mode
Usage Guide	The RGOS queries a 48-bit MAC address based on a 32-bit IP address in the ARP cache table. Since most hosts support dynamic ARP resolution, usually the static ARP mapping are not configured. Use the **clear arp-cache** command to delete the dynamic ARP entries.

Configuration Example

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

2. Configuring ARP

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Configure a static ARP entry on B to statically bind the IP address of A with the MAC address.
	QTECH (config)#arp 192.168.23.1 08c6.b322.334B arpa
Verification	Run the **show arp static** command to display the static ARP entry.
	QTECH (config)#show arp static
	Protocol Address Age(min) Hardware Type Interface
	Internet 192.168.23.1 <static> 08c6.b322.334B arpa
	1 static arp entries exist.

Common Errors

- The MAC address in static ARP is incorrect.

2.4.2 Configuring ARP Attributes

Configuration Effect

Users can specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on an interface.

Configuration Steps

Configuring the ARP Timeout

- Optional.
- In a LAN, if a user goes online/offline frequently, it is recommended to set the ARP timeout small to delete invalid ARP entries as soon as possible.
- Configure the ARP timeout in interface configuration mode.

Configuring the ARP Request Retransmission Interval and Times

- Optional.
- If the network resources are insufficient, it is recommended to set the ARP request

2. Configuring ARP

retransmission interval great and the retransmission times small to reduce the consumption of network bandwidths.

- Configure the ARP request retransmission interval and times in global configuration mode.

Configuring the Maximum Number of Unresolved ARP Entries

- Optional.
- If the network resources are insufficient, it is recommended to set the maximum number of unresolved ARP entries small to reduce the consumption of network bandwidths.
- Configure the maximum number of unresolved ARP entries in global configuration mode.

Configuring the Maximum Number of ARP Entries on an Interface

- Optional.
- Configure the maximum number of ARP entries on an interface in interface configuration mode.

Verification

Run the **show arp timeout** command to display the timeouts of all interfaces.

Run the **show running-config** command to display the ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on an interface.

Related Commands

Configuring the ARP Timeout

Command	arp timeout *seconds*
Parameter Description	*seconds*: Indicates the timeout in seconds, ranging from 0 to 2,147,483. The default value is 3,600.
Command Mode	Interface configuration mode
Usage Guide	The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth. Unless otherwise specified, do not configure the ARP timeout.

2. Configuring ARP

Configuring the ARP Request Retransmission Interval and Times

Command	arp retry interval *seconds*
Parameter Description	*seconds*: Indicates the ARP request retransmission interval in seconds, ranging from 1 to 3,600. The default value is 1.
Command Mode	**Global configuration mode**
Usage Guide	If a device frequently sends ARP requests, affecting network performance, you can set the ARP request retransmission interval longer. Ensure that this interval does not exceed the ARP timeout.

Configuring the Maximum Number of Unresolved ARP Entries

Command	arp unresolve *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ARP entries, ranging from 1 to 8,192. The default value is 8,192.
Command Mode	Global configuration mode
Usage Guide	If a large number of unresolved entries exist in the ARP cache table and remain in the table after a while, it is recommended to use this command to limit the number of unresolved ARP entries.

Configuring the Maximum Number of ARP Entries on an Interface

Command	arp cache interface-limit *limit*
Parameter Description	*limit*: Indicates the maximum number of ARP entries that can be learned on an interface, including configured ARP entries and dynamically learned ARP entries. The value ranges from 0 to the ARP entry capacity supported by the device. 0 indicates no limit on this number.

2. Configuring ARP

Command Mode	Interface configuration mode
Usage Guide	Limiting the number of ARP entries on an interface can prevent malicious ARP attacks from generating excessive ARP entries on the device and occupying entry resources. The configured value must be equal to or greater than the number of the ARP entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ARP entry capacity supported by the device.

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	- Set the ARP timeout to 60 seconds on port GigabitEthernet 0/1. - Set the maximum number of learned ARP entries to 300 on port GigabitEthernet 0/1. - Set the ARP request retransmission interval to 3 seconds. - Set the ARP request retransmission times to 4. - Set the maximum number of unresolved ARP entries to 4,096. - Set the maximum number of learned ARP entries to 1,000 on Sub Slot 2 of Slot 1.
	QTECH (config)#interface gigabitEthernet 0/1 QTECH (config-if-GigabitEthernet 0/1)#arp timeout 60 QTECH (config-if-GigabitEthernet 0/1)#arp cache interface-limit 300 QTECH (config-if-GigabitEthernet 0/1)#exit QTECH (config)#arp retry interval 3 QTECH (config)#arp retry times 4 QTECH (config)#arp unresolve 4096
Verification	- Run the **show arp timeout** command to display the timeout of the interface. - Run the **show running-config** command to display the ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on the interface.

2. Configuring ARP

```
QTECH #show arp timeout
Interface          arp timeout(sec)
---------------------  ----------------
GigabitEthernet 0/1    60
GigabitEthernet 0/2    3600
GigabitEthernet 0/4    3600
GigabitEthernet 0/5    3600
GigabitEthernet 0/7    3600
VLAN 100           3600
VLAN 111           3600
Mgmt 0             3600

QTECH (config)# show running-config
arp unresolve 4096
arp retry times 4
arp retry interval 3
interface GigabitEthernet 0/1
 arp cache interface-limit 300
```

2.4.3   Enabling Gratuitous ARP

Configuration Effect

The interface periodically sends gratuitous ARP packets.

Configuration Steps

- Optional.
- When a switch acts as the gateway, enable gratuitous ARP on an interface to prevent other users from learning incorrect gateway MAC address in case of ARP spoofing.
- Enable gratuitous ARP in interface configuration mode.

Verification

2. Configuring ARP

Run the **show running-config interface** *<name>* command to check whether the configuration is successful.

Related Commands

Enabling Gratuitous ARP

Command	arp gratuitous-send interval *seconds* [*number*]
Parameter Description	*seconds*: Indicates the interval for sending a gratuitous ARP request. The unit is second. The value ranges from 1 to 3,600. *number*: Indicates the number of gratuitous ARP requests that are sent. The default value is 1. The value ranges from 1 to 100.
Command Mode	Interface configuration mode
Usage Guide	If a network interface of a device acts as the gateway for downstream devices but a downstream device pretends to be the gateway, enable gratuitous ARP on the interface to advertise itself as the real gateway.

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Configure the GigabitEthernet 0/0 interface to send a gratuitous ARP packet every 5 seconds.
	QTECH (config-if-GigabitEthernet 0/0)#arp gratuitous-send interval 5
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.

2. Configuring ARP

```
QTECH #sh running-config interface gigabitEthernet 0/0

Building configuration...
Current configuration : 127 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 arp gratuitous-send interval 5
```

2.4.4 Enabling Proxy ARP

Configuration Effect

The device acts as a proxy to reply to ARP request packets from other users.

Notes

By default, Proxy ARP is disabled.

Configuration Steps

- Optional.
- If a user without any route information needs to obtain the MAC addresses of the IP users in other subnets, enable Proxy ARP on the device so that the device can act as a proxy to send ARP replies.
- Enable Proxy ARP in interface configuration mode.

Verification

Run the **show ip interface** [*name*] command to check whether the configuration takes effect.

Related Commands

Enabling Proxy ARP

2. Configuring ARP

Command	ip proxy-arp
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Enable Proxy ARP on port GigabitEthernet 0/0 .
	QTECH (config-if-GigabitEthernet 0/0)#ip proxy-arp
Verification	Run the show ip interface command to check whether the configuration takes effect.

2. Configuring ARP

```
QTECH #show ip interface gigabitEthernet 0/0
GigabitEthernet 0/0
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    No address configured
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachable is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Help address is: 0.0.0.0
  Proxy ARP is: ON
ARP packet input number: 0
  Request packet    : 0
  Reply packet      : 0
  Unknown packet    : 0
TTL invalid packet number: 0
ICMP packet input number: 0
  Echo request      : 0
  Echo reply        : 0
  Unreachable       : 0
  Source quench     : 0
  Routing redirect  : 0
```

2.4.5   Enabling Local Proxy ARP

Configuration Effect

2. Configuring ARP

The device acts as a proxy to reply to ARP request packets from other users in the same subnet.

Notes

Local Proxy ARP is supported only on SVIs.

Configuration Steps

- Optional.
- If a user enabled with port protection needs to communicate with users in the VLAN, enable local Proxy ARP on the device.
- Enable local Proxy ARP in interface configuration mode.

Verification

Run the **show run interface** [*name*] command to check whether the configuration takes effect.

Related Commands

Enabling Local Proxy ARP

Command	local-proxy-arp
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	**For the network topology, see Figure 2-1.**
Configuration Steps	Enable local Proxy ARP on the VLAN 1 interface.

QTECH МИР ДОСТУПНЕЕ | www.qtech.ru

2. Configuring ARP

	QTECH (config-if-VLAN 1)#local-proxy-arp
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	QTECH #show running-config interface vlan 1 Building configuration... Current configuration : 53 bytes interface VLAN 1 ip address 192.168.1.2 255.255.255.0 local-proxy-arp

2.4.6   Enabling Any IP ARP

Configuration Effect

Users can access the network with any IP address.

Notes

Any IP ARP is supported only on egress gateway products.

In the following two scenarios, users must modify the configuration before they can access the network.

1. The user's IP address is in the same network segment as the interface directly connected to the device. However, the IP address configured on the interface directly connected to the device is not the gateway address.
2. The user's IP address is not in the same network segment as the interface directly connected to the device, but in the network segment of another interface. That means an IP address conflict occurs.

As the user' IP address is not in the same network segment as the interface directly connected to the device, the dynamic ARP entries and direct routes are generated only when the user initiates ARP requests. Therefore, in some scenarios (including but not limited to the following ones), the user will not be able to access the network unless it clears the ARP entries and relearn the gateway address.

2. Configuring ARP

1. The device acts as a proxy to respond to ARP requests. After the user learns the MAC address of the device, dynamic ARP entries are cleared on the device. As a result, the user's dynamic ARP entries and direct routes are removed and the user cannot receive the reply packets.
2. The device acts as a proxy to respond to ARP requests. After the user learns the MAC address of the device, any IP ARP is disabled and then enabled again on the interface.

Note: Disabling any IP ARP on an interface will cause users' dynamic ARP entries and direct routes to be removed. Consequently, users cannot receive response packets.

On the other hand, if static ARP entries or ARP entries with VRRP IP addresses exist, dynamic ARP entries generated by any IP ARP will be overwritten or fail to be added, disabling the any IP ARP function.

Configuration Steps

- Optional.
- In a hotel, enable any IP ARP on the gateway so that users can access the network without changing the IP address.
- Enable any IP ARP in interface configuration mode.

Verification

Run the **show running-config interface** [*name*] command to check whether the configuration takes effect.

Related Commands

Enabling Any IP ARP

Command	arp any-ip
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	❗ Disabling any IP ARP on an interface will cause users' dynamic ARP entries and direct routes to be removed. Consequently, users cannot receive response packets. ❗ If static ARP entries or ARP entries with VRRP IP addresses exist, dynamic ARP entries generated by any IP ARP will be overwritten or fail to be added, disabling

	the any IP ARP function.

Configuration Example

Scenario Figure 2-3	
Configuration Steps	Enable any IP ARP on port GigabitEthernet 0/0.
	QTECH (config-if-GigabitEthernet 0/0)#arp any-ip
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	QTECH (config-if-GigabitEthernet 0/0)#sh run int gi0/0
	Building configuration...
	Current configuration : 140 bytes
	!
	interface GigabitEthernet 0/0
	duplex auto
	speed auto
	ip address 30.1.1.1 255.255.255.0
	arp gratuitous-send interval 5
	arp any-ip

2. Configuring ARP

2.4.7   Enabling ARP Trustworthiness Detection

Configuration Effect

Enable ARP trustworthiness detection. If the device receiving an ARP request packet fails to find the corresponding entry, it performs NUD. If the MAC address in the existing dynamic ARP entry is updated, the device immediately performs NUD to prevent ARP attacks.

Notes

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

Configuration Steps

- Optional.
- If there is a need for learning ARP entries, enable ARP trustworthiness detection on the device. If the device receiving an ARP request packet fails to find the corresponding entry, it needs to send a unicast ARP request packet to check whether the peer end exists. If yes, the device learns the ARP entry. If not, the device does not learn the ARP entry. If the MAC address in the ARP entry changes, the device will immediately perform NUD to prevent ARP spoofing.
- Enable ARP trustworthiness detection in interface configuration mode.

Verification

Run the **show running-config interface** *<name>* command to check whether the configuration take effect

Related Commands

Enabling ARP Trustworthiness Detection

2. Configuring ARP

Command	**arp trust-monitor enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	❗ Enable this function. If the corresponding ARP entry exists and the MAC address is not updated, the device does not perform NUD. ❗ Enable this function. If the MAC address of the existing dynamic ARP entry is updated, the device immediately performs NUD. ❗ After this function is disabled, the device does not perform NUD for learning or updating ARP entries.

Configuration Example

Scenario	**For the network topology, see Figure 2-1.**
Configuration Steps	Enable ARP trustworthiness detection on port GigabitEthernet 0/0.
	QTECH (config-if-GigabitEthernet 0/0)#arp trust-monitor enable
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.

```
QTECH #show running-config interface gigabitEthernet 0/0


Building configuration...
Current configuration : 184 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 arp trust-monitor enable
```

2.4.8 Configuring Scheduled Automatic ARP Scanning

Configuration Effect

After scheduled automatic ARP scanning is configured on an interface, the device scans neighbors in the specified range and learns ARP entries from the neighbors. After a time period of the scanning interval (5 minutes by default), the device starts the next scanning and learns the remaining ARP entries. The device repeats these operations until all ARP entries are learnt.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration in interface configuration mode.

Verification

Run the **show running-config interface** [*name*] command to display configurations.

Related Commands

Enabling Scheduled Automatic ARP Scanning

2. Configuring ARP

Command	arp scan auto *start-ip-address end-ip-address*
Parameter Description	*start-ip-address*: Specifies the start IP address of the ARP scan range. The start IP address must be smaller than or equal to the end IP address. *end-ip-address*: Specifies the end IP address of the ARP scan range. The end IP address must be greater than or equal to the start IP address.
Command Mode	Interface configuration mode
Usage Guide	This function is enabled to perform scheduled automatic ARP scanning once every 5 minutes by default. The IP address with existing neighboring ARP entries is not scanned. If you know the allocated IP address range in a LAN, you can specify the ARP scan range. The number of the specified IP addresses cannot be greater than 1,024. The start/end IP address of the ARP scan range must be in the same network segment as the interface IP address. ARP scanning takes effect on UP interfaces only.

Configuration Example
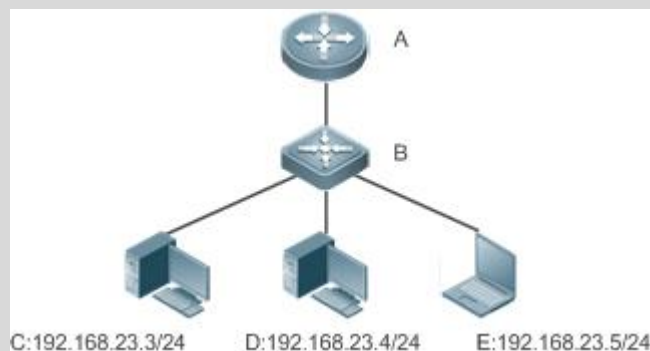
Scenario Figure 2-4	 C:192.168.23.3/24 D:192.168.23.4/24 E:192.168.23.5/24 **A is a router.** **B is a switch, serving as the gateway in the network segment where terminals reside.** **C, D, and E are terminals.**

2. Configuring ARP

Configuration Steps	Enable ARP scanning on an SVI.
	QTECH (config-if-VLAN 20)# arp scan auto 192.168.23.1 192.168.23.100
Verification	Run the **show running-config interface** command to display configurations.
	QTECH #sho running-config interface vlan 20 Building configuration... Current configuration : 57 bytes interface VLAN 20 arp scan auto 192.168.23.1 192.168.23.100 dut4(config-if-VLAN 20)#

Common Errors

1. The start IP address is greater than the end IP address in the configured ARP scanning range.
2. The start/end IP address is not in the same network segment as the interface IP address.

2.4.9 Enabling ARP-based IP Guard

Configuration Effect

When the CPU receives the specified number of packets in which the destination IP address hits the ARP entry, all packets with this destination IP address will not be sent to the CPU afterwards.

Notes

N/A

Configuration Steps

▪ Optional.

2. Configuring ARP

▪ By default, when three unknown unicast packets are sent to the CPU, the drop entry is set. Users can run this command to adjust the number of packets for triggering ARP drop based on the network environment. Users can also disable this function.

▪ Configure ARP-based IP guard in global configuration mode.

Verification

Run the **show run** command to check whether the configuration takes effect.

Related Commands

Enabling ARP-based IP Guard

Command	arp anti-ip-attack *num*
Parameter Description	*num*: Indicates the number of IP packets for triggering ARP drop. The value ranges from 0 to 100. 0 indicates that ARP-based IP guard is disabled. The default value is 3.
Command Mode	Interface configuration mode
Usage Guide	⬤ If hardware resources are sufficient, run the **arp anti-ip-attack** *num* command to set the number of IP packets for triggering ARP drop to a small value. If hardware resources are insufficient, run the **arp anti-ip-attack** *num* command to set the number of IP packets for triggering ARP drop to a large value, or disable this function.

Configuration Example

Scenario	**For the network topology, see Figure 2-1.**
Configuration Steps	Enable ARP-based IP guard on B. QTECH (config)#arp anti-ip-attack 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.

QTECH
МИР ДОСТУПНЕЕ

www.qtech.ru

2. Configuring ARP

	QTECH #show running-config Building configuration... Current configuration : 53 bytes arp anti-ip-attack 10

2.4.10 Refraining from Sending ARP Requests to Authentication VLANs

Configuration Effect

The device does not send ARP request packets to authentication VLANs.

Notes

This function is supported only on SVIs.

Configuration Steps

- ▪ Optional.
- ▪ In gateway authentication mode, the device does not send ARP request packets to authentication VLANs by default. If the device needs to send ARP request packets to authentication VLANs, run the **no arp suppress-auth-vlan-req** command to disable this function.
- ▪ Perform this configuration in interface configuration mode.

Verification

Run the **show run interface** *<name>* command to check whether the configuration takes effect.

Related Commands

Refraining from Sending ARP Requests to Authentication VLANs

Command	arp suppress-auth-vlan-req

2. Configuring ARP

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Disable the VLAN 2 interface from refraining from sending ARP requests to authentication VLANs. QTECH (config-if-VLAN 2)#no arp suppress-auth-vlan-req
Verification	Run the **show running-config interface** *<name>* command to check whether the configuration takes effect.
	QTECH #show running-config interface vlan 2 Building configuration... Current configuration : 53 bytes interface VLAN 2 ip address 192.168.1.2 255.255.255.0 no arp suppress-auth-vlan-req

2.4.11 Configuring ARP Packet Rate Statistics Collection

Configuration Effect

Measure the rate of receiving/sending ARP packets on each interface.

2. Configuring ARP

Notes

The default sampling interval is 5s, but the rate is measured at an interval of 1s.

Configuration Steps

- (Optional) Configure ARP packet rate statistics collection when needed.
- Perform the configuration in global configuration mode.

Command	arp rate-statistic enable
Parameter Description	N/A
Defaults	ARP packet rate statistics collection is disabled by default.
Command Mode	Global configuration mode
Usage Guide	ARP packet rate statistics collection is disabled by default. If the command result of **show arp rate-statistic** shows that statistics are all 0s, run the **show run-config** command to display configurations. If the function is not enabled, run the **arp rate-statistic enable** command to enable the function. To disable the function, run the **no arp rate-statistic enable** command.

Configuring the Interval for Collecting ARP Packet Rate Statistics

- (Optional) Configure the interval for collecting ARP packet rate statistics if the default value (5s) does not meet requirements.
- Perform the configuration in global configuration mode.

Command	arp rate-statistic compute interval *seconds*
Parameter Description	*seconds*: Indicates the interval in seconds, which cannot be less than 1s.
Defaults	The default value is 5s.

2. Configuring ARP

Command Mode	Global configuration mode
Usage Guide	If ARP packets are received/sent at an undesired rate on many interfaces, appropriately adjust the interval for collecting ARP packet rate statistics.

Verification

Run the **show running-config** command to display configurations.

Configuration Example

Configuration Steps	Enable ARP packet rate statistics collection in global configuration mode.
	QTECH (config)#arp rate-statistic enable
Verification	Run the **show running-config** command to display configurations.
	QTECH (config)#arp rate-statistic enable QTECH (config)#show running-config ! arp rate-statistic enable arp rate-statistic timeout 10 ! QTECH (config)#

Configuration Steps	Configure the interval for collecting ARP packet rate statistics in global configuration mode.
	QTECH (config)#arp rate-statistic compute interval 10
Verification	Run the **show running-config** command to display configurations.

2. Configuring ARP

```
QTECH (config)#arp rate-statistic enable
QTECH (config)#show running-config
!
arp rate-statistic enable
arp rate-statistic compute interval 10
!
QTECH (config)#
```

2.4.12 Enabling Fast Aging of ARP Entries

Configuration Effect

ARP entries cannot be learned under unusual circumstances. After MAC addresses age, ARP entries age fast.

Notes

N/A

Configuration Steps

- Optional.
- Perform the configuration in interface configuration mode.
- Only SVI and Overlay Router interfaces are supported.

Verification

Run the **show run** command to check whether the configuration is successful.

Related Commands
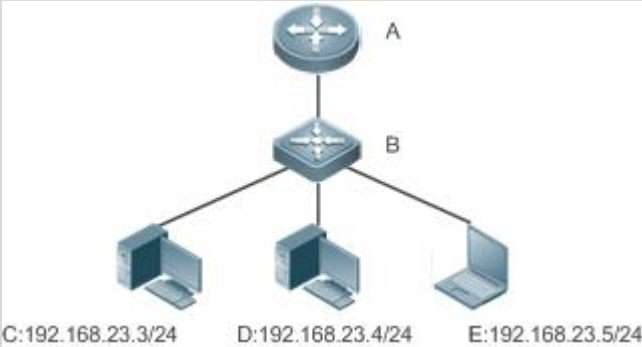
Enabling Fast Aging of ARP Entries

Command	arp fast-aging enable
Parameter Description	N/A
Command Mode	Interface configuration mode

2. Configuring ARP

Usage Guide	By default, dynamic ARP entries start aging one hour after the aging of their corresponding MAC addresses. If this feature is configured, after their corresponding MAC address age, the dynamic ARP entries age immediately.
	ℹ This command is supported on SVI and Overlay Router interfaces.
	ℹ When ARP-to-host conversion is configured, it is recommended to enable this function at the same time, to help achieve fast route convergence.

Configuration Example

Scenario Figure 2-5	C:192.168.23.3/24 D:192.168.23.4/24 E:192.168.23.5/24 **A: Router** **B: Switch serving as the gateway for the users** **C, D and E: Users**
Configuration Steps	Enabling fast aging of ARP entries on the SVI 2 interface.
	QTECH (config-if-VLAN 2)#arp fast-aging enable
Verification	Run the **show running-config** command to check whether the configuration is successful.
	QTECH #show running-config interface VLAN 2 ! arp fast-aging enable !

Common Errors

2. Configuring ARP

N/A

2.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears dynamic ARP entries. In gateway authentication mode, dynamic ARP entries in authentication VLANs are not cleared.	**clear arp-cache**
Clears ARP packet statistics.	**clear arp-cache packet statistics** [*interface*]

Displaying

Description	Command
Displays the ARP table in detail.	**show arp** [**detail**] **[** *interface-type interface-number* **|** [**vrf** *vrf-name*] [*ip* [*mask*]	*mac-address*	**static**	**complete**	**incomplete**]
Displays the ARP table.	**show ip arp [vrf** *vrf-name* **]**
Displays the ARP entry counter.	**show arp counter**
Displays the timeout of dynamic ARP entries.	**show arp timeout**
Displays ARP packet statistics.	**show arp packet statistics** [*interface*]
Displays ARP packet rate statistics.	**show arp rate-statistic** [*interface*]

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs ARP packet sending and receiving.	**debug arp**
Debugs the creation and deletion of ARP entries.	**debug arp event**

3 CONFIGURING IPV6

3.1 Overview

As the Internet develops rapidly and IPv4 address space is becoming exhausted, IPv4 limitations become more and more obvious. At present, many researches and practices on Internet Protocol Next Generation (IPng) have been conducted. The IPng working group of the Internet Engineering Task Force (IETF) has formulated an IPng protocol named IP Version 6 (IPv6), which is described in RFC 2460.

Main Features

Larger Address Space

Compared with 32 bits in an IPv4 address, the length of an IPv6 address is extended to 128 bits. Therefore, the address space has approximately 2^{128} addresses. IPv6 adopts a hierarchical address allocation mode to support address allocation of multiple subnets from the Internet core network to intranet subnet.

Simpler Packet Header Format

Since the design principle of the IPv6 packet header is to minimize the overhead of the packet header, some non-key fields and optional fields are removed from the packet header to the extended packet header. Therefore, although the length of an IPv6 address is four times of that of an IPv4 address, the IPv6 packet header is only two times of the IPv4 packet header. The IPv6 packet header makes device forwarding more efficient. For example, with no checksum in the IPv6 packet header, the IPv6 device does not need to process fragments (fragmentation is completed by the initiator).

Efficient Hierarchical Addressing and Routing Structure

IPv6 uses a convergence mechanism and defines a flexible hierarchical addressing and routing structure. Multiple networks at the same layer are represented as a uniform network prefix on the upstream device, greatly reducing routing entries maintained by the device and routing and storage overheads of the device.

3. Configuring IPv6

Easy Management: Plug and Play (PnP)

IPv6 provides automatic discovery and auto-configuration functions to simplify management and maintenance of network nodes. For example, Neighbor Discovery (ND), MTU Discovery, Router Advertisement (RA), Router Solicitation (RS), and auto-configuration technologies provide related services for PnP. Particularly, IPv6 offers two types of auto-configuration: stateful auto-configuration and stateless auto-configuration. In IPv4, Dynamic Host Configuration Protocol (DHCP) realizes auto-configuration of the host IP address and related parameters. IPv6 inherits this auto-configuration service from IPv4 and called it stateful auto-configuration (see DHCPv6). Besides, IPv6 also offers the stateless auto-configuration service.During stateless auto-configuration, a host automatically obtains the local address of the link, address prefix of the local device, and other related configurations.

Security

As an optional extension protocol of IPv4, Internet Protocol Security (IPSec) is a part of IPv6 to provide security for IPv6 packets. At present, IPv6 provides two mechanisms: Authentication Header (AH) and Encapsulated Security Payload (ESP). AH provides data integrity and authenticates IP packet sources to ensure that the packets originate from the nodes identified by the source addresses. ESP provides data encryption to realize end-to-end encryption.

Better QoS Support

A new field in the IPv6 packet header defines how to identify and process data streams. The Flow Label field in the IPv6 packet header is used to authenticate a data flow. Using this field, IPv6 allows users to propose requirements on the communication quality. , A device can identify all packets belonging to a specific data stream based on this field and process these packets according to user requirements.

New Protocol for Neighboring Node Interaction

IPv6 Neighbor Discovery Protocol (NDP) uses a series of Internet Control Message Protocol Version 6 (ICMPv6) packets to implement interactive management of neighboring nodes (nodes on the same link). IPv6 uses NDP packets and efficient multicast/unicast ND packets instead of broadcast-based Address Resolution Protocol (ARP) and Control Message Protocol Version 4 (ICMPv4) router discovery packets.

Extensibility

With strong extensibility, IPv6 features can be added to the extended packet header following the IPv6 packet header. Unlike IPv4, the IPv6 packet header can support at most 40 bytes of options. For an IPv6 packet, the length of the extended packet header is restricted only by the maximum number

3. Configuring IPv6

of bytes in the packet.

Protocols and Standards

- RFC 4291 - IP Version 6 Addressing Architecture
- RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification
- RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4861 - Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862 - IPv6 Stateless Address Auto-configuration
- RFC 5059 - Deprecation of Type 0 Routing Headers in IPv6

3.2 Applications

Application	Description
Communication Based on IPv6 Addresses	Two PCs communicate with each other using IPv6 addresses.

3.2.1 Communication Based on IPv6 Addresses

Scenario

As shown in Figure 3-1, Host 1 and Host 2 communicate with each other using IPv6 addresses.

Figure 3-1
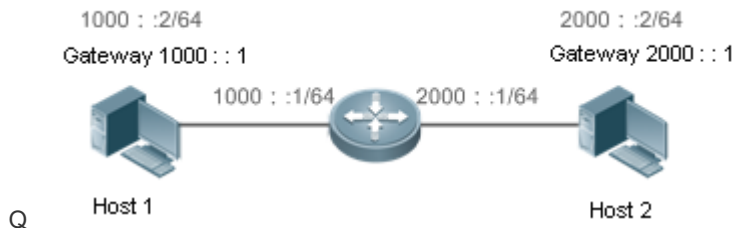
Deployment

Hosts can use the stateless address auto-configuration or DHCPv6 address assignment mode. After addresses are configured, hosts can communicate with each other using IPv6 addresses.

3. Configuring IPv6

3.3 Features

Overview

Feature	Description
IPv6 Address Format	The IPv6 address format makes IPv6 have a larger address space and flexible representation approach.
IPv6 Address Type	IPv6 identifies network applications based on addresses.
IPv6 Packet Header Format	IPv6 simplifies the fixed and extended packet headers to improve the data packet processing and forwarding efficiency of the device.
IPv6 PMTUD	A host dynamically discovers and adjusts the MTU size on the data Tx path, saving router resources and improving IPv6 network efficiency.
IPv6 Neighbor Discovery	ND functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD), and redirection.
IPv6 Source Routing	This feature is used to specify the intermediate nodes that a packet passes through along the path to the destination address. It is similar to the IPv4 loose source routing option and loose record routing option.
Restricting the Sending Rate of ICMPv6 Error Messages	This feature prevents DoS attacks.
IPv6 HOP-LIMIT	This feature prevents useless unicast packets from being unlimitedly transmitted on the network and wasting network bandwidth.
Refraining from Sending NS Packets to Authentication VLANs	In gateway authentication mode, a device is refrained from sending NS packets to authentication VLANs.

3. Configuring IPv6

Default Gateway on the Management Interface	The default gateway is configured on the management interface to generate a default route for this interface.

3.3.1   IPv6 Address Format

An IPv6 address is represented in the X:X:X:X:X:X:X:X format, where X is a 4-digit hexadecimal integer (16 bits). Each address consists of 8 integers, with a total of 128 bits (each integer contains 4 hexadecimal digits and each digit contains four bits). The following are three valid IPv6 addresses:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800:0:0:0:0:0:0:1

1080:0:0:0:8:800:200C:417A

These integers are hexadecimal, where A to F represent 10 to 15. Each integer in the address must be represented, except the leading zeros in each integer. If an IPv6 address contains a string of zeros (as shown in the second and third examples above), a double colon (::) can be used to represent these zeros. That is, 800:0:0:0:0:0:0:1 can be represented as 800::1.

A double colon indicates that this address can be extended to a complete 128-bit address. In this approach, only when the 16-bit integers are all 0s, can they can be replaced with a double colon. A double colon can exist once in an IPv6 address.

In IPv4/IPv6 mixed environment, an address has a mixed representation. In an IPv6 address, the least significant 32 bits can be used to represent an IPv4 address. This IPv6 address can be represented in a mixed manner, that is, X:X:X:X:X:X:d.d.d.d, where X is a hexadecimal integer and d is a 8-bit decimal integer. For example, 0:0:0:0:0:0:192.168.20.1 is a valid IPv6 address. It can be abbreviated to :::192.168.20.1. Typical applications are IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. If the first 96 bits are 0 in an IPv4-compatible IPv6 address, this address can be represented as ::A.B.C.D, e.g., ::1.1.1.1. IPv4-compatible addresses have been abolished at present. IPv4-mapped IPv6 addresses are represented as ::FFFF:A.B.C.D to represent IPv4 addresses as IPv6 addresses. For example, IPv4 address 1.1.1.1 mapped to an IPv6 address is represented as ::FFFF:1.1.1.1.

Since an IPv6 address is divided into two parts: subnet prefix and interface ID, it can be represented as an address with an additional value according to an address allocation method like Classless Inter-Domain Routing (CIDR). The additional value indicates how many bits (subnet prefix) in the address represent the network part. That is, the IPv6 node address contains the prefix length. The prefix length is separated from the IPv6 address by a slash. For example, in 12AB::CD30:0:0:0:0/60, the prefix length used for routing is 60 bits.

Related
Configuration

Configuring an IPv6 Address

- No IPv6 address is configured on interfaces by default.
- Run the **ipv6 address** command to configure an IPv6 address on an interface.
- After configuration, a host can communicate with others using the configured IPv6 address based on DAD.

3.3.2   IPv6 Address Type

RFC 4291 defines three types of IPv6 addresses:

- Unicast address: ID of a single interface. Packets destined to a unicast address are sent to the interface identified by this address.
- Multicast address: ID of an interface group (the interfaces generally belong to different nodes). Packets destined to a multicast address are sent to all interfaces included in this address.
- Anycast address: ID of an interface group. Packets destined to an anycast address are sent to one interface included in this address (the nearest interface according to the routing protocol).

⚠️ IPv6 does not define broadcast addresses.

These three types of addresses are described as follows:

Unicast Addresses

Unicast addresses fall into five types: unspecified address, loopback address, link-local address, site-local address, and global unicast address. At present, site-local addresses have been abolished. Except unspecified, loopback, and link-local addresses, all other addresses are global unicast addresses.

- Unspecified address

The unspecified address is 0:0:0:0:0:0:0:0, which is usually abbreviated to ::. It has two general purposes:

1. If a host has no unicast address when started, it uses the unspecified address as the source address to send an RS packet to obtain prefix information from the gateway and thereby generate a unicast address.
2. When an IPv6 address is configured for a host, the device detects whether the address conflicts with addresses of other hosts in the same network segment and uses the unspecified address as the source address to send a Neighbor Solicitation (NS) packet (similar to a free ARP packet).

- Loopback address

3. Configuring IPv6

The loopback address is 0:0:0:0:0:0:0:1, which is usually abbreviated to ::1. Similar to IPv4 address 127.0.0.1, the loopback address is generally used by a node to send itself packets.

- Link-local address

The format of a link-local address is as follows:

Figure 3-2

10 bits	54 bits	64 bits
1111 1110 10	0	Interface ID
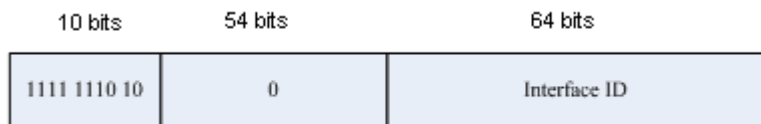
The link-local address is used on a single network link to assign IDs to hosts. The address identified by the first 10 bits in the prefix is the link-local address. A device never forwards packets in which the source or destination address contains the link-local address. The intermediate 54 bits in the address are all 0s. The last 64 bits represent the interface ID, which allows a single network to connect 2^{64}-1 hosts.

- Site-local address

The format of a site-local address is as follows:

Figure 3-3

10 bits	54 bits	64 bits
1111 1110 11	Subnet ID	Interface ID

A site-local address is used to transmit data within a site. A device never forwards packets in which the source or destination address contains the site-local address to the Internet. That is, these packets can be forwarded only within the site. A site can be assumed as an enterprise's local area network (LAN). Such addresses are similar to IPv4 private addresses such as 192.168.0.0/16. RFC 3879 has abolished site-local addresses. New addresses do not support the first 10 bits as the prefix and are all regarded as global unicast addresses. Existing addresses can continue to use this prefix.

- Global unicast address

The format of a global unicast address is as follows:

Figure 3-4

n bits	m bits	128- n- m bits
Global Routing Prefix	Subnet ID	Interface ID
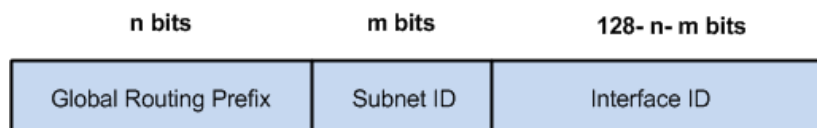
3. Configuring IPv6

Among global unicast addresses, there is a type of IPv4-embedded IPv6 addresses, including IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. They are used for interconnection between IPv4 nodes and IPv6 nodes.

The format of an IPv4-compatible IPv6 address is as follows:

Figure 3-5

80 bits	16 bits	32 bits
0000...0000	0000	IPv4 Address
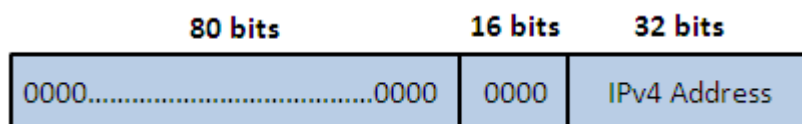
The format of an IPv4-mapped IPv6 address is as follows:

Figure 3-6

80 bits	16 bits	32 bits
0000...0000	FFFF	IPv4 Address
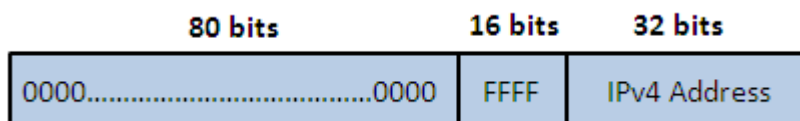
IPv4-compatible IPv6 addresses are mainly used on automatic tunnels. Nodes on automatic tunnels support both IPv4 and IPv6. Using these addresses, IPv4 devices transmit IPv6 packets over tunnels. At present, IPv4-compatible IPv6 addresses have been abolished. IPv4-mapped IPv6 addresses are used by IPv6 nodes to access IPv4-only nodes. For example, if the IPv6 application on an IPv4/IPv6 host requests to resolve the name of an IPv4-only host, the name server dynamically generates an IPv4-mapped IPv6 address and returns it to the IPv6 application.

Multicast Addresses

The format of an IPv6 multicast address is as follows:

```
|   8   | 4 | 4 |              112 bits            |
+--------+----+----+---------------------------------------------+
|11111111|flgs|scop|              group ID              |
+--------+----+----+---------------------------------------------+
```
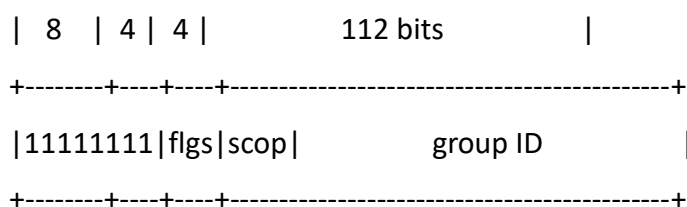
The first byte in the address is all 1s, representing a multicast address.

▪ Flag field

The flag field consists of four bits. Currently only the fourth bit is specified to indicate whether this address is a known multicast address assigned by the Internet Assigned Numbers Authority (IANA) or a temporary multicast address in a certain scenario. If the flag bit is 0, this address is a known multicast address. If the flag bit is 1, this address is a temporary multicast address. The remaining three flag bits are reserved for future use.

3. Configuring IPv6

▪ Scope field

The scope field consists of four bits to indicate the multicast range. That is, a multicast group includes the local node, local link, local site, and any node in the IPv6 global address space.

▪ Group ID field

The group ID consists of 112 bits to identify a multicast group. A multicast ID can represent different groups based on the flag and scope fields.

IPv6 multicast addresses are prefixed with FF00::/8. One IPv6 multicast address usually identifies interfaces on a series of different nodes. After a packet is sent to a multicast address, the packet is then forwarded to the interfaces on each node identified by this multicast address. For a node (host or device), you must add the following multicast addresses:

1. Multicast address for all nodes on the local link, that is, FF02::1
2. Solicited-node multicast address, prefixed with FF02:0:0:0:0:1:FF00:0000/104

If the node is a device, it also has to be added to the multicast address of all devices on the local link, that is, FF02::2.

The solicited-node multicast address corresponds to the IPv6 unicast and anycast address. You must add a corresponding solicited-node multicast address for each configured unicast and anycast address of an IPv6 node. The solicited-node multicast address is prefixed with FF02:0:0:0:0:1:FF00:0000/104. The remaining 24 bits are composed of the least significant 24 bits of the unicast or anycast address. For example, if the unicast address is FE80::2AA:FF:FE21:1234, the solicited-node multicast address is FF02::1:FF21:1234.

The solicited-node multicast address is usually used in NS packets. Its address format is as follows:

Figure 3-7
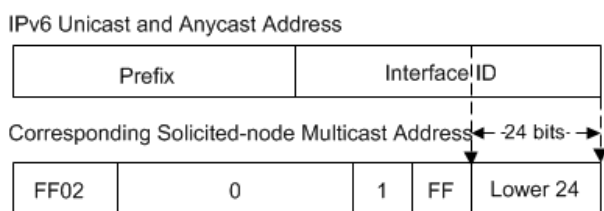
Anycast Addresses

Similar to a multicast address, an anycast address can also be shared by multiple nodes. The difference is that only one node in the anycast address receives data packets while all nodes included in the multicast address receive data packets. Since anycast addresses are allocated to the normal IPv6 unicast address space, they have the same formats with unicast addresses. Every member in an anycast address must be configured explicitly for easier recognition.

⚠ Anycast addresses can be allocated only to devices and cannot be used as source addresses of

3. Configuring IPv6

packets.

RFC 2373 redefines an anycast address called subnet-router anycast address. Figure 3-8 shows the format of a subnet-router anycast address. Such an address consists of the subnet prefix and a series of 0s (interface ID).

The subnet prefix identifies a specified link (subnet). Packets destined to the subnet-router anycast address will be forwarded to a device on this subnet. A subnet-router anycast address is usually used by the application on a node to communicate with a device on a remote subnet.

Figure 3-8

Format of a Subnet-router Anycast Address
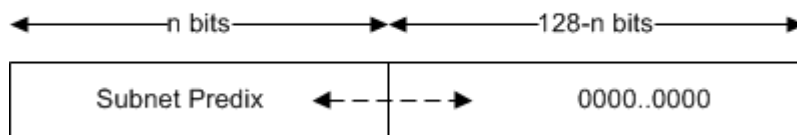
**Related
Configuration**

Configuring an IPv6 Address

- No IPv6 address is configured on interfaces by default.
- Run the **ipv6 address** command to configure the IPv6 unicast address and anycast address of an interface.
- After an interface goes up, it will automatically join the corresponding multicast group.

3.3.3 IPv6 Packet Header Format

Figure 3-9 shows the format of the IPv6 packet header.

Figure 3-9

3. Configuring IPv6
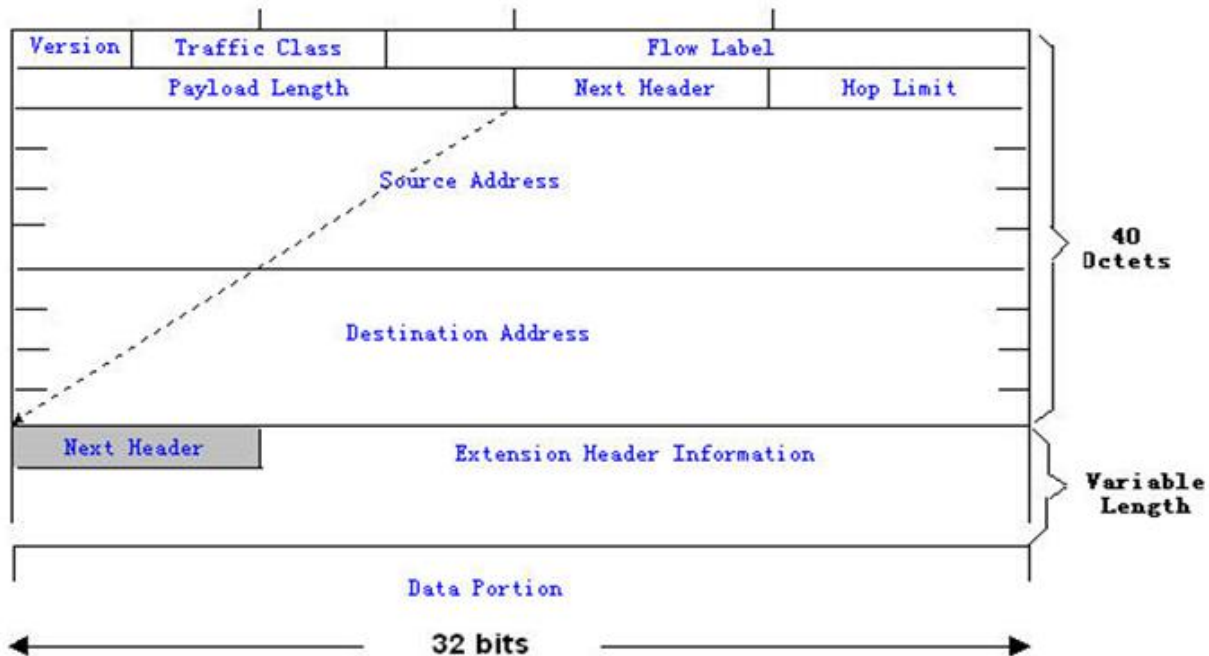
The IPv4 packet header is in unit of four bytes. The IPv6 packet header consists of 40 bytes, in unit of eight bytes. The IPv6 packet header has the following fields:

- Version

This field consists of 4 bits. In an IPv6 address, this field must be 6.

- Traffic Class

This field consists of 8 bits. This field indicates the service provided by this packet, similar to the TOS field in an IPv4 address.

- Flow Label

This field consists of 20 bits to identify packets belonging to the same service flow. One node can act as the Tx source of multiple service flows. The flow label and source address uniquely identify one service flow.

- Payload Length

This field consists of 16 bits, including the packet payload length and the length of IPv6 extended options (if available). That is, it includes the IPv6 packet length except the IPv6 packet header.

- Next Header

This field indicates the protocol type in the header field following the IPv6 packet header. Similar to the Protocol field in the IPv4 address header, the Next Header field is used to indicate whether the upper layer uses TCP or UDP. It can also be used to indicate existence of the IPv6 extension header.

3. Configuring IPv6

- Hop Limit

This field consists of 8 bits. Every time a device forwards a packet, the field value reduced by 1. If the field value reaches 0, this packet will be discarded. It is similar to the Lifetime field in the IPv4 packet header.

- Source Address

This field consists of 128 bits and indicates the sender address in an IPv6 packet.

- Destination Address

This field consists of 128 bits and indicates the receiver address in an IPv6 packet.

At present, IPv6 defines the following extension headers:

- Hop-By-Hop Options

This extension header must follow the IPv6 packet header. It consists of option data to be checked on each node along the path.

- Routing Options (Type 0 routing header)

This extension header indicates the nodes that a packet passes through from the source address to the destination address. It consists of the address list of the passerby nodes. The initial destination address in the IPv6 packet header is the first address among the addresses in the routing header, but not the final destination address of the packet. After the node corresponding to the destination address in the IPv6 packet header receives a packet, it processes the IPv6 packet header and routing header, and sends the packet to the second address, the third address, and so on in the routing header list till the packet reaches the final destination address.

- Fragment

The source node uses this extension header to fragment the packets of which the length exceeds the path MTU (PMTU).

- Destination Options

This extension header replaces the option fields of IPv4. At present, the Destination Options field can only be filled with integral multiples of 64 bits (eight bytes) if required. This extension header can be used to carry information to be checked by the destination node.

- Upper-layer header

This extension header indicates the protocol used at the upper layer, such as TCP (6) and UDP (17).

Another two extension headers AH and ESP will be described in the *Configuring IPSec*.

3. Configuring IPv6

3.3.4 IPv6 PMTUD

Similar to IPv4 Path MTU Discovery (PMTUD), IPv6 PMTUD allows a host to dynamically discover and adjust the MTU size on the data Tx path. If the length of a data packet to be sent by a host is greater than the PMTU, the host performs packet fragmentation on its own. In this manner, the IPv6 device does not need to perform fragmentation, saving device resources and improving the IPv6 network efficiency.

Figure 3-10
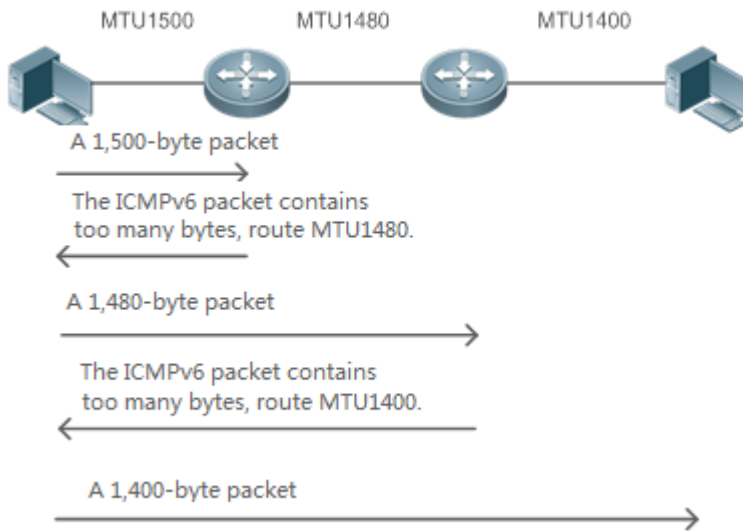
As shown in Figure 3-10, if the length of a packet to be sent by the host is greater than the PMTU, the router discards this packet and sends an ICMPv6 Packet Too Big message containing its PMTU to the host. The host then fragments the packet based on the new PMTU. In this manner, the router does not need to perform fragmentation, saving router resources and improving the IPv6 network efficiency.

Related Configuration

Configuring the IPv6 MTU of an Interface

- The default IPv6 MTU is 1500 on an Ethernet interface.
- To reduce traffic caused by dropping packets, a proper MTU value needs to be set according to the actual networking environment. Run the **ipv6 mtu** command to modify the IPv6 MTU of an interface.

3. Configuring IPv6

3.3.5 IPv6 Neighbor Discovery

NDP is a basic part of IPv6. Its main functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, NUD, DAD, and redirection. NDP defines five ICMP packets: RS (ICMP type: 133), RA (ICMP type: 134), NS (similar to ARP request, ICMP type: 135), NA (similar to ARP reply, ICMP type: 136), ICMP Redirect (ICMP type: 137).

All the above ICMP packets carry one or multiple options. These options are optional in some cases but are significant in other cases. NDP mainly defines five options: Source Link-Layer Address Option, Type=1; Target Link-Layer Address Option, Type=2; Prefix Information Option, Type=3; Redirection Header Option, Type=4; MTU Option, Type=5.

Address Resolution

When a node attempts to communicate with another, the node has to obtain the link-layer address of the peer end by sending it an NS packet. In this packet, the destination address is the solicited-node multicast address corresponding to the IPv6 address of the destination node. This packet also contains the link-layer address of the source node. After receiving this NS packet, the peer end replies with an NA packet in which the destination address is the source address of the NS packet, that is, the link-layer address of the solicited node. After receiving this NA packet, the source node can communicate with the destination node.

Figure 3-11 shows the address resolution process.

Figure 3-11

Ipv6 Neighbor Discovery (Neighbor solicitation packet)
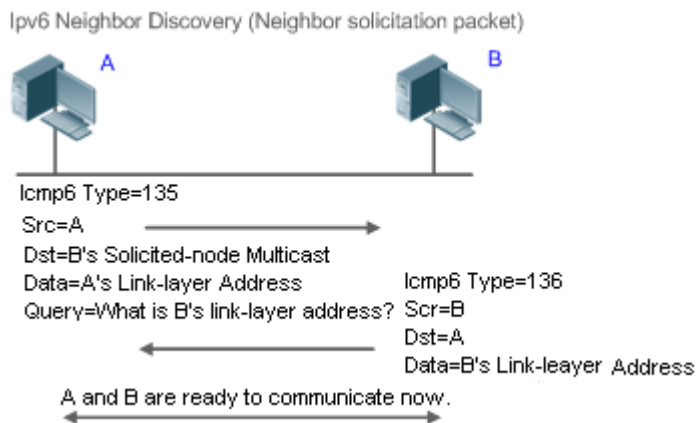
NUD

If the reachable time of a neighbor has elapsed but an IPv6 unicast packet needs to be sent to it, the device performs NUD.

While performing NUD, the device can continue to forward IPv6 packets to the neighbor.

DAD

3. Configuring IPv6

To know whether the IPv6 address configured for a host is unique, the device needs to perform DAD by sending an NS packet in which the source IPv6 address is the unspecified address.

If a device detects an address conflict, this address is set to the duplicate status so that the device cannot receive IPv6 packets with this address being the destination address. Meanwhile, the device also starts a timer for this duplicate address to periodically perform DAD. If no address conflict is detected in re-detection, this address can be properly used.

Router, Prefix, and Parameter Discovery

A device periodically sends RA packets to all local nodes on the link.

Figure 3-12 shows the RA packet sending process.

Figure 3-12
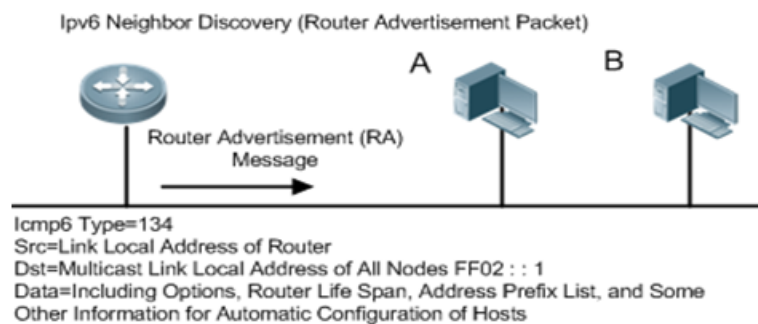
An RA packet usually contains the following content:

▪ One or multiple IPv6 address prefixes (used for on-link determination or stateless address auto-configuration)
▪ Validity of the IPv6 address prefix
▪ Host auto-configuration method (stateful or stateless)
▪ Default device information (whether the device acts as the default device; if yes, the interval for acting as the default device is also included.)
▪ Other information provided for host configuration, such as hop limit, MTU, and NS retransmission interval

3. Configuring IPv6

RA packets can also be used as replies to the RS packets sent by a host. Using RS packets, a host can obtain the auto-configured information immediately after started rather than wait for the RA packets sent by the device. If no unicast address is configured for a newly started host, the host includes the unspecified address (0:0:0:0:0:0:0:0) as the source address in the RS packet. Otherwise, the host uses the configured unicast address as the source address and the multicast address of all local routing devices (FF02::2) as the destination address in the RS packet. As an reply to the RS packet, the RA packet uses the source address of the RS packet as the destination address (if the source address is the unspecified address, it uses the multicast address of all local nodes (FF02::1).

In an RA packet, the following parameters can be configured:

- Ra-interval: Interval for sending the RA packet.
- Ra-lifetime: Lifetime of a router, that is, whether the device acts as the default router on the local link and the interval for acting as the default router.
- Prefix: Prefix of an IPv6 address on the local link. It is used for on-link determination or stateless address auto-configuration, including other parameter configurations related to the prefix.
- Ns-interval: NS packet retransmission interval.
- Reachabletime: Period when the device regards a neighbor reachable after detecting a Confirm Neighbor Reachability event.
- Ra-hoplimit: Hops of the RA packet, used to set the hop limit for a host to send a unicast packet.
- Ra-mtu: MTU of the RA packet.
- Managed-config-flag: Whether a host receiving this RA packet obtains the address through stateful auto-configuration.
- Other-config-flag: Whether a host receiving this RA packet uses DHCPv6 to obtain other information except the IPv6 address for auto-configuration.

Configure the above parameters when configuring IPv6 interface attributes.

Redirection

If a router receiving an IPv6 packet finds a better next hop, it sends the ICMP Redirect packet to inform the host of the better next hop. The host will directly send the IPv6 packet to the better next hop next time.

Maximum Number of Unresolved ND Entries

- You can configure the maximum number of unresolved ND entries to prevent malicious scanning network segments from generating a large number of unresolved ND entries and occupying excessive memory space.

Maximum Number of Neighbor Learning Entries on an Interface

- You can configure the maximum number of neighbor learning entries on an interface to prevent neighbor learning attacks from occupying ND entries and memory space of the device and affecting forwarding efficiency of the device.

Related Configuration

Enabling IPv6 Redirection

- By default, ICMPv6 Redirect packets can be sent on IPv6 interfaces.
- Run the **no ipv6 redirects** command in interface configuration mode to prohibit an interface from sending Redirect packets.

Configuring IPv6 DAD

- By default, an interface sends one NS packet to perform IPv6 DAD.
- Run the **ipv6 nd dad attempts** *value* command in interface configuration mode to configure the number of NS packets consecutively sent by DAD. Value 0 indicates disabling DAD for IPv6 addresses on this interface.
- Run the **no ipv6 nd dad attempts** command to restore the default configuration.
- By default, the device performs DAD on duplicate IPv6 addresses every 60 seconds.
- Run the **ipv6 nd dad retry** value command in global configuration mode to configure the DAD interval. Value 0 indicates disabling DAD for the device.
- Run the **no ipv6 nd dad retry** command to restore the default configuration.

Configuring the Reachable Time of a Neighbor

- The default reachable time of an IPv6 neighbor is 30s.
- Run the **ipv6 nd reachable-time** *milliseconds* command in interface configuration mode to modify the reachable time of a neighbor.

Configuring the Stale Time of a Neighbor

- The default stale time of an IPv6 neighbor is 1 hour. After the time elapses, the device performs NUD.
- Run the **ipv6 nd stale-time** *seconds* command in interface configuration mode to modify the stale time of a neighbor.

Configuring Prefix Information

- By default, the prefix in an RA packet on an interface is the prefix configured in the **ipv6 address** command on the interface.
- Run the **ipv6 nd prefix** command in interface configuration mode to add or delete prefixes and prefix parameters that can be advertised.

Enabling/disabling RA Suppression

- By default, an IPv6 interface does not send RA packets.
- Run the **no ipv6 nd suppress-ra** command in interface configuration mode to disable RA suppression.

Configuring the Maximum Number of Unresolved ND Entries

3. Configuring IPv6

- The default value is 0, indicating no restriction. It is only restricted to the ND entry capacity supported by the device.
- Run the **ipv6 nd unresolved** *number* command in global configuration mode to restrict the number of unresolved neighbors. After the entries exceed this restriction, the device does not actively resolve subsequent packets.

Configuring the Maximum Number of ND Entries Learned on an Interface

- Run the **ipv6 nd cache interface-limit** *value* command in interface configuration mode to restrict the number of neighbors learned on an interface. The default value is 0, indicating no restriction.

3.3.6   IPv6 Source Routing

**Working
Principle**

Similar to the IPv4 loose source routing and loose record routing options, the IPv6 routing header is used to specify the intermediate nodes that the packet passes through along the path to the destination address. It uses the following format:

Figure 3-13
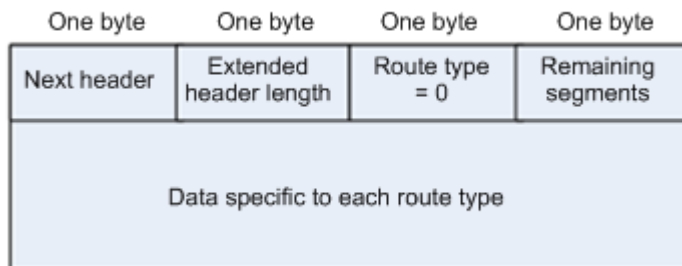
The Segments Left field is used to indicate how many intermediate nodes are specified in the routing header for the packet to pass through from the current node to the final destination address.

Currently, two routing types are defined: 0 and 2. The Type 2 routing header is used for mobile communication. RFC 2460 defines the Type 0 routing header (similar to the loose source routing option of IPv4). The format of the Type 0 routing header is as follows:

Figure 3-14

3. Configuring IPv6

One byte	One byte	One byte	One byte
Next header	Extended header length	Route type = 0	Remaining segments
Reserved			
Address 1			
Address N			
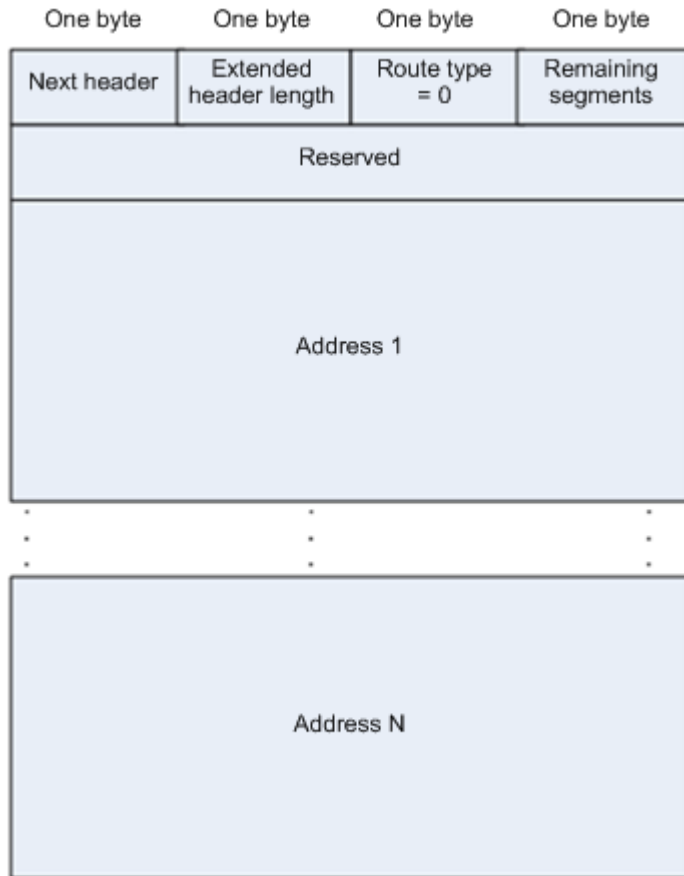
The following example describes the application of the Type 0 routing header, as shown in Figure 3-15.

Figure 3-15
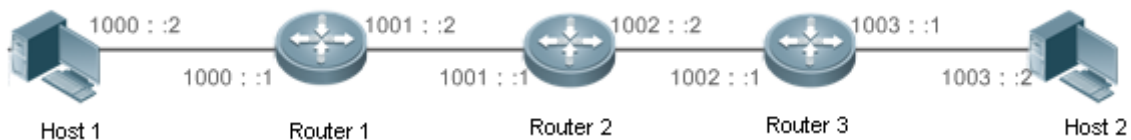
Host 1 sends Host 2 a packet specifying the intermediate nodes Router 2 and Router 3. The following table lists the changes of fields related to the IPv6 header and routing header during the forwarding process.

3. Configuring IPv6

Transmission Node	Fields in the IPv6 Header	Fields Related to the Type 0 Routing Header
Host 1	Source address=1000::2 Destination address=1001::1 (Address of Router 2)	Segments Left=2 Address 1=1002::1 (Address of Router 3) Address 2=1003::2 (Address of Host 2)
Router 1	No change	
Router 2	Source address=1000::2 Destination address=1002::1 (Address of Router 3)	Segments Left=1 Address 1=1001::1 (Address of Router 2) Address 2=1003::2 (Address of Host 2)
Router 3	Source address=1000::2 Destination address=1003::2 (Address of Host 2)	Segments Left=0 Address 1=1001::1 (Address of Router 2) Address 1=1002::2 (Address of Router 3)
Host 2	No change	

The forwarding process is as follows:

1. Host 1 sends a packet in which the destination address is Router 2's address 1001::1, the Type 0 routing header is filled with Router 3's address 1002::1 and Host 2's address 1003::2, and the value of the Segments Left field is 2.
2. Router 1 forwards this packet to Router 2.
3. Router 2 changes the destination address in the IPv6 header to Address 1 in the routing header. That is, the destination address becomes Router 3's address 1002::1, Address 1 in the routing header becomes Router 2's address 1001::1, and the value of the Segments Left field becomes 1. After modification, Router 2 forwards the packet to Router 3.
4. Router 3 changes the destination address in the IPv6 header to Address 2 in the routing header. That is, the destination address becomes Host 2's address 1003::2, Address 2 in the routing header becomes Router 3's address 1002::1, and the value of the Segments Left field becomes 0. After modification, Router 3 forwards the packet to Host 2.

3. Configuring IPv6

The Type 0 routing header may be used to initiate DoS attacks. As shown in Figure 3-16, Host 1 sends packets to Host 2 at 1 Mbps and forges a routing header to cause multiple round-trips between Router 2 and Router 3 (50 times from Router 2 to Router 3 and 49 times from Router 3 to Router 2). At the time, the routing header generates the traffic amplification effect:" 50 Mbps from Router 2 to Router 3 and 49 Mbps from Router 3 to Router 2." Due to this security problem, RFC 5095 abolished the Type 0 routing header.

Figure 3-16

IPv6 Packet
Source Address 1000::2
Destination Address 1001:1

Segments Left in the Type 0
Routing Header: 100
Address 1: 1002::1
Address 2: 1001::1
Address 3: 1002::1
Address 4: 1002::1
...
Address 99: 1002::1
Address 100: 100:3::2

Host 1 sends packets to Host 2, passing through Router 2, Router 3, Router 2, and Router 3, ...
Each packet is sent 50 times from Router 2 to Router 3 and 49 times from Router 3 to Router 2.
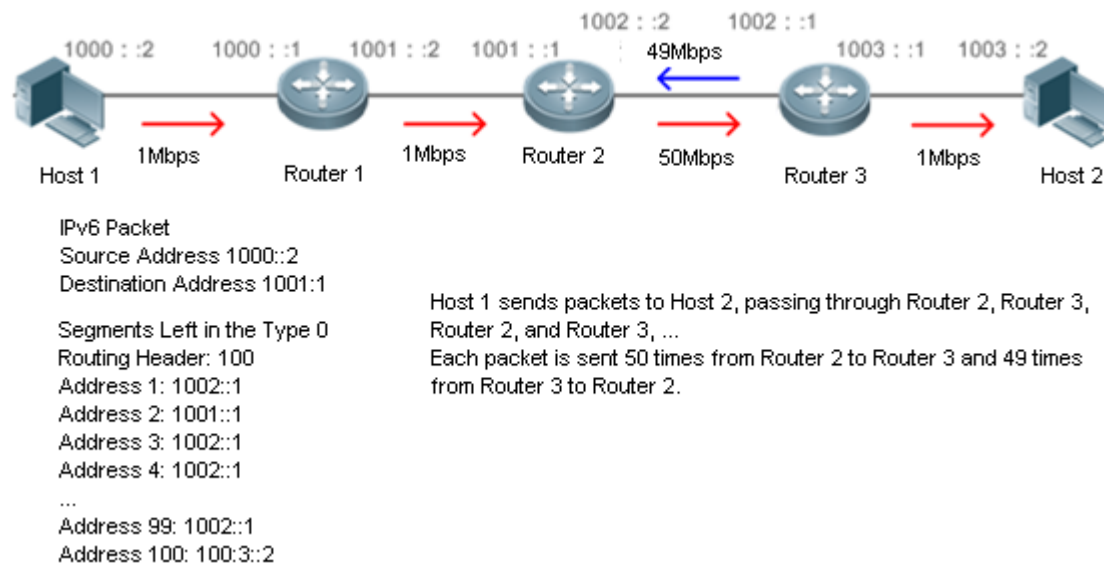
Related Configuration

Enabling IPv6 Source Routing

- The Type 0 routing header is not supported by default.
- Run the **ipv6 source-route** command in global configuration mode to enable IPv6 source routing.

3.3.7 Restricting the Sending Rate of ICMPv6 Error Messages

Working Principle

The destination node or intermediate router sends ICMPv6 error messages to report the errors incurred during IPv6 data packet forwarding and transmission. There are mainly four types of error messages: Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problem.

When receiving an invalid IPv6 packet, a device discards the packet and sends back an ICMPv6 error

3. Configuring IPv6

message to the source IPv6 address. In the case of invalid IPv6 packet attacks, the device may continuously reply to ICMPv6 error messages till device resources are exhausted and thereby fail to properly provide services. To solve this problem, you can restrict the sending rate of ICMPv6 error messages.

If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If the sending rate of ICMPv6 error messages is restricted due to excessive other ICMPv6 error messages, ICMPv6 Packet Too Big messages may be filtered, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages.

Although ICMPv6 Redirect packets are not ICMPv6 error messages, QTECH recommends restricting their rates together with ICMPv6 error messages except Packet Too Big messages.

Related Configuration

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval too-big** command to configure the sending rate of ICMPv6 Packet Too Big messages.

Configuring the Sending Rate of Other ICMPv6 Error Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval** command to configure the sending rate of other ICMPv6 error messages.

3.3.8 IPv6 Hop Limit

Working Principle

An IPv6 data packet passes through routers from the source address and destination address. If a hop limit is configured, it decreases by one every time the packet passes through a router. When the hop limit decreases to 0, the router discards the packet to prevent this useless packet from being unlimitedly transmitted on the network and wasting network bandwidth. The hop limit is similar to the TTL of IPv4.

Related Configuration

3. Configuring IPv6

Configuring the IPv6 Hop Limit

- The default IPv6 hop limit of a device is 64.
- Run the **ipv6 hop-limit** command to configure the IPv6 hop limit of a device.

3.3.9 Refraining from Sending NS Packets to Authentication VLANs

Working Principle

In gateway authentication mode, all sub VLANs in a super VLAN are authentication VLANs by default. Users in an authentication VLAN have to pass authentication to access the network. After authentication, a static ND entry is generated on the device. Therefore, when accessing an authenticated user, the device does not need to send NS packets to the authentication VLAN. If the device attempts to access users in an authentication-free VLAN, it only needs to send NS requests to the authentication-free VLAN.

In gateway authentication mode, the function of refraining from sending NS packets to authentication VLANs is enabled on the device by default. If the device needs to access authentication-free users in an authentication VLAN, disable this function.

Related Configuration

Enabling the Function of Refraining from Sending NS Packets to Authentication VLANs

- Run the **ipv6 nd suppress-auth-vlan-ns** command in interface configuration mode to enable the function of refraining from sending NS packets to authentication VLANs.
- This function is enabled by default.
- This function is supported only on switch virtual interfaces (SVIs) and takes effect only in gateway authentication mode.

3.3.10 Default Gateway on the Management Interface

Working Principle

The default gateway is configured on the management interface to generate a default route for this interface.

Related
Configuration

Configuring the Default Gateway on the Management Interface

- Run the **ipv6 gateway** *ipv6-address* command in interface configuration mode to configure the default gateway on the management interface.
- No default gateway is configured on the management interface by default.

3.4 Configuration

Configuration	Description and Command	
Configuring an IPv6 Address	⚠ (Mandatory) It is used to configure IPv6 addresses and enable IPv6.	
	ipv6 enable	Enables IPv6 on an interface.
	ipv6 address	Configures the IPv6 unicast address of an interface.
Configuring IPv6 NDP	⚠ (Optional) It is used to enable IPv6 redirection on an interface.	
	ipv6 redirects	Enables IPv6 redirection on an interface.
	⚠ (Optional) It is used to enable DAD.	
	ipv6 nd dad attempts	Configures the number of consecutive NS packets sent during DAD.
	⚠ (Optional) It is used to configure ND parameters.	
	ipv6 nd reachable-time	Configures the reachable time of a neighbor.
	ipv6 nd prefix	Configures the address prefix to be advertised in an RA packet.
	ipv6 nd suppress-ra	Enables RA suppression on an interface.

3. Configuring IPv6

	⚠ (Optional) It is used to configure the maximum number of unresolved ND entries.	
	ipv6 nd unresolved	Configures the maximum number of unresolved ND entries.
	⚠ (Optional) It is used to configure the maximum number of neighbors learned on an interface.	
	ipv6 nd cache interface-limit	Configures the maximum number of neighbors learned on an interface.
[Enabling MTD on an Interface](#)	⚠ (Optional) It is used to restrict the MTU of IPv6 packets sent on an interface.	
	ipv6 mtu	Configures the IPv6 MTU.
[Enabling IPv6 Source Routing](#)	⚠ (Optional) It is used to enable IPv6 source routing.	
	ipv6 source-route	Configures the device to forward IPv6 packets carrying the routing header.
[Configuring the Sending Rate of ICMPv6 Error Messages](#)	⚠ Optional.	
	ipv6 icmp error-interval too-big	Configures the sending rate of ICMPv6 Packet Too Big messages.
	ipv6 icmp error-interval	Configures the sending rates of other ICMPv6 error messages and ICMPv6 Redirect packets.
[Configuring the IPv6 Hop Limit](#)	⚠ (Optional) It is used to restrict the hop limit of IPv6 unicast packets sent on an interface.	
	ipv6 hop-limit	Configures the IPv6 hop limit.
[Enabling Refraining from Sending NS Packets to Authentication VLANs](#)	⚠ (Optional) It is used to restrict sending NS packets to authentication VLANs in gateway authentication mode.	
	ipv6 nd suppress-auth-vlan-ns	Enables NS broadcast suppression in authentication VLANs.

3. Configuring IPv6

Configuring the Default Gateway on the Management Interface	⚠ (Optional) It is used to configure the default gateway on the management interface.
	ipv6 gateway *ipv6-address*
	Configures the default gateway on the management interface.

3.4.1 Configuring an IPv6 Address

Configuration Effect

Configure the IPv6 address of an interface to implement IPv6 network communication.

Configuration Steps

Enabling IPv6 on an Interface

- (Optional) If you do not want to enable IPv6 by configuring an IPv6 address, run the **ipv6 enable** command.

Configuring the IPv6 Unicast Address of an Interface

- Mandatory.

Verification

Run the **show ipv6 interface** command to check whether the configured address takes effect.

Related Commands

Enabling IPv6 on an Interface

Command	**ipv6 enable**
Parameter Description	N/A

3. Configuring IPv6

Command Mode	Interface configuration mode
Usage Guide	IPv6 can be enabled on an interface by two methods: 1) running the **ipv6 enable** command in interface configuration mode; 2) configuring an IPv6 address on the interface.
	ⓘ If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, IPv6 cannot be enabled on this interface. You can enable IPv6 on this interface only after configuring an IPv6 address family for the multiprotocol VRF.
	If an IPv6 address is configured on an interface, IPv6 is automatically enabled on this interface. In this case, IPv6 cannot be disabled even when you run the **no ipv6 enable** command.

Configuring the IPv6 Unicast Address of an Interface

Command	**ipv6 address ipv6-address / prefix-length** **ipv6 address ipv6-prefix / prefix-length eui-64** **ipv6 address prefix-name sub-bits / prefix-length [eui-64]**
Parameter Description	ipv6-address: Indicates the IPv6 address, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits.
	ipv6-prefix: Indicates the IPv6 address prefix, which must comply with the address format defined in RFC 4291.
	prefix-length: Indicates the length of the IPv6 address prefix, that is, the part representing the network in the IPv6 address.
	prefix-name: Indicates the name of the universal prefix. This specified universal prefix is used to create the interface address.
	sub-bits: Indicates the subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the prefix-name parameter. This value is combined with the universal prefix to create the interface address. This value must be in the form documented in RFC 4291.
	eui-64: Indicates the created IPv6 address, consisting of the configured address prefix and 64-bit interface ID.
Command Mode	Interface configuration mode

3. Configuring IPv6

Usage Guide	
	❗ If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, the IPv6 address cannot be configured for this interface. You can configure the IPv6 address of this interface only after configuring an IPv6 address family for the multiprotocol VRF.
	If an IPv6 interface is created and is Up state, the system automatically generates a link-local address for this interface.
	The IPv6 address of an interface can also be created by the universal prefix mechanism. That is, IPv6 address = Universal prefix + Sub prefix + Host bits. The universal prefix can be configured by running the **ipv6 general-prefix** command or learned by the prefix discovery function of the DHCPv6 client (see the *Configuring DHCPv6*). Sub prefix + Host bits are specified by the *sub-bits* and *prefix-length* parameters in the **ipv6 address** command.
	If you run the **no ipv6 address** command without specifying an address, all manually configured addresses will be deleted.
	Run the **no ipv6 address** *ipv6-prefix/prefix-length* **eui-64** command to delete the configured address.

Configuration Example

Configuring an IPv6 Address on an Interface

Configuration Steps	Enable IPv6 on the GigabitEthernet 0/0 interface and add IPv6 address 2000::1 to the interface.
	QTECH (config)#interface gigabitEthernet 0/0 QTECH (config-if-GigabitEthernet 0/0)#ipv6 enable QTECH (config-if-GigabitEthernet 0/0)#ipv6 address 2000::1/64
Verification	Run the **show ipv6 interface** command to verify that an address is successfully added to the GigabitEthernet 0/0 interface.
	QTECH (config-if-GigabitEthernet 0/0)#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es):

3. Configuring IPv6

Mac Address: 00:00:00:00:00:00

INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64

INET6: 2000::1 [TENTATIVE], subnet is 2000::/64

Joined group address(es):

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND router advertisements are sent every 200 seconds<160--240>

ND router advertisements live for 1800 seconds

3.4.2   Configuring IPv6 NDP

**Configuration
Effect**

Configure NDP-related attributes, for example, enable IPv6 redirection and DAD.

Notes

RA suppression is enabled on interfaces by default. To configure a device to send RA packets, run the **no ipv6 nd suppress-ra** command in interface configuration mode.

**Configuration
Steps**

Enabling IPv6 Redirection on an Interface

- (Optional) IPv6 redirection is enabled by default.
- To disable IPv6 redirection on an interface, run the **no ipv6 redirects** command.

Configuring the Number of Consecutive NS Packets Sent During DAD

- Optional.
- To prevent enabling DAD for IPv6 addresses on an interface or modify the number of consecutive NS packets sent during DAD, run the **ipv6 nd dad attempts** command.

3. Configuring IPv6

Configuring the Reachable Time of a Neighbor

- Optional.
- To modify the reachable time of a neighbor, run the **ipv6 nd reachable-time** command.

Configuring the Address Prefix to Be Advertised in an RA Packet

- By default, the prefix in an RA packet on an interface is the prefix configured in the **ipv6 address** command on the interface.
- (Optional) Run the **ipv6 nd prefix** command to add or delete prefixes and prefix parameters that can be advertised.

Enabling/Disabling RA Suppression on an Interface

- Optional.
- If a device needs to send RA packets, run the **no ipv6 nd suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

- Optional.
- If a large number of unresolved ND entries are generated due to scanning attacks, run the **ipv6 nd unresolved** command to restrict the number of unresolved neighbors.

Configuring the Maximum Number of ND Entries Learned on an Interface

- Optional.
- If the number of IPv6 hosts is controllable, run the **ipv6 nd cache interface-limit** command to restrict the number of neighbors learned on an interface. This prevents ND learning attacks from occupying the memory space and affecting device performance.

Verification

Run the following commands to check whether the configuration is correct:

- **show ipv6 interface** *interface-type interface-num*: Check whether the configurations such as the redirection function, reachable time of a neighbor, and NS sending interval take effect.
- **show ipv6 interface** *interface-type interface-num* **ra-inifo**: Check whether the prefix and other information configured for RA packets are correct.
- **show run**

Related Commands

Enabling IPv6 Redirection on an Interface

3. Configuring IPv6

Command	ipv6 redirects
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	All ICMPv6 error messages are transmitted at a limited transmission rate. By default, a maximum number of 10 ICMPv6 error messages are transmitted per second (10 pps).

Configuring the Number of Consecutive NS Packets Sent During DAD

Command	ipv6 nd dad attempts *value*
Parameter Description	*value*: Indicates the number of NS packets.
Command Mode	Interface configuration mode
Usage Guide	You need to enable DAD before configuring an IPv6 address on an interface. Then the address is in tentative state. If no address conflict is detected by DAD, this address can be correctly used. If an address conflict is detected and the interface ID of this address uses EUI-64, duplicate link-layer addresses exist on this link. In this case, the system automatically disables this interface to prevent IPv6-related operations on this interface). At the time, you must configure a new address and restart the interface to re-enable DAD. When an interface changes from the down state to the up state, DAD is re-enabled for the addresses on this interface.

Configuring the Reachable Time of a Neighbor

Command	ipv6 nd reachable-time *milliseconds*
Parameter Description	*milliseconds*: Indicates the reachable time of a neighbor, ranging from 0 to 3,600,000. The unit is millisecond. The default value is 30s.

3. Configuring IPv6

Command Mode	Interface configuration mode
Usage Guide	A device detects unreachable neighbors based on the configured reachable time. The shorter the configured reachable time, the faster the device detects unreachable neighbors but the more it consumes network bandwidth and device resources. Therefore, it is not recommended to set this time too small.
	The configured value is advertised in an RA packet and is also used on the device. If the value is 0, the reachable time is not specified on the device and it is recommended to use the default value.

Configuring the Address Prefix to Be Advertised in an RA Packet

Command	ipv6 nd prefix {*ipv6-prefix/prefix-length* | default} [[*valid-lifetime* { infinite | *preferred-lifetime* }] | [at *valid-date preferred-date*] | [infinite {infinite | *preferred-lifetime*}]] [no-advertise] | [[off-link] [no-autoconfig]]
Parameter Description	*ipv6-prefix*: Indicates the network ID of IPv6, which must comply with the address representation format in RFC 4291.
	prefix-length: Indicates the length of the IPv6 address prefix. A slash (/) must be added before the prefix.
	valid-lifetime: Indicates the period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 30 days.
	preferred-lifetime: Indicates the preferred period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 7 days.
	at *valid-date preferred-date*: Indicates the valid date and preferred deadline configured for the RA prefix. It uses the format of *dd+mm+yyyy+hh+mm*.
	infinite: Indicates that the prefix is permanently valid.
	default: Indicates that the default parameter configuration is used.
	no-advertise: Indicates that the prefix is not advertised by a router.
	off-link: If the prefix of the destination address in the IPv6 packet sent by a host matches the configured prefix, the device regards the destination address on the same link and directly reachable. This parameter indicates that this prefix does not require on-link determination.
	no-autoconfig: Indicates that the prefix in the RA packet received by a host cannot be used for address auto-configuration.

3. Configuring IPv6

Command Mode	Interface configuration mode
Usage Guide	This command can be used to configure parameters related to each prefix, including whether to advertise this prefix. By default, an RA packet uses the prefix configured by running the **ipv6 address** command. Run the **ipv6 nd prefix** command to add other prefixes. Run the **ipv6 nd prefix default** command to configure the default parameters for an interface. That is, if no parameter is specified when a prefix is added, use the parameters configured in the **ipv6 nd prefix default** command as the parameters of the new prefix. The default parameter configurations are abandoned once a parameter is specified for the prefix. That is, when you use the **ipv6 nd prefix default** command to modify the default parameter configurations, only the prefix configured for the default parameters changes and configurations of the prefix remain the same. **at** *valid-date preferred-date*: You can specify the valid date of the prefix in two methods: 1) specifying a fixed time for each prefix in an RA packet; 2) specifying the deadline. In the second method, the valid date of the prefix in each RA packet decreases till it becomes 0.

Enabling/Disabling RA Suppression on an Interface

Command	ipv6 nd suppress-ra
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	To enable RA suppression on an interface, run the **ipv6 suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

Command	ipv6 nd unresolved *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ND entries.

3. Configuring IPv6

Command Mode	Global configuration mode
Usage Guide	To prevent malicious scanning attacks from creating a large number of unresolved ND entries and occupying entry resources, you can restrict the number of unresolved ND entries.

Configuring the Maximum Number of ND Entries Learned on an Interface

Command	ipv6 nd cache interface-limit *value*
Parameter Description	*value*: Indicates the maximum number of neighbors learned by an interface.
Command Mode	Interface configuration mode
Usage Guide	Restricting the number of ND entries learned on an interface can prevent malicious neighbor attacks. If this number is not restricted, a large number of ND entries will be generated on the device, occupying excessive memory space. The configured value must be equal to or greater than the number of the ND entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ND entry capacity supported by the device.

Configuration Example

Enabling IPv6 Redirection on an Interface

Configuration Steps	Enable IPv6 redirection on interface GigabitEthernet 0/0.
	QTECH (config-if-GigabitEthernet 0/0)#ipv6 redirects
Verification	Run the show ipv6 interface command to check whether the configuration takes effect.

QTECH
МИР ДОСТУПНЕЕ

www.qtech.ru

3. Configuring IPv6

QTECH #show ipv6 interface gigabitEthernet 0/0

interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
 address(es):
   Mac Address: 00:00:00:00:00:00
   INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64
 Joined group address(es):
 MTU is 1500 bytes
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds
 ND advertised reachable time is 0 milliseconds
 ND retransmit interval is 1000 milliseconds
 ND advertised retransmit interval is 0 milliseconds
 ND router advertisements are sent every 200 seconds<160--240>
 ND router advertisements live for 1800 seconds

Configuring IPv6 DAD

Configuration Steps	Configure the interface to send three consecutive NS packets during DAD.
	QTECH (config-if-GigabitEthernet 0/0)# ipv6 nd dad attempts 3
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	QTECH #show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0

QTECH | www.qtech.ru

3. Configuring IPv6

address(es):

  Mac Address: 00:00:00:00:00:00

  INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64

Joined group address(es):

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ND DAD is enabled, number of DAD attempts: 3

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND router advertisements are sent every 200 seconds<160--240>

ND router advertisements live for 1800 seconds

QTECH (config-if-GigabitEthernet 0/0)#

Configuring Prefix Information in an RA Packet

Configuration Steps	Add a prefix 1234::/64 to interface GigabitEthernet 0/0.
	QTECH (config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	QTECH #show ipv6 interface gigabitEthernet 0/0 ra-info GigabitEthernet 0/0: DOWN (RA is suppressed)

QTECH | www.qtech.ru

3. Configuring IPv6

RA timer is stopped

waits: 0, initcount: 0

statistics: RA(out/in/inconsistent): 0/0/0, RS(input): 0

Link-layer address: 00:00:00:00:00:00

Physical MTU: 1500

ND router advertisements live for 1800 seconds

ND router advertisements are sent every 200 seconds<160--240>

Flags: !M!O, Adv MTU: 1500

ND advertised reachable time is 0 milliseconds

ND advertised retransmit time is 0 milliseconds

ND advertised CurHopLimit is 64

Prefixes: <total: 1>

  1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)

Configuring RA Packets to Obtain Prefixes from the Prefix Pool

Configuration Steps	Configure RA packets to obtain prefixes from the prefix pool "ra-pool".
	QTECH (config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool
Verification	Run the **show run** command to check whether the configuration takes effect.
	QTECH (config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0 Building configuration... Current configuration : 125 bytes interface GigabitEthernet 0/0 ipv6 enable no ipv6 nd suppress-ra peel default ipv6 pool ra-pool !

3. Configuring IPv6

Disabling RA Suppression

Configuration Steps	Disable RA suppression on an interface.
	QTECH (config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra
Verification	Run the **show run** command to check whether the configuration takes effect.
	QTECH (config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0 Building configuration... Current configuration : 125 bytes interface GigabitEthernet 0/0 ipv6 enable no ipv6 nd suppress-ra !

Configuring the Maximum Number of Unresolved ND Entries

Configuration Steps	Set the maximum number of unresolved ND entries to 200.
	QTECH (config)# ipv6 nd unresolved 200
Verification	Run the **show run** command to check whether the configuration takes effect.
	QTECH #show run ipv6 nd cache interface-limit 100 !

Configuring the Maximum Number of ND Entries Learned on an Interface

Configuration Steps	Set the maximum number of ND entries learned on an interface to 100.

3. Configuring IPv6

	QTECH (config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
Verification	Run the **show run** command to check whether the configuration takes effect.
	QTECH #show run ! interface GigabitEthernet 0/1 ipv6 nd cache interface-limit 100 !

3.4.3 Configuring IPv6 MTU on an Interface

Configuration Effect

According to the actual networking environment, configure a proper IPv6 to avoid package loss.

Notes

The IPv6 MTU of an interface must be less than or equal to the interface MTU. Generally, the range of the IPv6 MTU is from 1,280 to 1,500.

Configuration Steps

Configuring the IPv6 MTU of an Interface

Optional.

When the internet minimum MTU is less than the IPv6 MTU of the interface, use this configuration to set a proper interface MTU.

Verification

Run the **show run** or **show ipv6 interface** command to check whether the configuration is correct.

Capture the locally sent IPv6 packets of which the length exceeds the IPv6 MTU. The packet capture result shows that the IPv6 packet is fragmented based on the IPv6 MTU of the interface.

Related Commands

3. Configuring IPv6

Configuring the IPv6 MTU of an Interface

Command	ipv6 mtu *bytes*
Parameter Description	*bytes*: Indicates the MTU of an IPv6 packet, ranging from 1,280 to 1,500. The unit is byte.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring the IPv6 MTU of an Interface

Configuration Steps	Change the IPv6 MTU of interface GigabitEthernet 0/0 to 1,300.
	QTECH (config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.

	QTECH (config-if-GigabitEthernet 0/0)#show ipv6 interface
	
	interface GigabitEthernet 0/ is Down, ifindex: 1, vrf_id 0
	  address(es):
	    Mac Address: 08:c6:b3:22:33:47
	    INET6: FE80::2D0:F8FF:FE22:3347 [TENTATIVE], subnet is FE80::/64
	    INET6: 1020::1 [TENTATIVE], subnet is 1020::/64
	    INET6: 1023::1 [TENTATIVE], subnet is 1023::/64

> Joined group address(es):
>
> MTU is 1300 bytes
>
> ICMP error messages limited to one every 100 milliseconds
>
> ICMP redirects are enabled
>
> ND DAD is enabled, number of DAD attempts: 1
>
> ND reachable time is 30000 milliseconds
>
> ND advertised reachable time is 0 milliseconds
>
> ND retransmit interval is 1000 milliseconds
>
> ND advertised retransmit interval is 0 milliseconds
>
> ND router advertisements are sent every 200 seconds<160--240>
>
> ND router advertisements live for 1800 seconds

3.4.4   Enabling IPv6 Source Routing

Configuration Effect

RFC 5095 abolished the Type 0 routing header. QTECH devices do not support the Type 0 routing header by default. The administrator can run the **ipv6 source-route** command to in global configuration mode to enable IPv6 source routing.

Configuration Steps

Enabling IPv6 Source Routing

Optional.

To enable IPv6 source routing, run the **ipv6 source-route** command.

Verification

The device can properly forward packets carrying the Type 0 routing header.

3. Configuring IPv6

Enabling IPv6 Source Routing

Command	ipv6 source-route
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Since the Type 0 header may cause the device prone to DoS attacks, the device does not forward IPv6 packets carrying the routing header by default, but still processes IPv6 packets with itself being the final destination address and the Type 0 routing header.

Enabling IPv6 Source Routing

Configuration Steps	Enable IPv6 source routing.
	QTECH (config)#ipv6 source-route
Verification	Run the **show run** command to check whether the configuration takes effect.
	QTECH #show run | inc ipv6 source-route ipv6 source-route

3.4.5 Configuring the Sending Rate of ICMPv6 Error Messages

Configure the sending rate of ICMPv6 error messages.

3. Configuring IPv6

Configuration Steps

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

Optional.

If a device receives many IPv6 packets with the packet length exceeding the IPv6 MTU of the outbound interface and thereby sends many ICMPv6 Packet Too Big messages to consume much CPU resources, run the **ipv6 icmp error-interval too-big** command to restrict the sending rate of this error message.

Configuring the Sending Rate of Other ICMPv6 Error Messages

Optional.

If a device receives many illegal IPv6 packets and thereby generates many ICMPv6 error messages, run the **ipv6 icmp error-interval** command to restrict the sending rate of ICMPv6 error messages. (This command does not affect the sending rate of ICMPv6 Packet Too Big messages.)

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

Command	ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command Mode	Global configuration mode

3. Configuring IPv6

Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages.
	If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If other ICMPv6 error messages are excessive, ICMPv6 Packet Too Big messages cannot be sent, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages.
	Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuring the Sending Rate of Other ICMPv6 Error Messages

Command	ipv6 icmp error-interval *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted.
	bucket-size: Indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages.
	Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

Configuration Example

Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Steps	Set the sending rate of the ICMPv6 Packet Too Big message to 100 pps and that of other ICMPv6 error messages to 10 pps.
	QTECH (config)#ipv6 icmp error-interval too-big 1000 100 QTECH (config)#ipv6 icmp error-interval 1000 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	QTECH #show running-config | include ipv6 icmp error-interval ipv6 icmp error-interval 1000 10 ipv6 icmp error-interval too-big 1000 100

3.4.6 Configuring the IPv6 Hop Limit

Configuration Effect

Configure the number of hops of a unicast packet to prevent the packet from being unlimitedly transmitted.

Configuration Steps

Configuring the IPv6 Hop Limit

Optional.

To modify the number of hops of a unicast packet, run the **ipv6 hop-limit value** command.

Verification

Run the **show running-config** command to check whether the configuration is correct.

Capture the IPv6 unicast packets sent by a host. The packet capture result shows that the hop-limit field value in the IPv6 header is the same as the configured hop limit.

QTECH | www.qtech.ru

3. Configuring IPv6

Configuring the IPv6 Hop Limit

Command	ipv6 hop-limit value
Parameter Description	*value*: Indicates the number of hops of a unicast packet sent by the device. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the IPv6 Hop Limit

Configuration Steps	Change the IPv6 hop limit of a device to 250.
	QTECH (config)#ipv6 hop-limit 250
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	QTECH #show running-config ipv6 hop-limit 254

3.4.7 Enabling/Disabling the Function of Refraining from Sending NS Packets to Authentication VLANs

Enable or disable the function of refraining from sending NS packets to authentication VLANs on an

QTECH МИР ДОСТУПНЕЕ | www.qtech.ru

3. Configuring IPv6

SVI.

Notes

The configuration is supported only on SVIs and takes effect only in gateway authentication mode.

Configuration Steps

Enabling/Disabling the Function of Refraining from Sending NS Packets to Authentication VLANs

Optional.

In gateway authentication mode, run the **no ipv6 nd suppress-auth-vlan-ns** command so that the device can send NS packets to authentication VLANs.

Verification

Run the **show running-config** command to check whether the configuration is correct.

Related Commands

Enabling/Disabling the Function of Refraining from Sending NS Packets to Authentication VLANs

Command	ipv6 nd suppress-auth-vlan-ns
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Use the no form of this command to disable this function.

Configuration Example

Disabling the Function of Refraining from Sending NS Packets to Authentication VLANs

3. Configuring IPv6

Configuration Steps	Disable the function of refraining from sending NS packets to authentication VLANs.
	QTECH (config-if-VLAN 2)#no ipv6 nd suppress-auth-vlan-ns
Verification	Run the **show running-config interface vlan 2** command to check whether the configuration takes effect.
	QTECH #show running-config interface vlan 2 no ipv6 nd suppress-auth-vlan-ns

3.4.8 Configuring the Default Gateway on the Management Interface

Configuration Effect

Configure the default gateway on the management interface. A default route is generated, with the outbound interface being the management interface and the next hop being the configured gateway.

Notes

The configuration is supported only on the management interface.

Configuration Steps

Configuring the Default Gateway on the Management Interface

Optional.

To configure a default route and the next hop for the management interface, run the **ipv6 gateway** command.

Verification

Run the **show running-config** command to check whether the configuration is correct.

Related Commands

Configuring the Default Gateway on the Management Interface

3. Configuring IPv6

Command	ipv6 gateway *ipv6-address*
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	This command is supported only on the management interface.

Configuration Example

Configuring the Default Gateway on the Management Interface

Configuration Steps	Sett the default gateway of the management interface to 2000::1.
	QTECH (config)# interface mgmt 0 QTECH (config-mgmt)# ipv6 gateway 2000::1
Verification	Run the **show running-config interface vlan 2** command to check whether the configuration takes effect.
	QTECH #show running-config interface mgmt 0 Ipv6 gateway 2000::1

3.5   Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

3. Configuring IPv6

Description	Command
Clears the dynamically learned neighbors.	**clrear ipv6 neighbors** [**vrf** *vrf-name*] [**oob**] [*interface-id*]

Displaying

Description	Command
Displays IPv6 information of an interface.	**show ipv6 interface** [[*interface-id*] [ra-info]] [brief [*interface-id*]]
Displays neighbor information.	**show ipv6 neighbors** [**vrf** *vrf-name*] [**verbose**] [*interface-id*] [*ipv6-address*] [static] [oob]
Displays information of the IPv6 routing table.	**show ipv6** route [**vrf** *vrf-name*] [**static** | local | connected | bgp | rip | ospf | isis **]**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs ND entry learning.	**debug ipv6 nd**

4 CONFIGURING DHCP

4.1 Overview

The Dynamic Host Configuration Protocol (DHCP) is a LAN protocol based on the User Datagram Protocol (UDP) for dynamically assigning reusable network resources, for example, IP addresses.

The DHCP works in Client/Server mode. A DHCP client sends a request message to a DHCP server to obtain an IP address and other configurations. When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Protocols and Standards

RFC2131: Dynamic Host Configuration Protocol

RFC2132: DHCP Options and BOOTP Vendor Extensions

RFC3046: DHCP Relay Agent Information Option

4.2 Applications

Application	Description
Providing DHCP Service in a LAN	Assigns IP addresses to clients in a LAN.
Enabling DHCP Client	Enable DHCP Client.
Applying AM Rule on DHCP Server	Apply DHCP Server in Super VLAN environment.
Deploying DHCP Relay in Wired Network	In a wired network, users from different network segments requests IP addresses.
Applying AM Rule on DHCP Relay	In a Super VLAN, users from different network segments requests IP addresses.

4.2.1 Providing DHCP Service in a LAN

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

4. Configuring DHCP

Scenario

Assign IP addresses to four users in a LAN.

For example, assign IP addresses to User 1, User 2, User 3 and User 4, as shown in the following figure.

The four users are connected to Server S through A, B, C and D.

Figure 4-1
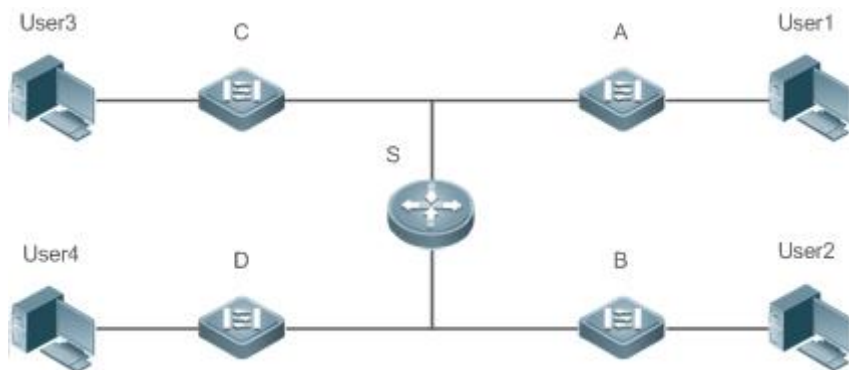
Remark s	S is an egress gateway working as a DHCP server. A, B, C and D are access switches achieving layer-2 transparent transmission. User 1, User 2, User 3 and User 4 are LAN users.

Deployment

Enable DHCP Server on S.

Deploy layer-2 VLAN transparent transmission on A, B, C and D.

User 1, User 2, User 3 and User 4 initiate DHCP client requests.

4.2.2 Enabling DHCP Client

Scenario

Access switches A, B, C and D in a LAN request server S to assign IP addresses.

For example, enable DHCP Client on the interfaces of A, B, C and D to request IP addresses, as shown in the following figure.

Figure 4-2

4. Configuring DHCP
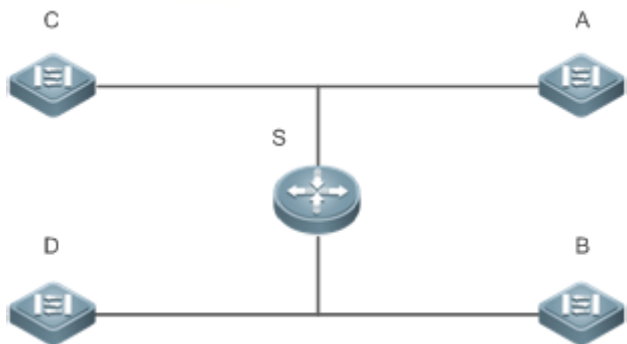
Remarks	S is an egress gateway working as a DHCP server. A, B, C and D are access switches with DHCP Client enabled on the interfaces.

Deployment

Enable DHCP Server on S.

Enable DHCP Client on the interfaces of A, B, C and D.

4.2.3   Applying AM Rule on DHCP Server

Scenario

As shown in Figure 4-3, create a Super VLAN, configure an AM rule and enable DHCP Server on the core switch A. B is an aggregation switch, C an access switch, and D a wireless access device. The requirements are listed as follows:

Assign IP addresses dynamically based on the VLAN and port;

Assign IP addresses statically based on the VLAN;

Assign IP addresses dynamically based on the default AM rule.

Figure 4-3 Applying AM Rule on a DHCP Server

Руководство пользователя

4. Configuring DHCP
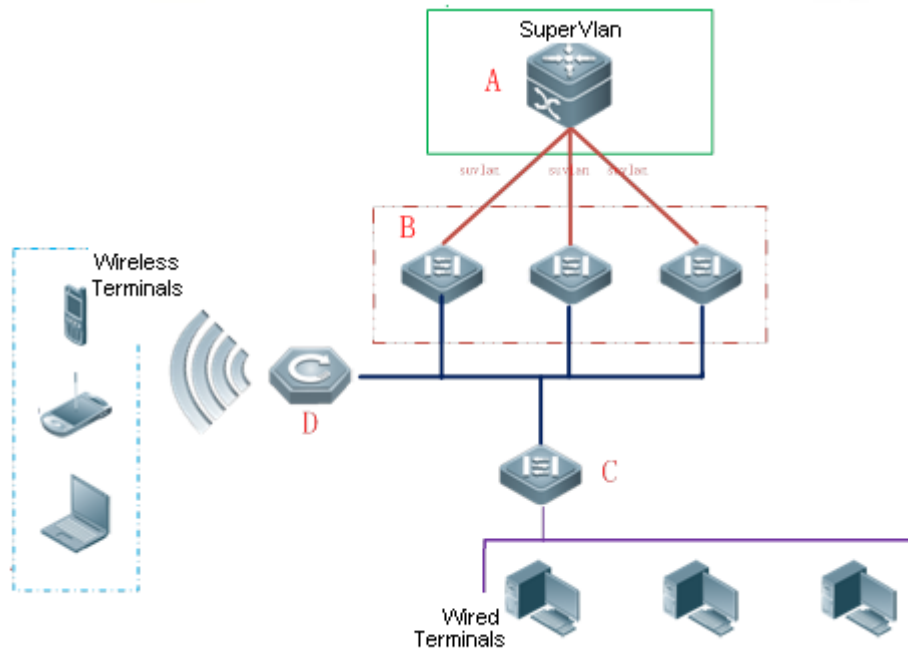
Remark s	A is a core device.
	B is an aggregation device.
	C is a wired access device.
	D is a wireless access device.

Deployment

Configure an AM rule, enable DHCP Server and create a Super VLAN on A.

Create VLANs on B and C to transparently transmit DHCP packets from wired users to A to request IP addresses.

Enable the wireless function on D to transparently transmit DHCP packets from wireless users to A to request IP addresses.

4.2.4 Deploying DHCP Relay in Wired Network

Scenario

As shown in the following figure, Switch C and Switch D are access devices for the users in VLAN 10 and VLAN 20 respectively. Switch B is a gateway, and Switch A a core device. The requirements are listed as follows:

4. Configuring DHCP

Switch A works as a DHCP server to assign IP addresses of different network segments dynamically to users in different VLANs.

Users in VLAN 10 and VLAN 20 obtain IP addresses dynamically.

Figure 4-4 DHCP Relay
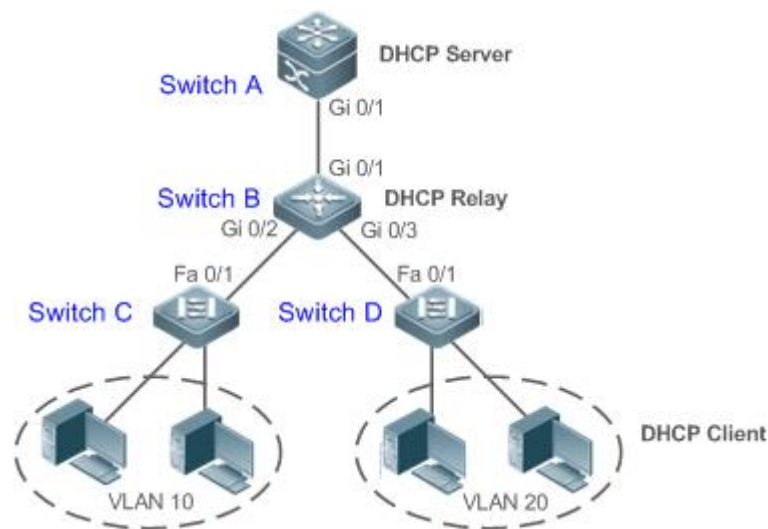
Remarks	Switch C and Switch D are access devices.
	Switch B is a gateway.
	Switch A is a core device.

Deployment

Configure layer-2 communication between Switch B and Switch C as well as between Switch B and Switch D.

On Switch B, specify a DHCP server address and enable DHCP Relay.

On Switch A, create DHCP address pools for VLAN 10 and VLAN 20 respectively, and enable DHCP Server.

4.2.5   Applying AM Rule on DHCP Relay

Scenario

As shown in Figure 4-5, A is a DHCP server, B a core switch configured with Super VLAN, an AM rule and DHCP Relay, C an aggregation switch, D an access switch, and E a wireless access device. The requirements are listed as follows:

Based on the VLAN-port AM rule, the DHCP relay agent chooses a subnet address as Giaddress of relay packets and forwards them to the DHCP server to request an IP address for the client.

4. Configuring DHCP

Based on default AM rule, the DHCP relay agent chooses a subnet address as Giaddress of relaying packets and forwards them to the DHCP server to request an IP address for the client.

Figure 4-5 Applying AM Rule on DHCP Relay
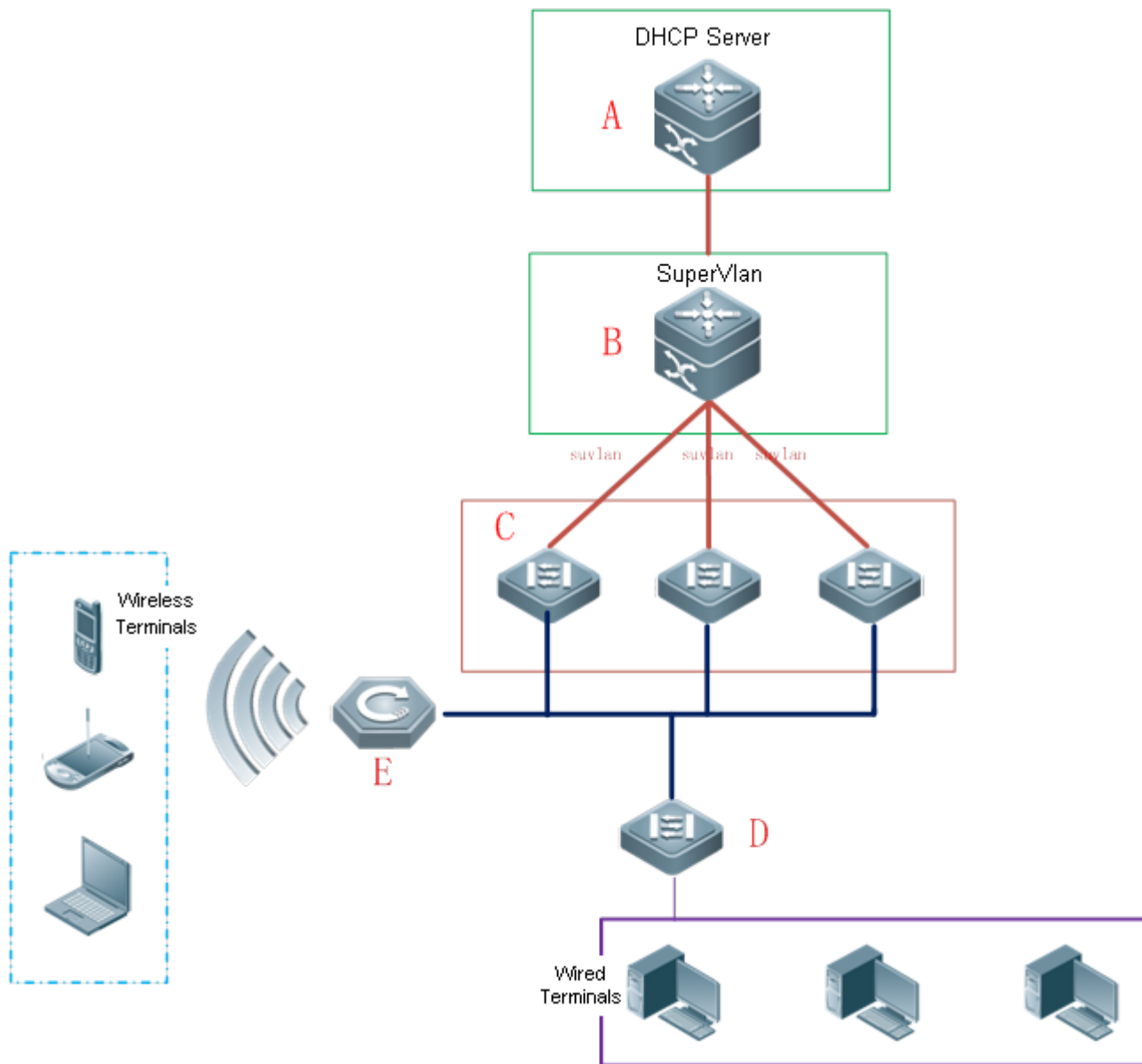
Remarks	A is a core device.
	B is a core device.
	C is an aggregation device.
	D is a wired access device.
	E is a wireless access device.

4. Configuring DHCP

Deployment

Enable DHCP Server on A.

Configure an AM rule, enable DHCP Relay and create a Super VLAN on B.

Create VLANs on C and D to transparently transmit DHCP packets from wired users to B to request IP addresses.

Enable the wireless function on E to transparently transmit DHCP packets from wireless users to B to request IP addresses.

4.3 Features

Basic Concepts

DHCP Server

Based on the RFC 2131, QTECH DHCP server assigns IP addresses to clients and manages these IP addresses.

DHCP Client

DHCP Client enables a device to automatically obtain an IP address and configurations from a DHCP server.

DHCP Relay

When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Lease

Lease is a period of time specified by a DHCP server for a client to use an assigned IP address. An IP address is active when leased to a client. Before a lease expires, a client needs to renew the lease through a server. When a lease expires or is deleted from a server, the lease becomes inactive.

Excluded Address

An excluded address is a specified IP address not assigned to a client by a DHCP server.

Address Pool

An address pool is a collection of IP addresses that a DHCP server may assign to clients.

4. Configuring DHCP

Option Type

An option type is a parameter specified by a DHCP server when it provides lease service to a DHCP client. For example, a public option include the IP addresses of a default gateway (router), WINS server and a DNS server. DHCP server allows configuration of other options. Though most options are defined in the RFC 2132, you can add user-defined options.

Overview

Feature	Description
DHCP Server	Enable DHCP Server on a device, and it may assign IP addresses dynamically and pushes configurations to DHCP clients.
DHCP Relay	Enable DHCP Relay on a device, and it may forward DHCP request and reply packets across different network segments.
DHCP Client	Enable DHCP Client on a device, and it may obtain IP addresses and configurations automatically from a DHCP server.
AM Rule	Enable an AM rule on a device, and it may assign IP addresses according to the rule.

4.3.1   DHCP Server

Working Principle

DHCP Working Principle

Figure 4-6
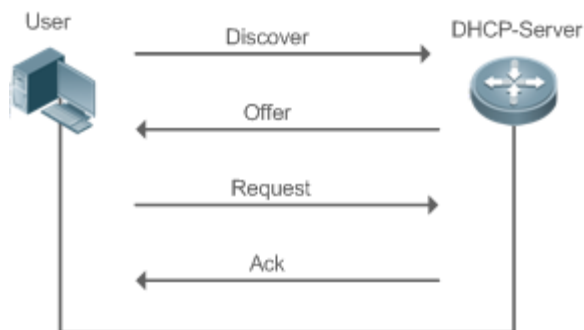
A host requests an IP address through DHCP as follows:

4. Configuring DHCP

1. A host broadcasts a DHCP discover packet to find DHCP servers in a network.
2. DHCP servers unicast/broadcast (based on the property of the host packet) DHCP offer packets to the host, containing an IP address, a MAC address, a domain name and a lease.
3. The host broadcasts a DHCP request packet to formally request an IP address.
4. A DHCP server sends a DHCP ACK unitcast packet to the host to acknowledge the request.

ℹ A DHCP client may receive DHCPOFFER packets from multiple DHCP servers, but usually it accepts only the first DHCPOFFER packet. Besides, the address specified in a DHCPOFFER packet is not necessarily assigned. Instead, it is retained by the DHCP server until a client sends a formal request.

To formally request an IP address, a client broadcasts a DHCPREQUEST packet so that all DHCP servers sending DHCPOFFER packets may receive the packet and release OFFER IP addresses.

If a DHCPOFFER packet contains invalid configuration parameters, a client will send a DHCPDECLINE packet to the server to decline the configuration.

During the negotiation, if a client does not respond to the DHCPOFFER packets in time, servers will send DHCPNAK packets to the client and the client will reinitiate the process.

During network construction, QTECH DHCP servers have the following features:

Low cost. Usually the static IP address configuration costs more than DHCP configuration.

Simplified configuration. Dynamic IP address assignment dramatically simplifies device configuration

Centralized management. You can modify the configuration for multiple subnets by simply modifying the DHCP server configuration.

Address Pool

After a server receives a client's request packet, it chooses a valid address pool, determines an available IP address from the pool through PING, and pushes the pool and address configuration to the client. The lease information is saved locally for validity check upon lease renewal.

An address pool may carry various configuration parameters as follows:

An IP address range, which is the range of IP addresses that are available.

A gateway address. A maximum of 8 gateway addresses are supported.

A DNS address. A maximum of 8 DNS addresses are supported.

A lease period notifying clients of when to age an address and request a lease renewal.

4. Configuring DHCP

VRRP Monitoring

In a Virtual Router Redundancy Protocol (VRRP) scenario, QTECH devices enabled with DHCP provide a command to monitor the VRRP status of the interface. To an interface configured with VRRP address and VRRP monitoring, a DHCP server only processes the DHCP clients' request packets from the interface in Master state, and other packets are discarded. If no VRRP address is configured, the DHCP server does not monitor the VRRP status, and all DHCP packets are processed. VRRP monitoring is configured on only layer-3 interfaces. It is disabled by default, namely, only the Master device processes the DHCP service.

IP Address Assignment Based on VLANs, Ports and IP Range

After an IP address pool is deployed, the specified IP address range is assigned based on VLANs and ports. There are three scenarios. 1. Global configuration. 2. Configuration based on VLANs, ports and IP range. 3. Both 1 and 2. In scenario 1, the addresses are assigned globally. In scenario 2, the addresses in the specified IP range are assigned only to the clients of the specified VLANs and ports. In scenario 3, the clients of the specified VLANs and ports are assigned the addresses in the specified IP range, and the other clients are configured with default global addresses.

**Related
Configuration**

Enabling DHCP Server Globally

By default, DHCP Server is disabled.

Run the **service dhcp** command to enable the DHCP Server.

Run the **service dhcp** command globally to enable DHCP service.

Configuring Address Pool

By default, no address pool is configured.

Run the **ip dhcp pool** command to configure an IP address range, a gateway and a DNS.

If no address pool is configured, no addresses will be assigned.

4.3.2   DHCP Relay Agent

**Working
Principle**

4. Configuring DHCP

The destination IP address of DHCP request packets is 255.255.255.255, and these packets are forwarded within a subnet. To achieve IP address assignment across network segments, a DHCP relay agent is needed. The DHCP relay agent unicasts DHCP request packets to a DHCP server and forwards DHCP reply packets to a DCHP client. The DHCP relay agent serves as a repeater connecting a DHCP client and a DHCP server of different network segments by forwarding DHCP request packets and DHCP reply packets. The Client-Relay-Server mode achieves management of IP addresses across multiple network segments by only one DHCP server. See the following figure.

Figure 4-7 DHCP Relay Scenario
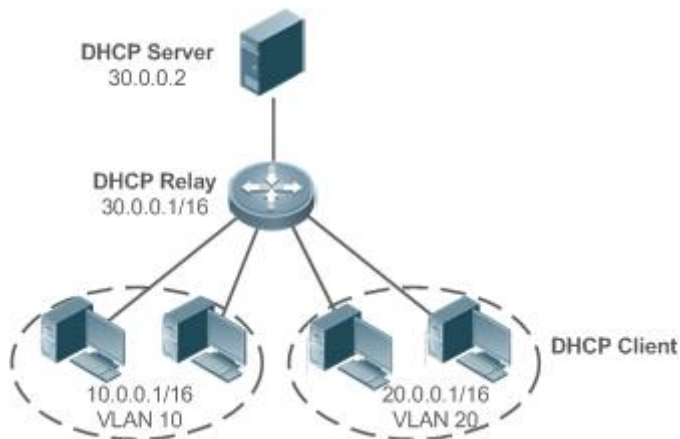
VLAN 10 and VLAN 20 correspond to the segments 10.0.0.1/16 and 20.0.0.1/16 respectively. A DHCP server with IP address 30.0.0.2 is in segment 30.0.0.1/16. To achieve management of dynamic IP addresses in VLAN 10 and VLAN 20 by the DHCP server, you only need to enable DHCP Relay on a gateway and configure IP address 30.0.0.2 for the DHCP server.

DHCP Relay Agent Information (Option 82)

As defined in RFC3046, an option can be added to indicate a DHCP client's network information when DHCP Relay is performed, so that a DHCP server may assign IP addresses of various privileges based on more accurate information. The option is called Option 82. Currently, QTECH devices support four schemes of relay agent information, which are described respectively as follows:

1. Relay agent information option dot1x: This scheme should be implemented with 802.1X authentication and the RG-SAM products. Specifically, RG-SAM products push the IP privilege during 802.1X authentication. A DHCP relay agent forms a Circuit ID sub-option based on the IP privilege and the VLAN ID of a DHCP client. The option format is shown in the following figure.

Figure 4-8 Option Format

4. Configuring DHCP
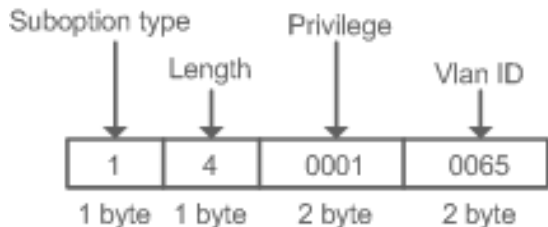
2. Relay agent information option82: This scheme serves without correlation with other protocol modules. A DHCP relay agent forms an Option 82 based on the physical port receiving DHCP request packets and the MAC address of the device. The option format is shown in the following figure.

Figure 4-9 Agent Circuit ID
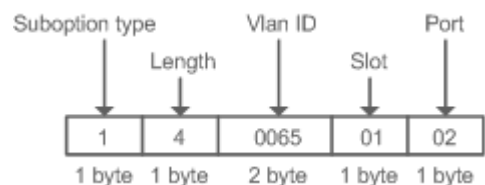
Figure 4-10 Agent Remote ID
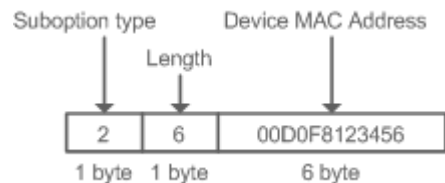
1. Relay agent information option VPN: This scheme should be implemented with MPLS VPN functions.

Figure 4-11 Application in MPLS VPN Environment
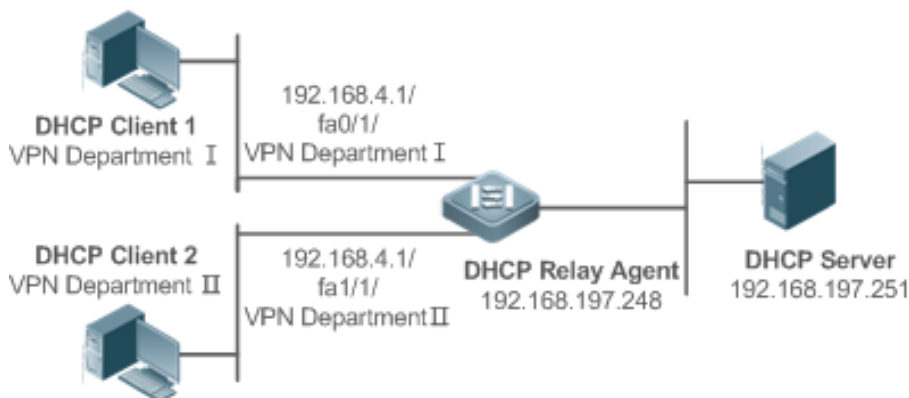
4. Configuring DHCP

As shown in Figure 4-11, in MPLS VPN environment, DHCP Client 1 is connected to fa0/1 on a DHCP relay agent and DHCP Client 2 to fa1/1. Interfaces fa0/1 and fa1/1 belongs to different VRFs. DHCP Client 1 and DHCP Client 2 obtain IP addresses through DHCP. According to network planning, VPN Department I and VPN Department II are in a same segment 192.168.4.0/24. In this case, conventional DHCP application cannot meet the demand. To support DHCP Relay in MPLS VPN environment, **option vpn** is introduced, which includes the three sub-options, namely, VPN-ID, Subnet-Selection and Server-Identifier-Override.

- VPN-ID: When a DHCP relay agent receives a DHCP request packet, it adds the information of the VPN the DHCP client resides to the packet as an option. The DHCP server keeps the VPN-ID in a reply packet, and the DHCP relay agent forwards the packet to the corresponding VRF according to the option. The option format is shown in the following figure.

Figure 4-12 VPN-ID
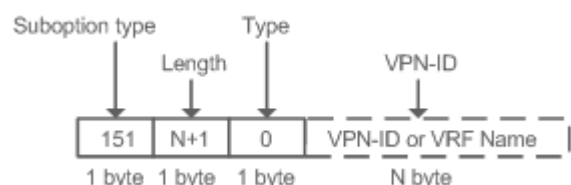
- Subnet-Selection: In conventional DHCP Relay, the information of a client network and the addresses of a DHCP server and a DHCP relay agent are indicated by the **gateway address**[**giaddr**] field. In MPLS VPN environment, set **giaddr** to the IP address of the interface of a DHCP relay agent connected to a DHCP server, so that the server may communicate directly with the relay agent. Besides, the information of the client subnet is indicated by a Subnet-Selection option. The option format is shown in the following figure.

Figure 4-13 Subnet-Selection
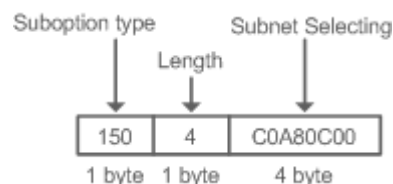
- Server-Identifier-Override: In MPLS VPN environment, request packets from a DHCP client cannot be sent directly to a DHCP server. A DHCP relay agent use this option to carry the information of the interface connecting the relay agent and the DHCP server. When the server sends a reply message, this option overrides the Server-Identifier option. In this way, the DHCP client sends packets to DHCP relay agent, and the DHCP relay agent forwards them to the DHCP server. The option format is shown in the following figure.

Figure 4-14 Server-Identifier-Override

4. Configuring DHCP
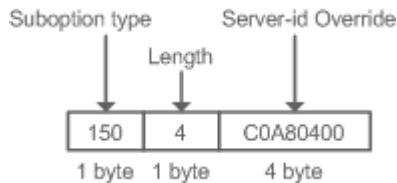
DHCP Relay Check Server-ID

In DHCP environment, multiple DHCP servers are deployed for a network, achieving server backup to ensure uninterrupted network operation. After this function is enabled, the DHCP request packet sent by a client contains a **server-id** option specifying a DHCP server. In alleviating the burden on servers in specific environments, you need to enable this function on a relay agent to send a packet to a specified DHCP server rather than all DHCP servers.

DHCP Relay suppression

After you configure the **ip DHCP Relay suppression** command on an interface, DHCP request packets received on the interface will be filtered, and the other DHCP request packets will be forwarded.

**Related
Configuration**

Enabling DHCP Relay

▪ By default, DHCP Relay is disabled.
▪ You may run the **service dhcp** command to enable DHCP Relay.
▪ You need to enable DHCP Relay before it works.

Configuring IP Address for DHCP Server

▪ By default, no IP address is configured for a DHCP server.
▪ You may run the **ip helper-address** command to configure an IP address for a DHCP server. The IP address can be configured globally or on a layer-3 interface. A maximum of 20 IP addresses can be configured for a DHCP server.
▪ When an interface receives a DHCP request packet, the DHCP server configuration on the interface prevails over that configured globally. If the interface is not configured with DHCP server addresses, the global configuration takes effect.

Enabling DHCP Option 82

▪ By default, DHCP Option 82 is disabled.
▪ You may run the **ip dhcp relay information option82** command to enable DHCP Option 82.

Enabling DHCP Relay Check Server-ID

▪ By default, DHCP Relay check server-id is disabled.
▪ You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

4. Configuring DHCP

Enabling DHCP Relay Suppression

- By default, DHCP Relay suppression is disabled on all interfaces.
- You may run the **ip dhcp relay suppression** command to enable it on an interface.

Enabling the Function of Multiple Gateway IP Addresses

- By default, the function of multiple gateway IP addresses is enabled.
- You may run the **ip dhcp relay multiple-giaddr** command to enable the function of multiple gateway IP addresses.

4.3.3 DHCP Client

Working Principle

A DHCP client broadcasts a DHCP discover packet after entering the Init state. Then it may receive multiple DHCP offer packets. It chooses one of them and responds to the corresponding DHCP server. After that, it sends lease renewal request packets in the Renew and Rebind processes of an aging period to request lease renewal.

Related Configuration

Enabling DHCP Client on Interface

- By default, DHCP Client is disabled.
- In interface configuration mode, you may run the **ip address dhcp** command to enable DHCP Client.
- You need to enable DHCP Client to enable DHCP service.

- The configuration takes effect on a layer-3 interface, for example, an SVI or a routed port.

4.3.4 AM Rule

Working Principle

An AM rule defines the range of IP addresses assigned to DHCP clients in different VLANs and ports. It can be used to quickly identify the VLAN and port of a faulty DHCP client and effectively assign addresses. After an AM rule is configured, all DHCP clients from the set VLAN and ports may obtain IP addresses. If no AM rule is configured, there are two following cases: If a default AM rule is configured, the client obtains an IP address from the default range; if no default AM rule is configured, the client cannot obtain an IP address.

4. Configuring DHCP

Configuring AM Rule in Global Configuration Mode

▪ In global configuration mode, run the **address-manage** command to enter AM rule configuration mode.

▪ Run the **match ip default** command to configure a default AM rule.

▪ Run the **match ip** command to configure an AM rule based on VLAN & port or port.

4.4 Configuration

Configuring DHCP Server

Configuration	Description and Command	
Configuring Dynamic IP Address	⚠ (Mandatory) It is used to enable DHCP Server to achieve dynamic IP address assignment.	
	service dhcp	Enables DHCP Server.
	ip dhcp pool	Configures an address pool.
	network	Configures the network number and subnet mask of a DHCP address pool.
	⚠ (Optional) It is used to configure the properties of an address pool.	
	default-router	Configures a default gateway of a client.
	lease	Configures an address lease.
	next-server	Configures a TFTP server address
	bootfile	Configures a boot file of a client.

	domain-name	Configures a domain name of a client.
	dns-server	Configures a domain name server.
	netbios-name-server	Configures a NetBIOS WINS server.
	netbios-node-type	Configures a NetBIOS node type on a client.
	lease-threshold	Configures an alarm threshold of an address pool.
	option	Configures a user-defined option.
	pool-status	Enables or disables an address pool.
Configuring Static IP Address	⚠ (Optional) It is used to statically assign an IP address to a client.	
	ip dhcp pool	Configures an address pool name and enters address pool configuration mode.
	host	Configures the IP address and subnet mask of a client host.
	hardware-address	Configures a client hardware address.
	client-identifier	Configures a unique client identifier.
	client-name	Configures a client name.
Configuring AM Rule for DHCP	⚠ (Optional) It is used to configure the properties of a DHCP server.	

4. Configuring DHCP

Server	ip dhcp excluded-address	Configures an excluded IP address.
	ip dhcp force-send-nak	Configures Compulsory NAK reply by a DHCP server.
	ip dhcp monitor-vrrp-state	Configures VRRP status monitoring.
	ip dhcp ping packets	Configures ping times.
	ip dhcp ping timeout	Configures a ping timeout.
	ip dhcp server arp-detect	Configures a DHCP server to detect user offline.
Configuring Global Properties of DHCP Server	⚠ (Optional) It is used to configure the AM rule of a DHCP server.	
	match ip default	Configures a default AM rule.
	match ip ip-address	Configures an AM rule based on the VLAN and port.

Configuring DHCP Relay

Configuration	Description and Command	
Configuring Basic DHCP Relay Functions	⚠ (Mandatory) It is used to enable DHCP Relay.	
	service dhcp	Enables DHCP Relay.
	ip helper-address	Configures an IP Address of a DHCP Server.
Configuring DHCP Relay Option 82	⚠ (Optional) It is used to assign IP addresses of different privileges to clients in combination with the information of a physical port. This function cannot be used together with the **dhcp option dot1x** command.	
	ip dhcp relay information option82	Enables DHCP option82.

4. Configuring DHCP

Configuring DHCP Relay Check Server-ID	⚠ (Optional) It is used to enable a DHCP Relay agent to send DHCP request packets only to a specified server.	
	ip dhcp relay check server-id	Enables a DHCP Relay agent to send DHCP request packets only to a specified server
Configuring DHCP Relay Suppression	⚠ (Optional) It is used to shield DHCP request packets on an interface.	
	ip dhcp relay suppression	Enables DHCP Relay Suppression.
Enabling DHCP Relay to Discard DHCP Request Packets from VxLAN Tunnels	⚠ (Optional) It is used to discard DHCP request packets from VxLAN tunnels.	
	ip dhcp relay discard overlay-tunnel	Discards DHCP request packets from VxLAN tunnels.

Configuring DHCP Client

Configuration	Description and Command	
Configuring DHCP Client	⚠ (Mandatory) It is used to enable DHCP Client.	
	ip address dhcp	Enables an Ethernet interface, a PPP/HDLC-encapsulated or FR-encapsulated interface to obtain IP addresses through DHCP.

4.4.1   Configuring Dynamic IP Address

Configuration Effect

Provide all DHCP clients with DHCP service including assigning IP addresses and gateways.

Notes

A DHCP server and a DHCP relay share the **service dhcp** command, but a device cannot function as a DHCP server and relay at the same time. When a device is configured with a valid address pool, it

4. Configuring DHCP

acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Configuration Steps

Enabling DHCP Server

- Mandatory. It achieves dynamic IP address assignment.
- Run the **service dhcp** command in global configuration mode.

Configuring Address Pool

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

- Mandatory. It defines a range of dynamically assigned addresses.
- Run the **network** command in DHCP address pool configuration mode.

Configuring Default Gateway of Client

- Optional. It is used to configure a gateway address.
- Run the **default-router** command in DHCP address pool configuration mode.

Configuring Address Lease

- Optional. It is used to configure an IP address lease, which is 24h by default.
- Run the **lease** command in DHCP address pool configuration mode.

Configuring TFTP Server Address

- Optional. It is used to configure a TFTP server address.
- Run the **next-server** command in DHCP address pool configuration mode.

Configuring Domain Name of Client

- Optional. It is used to configure the domain name of a client.
- Run the **domain-name** command in DHCP address pool configuration mode.

Configuring DNS

- Optional. It is used to configure a DNS address.
- Run the **dns** command in DHCP address pool configuration mode.

Configuring NetBIOS WINS Server

- Optional. It is used to configure a NetBIOS WINS server address.
- Run the **netbios-name-server** command in DHCP address pool configuration mode.

4. Configuring DHCP

Configuring NetBIOS Node Type on Client

- Optional. It is used to configure a NetBIOS node type.
- Run the **netbios-name-type** command in DHCP address pool configuration mode.

Configuring Alarm Threshold of Address Pool

- Optional. It is used to manage the number of leases. When a threshold (90% by default) is reached, an alarm will be printed.
- Run the **lease-threshold** command in DHCP address pool configuration mode.

Configuring User-Defined Option

- Optional. It is used to configure user-defined options.
- Run the **option** command in DHCP address pool configuration mode.

Enabling or Disabling Address Pool

- Optional. It is used to enable or disable an address pool. It is enabled by default.
- Run the **pool-status** command in DHCP address pool configuration mode.

Verification

Connect a DHCP client and a DHCP server.

- Check whether the client obtains configurations on the server.

Related Commands

Enabling DHCP Server

Command	service dhcp
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable DHCP Server and DHCP Relay. A DHCP server and a DHCP relay share the **service dhcp** command. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

4. Configuring DHCP

Configuring Address Pool

Command	ip dhcp pool *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter DHCP address pool configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

Command	network *network-number mask* [*low-ip-address high-ip-address*]
Parameter Description	*network-number:* Indicates the network number of an IP address pool. *mask:* Indicates the subnet mask of an IP address pool. If no subnet mask is defined, the natural subnet mask is applied.
Command Mode	DHCP address pool configuration mode
Usage Guide	To configure dynamic address assignment, you need to configure a network number and subnet mask of an address pool to provide a DHCP server with a range of addresses. The IP addresses in a pool are assigned in order. If an address is assigned or exists in the target network segment, the next address will be checked until a valid address is assigned. QTECH wireless products provide available network segments by specifying start and end addresses. The configuration is optional. If the start and end address are not specified, all IP addresses in the network segment are assignable. For QTECH products, addresses are assigned based on the client's physical address and ID. Therefore, one client will not be assigned two leases from one address pool. In case of topological redundancy between a client and a server, address assignment may fail. To avoid such failures, a network administrator needs to prevent path redundancy in network construction, for example, by adjusting physical links or network paths.

4. Configuring DHCP

Configuring Default Gateway of Client

Command	default-router *address* [*address2...address8*]
Parameter Description	*address*: Indicates the IP address of a default gateway. Configure at least one IP address. *ip-address2...ip-address8:* (Optional) A maximum of 8 gateways can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	Configure a default gateway of a client, and a server will push the gateway configuration to the client. The IP addresses of the default gateway and the client should be in a same network.

Configuring Address Lease

Command	lease {*days* [*hours*] [*minutes*]	infinite}
Parameter Description	*days:* Defines a lease in the unit of day. *hours:* (Optional) Defines a lease in the unit of hour. Please define *days* before *hours*. *minutes:* (Optional) Defines a lease in the unit of minute. Please define *days* and *hours* before *minutes*. **infinite:** Defines an unlimited lease.
Command Mode	DHCP address pool configuration mode
Usage Guide	The default lease of an IP address assigned by a DHCP server is 1 day. When a lease is expiring soon, a client needs to request a lease renewal. Otherwise the IP address cannot be used after the lease is expired.

Configures Boot File on Client

Command	bootfile *filename*
Parameter Description	*file-name*: Defines a boot file name.

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

4. Configuring DHCP

Command Mode	DHCP address pool configuration mode
Usage Guide	A boot file is a bootable image file used when a client starts up. The file is usually an OS downloaded by a DHCP client.

Configuring Domain Name of Client

Command	**domain-name** *domain*
Parameter Description	*domain-name:* Defines a domain name of a DHCP client.
Command Mode	DHCP address pool configuration mode
Usage Guide	You may define a domain name for a client. When the client accesses network through the host name, the domain name will be added automatically to complete the host name.

Configuring DNS

Command	**dns-server { *ip-address* [*ip-address2…ip-address8*]**
Parameter Description	*ip-address:* Defines an IP address of a DNS server. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 DNS servers can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	If a client accesses network resources through the domain name, you need to configure a DNS server to resolve the domain name.

Configuring NetBIOS WINS Server

Command	**netbios-name-server** *address* [*address2…address8*]
Parameter Description	*address:* Defines an IP address of a WINS server. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 WINS servers can be configured.

QTECH | www.qtech.ru
МИР ДОСТУПНЕЕ

4. Configuring DHCP

Command Mode	DHCP address pool configuration mode
Usage Guide	WINS is a domain name service through which a Microsoft TCP/IP network resolves a NetNBIOS name to an IP address. A WINS server is a Windows NT server. When a WINS server starts, it receives a registration request from a WINS client. When the client shuts down, it sends a name release message, so that the computers in the WINS database and on the network are consistent.

Configuring NetBIOS Node Type on Client

Command	netbios-node-type *type*
Parameter Description	type: Defines a NetBIOS node type with one of the following approaches. 1. A hexadecimal number, ranging from 0 to FF. Only followings values are available. ▪ b-node ▪ p-node ▪ m-node ▪ 8 for h-node 2. A character string. ▪ b-node for a broadcast node; ▪ p-node for a peer-to-peer node; ▪ m-node for a mixed node; ▪ h-node for a hybrid mode.
Command Mode	DHCP address pool configuration mode
Usage Guide	There are four types of NetBIOS nodes of a Microsoft DHCP client. 1) A broadcast node. For such a node, NetBIOS name resolution is requested through broadcast.2) A peer-to-peer node. The client sends a resolution request to the WINS server. 3) A mixed node. The client broadcasts a resolution request and sends the resolution request to the WINS server.. 4) A hybrid node. The client sends a resolution request to the WINS server. If no reply is received, the client will broadcast the resolution request. By default, a Microsoft operating system is a broadcast or hybrid node. If no WINS server is configured, it is a broadcast node. Otherwise, it is a hybrid node.

4. Configuring DHCP

Configuring User-Defined Option

Command	option *code* { ascii *string* | hex *string* | ip *ip-address* }
Parameter Description	*code:* Defines a DHCP option code. **ascii** *string:* Defines an ASCII character string. **hex** *string:* Defines a hexadecimal character string. **ip** *ip-address:* Defines an IP address.
Command Mode	DHCP address pool configuration mode
Usage Guide	The DHCP allows transmitting configuration information to a host via a TCP/IP network. DHCP packets contain the option field of definable content. A DHCP client should be able to receive a DHCP packet carrying at least 312 bytes option. Besides, the fixed data field in a DHCP packet is also called an option. In a WLAN, a DHCP client on an AP dynamically requests the IP address of an AC. You may configure on a DHCP server the **option** command specifying the AC address.

Enabling or Disabling Address Pool

Command	pool-status {enable | disable}
Parameter Description	**enable***:* Enables an address pool. **disable***:* Disable an address pool. It is enabled by default.
Command Mode	DHCP address pool configuration mode
Usage Guide	A QTECH wireless product provides a command for you to enable/disable a DHCP address pool.

Configuration Example

Configuring Address Pool

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

4. Configuring DHCP

Configuration Steps	**Define an address pool net172.** **The network segment is 172.16.1.0/24.** **The default gateway is 172.16.1.254.** **The address lease is 1 day.** **xcluded addresses range from 172.16.1.2 to 172.16.1.100.**
	QTECH (config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100 QTECH (dhcp-config)# ip dhcp pool net172 QTECH (dhcp-config)# network 172.16.1.0 255.255.255.0 default-router 172.16.1.254 lease 1
Verification	Run the **show run** command to display the configuration.
	QTECH (config)#show run | begin ip dhcp ip dhcp excluded-address 172.16.1.2 172.16.1.100 ip dhcp pool net172 network 172.16.1.0 255.255.255.0 default-router 172.16.1.254lease 1

4.4.2   Configuring Static IP Address

Configuration Effect

Assign specific IP addresses and push configuration to specific DHCP clients.

Notes

N/A

Configuration Steps

Configuring Address Pool Name and Entering Address Pool Configuration Mode

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring IP Address and Subnet Mask of Client

- Mandatory. It is used to configure a static IP address and a subnet mask.
- Run the **host** command in DHCP address pool configuration mode.

4. Configuring DHCP

Configuring Hardware Address of Client

- ▪ Optional. It is used to configure a MAC address.
- ▪ Run the **hardware** command in DHCP address pool configuration mode.

Configures Unique Client Identifier

- ▪ Optional. It is used to configure a static user identifier (UID).
- ▪ Run the **client-identifier** command in DHCP address pool configuration mode.

Configuring Client Name

- ▪ Optional. It is used to configure a static client name.
- ▪ Run the **host-name** command in DHCP address pool configuration mode.

Verification

Check whether the client obtains the IP address when it is online.

Related Commands

Configuring Address Pool

Command	ip dhcp pool *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter address pool configuration mode.

Manual IP Address Binding

Command	host *ip-address* [*netmask*] client-identifier *unique-identifier* client-name *name*

4. Configuring DHCP

Parameter Description	*ip-address:* Defines the IP address of a DHCP client. *netmask:* Defines the subnet mask of a DHCP client. *unique-identifier:* Defines the hardware address (for example, aabb.bbbb.bb88) and identifier (for example, 01aa.bbbb.bbbb.88) of a DHCP client. *name:* (Optional) It defines a client name using ASCII characters. The name excludes a domain name. For example, name a host mary rather than mary.rg.com.
Command Mode	DHCP address pool configuration mode
Usage Guide	Address binding means mapping between an IP address and a client's MAC address. There are two kind of address binding. 1) Manual binding. Manual binding can be deemed as a special DHCP address pool with only one address. 2) Dynamic binding. A DHCP server dynamically assigns an IP address from a pool to a client when it receives a DHCP request, creating mapping between the IP address and the client's MAC address. To configure manual binding, you need to define a host pool and then specify a DHCP client's IP address and hardware address or identifier. A hardware address is a MAC address. A client identifier includes a network medium type and a MAC address. A Microsoft client is usually identified by a client identifier rather than a MAC address. For the codes of medium types, refer to the *Address Resolution Protocol Parameters* section in the RFC 1700. The Ethernet type is 01.

Configuration Example

Dynamic IP Address Pool

Configuration Steps	**Configure address pool VLAN 1 with IP address 20.1.1.0 and subnet mask 255.255.255.0.** **The default gateway is 20.1.1.1.** **The lease time is 1 day.**
	QTECH (config)# ip dhcp pool vlan1 QTECH (dhcp-config)# network 20.1.1.0 255.255.255.0 QTECH (dhcp-config)# default-router 20.1.1.1 QTECH (dhcp-config)# lease 1 0 0
Verification	Run the **show run** command to display the configuration.

4. Configuring DHCP

```
QTECH (config)#show run | begin ip dhcp
ip dhcp pool vlan1
network 20.1.1.0 255.255.255.0
default-router 20.1.1.1
lease 1 0 0
```

Manual Binding

Configuration Steps	▪ **The host address is 172.16.1.101 and the subnet mask is 255.255.255.0.** ▪ **The host name is user.** ▪ **The default gateway is 172.16.1.254.** ▪ **The MAC address is 00d0.df34.32a3.**
	QTECH (config)# ip dhcp pool test QTECH (dhcp-config)# host 172.16.1.101 255.255.255.0 QTECH (dhcp-config)# client-name user QTECH (dhcp-config)# hardware-address 08c6.b334.32a3 Ethernet QTECH (dhcp-config)# default-router 172.16.1.254
Verification	Run the show run command to display the configuration.
	QTECH (config)#show run | begin ip dhcp ip dhcp pool test host 172.16.1.101 255.255.255.0 client-name user hardware-address 08c6.b334.32a3 Ethernet default-router 172.16.1.254

4.4.3 Configuring AM Rule for DHCP Server

Configuration Effect

Assign IP addresses according to an AM rule based on a port and a VLAN.

Notes

4. Configuring DHCP

QTECH products support AM rule configuration on Ethernet, GB, FR, PPP and HDLC interfaces.

Configuration Steps

Configuring Address Management

- Mandatory. Enter address management mode.
- Run the **address-manage** command in address management configuration mode.

Configuring AM Rule

- Mandatory. Configure an AM rule based on a port and a VLAN.
- Run the **match ip** command in address management configuration mode.

Verification

Check whether clients in different VLANs and ports obtain the valid IP addresses.

Related Commands

Configuring Default Range

Command	match ip default *ip-address netmask*
Parameter Description	*ip-address:* Defines an IP address. *netmask:* Defines a subnet mask.
Command Mode	Address management mode
Usage Guide	After configuration, all DHCP clients are assigned IP addresses from the default range based on the VLAN and port. If this command is not configured, IP addresses will be assigned through the regular process.

Assigning Dynamic IP Address Based on VLAN and Port

Command	match ip *ip-address netmask interface* [add/remove] vlan *vlan-list*

4. Configuring DHCP

Parameter Description	ip-address: Defines an IP address. netmask: Defines a subnet mask. interface: Defines an interface name. add/remove: Adds or deletes a specific VLAN. vlan-list: Indicates a VLAN index.
Command Mode	Address management mode
Usage Guide	After configuration, DHCP clients are assigned IP addresses from the default address range based on the VLAN and port.

Assigning Static IP Address Based on VLAN

Command	match ip ip-address netmask [add/remove] vlan vlan-list
Parameter Description	ip-address: Defines an IP address. netmask: Defines a subnet mask. add/remove: Adds or deletes a specific VLAN. vlan-list: Indicates a VLAN index.
Command Mode	Address management mode
Usage Guide	In a Super VLAN, a client may be assigned a fixed static address no matter which Super VLAN the client resides in. You do not need to configure an AM rule for this IP address based on all sub-VLANs and ports, but only configure an AM rule based on the VLAN. This rule takes effect for only static address assignment.

Configuration Example

Configuring AM Rule

4. Configuring DHCP

Configuration Steps	**Configure a default rule.** **Configure a rule based on a specific VLAN + port + address range.** **Configure a rule based on a specific VLAN + address range.**
	QTECH (config)# address-manage QTECH (config-address-manage)# match ip default 172.50.128.0 255.255.128.0 QTECH (config-address-manage)# match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005 QTECH (config-address-manage)# match ip 10.1.6.0 255.255.255.0 vlan 1006
Verification	1: Run the show run command to display the configuration.
	address-manage match ip default 172.50.128.0 255.255.128.0 match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005 match ip 10.1.6.0 255.255.255.0 vlan 1006

4.4.4   Configuring Global Properties of DHCP Server

Configuration Effect

Enable a server with specific functions, for example, ping and compulsory NAK.

Notes

Configuring the command may cause exceptions on other servers.

Configuration Steps

Configuring Excluded IP Address

- Optional. Configure some addresses or address ranges as unavailable.
- Run the **ip dhcp excluded-address** command in global configuration mode.

Configuring Compulsory NAK Reply

- Optional. A server replies to a wrong address request with a NAK packet.
- Run the **ip dhcp force-send-nak** command in global configuration mode.

4. Configuring DHCP

Configuring VRRP Status Monitoring

- Optional. After configuration, DHCP packets are processed by the Master server.
- Run the **ip dhcp monitor-vrrp-state** command in global configuration mode.

Configuring Ping Times

- Optional. Check the address reachability with the **ping** command. The default is 2.
- Run the **ip dhcp ping packet** command in global configuration mode.

Configuring Ping Timeout

- Optional. Check the address reachability with the **ping** command. The default is 500 ms.
- Run the **ip dhcp ping timeout** command in global configuration mode.

Detecting User Offline Detection

- Configure a DHCP server to detect whether the client is offline or not. If a client does not get online after being offline for a period, the address assigned to the client will be retrieved.
- Run the **ip dhcp server arp-detect** command in global configuration mode.

Verification

Run the **dhcp-server** command, and check the configuration during address assignment.

Related Commands

Configuring Excluded IP Address

Command	ip dhcp excluded-address *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address:* Indicates a start IP address. *high-ip-address:* Indicates an end IP address.
Command Mode	Global configuration mode
Usage Guide	Unless otherwise specified, a DHCP server assigns all the addresses from an IP address pool to DHCP clients. To reserve some addresses(e.g., addresses already assigned to the server or devices), you need to configure these addresses as excluded addresses. To configure a DHCP server, it is recommended to configure excluded addresses to avoid address conflict and shorten detection time during address assignment.

QTECH МИР ДОСТУПНЕЕ | www.qtech.ru

4. Configuring DHCP

Configuring Compulsory NAK Reply

Command	ip dhcp force-send-nak
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In a WLAN, a DHCP client often moves from one network to another. When a DHCP server receives a lease renewal request from a client but finds that the client crosses the network segment or that the lease is expired, it replies with a NAK packet to require the client to obtain an IP address again. This prevents the client from sending request packets continually before obtaining an IP address again after timeout. The server sends a NAK packet only when it finds the client's lease record. When a DHCP client crosses the network, a DHCP server cannot find lease record of the client and will not reply with a NAK packet. The client sends request packets continually before obtaining an IP address again after timeout. Consequently, it takes a long to obtain an IP address. This also occurs when a DHCP server loses a lease after restart and a client requests lease renewal. In this case, you may configure a command to force the DHCP server to reply with a NAK packet even though it cannot find the lease record so that the client may obtain an IP address rapidly. Please note that the command is disabled by default. To enable it, only one DHCP server can be configured in a broadcast domain.

Configuring Ping Times

Command	ip dhcp ping packets [*number*]
Parameter Description	*number:* (Optional) Ranges from 0 to 10. 0 indicates the ping function is disabled. The default is two pings.
Command Mode	Global configuration mode
Usage Guide	By default, when a DHCP server assigns an IP address from a pool, it runs the Ping command twice (one packet per time). If there is no reply, the server takes the address as idle and assigns it to a client. If there is a reply, the server takes the address as occupied and assigns another address.

4. Configuring DHCP

Configuring Ping Timeout

Command	ip dhcp ping timeout *milliseconds*
Parameter Description	*milli-seconds:* Indicates the time that it takes for a DHCP server to wait for a ping reply. The value ranges from 100 ms to 10,000 ms.
Command Mode	Global configuration mode
Usage Guide	By default, if a DHCP server receives no Ping reply within 500 ms, the IP address is available. You may adjust the ping timeout to change the time for a server to wait for a reply.

Configuration Example

Configuring Ping

Configuration Steps	**Set ping times to 5.** **Set ping timeout to 800 ms.**
	QTECH (config)# ip dhcp ping packet 5 QTECH (config)# ip dhcp ping timeout 800
Verification	Run the show run command to display the configuration.
	QTECH (config)#show run | begin ip dhcp ip dhcp ping packet 5 ip dhcp ping timeout 800

Configuring Excluded IP Address

Configuration Steps	**Configure the excluded IP address from 192.168.0.0 to 192.168.255.255.**
	QTECH (config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
Verification	Run the **show run** command to display the configuration.

4. Configuring DHCP

```
QTECH (config)#show run | begin ip dhcp
ip dhcp excluded-address 192.168.0.0 192.168.255.255
```

4.4.5 Configuring Basic DHCP Relay Functions

Configuration Effect

- Deploy dynamic IP management in Client–Relay–Server mode to achieve communication between a DHCP client and a DHCP server, which are in different network segments.

Notes

- To enable DHCP Relay, you need to configure IPv4 unicast routing in a network.

Configuration Steps

Enabling DHCP Relay

- Mandatory.

- Unless otherwise specified, you need to enable DHCP Relay on a device.

Configuring IP Address for DHCP Server

- Mandatory.
- You need to configure an IP address for a DHCP server.

Verification

- Check whether a client obtains an IP address through DHCP Relay.

Related Commands

Enabling DHCP Relay

Command	service dhcp
Parameter Description	N/A

4. Configuring DHCP

Command Mode	Global configuration mode
Usage Guide	N/A

Configuring IP Address for DHCP Server

Command	ip helper-address { cycle-mode	[vrf { *vrf-name* }] A.B.C.D }
Parameter Description	*cycle-mode*: Indicates that DHCP request packets are forwarded to all DHCP servers. *vrf-name*: Indicates a VPN Routing & Forwarding (VRF) name. *A.B.C.D*: Indicates the IP address of a server.
Command Mode	Global configuration mode/interface configuration mode
Usage Guide	You may configure the function on a layer-3 interface, such as a routed port, a L3 AP port, SVI and loopback interface. The configured interface must be accessible via IPv4 unicast routing.

Configuration Example

Configuring DHCP Relay in Wired Connection

Scenario Figure 4-15	
Configuration Steps	▪ Enable a client with DHCP to obtain an IP address. ▪ Enable the DHCP Relay function on a DHCP relay agent. ▪ Configure DHCP Server.

4. Configuring DHCP

A	Enable a client with DHCP to obtain an IP address.
B	Enable DHCP Relay.
	QTECH (config)# service dhcp
	Configure a global IP address of a DHCP server.
	QTECH (config)# ip helper-address 172.2.2.1
	Configure an IP address for the port connected to the client.
	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 connected to the server.
	QTECH (config)# interface gigabitEthernet 0/2
	QTECH (config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
C	Enable DHCP Server.
	QTECH (config)# service dhcp
	Configure an address pool.
	QTECH (config)# ip dhcp pool relay
	QTECH (dhcp-config)#network 192.1.1.0 255.255.255.0
	QTECH (dhcp-config)#default-router 192.1.1.1
	Configure an IP address for the port connected to the relay agent.
	QTECH (config)# interface gigabitEthernet 0/1
	QTECH (config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0
Verification	Check whether the client obtains an IP address.
	▪ Check whether the client obtains an IP address.
	▪ Check the DHCP Relay configuration.
A	The user device obtains an IP address.
B	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	QTECH # show running-config
	service dhcp
	ip helper-address 172.2.2.1
	!

4. Configuring DHCP

```
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
!
```

Common Errors

- IPv4 unicast routing configuration is incorrect.
- DHCP Relay is disabled.
- No routing between DHCP relay agent and DHCP server is configured.
- No IP address is configured for the DHCP server.

4.4.6   Configuring DHCP Relay Option 82

Configuration Effect

- Through a DHCP relay agent, a server may assign IP addresses of different privileges to the clients more accurately based on the option information.

Notes

- You need to enable the DHCP Relay function.

Configuration Steps

Enabling Basic DHCP Relay Functions

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

Enables DHCP Option82

- By default, DHCP Option 82 is disabled.
- You may run the **ip dhcp relay information option82** command to enable or disable DHCP Option 82.

4. Configuring DHCP

Verification

▪ Check whether the client obtains an IP address based on Option 82.

Related
Commands

Enabling DHCP Option 82

Command	ip dhcp relay information option82
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration
Example

Enabling DHCP Option 82

Configuration Steps	Enable DHCP Option 82.
	QTECH (config)# ip dhcp relay information option82
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	QTECH #show ru	incl ip dhcp relay ip dhcp relay information option82

Common
Errors

4. Configuring DHCP

▪ Basic DHCP Relay functions are not configured.

4.4.7 Configuring DHCP Relay Check Server-ID

Configuration Effect

▪ After you configure the **ip dhcp relay check server-id**, a DHCP Relay agent will forward DHCP request packets only to the server specified by the **option server-id** command. Otherwise, they are forwarded to all DHCP servers.

Notes

▪ You need to enable basic DHCP Relay functions.

Configuration Steps

Enabling DHCP Relay Check Server-ID

▪ By default, DHCP Relay check server-id is disabled.
▪ You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

Verification

Check whether a DHCP Relay agent sends DHCP request packets only to the server specified by the **option server-id** command.

Related Commands

Configuring DHCP Relay Check Server-ID

Command	ip dhcp relay check server-id
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

4. Configuring DHCP

Configuring DHCP Relay Check Server-ID

Configuration Steps	▪ **Enable DHCP Relay.Omitted.** ▪ **Enable DHCP Relay check server-id on an interface.**
	QTECH # configure terminal QTECH (config)# ip dhcp relay check server-id
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	QTECH # show running-config | include check server-id ip dhcp relay check server-id QTECH #

Common

Errors

▪ Basic DHCP Relay functions are not configured.

4.4.8 Configuring DHCP Relay Suppression

Configuration

Effect

▪ After you configure the **ip DHCP Relay suppression** command on an interface, DHCP request packets received on the interface will be filtered, and the other DHCP requests will be forwarded.

Notes

▪ You need to enable basic DHCP Relay functions.

Configuration

Steps

Enabling DHCP Relay Suppression

By default, DHCP Relay suppression is disabled on all interfaces.

4. Configuring DHCP

You may run the **ip dhcp relay suppression** command to enable DHCP Relay suppression.

Verification

▪ Check whether the DHCP request packets received on the interface are filtered.

Related Commands

Configuring DHCP Relay Suppression

Command	ip dhcp relay suppression
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring DHCP Relay Suppression

Configuration Steps	Configure basic DHCP Relay functions. Configure DHCP Relay suppression on an interface.
	QTECH # configure terminal QTECH (config)# interface gigabitEthernet 0/1 QTECH (config-if-GigabitEthernet 0/1)# ip dhcp relay suppression QTECH (config-if-GigabitEthernet 0/1)#end QTECH #
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.

QTECH МИР ДОСТУПНЕЕ | www.qtech.ru

4. Configuring DHCP

	QTECH # show running-config | include relay suppression ip dhcp relay suppression QTECH #

Common Errors

Basic DHCP Relay functions are not configured.

4.4.9 Configuring Multiple Gateway IP Addresses on DHCP Relay

Configuration Effect

Enable the function of multiple gateway IP addresses by running the ip dhcp relay multiple-giaddr command.

Notes

Basic DHCP Relay functions should be configured.

Configuration Steps

By default, this function is disabled.

Run the **ip dhcp relay multiple-giaddr** command to enable this function.

Verification

When more than one IP address is configured on a specified interface, check whether the DHCP request packet forwarded to the DHCP server contains different IP addresses.

Related Commands

Configuring Multiple Gateway IP Addresses

Command	ip dhcp relay multiple-giaddr
Parameter Description	N/A

4. Configuring DHCP

Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Multiple Gateway IP Addresses

Configuration Steps	▪ **1: Configure basic DHCP Relay functions.** ▪ **2: Configure the function of multiple gateway IP addresses.**
	QTECH # configure terminal QTECH (config)# ip dhcp relay multiple-giaddr
Verification	▪ 1: Log in the DHCP Relay Agent; and then in Privileged EXEC mode, run the **show running-config** command to display the DHCP Relay configuration.
	QTECH # show running-config ip dhcp relay multiple-giaddr

Common Errors

Basic DHCP Relay functions are not configured.

4.4.10 Configuring DHCP Client

Configuration Effect

Enable DHCP Client on a device so that it obtains IP addresses and configurations dynamically.

Notes

QTECH products support DHCP Client configuration on Ethernet, FR, PPP and HDLC interfaces.

Configuration Steps

4. Configuring DHCP

Run the **ip address dhcp** command on an interface.

Verification

Check whether the interface obtains an IP address.

Related
Commands

Configuring DHCP Client

Command	ip address dhcp
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	▪ QTECH products support dynamic IP address obtainment by an Ethernet interface. ▪ QTECH products support dynamic IP address obtainment by a PPP-encapsulated interface. ▪ QTECH products support dynamic IP address obtainment by an FR-encapsulated interface. ▪ QTECH products support dynamic IP address obtainment by an HDLC-encapsulated interface.

Configuration
Example

Configuring DHCP Client

Configuration Steps	▪ **1: Enable port FastEthernet 0/0 with DHCP to obtain an IP address.**
	QTECH (config)# interface FastEthernet0/0 QTECH (config-if-FastEthernet 0/0)#ip address dhcp

4. Configuring DHCP

Verification	▪ 1: Run the **show run** command to display the configuration.
	QTECH (config)#show run	begin ip address dhcp ip address dhcp

4.4.11 Configuring the Source IP Address of DHCP Relay Packets

Configuration Effect

Run the **ip dhcp relay source** command on an interface to configure the source IP address of DHCP Relay packets.

Notes

- ▪ Basic DHCP Relay functions should be enabled.
- ▪ Only one source IP address of DHCP Relay packets can be configured on one interface.
- ▪ To assign correct subnet addresses to users, this function should be used with Option 82.

Configuration Steps

Configuring the Source IP Address of DHCP Relay Packets

- ▪ By default, no source IP address of DHCP Relay packets is configured.
- ▪ Run the **ip dhcp relay source** *ip-address* command on an interface to configure the source IP address of DHCP Relay packets.

Verification

After this function is enabled, the source IP address of Relay packets sent to the DHCP server is the configured address.

Related Commands

Configuring the Source IP Address of DHCP Relay Packets

Command	ip dhcp relay source *ip-address*
Parameter Description	*ip-address*: Specifies the source IP address of DHCP Relay packets.

4. Configuring DHCP

Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Source IP Address of DHCP Relay Packets

Configuration Steps	**1: Enable basic DHCP Relay functions.** **2: Configure the source IP address of DHCP Relay packets.**
	QTECH (config-if)# ip dhcp relay source 1.1.1.1
Verification	1: Login the DHCP Relay Agent. 2: Enter the Privileged EXEC mode. 3: Run the show running-config command to display DHCP Relay configurations.

Common Errors

Basic DHCP Relay functions are not configured.

4.4.12 Enabling DHCP Relay to Discard DHCP Request Packets from VxLAN Tunnels

Configuration Effect

Run the **ip dhcp relay discard overlay-tunnel** command in global configuration mode to enable DHCP replay to discard DHCP request packets from VxLAN tunnels.

Notes

- Basic DHCP Relay functions should be enabled.

Configuration Steps

4. Configuring DHCP

Enabling DHCP Relay to Discard DHCP Request Packets from VxLAN Tunnels

▪ By default, DHCP Relay is allowed to receive DHCP request packets from VxLAN tunnels.

▪ Run the command to stop DHCP Relay from receiving DHCP request packets from VxLAN tunnels.

Verification

After the command in run, DHCP request packets from VxLAN tunnels are not further forwarded to DHCP servers.

Related Commands

Enabling DHCP Relay to Discard DHCP Request Packets from VxLAN Tunnels

Command	ip dhcp relay discard overlay-tunnel
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling DHCP Relay to Discard DHCP Request Packets from VxLAN Tunnels

Configuration Steps	1: Enable basic DHCP Relay functions. 2: Enables DHCP Relay to discard DHCP request packets from VxLAN tunnels in global configuration mode.
	QTECH (config)# ip dhcp relay discard overlay-tunnel
Verification	1: Login the DHCP Relay Agent. 2: Enter the Privileged EXEC mode. 3: Run the **show running-config** command to display DHCP Relay configurations.

4. Configuring DHCP

Common Errors

Basic DHCP Relay functions are not configured.

4.4.13 Configuring DHCP Client

Configuration Effect

Enable DHCP Client on a device so that it obtains IP addresses and configurations dynamically.

Notes

QTECH products support DHCP Client configuration on Ethernet, FR, PPP and HDLC interfaces.

Configuration Steps

Run the **ip address dhcp** command on an interface.

Verification

Check whether the interface obtains an IP address.

Related Commands

Configuring DHCP Client

Command	ip address dhcp
Parameter Description	N/A
Command Mode	Interface configuration mode

4. Configuring DHCP

Usage Guide	▪ QTECH products support dynamic IP address obtainment by an Ethernet interface. ▪ QTECH products support dynamic IP address obtainment by a PPP-encapsulated interface. ▪ QTECH products support dynamic IP address obtainment by an FR-encapsulated interface. ▪ QTECH products support dynamic IP address obtainment by an HDLC-encapsulated interface.

Configuration Example

Configuring DHCP Client

Configuration Steps	1: Enable port FastEthernet 0/0 with DHCP to obtain an IP address.
	QTECH (config)# interface FastEthernet0/0 QTECH (config-if-FastEthernet 0/0)#ip address dhcp
Verification	1: Run the show run command to display the configuration.
	QTECH (config)#show run | begin ip address dhcp ip address dhcp

4.5 Monitoring

Clearing

⚠ Running the clear commands may lose vital information and interrupt services.

Description	Command
Clears DHCP address binding.	clear ip dhcp binding { *address* | *}
Clears DHCP address conflict.	clear ip dhcp conflict { *address* | *}

4. Configuring DHCP

Clears statistics of a DHCP server.	clear ip dhcp server statistics
Clears statistics of a DHCP relay.	clear ip dhcp relay statistics
Clears statistics of DHCP server performance.	clear ip dhcp server rate

Displaying

Description	Command
Displays DHCP lease.	**show dhcp lease**
Displays DHCP sockets.	**show ip dhcp socket**
Displays assigned IP addresses.	**show ip dhcp binding**
Displays created address pools.	**show ip dhcp pool**
Displays statistics of DHCP Server.	**show ip dhcp server statistic**
Displays statistics of DHCP Relay.	**show ip dhcp relay statistic**
Displays conflicted addresses.	**show ip dhcp conflict**
Displays DHCP lease history.	**show ip dhcp history**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

4. Configuring DHCP

Description	Command
Debugs DHCP agent.	**debug ip dhcp server agent**
Debugs DHCP hot backup.	**debug ip dhcp server ha**
Debugs DHCP address pools.	**debug ip dhcp server pool**
Debugs DHCP VRRP.	**debug ip dhcp server vrrp**
Debugs all DHCP servers.	**debug ip dhcp server all**
Debugs DHCP packets.	**debug ip dhcp client**
Debugs DHCP Relay events.	**debug ip dhcp relay**

5 CONFIGURING DHCPV6

5.1 Overview

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a protocol that allows a DHCP server to transfer configurations (such as IPv6 addresses) to IPv6 nodes.

As compared with other IPv6 address allocation methods, such as manual configuration and stateless automatic address configuration, DHCPv6 provides the address allocation, prefix delegation, and configuration parameter allocation.

- DHCPv6 is a stateful protocol for automatically configuring addresses and flexibly adding and reusing network addresses, which can record allocated addresses and enhance network manageability.
- By using the prefix delegation of DHCPv6, uplink network devices can allocate address prefixes to downlink network devices, which implements flexible station-level automatic configuration and flexible control of station address space.
- The DHCPv6 configuration parameter allocation solves the problem that parameters cannot be obtained through a stateless automatic address configuration protocol and allocates DNS server addresses and domain names to hosts.

DHCPv6 is a protocol based on the client/server model. A DHCPv6 client is used to obtain various configurations whereas a DHCPv6 server is used to provide various configurations. If the DHCPv6 client and DHCPv6 server are not on the same network link, they can interact with each other by using a DHCPv6 relay agent.

The DHCPv6 client usually discovers the DHCPv6 server by reserving multicast addresses within a link; therefore, the DHCPv6 client and DHCPv6 server must be able to directly communicate with each other, that is, they must be deployed within the same link. This may cause management inconvenience, economic waste (a DHCPv6 server is deployed for each subnet) and upgrade inconvenience. The DHCPv6 relay agent function can solve these problems by enabling a DHCPv6 client to send packets to a DHCPv6 server on a different link. The DHCP relay agent is often deployed within the link where a DHCPv6 client resides and is used to relay interaction packets between the DHCPv6 client and DHCPv6 server. The DHCP relay agent is transparent to the DHCPv6 client.

Figure 5-1
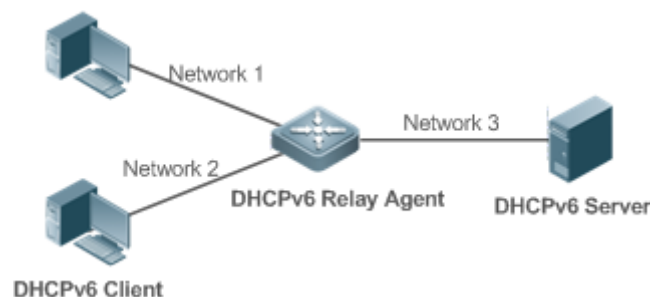
Protocols and

Standards

- RFC3315: Dynamic Host Configuration Protocol for IPv6
- RFC3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6
- RFC3646: DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC3736: Stateless DHCP Service for IPv6
- RFC5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

5.2 Applications

Application	Description
Requesting/Allocating Addresses and Configuration Parameters	A DHCPv6 client requests addresses from a DHCPv6 server. The DHCPv6 server allocates addresses and configuration parameters to the DHCPv6 client.
Requesting/Allocating Prefixes	The DHCPv6 client requests a prefix from the DHCPv6 server. The DHCPv6 server allocates a prefix to the DHCPv6 client and then the DHCPv6 client configures IPv6 addresses by using this prefix.
Relay Service	The DHCPv6 relay is used to enable communication between the DHCPv6 client and DHCPv6 server on different links.

5.2.1 Requesting/Allocating Addresses and Configuration Parameters

Scenario

In a subnet, a DHCPv6 client requests addresses from a DHCPv6 server. The DHCPv6 server allocates addresses and configuration parameters to the DHCPv6 client.

As shown in Figure 5-2:

- The DHCPv6 server is configured with IPv6 addresses, DNS servers, domain names and other configuration parameters to be allocated.
- A host works as a DHCPv6 client to request an IPv6 address from the DHCPv6 server. After receiving the request, the DHCPv6 server selects an available address and allocates the address to the host.
- The host can also request a DNS server, domain name and other configuration parameters from the DHCPv6 server.

Figure 5-2
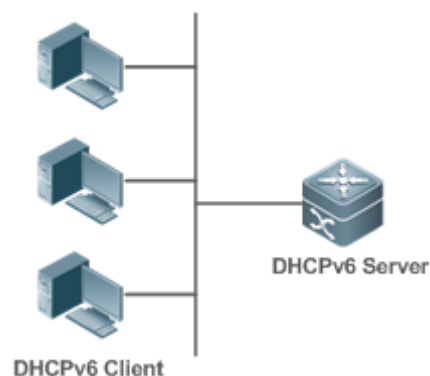
DHCPv6 Client

Deployment

- Run the DHCPv6 client on a host in the subnet to obtain an IPv6 address and other parameters.
- Run the DHCPv6 server on a device and configure the IPv6 address and other parameters to allocate the IPv6 address and parameters.

5.2.2 Requesting/Allocating Prefixes

Scenario

As shown in Figure 5-3, an uplink device (PE) allocates an IPv6 address prefix for a downlink device (CPE). The CPE generates a new address prefix for the internal subnet based on the obtained prefix. Hosts in the internal subnet of the CPE are configured with addresses through Router Advertisement (RA) by using the new address prefix.

- The PE provides the prefix delegation service as a DHCPv6 server.
- The CPE requests an address prefix from the PE as a DHCPv6 client. After obtaining the address prefix, the CPE generates a new address prefix for the internal subnet and sends an RA message to hosts in the internal subnet.
- The hosts in the internal subnet where CPE resides configure their addresses based on the RA message sent by the CPE.

Figure 5-3
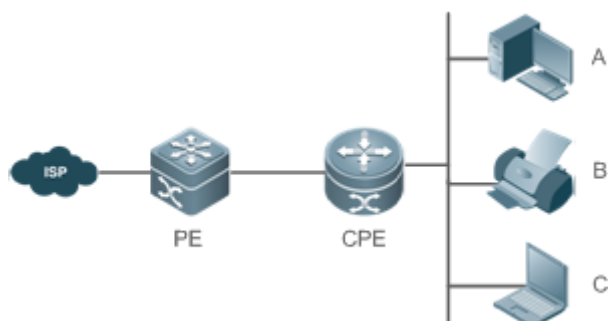
Remarks	The Provider Edge (PE) works as a DHCPv6 server for providing prefixes and is also called a delegating router.

> **The Customer Premises Equipment (CPE) works as a DHCPv6 client for requesting prefixes and is also called a requesting router.**
>
> **A, B and C are various hosts.**

Deployment

- Run the DHCPv6 server on the PE to implement the prefix delegation service.
- Run the DHCPv6 client on the CPE to obtain address prefixes.
- Deploy IPv6 ND between the CPE and the hosts to configure the host addresses in the subnet through RA.

5.2.3 Relay Service

Scenario

The DHCPv6 relay agent provides the relay service for the DHCPv6 client ad DHCPv6 server on different links to enable communication between them.

As shown in Figure 5-4:

- Device 1 is enabled with the DHCPv6 relay agent and destined to 3001::2.
- Device 2 wants to forward packets to other servers through a next-level relay service. Enable the DHCPv6 relay agent on Device 2, set the destination address to FF02::1:2 (all servers and Relay multicast addresses) and specify the egress interface as the layer-3 interface gi 0/1.

Figure 5-4

①L3 gateway device, enabled with
   DHCPv6 Relay Agent

②L2 access device, enabled with LDRA

③L3 gateway device, enabled with
   DHCPv6 Relay Agent
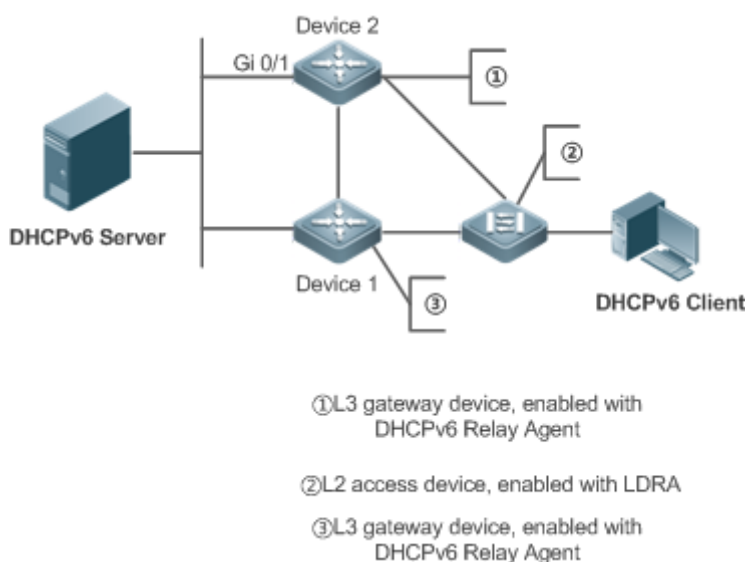
Deployment

- Enable the DHCPv6 relay agent on device 1 and specify the address as 3000::1.

- Enable the DHCPv6 relay agent on device 2 and specify the address as FF02::1:2.

5.3   Features

Basic
Concept

DUID

The DHCP Unique Identifier (DUID) identifies a DHCPv6 device. As defined in RFC3315, each DHCPv6 device (DHCPv6 client, relay or server) must have a DUID, which is used for mutual authentication during DHCPv6 message exchange.

RFC3315 defines three types of DUIDs:

- DUID Based on Link-Layer address plus Time (DUID-LLT).
- DUID Assigned by Vendor Based on Enterprise Number (DUID-EN).
- Link-Layer address (DUID-LL).

QTECH DHCPv6 devices use DUID-LLs. The structure of a DUID-LL is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              3                |      hardware type (16 bits)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.              link-layer address (variable length)            .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
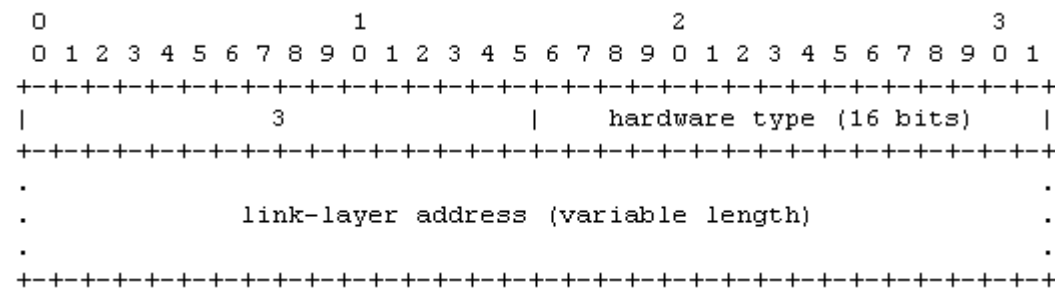
The values of *DUID-LL*, *Hardware type*, and *Link-layer address* are 0x0003, 0x0001 (indicating the Ethernet), and MAC address of a device respectively.

Identity Association (IA)

A DHCPv6 server allocates IAs to DHCPv6 clients. Each IA is uniquely identified by an identity association identifier (IAID). IAIDs are generated by DHCPv6 clients. A one-to-one mapping is established between IAs and clients. An IA may contain several addresses, which can be allocated by the client to other interfaces. An IA may contain one of the following types of addresses:

- Non-temporary Addresses (NAs), namely, globally unique addresses.
- Temporary Addresses (TAs), which are hardly used.
- Prefix Delegation (PD).

Based on the address type, IAs are classified into IA_NA, IA_TA, and IA_PD (three IA-Types). QTECH DHCPv6 servers support only IA_NA and IA_PD.

Binding

A DHCPv6 binding is a manageable address information structure. The address binding data on a DHCPv6 server records the IA and other configurations of every client. A client can request multiple bindings. The address binding data on a server is present in the form of an address

binding table with DUID, IA-Type and IAID as the indexes. A binding containing configurations uses DUID as the index.

DHCPv6 Conflict

When an address allocated by a DHCPv6 client is in conflict, the client sends a Decline packet to notify the DHCPv6 server that the address is rebound. Then, the server adds the address to the address conflict queue. The server will not allocate the addresses in the address conflict queue. The server supports viewing and clearing of address information in the address conflict queue.

Packet Type

RFC3315 stipulates that DHCPv6 uses UDP ports 546 and 547 for packet exchange. Specifically, a DHCPv6 client uses port 546 for receiving packets, while a DHCPv6 server and DHCPv6 relay agent use port 547 for receiving packets. RFC3315 defines the following types of packets that can be exchanged among the DHCPv6 server, client, and relay agent:

- Packets that may be sent by a DHCPv6 client to a DHCPv6 server include Solicit, Request, Confirm, Renew, Rebind, Release, Decline, and Information-request.
- Packets that may be sent by a DHCPv6 server to a DHCPv6 client include Advertise, Reply, and Reconfigure.
- Packets that may be sent by a DHCPv6 relay agent to another DHCPv6 relay agent or a DHCPv6 server include Relay-forward.
- Packets that may be sent by a DHCPv6 relay agent to another DHCPv6 relay agent or a DHCPv6 server include Relay-reply.

✅ QTECH DHCPv6 servers do not support the Reconfigure packet.

✅ QTECH DHCPv6 clients do not support the Confirm and Reconfigure packets.

Overview

Feature	Description
Requesting/Allocating Addresses	Dynamically obtains/allocates IPv6 addresses in a network in the client/server mode.
Requesting/Allocating Prefixes	Dynamically obtains/allocates IPv6 prefixes in a network in the client/server mode.
Stateless Service	Provides stateless configuration service for hosts in a network.
Relay Service	Provides the DHCPv6 server service for hosts in different networks by using the relay service.

5.3.1 Requesting/Allocating Addresses

A DHCPv6 client can request IPv6 addresses from a DHCPv6 server.

After being configured with available addresses, a DHCPv6 server can provide IPv6 addresses to hosts in the network, record the allocated addresses and improve the network manageability.

**Working
Principle**

Network hosts serve as DHCPv6 clients and DHCPv6 servers to implement address allocation, update, confirmation, release and other operations through message exchange.

Four-Message Exchange

Figure 1-3 shows the four-message exchange process.

Figure 5-5
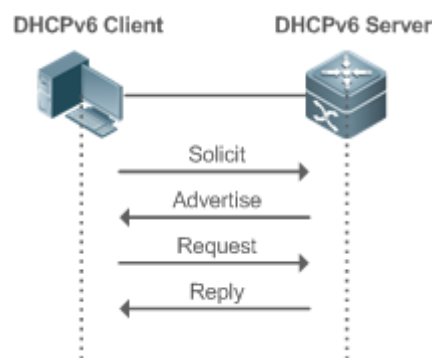
- A DHCPv6 client sends a Solicit message whose destination address is FF02::1:2 and destination port number is 547 within the local link to request address, prefix and configuration parameter allocation. All DHCPv6 servers or DHCPv6 relay agents within the link will receive the Solicit message.
- After receiving the Solicit message, a DHCPv6 server will send an Advertise message in the unicast mode if it can provide the information requested in the Solicit message. The Advertise message includes the address, prefix and configuration parameters.
- The DHCPv6 client may receive the Advertise message from multiple DHCPv6 servers. After selecting the most suitable DHCPv6 server, the DHCPv6 client sends a Request message whose destination address is FF02::1:2 and destination port number is 547 to request address, prefix and configuration parameter allocation.
- After receiving the Request message, the DHCPv6 server creates a binding locally and sends a Reply message in the unicast mode. The Reply message includes the address, prefix and configuration parameters that the DHCPv6 server will allocate to the DHCPv6 client. The DHCPv6 client obtains address, prefix or configuration parameters based on the information in the Reply message.

Two-Message Exchange

Two-message exchange can be used to complete address, prefix and parameter configuration for DHCPv6 clients more quickly.

Figure 5-6
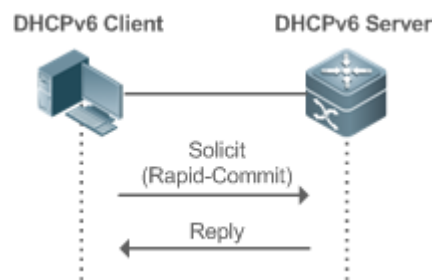
- A DHCPv6 client sends a Solicit message whose destination address is FF02::1:2 and destination port number is 547 within the local link to request address, prefix and configuration parameter allocation. The Solicit message contains Rapid Commit.

- If a DHCPv6 server supports the Rapid Commit option, the DHCPv6 server creates a binding locally and sends a Reply message in the unicast mode. The Reply message includes the address, prefix and configuration parameters to be allocated to the DHCPv6 client. The DHCPv6 client completes configuration based on the information in the Reply message.

Update and Rebinding

The DHCPv6 server provides the control address and the updated T1 and T2 in the IA of the message sent to the DHCPv6 client.

Figure 5-7
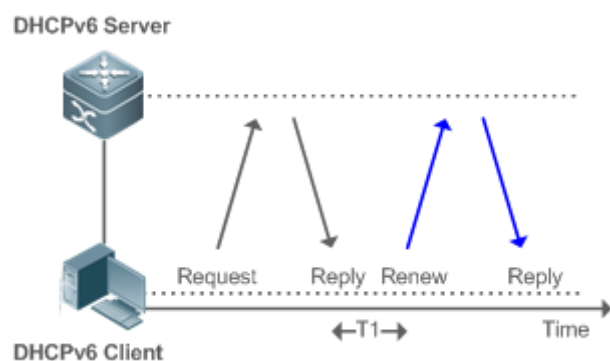
- The DHCPv6 client will send a Renew multicast message to the DHCPv6 server for updating the address and prefix after T1 seconds. The Renew message contains the DUID of the DHCPv6 server and the IA information to be updated.
- After receiving the Renew message, the DHCPv6 server checks whether the DUID value in the Renew message is equal to the DUID value of the local device. If yes, the DHCPv6 server updates the local binding and sends a Reply message in the unicast mode. The Reply message contains the new T1 and other parameter s.

Figure 5-8
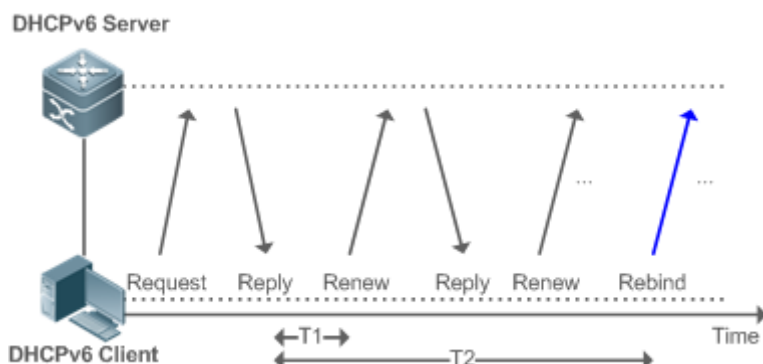
- If no response is received after the DHCPv6 client sends a Renew message to the DHCPv6 server, the DHCPv6 client will send a Rebind multicast message to the DHCPv6 server for rebinding the address and prefix after T2 expires.
- After receiving the Rebind message, the DHCPv6 server (perhaps a new DHCPv6 server) sends a Reply message according to the content of the Rebind message.

Release

If a DHCPv6 client needs to release an address or a prefix, the DHCPv6 client needs to send a Release message to a DHCPv6 server to notify the DHCPv6 server of the released addresses or prefixes. In this way, the DHCPv6 server can allocate these addresses and prefixes to other DHCPv6 clients.

Figure 5-9
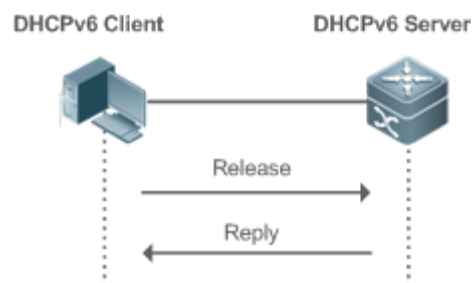
- After receiving the Release message, the DHCPv6 server removes the corresponding bindings based on the addresses or prefixes in the Release message, and sends a Reply message carrying the state option to the DHCPv6 client.

Confirmation

After moving to a new link (for example, after restart), a DHCPv6 client will send a Confirm message to the DHCPv6 server on the new link to check whether the original addresses are still available.

Figure 5-10
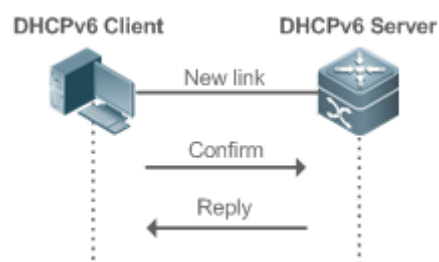
- After receiving the Confirm message, the DHCPv6 server performs confirmation based on the address information in the Confirm message, and sends a Reply message carrying the state option to the DHCPv6 client. If the confirmation fails, the DHCPv6 client may initiate a new address allocation request.

DHCPv6 Conflict

If the DHCPv6 client finds that the allocated addresses have been used on the link after address allocation is completed, the DHCPv6 client sends a Decline message to notify the DHCPv6 server of the address conflict.

Figure 5-11
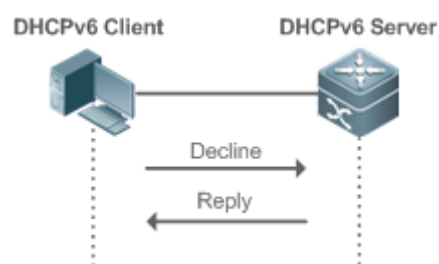
- The DHCPv6 client includes the IA information of the conflicted addresses in the Decline message.
- After receiving the Decline message, the DHCPv6 server marks the addresses in the Decline message as "declined" and will not allocate these addresses . Then, the DHCPv6 server sends a Reply message carrying the state option to the DHCPv6 client. You can manually clear addresses marked as "declined" to facilitate re-allocation.

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

- By default, an interface is not enabled with the DHCPv6 server function.
- You can run the **ipv6 dhcp server** command to enable the DHCPv6 server function for the interface.

⚠️ The DHCPv6 server function must be enabled on a layer-3 interface.

Allocating Addresses Through the DHCPv6 Server

- By default, the DHCPv6 server has no configuration pool and is not configured with addresses to be allocated.
- You can run the **ipv6 dhcp pool** command to create a configuration pool.

- You can run the **iana-address** command to configure addresses to be allocated and the **preferred lifetime** and **valid lifetime** values.

Clearing Conflicted Addresses Through the DHCPv6 Server

- By default, the DHCPv6 server does not clear conflicted addresses that are detected.
- You can run the **clear ipv6 dhcp conflict** command to clear conflicted addresses so that these addresses can be reused.

5.3.2 Requesting/Allocating Prefixes

Configure available prefixes on the DHCPv6 server. By using the prefix delegation of DHCPv6, uplink network devices can allocate address prefixes to downlink network devices, which implements flexible station-level automatic configuration and flexible control of station address space.

Working Principle

Downlink network devices serve as DHCPv6 clients to exchange messages with the DHCPv6 server to implement address allocation, update, release and other operations. Downlink network devices obtain, update, rebind and release prefixes by using the four-/two-message exchange mechanism similar to that for allocating addresses. However, prefix allocation is different from address allocation in the following aspects:

- In message exchange using the prefix delegation, the Confirm and Decline messages are not used.
- If a DHCPv6 client moves to a new link and needs to check whether the prefix information is available, it performs confirmation through Rebind and Reply message exchange.
- The IA type in various messages is IA_PD.

> ℹ️ For the message exchange using the prefix delegation, refer to the section "Requesting/Allocating Addresses".

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

- By default, an interface is not enabled with the DHCPv6 server function.
- You can run the **ipv6 dhcp server** command to enable the DHCPv6 server function for the interface.

> ⚠️ The DHCPv6 server function is effective only on a layer-3 interface.

Prefix Delegation of the DHCPv6 Server

- By default, the DHCPv6 server has no configuration pool and is not configured with prefixes.
- You can run the **ipv6 dhcp pool** command to create a configuration pool.

▪ You can run the **prefix-delegation** command to allocate specified prefixes to a specific DHCPv6 client.
▪ You can run the **prefix-delegation pool** command to configure a prefix pool so that all prefixes requested by the DHCPv6 client are allocated from this pool.

5.3.3   Stateless Service

When a DHCPv6 client needs only configuration parameters, the DHCPv6 stateless service can be used to obtain related configuration parameters which cannot be obtained through a stateless automatic address configuration protocol, such as the DNS server address.

Working Principle

Network hosts serve as DHCPv6 clients to exchange messages with the DHCPv6 server to obtain and update configuration parameters.

Message Exchange Using the Stateless Service

Figure 5-12
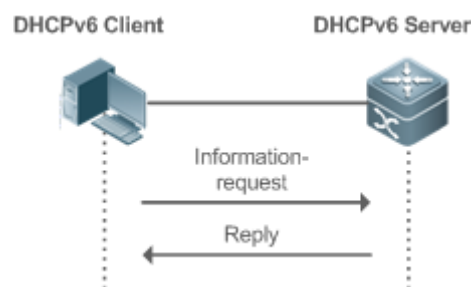
▪ A DHCPv6 client sends an Information-request message to a DHCPv6 server to request stateless messages. Usually, this message does not contain the DUID of the specified DHCPv6 server.
▪ The DHCPv6 server sends a Reply message containing the configuration parameters to the DHCPv6 client.

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

▪ By default, an interface is not enabled with the DHCPv6 server function.
▪ You can run the **ipv6 dhcp server** command to enable or disable the DHCPv6 server function for the interface.

⚠ The DHCPv6 server function is effective only on a layer-3 interface.

Stateless Service of a DHCPv6 Server

▪ By default, the DHCPv6 server has no configuration pool and is not configured with configuration parameters.
▪ You can run the **ipv6 dhcp pool** command to create a configuration pool.

- You can run the **dns-server** command to add a DNS server.
- You can run the **domain-name** command to add a domain name.
- You can run the **option52** command to add the IPv6 address of the CAPWAP AC.

5.3.4 Relay Service

When the DHCPv6 client and DHCPv6 server are on different links, the DHCPv6 client can relay related messages to the DHCPv6 server through the DHCPv6 relay agent. The DHCPv6 server also relays the response to the DHCPv6 client through the relay agent.

**Working
Principle**

When receiving a message from the DHCPv6 client, the DHCPv6 relay agent creates a Relay-forward message. This message contains the original message from the DHCPv6 client and some options added by the relay agent. Then, the relay agent sends the Relay-forward message to a specified DHCPv6 server or a specified multicast address FF05::1:3.

After receiving the Relay-forward message, the DHCPv6 server extracts the original message from the DHCPv6 client f for processing. Then, the DHCPv6 server constructs a response to the original message, encapsulates the response in a Relay-reply message, and then sends the Relay-reply message to the DHCPv6 relay agent.

After receiving the Relay-reply message, the DHCPv6 relay agent extracts the original message from the DHCPv6 server for processing, and forwards the message to the DHCPv6 client.

Multi-level relay agents are allowed between the DHCPv6 client and DHCPv6 server.

DHCPv6 Relay Agent

Figure 5-13
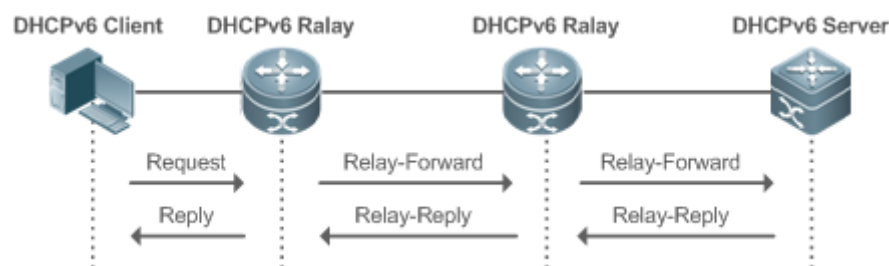
- The DHCPv6 relay agent performs message encapsulation and decapsulation between the DHCPv6 client and DHCPv6 server to enable communication between the DHCPv6 client and DHCPv6 server on different links.

5.4 Configuration

Configuration	Description and Command
Configuring the	⚠ (Mandatory) It is used to create a configuration pool.

DHCPv6 Server	**ipv6 dhcp pool**	Configures a configuration pool for a DHCPv6 server.
	⚠ (Optional) It is used to allocate addresses.	
	iana-address prefix	Configures the address prefixes to be allocated on the DHCPv6 server.
	⚠ (Optional) It is used to allocate prefixes.	
	prefix-delegation	Configures prefixes of statically bound addresses on the DHCPv6 server.
	prefix-delegation pool	Configures the DHCPv6 server to allocate prefixes from a local prefix pool.
	ipv6 local pool	Configures a local IPv6 prefix pool.
	⚠ (Optional) It is used to allocate configuration parameters.	
	dns-server	Configures the DNS server on the DHCPv6 server.
	domain-name	Configures the domain name of the DHCPv6 server.
	option52	Configures the IPv6 address of the CAPWAP AC on the DHCPv6 server.
	⚠ (Mandatory) It is used to enable the DHCPv6 server service.	
	ipv6 dhcp server	Enables the DHCPv6 server service on an interface.
Configuring the DHCPv6 Relay	⚠ (Mandatory) It is used to enable the DHCPv6 relay agent service.	
	ipv6 dhcp relay destination	Configures the DHCPv6 relay agent function.

5.4.1   Configuring the DHCPv6 Server

**Configur
ation
Effect**

- An uplink device can automatically allocate DHCPv6 addresses, prefixes and configuration parameters to a downlink device.

Notes

- To provide the DHCPv6 server service, you must specify a DHCPv6 server configuration pool.
- The name of the configuration pool cannot be too long.
- When enabling the DHCPv6 server service, you must specify a configuration pool.
- Only the Switch Virtual Interface (SVI), routed port and L3 aggregate port (AP) support this configuration.

**Configur
ation
Steps**

Configuring a DHCPv6 Server Configuration Pool

- Mandatory.
- Unless otherwise specified, you should configure a DHCPv6 server configuration pool on all devices that need to provide the DHCPv6 server service.

Configuring the Address Prefixes to Be Allocated on the DHCPv6 Server

- Optional.
- To provide the address allocation service, you should configure address prefixes to be allocated on all devices that need to provide the DHCPv6 server service.

Configuring Prefixes of Static Addresses on the DHCPv6 Server

- Optional.
- To provide the prefix delegation service for statically bound addresses, you should configure prefixes of statically bound addresses on all devices that need to provide the DHCPv6 server service.

Configuring the DHCPv6 Server to Allocate Prefixes from a Local Prefix Pool

- Optional.
- To provide the prefix delegation service, you should specify a local prefix pool on all devices that need to provide the DHCPv6 server service.

Configuring a Local IPv6 Prefix Pool

- Optional.
- To provide the prefix delegation service through a prefix pool, you should specify a local prefix pool on all devices that need to provide the DHCPv6 server service.

Configuring the DNS Server on the DHCPv6 Server

- ▪ Optional.
- ▪ To allocate DNS servers, you should configure the DNS server on all devices that need to provide the DHCPv6 server service.

Configuring Domain Names on the DHCPv6 Server

- ▪ Optional.
- ▪ To allocate domain names, you should configure domain names on all devices that need to provide the DHCPv6 server service.

Configuring the IPv6 Address of the CAPWAP AC on the DHCPv6 Server

- ▪ Optional.
- ▪ To allocate CAPWAP AC information, you should configure the IPv6 address of the CAPWAP AC on all devices that need to provide the DHCPv6 server service.

Enabling the DHCPv6 Server Service

- ▪ Mandatory.
- ▪ Unless otherwise specified, you should enable the DHCPv6 server service on specific interfaces of all devices that need to provide the DHCPv6 server service.

Verification

The DHCPv6 server allocates addresses, prefixes or configuration parameters for the DHCPv6 client.

- ▪ The DHCPv6 client obtains the required information.
- ▪ The DHCPv6 server successfully creates a local binding.

Related Commands

Configuring a DHCPv6 Server Configuration Pool

Command	ipv6 dhcp pool *poolname*
Parameter Description	*poolname*: Indicates the name of a user-defined DHCPv6 configuration pool.
Command Mode	Global configuration mode
Usage Guide	Run the **ipv6 dhcp pool** command to create a DHCPv6 server configuration pool. After configuring this command, you may enter the DHCPv6 pool configuration mode, in which you can configure the pool parameters such as the prefix and DNS server. After creating a DHCPv6 server configuration pool, you can run the **ipv6 dhcp**

	server command to associate the configuration pool with the DHCPv6 server service on an interface.

Configuring the IA_NA Address Prefix for the DHCPv6 Server

Command	**iana-address prefix** *ipv6-prefix/prefix-length* **[lifetime {** *valid-lifetime* **|** *preferred-lifetime* **}]**
Parameter Description	*ipv6-prefix/prefix-length*: Indicates an IPv6 address prefix and the prefix length. **lifetime**: Sets the valid time of the address allocated to a client. This keyword must be configured together with *valid-lifetime* and *preferred-lifetime*. *valid-lifetime***:** Indicates the valid time of the address allocated to a client. *preferred-lifetime*: Indicates the time when an address is preferentially allocated to a client.
Command Mode	Interface configuration mode
Usage Guide	Run the **iana-address prefix** command to configure IA_NA address prefixes for a DHCPv6 server, some of which are allocated to the client. When receiving an IA_NA address request from a client, the DHCPv6 server selects an available address according to the IA_NA address range and allocates the address to the client. When the client does not use this address, the DHCPv6 server marks this address as available for another client.

Configuring Prefixes of Statically Bound Addresses on the DHCPv6 Server

Command	**prefix-delegation** *ipv6-prefix/prefix-length client-DUID* **[** *lifetime* **]**
Parameter Description	*ipv6-prefix/prefix-length*: Indicates an IPv6 address prefix and the prefix length. *client-DUID*: Indicates the DUID of a client. *lifetime*: Sets the time when the client can use this prefix.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **prefix-delegation** command to manually configure a prefix list for an IA_PD of a client and specify the valid time of these prefixes. Use the *client-DUID* parameter to specify the client to which the address prefix is allocated. The address prefix will be allocated to the first IA_PD of the client.

QTECH МИР ДОСТУПНЕЕ | www.qtech.ru

| | After receiving a request for the address prefix from the client, the DHCPv6 server checks whether a static binding is available. If yes, the DHCPv6 server directly returns the static binding. If not, the DHCPv6 server allocates the address prefix from another prefix source. |

Configuring the DCHPv6 Server to Allocate Prefixes from a local prefix pool

Command	prefix-delegation pool *poolname* [lifetime { *valid-lifetime* | *preferred-lifetime* }]
Parameter Description	*poolname***:** Indicates the name of a user-defined local prefix pool. **lifetime:** Sets the valid time of the prefix allocated to a client. This keyword must be configured together with *valid-lifetime* and *preferred-lifetime*. *valid-lifetime*: Indicates the valid time of the prefix allocated to the client. *preferred-lifetime*: Indicates the time when a prefix is preferentially allocated to a client.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	Run the **prefix-delegation pool** command to configure a prefix pool for a DHCPv6 server to allocate prefixes to clients. The **ipv6 local pool** command is used to configure a prefix pool. When receiving a prefix request from a client, the DHCPv6 server selects an available prefix from the prefix pool and allocates the prefix to the client. When the client does not use this prefix, the DHCPv6 server retrieves the prefix .

Configuring a Local IPv6 Prefix Pool

Command	ipv6 local pool *poolname prefix/prefix-length assigned-length*
Parameter Description	*poolname*: Indicates the name of a local prefix pool. *prefix/prefix-length***:** Indicates the prefix and prefix length. *assigned-length***:** Indicates the length of the prefix allocated to a user.
Command Mode	Global configuration mode
Usage Guide	Run the **ipv6 local pool** command to create a local prefix pool. If the DHCPv6 server needs prefix delegation, you can run the **prefix-delegation pool** command to specify a local prefix pool. Afterwards, prefixes will be allocated from the

	specified local prefix pool.

Configuring the DNS Server on the DHCPv6 Server

Command	dns-server *ipv6-address*
Parameter Description	*ipv6-address*: Indicates the IPv6 address of the DNS server.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **dns-server** command for multiple times to configure multiple DNS server addresses. A new DNS server address will not overwrite old DNS server addresses.

Configuring Domain Names on the DHCPv6 Server

Command	domain-name *domain*
Parameter Description	*domain*: Defines a domain name to be allocated to a user.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **domain-name** command for multiple times to create multiple domain names. A new domain name will not overwrite old domain names.

Configuring the option52 on the DHCPv6 Server

Command	option52 *ipv6-address*
Parameter Description	*ipv6-address*: Specifies the IPv6 address of the CAPWAP AC.
Command Mode	DHCPv6 pool configuration mode

Usage Guide	You can run the **option52** command to configure IPv6 addresses for the multiple CAPWAP ACs. A new CAPWAP AC IPv6 address will not overwrite old IPv6 addresses.

Enabling the DHCPv6 Server Service

Command	ipv6 dhcp server *poolname* [rapid-commit] [preference *value*]
Parameter Description	*poolname*: Indicates the name of a user-defined DHCPv6 configuration pool. **rapid-commit:** Permits the two-message exchange process. **preference** *value***:** Configures the priority of the advertise message, ranging from 0 to 255. The default value is 0.
Command Mode	Interface configuration mode
Usage Guide	Run the **ipv6 dhcp server** command to enable the DHCPv6 service on an interface. When the **rapid-commit** keyword is configured, the two-message exchange with a client is permitted during allocation of address prefixes and other configurations. After this keyword is configured, if the Solicit message from a client contains the **rapid-commit** option, the DHCPv6 server will send a Reply message directly. If **preference** is set to a non-0 value, the advertise message sent by the DHCPv6 server contains the **preference** option. The **preference** field affects the server selection by a client. If an advertise message does not contain this field, the value of **preference** is considered **0**. If the value of **preference** received by the client is 255, the client sends a request to the server immediately to obtain configurations. The DHCPv6 client, server, and relay functions are mutually exclusive. An interface can be configured with only one function at a time.

Configuration Example

Configuring the DHCPv6 Server

Configurati	▪ **Configure a configuration pool named "pool1".** ▪ **Configure the IA_NA address prefix for the DHCPv6 server.**

on Steps	▪ **Configure prefixes of statically bound addresses on the DHCPv6 server.** ▪ **Configure two DNS servers.** ▪ **Configure the domain name.** ▪ **Enable the DHCPv6 server service on an interface.**
	QTECH # configure terminal QTECH (config)# ipv6 dhcp pool pool1 QTECH (config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000 1000 QTECH (config-dhcp)# prefix-delegation 2008:2::/64 0003000100d0f82233ac QTECH (config-dhcp)# dns-server 2008:1::1 QTECH (config-dhcp)# dns-server 2008:1::2 QTECH (config-dhcp)# domain-name example.com QTECH (config-dhcp)#exit QTECH (config)# interface GigabitEthernet 0/1 QTECH (config-if)# ipv6 dhcp server pool1
Verificatio n	▪ Run the **show ipv6 dhcp pool** command to display the created configuration pool.

	QTECH # show ipv6 dhcp pool
	
	DHCPv6 pool: pool1
	
	 Static bindings:
	
	  Binding for client 0003000100d0f82233ac
	
	   IA PD prefix: 2008:2::/64
	
	    preferred lifetime 3600, valid lifetime 3600
	
	IANA address range: 2008:50::1/64 -> 2008:50::ffff:ffff:ffff:ffff/64
	
	    preferred lifetime 1000, valid lifetime 2000
	
	DNS server: 2008:1::1
	
	DNS server: 2008:1::2
	
	Domain name: example.com

Commo n Errors

▪ The specified pool name is too long.
▪ The number of the configuration pools exceeds the system limit (256).

- The configuration is performed on other interfaces than the Switch Virtual Interface (SVI), routed port and L3 AP port.
- The number of interfaces configured with the DHCPv6 server service exceeds the system limit (256).
- The specified value of **valid lifetime** is larger than that of **preferred lifetime**.
- An invalid IA_NA address is specified.
- The number of address ranges exceeds the system limit (20).
- When prefixes of statically bound addresses are configured, the specified DUIDs are too long.
- The number of prefixes of statically bound addresses exceeds the system limit (1024).
- When a local prefix pool is configured, the specified value of **valid lifetime** is smaller than that of **preferred lifetime**.
- The number of DNS servers exceeds the system limit (10).
- The number of domain names exceeds the system limit (10).
- The number of option52 addresses exceeds the system limit (10).

5.4.2 Configuring the DHCPv6 Relay

Configuration Effect

- A DHCPv6 relay agent can be configured for address allocation, prefix delegation and parameter allocation to enable communication between the DHCPv6 client and server on different links.

Notes

- A destination address must be specified. If the destination address is a multicast address (such as FF05::1:3), you also need to specify an egress interface.

Configuration Steps

Configuring the DHCPv6 Relay Agent Function

- Mandatory.
- Unless otherwise specified, you should configure the DHCPv6 relay agent function on all devices that need to provide the DHCPv6 relay agent service.

Verification

The DHCPv6 client and DHCPv6 server exchange messages through the relay agent.

- Check whether the interface is enabled with the DHCPv6 relay.
- Check whether the DHCPv6 relay agent can receive and send messages.

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

Related Commands

Configuring the DHCPv6 Relay Agent Function

Command	ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*]
Parameter Description	*ipv6-address*: Specifies the destination address of the relay agent. *interface-type*: Specifies the type of the destination interface (optional). *interface-number*: Specifies the destination interface number (optional).
Command Mode	Interface configuration mode
Usage Guide	All DHCPv6 packets from clients received by an interface enabled with the DHCPv6 relay function will be encapsulated and sent to a specified destination address (or multiple destination addresses) through a specified interface (optional).

Configuration Example

Configuring the DHCPv6 Relay

Configuration Steps	Specify an interface enabled with the relay service to forward received DHCPv6 client packets to a specified destination address through the specified interface (optional).
	QTECH #configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH (config)#interface vlan 1 QTECH (config-if)#ipv6 dhcp relay destination 3001::2 QTECH (config-if)#ipv6 dhcp relay destination ff02::1:2 vlan 2
Verification	Run the **show ipv6 dhcp relay destination all** command to display the configured destination addresses.
	Interface:VLAN 1 Destination address(es) Output Interface

3001::2	
ff02::1:2	VLAN 2

Common Errors

- The configuration is performed on other interfaces than the Switch Virtual Interface (SVI), routed port and L3 AP port.

5.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears DHCPv6 bindings.	**clear ipv6 dhcp binding** [*ipv6-address*]
Clears DHCPv6 server statistics.	**clear ipv6 dhcp server statistics**
Clears conflicted addresses on the DHCPv6 server.	**clear ipv6 dhcp conflict** { *ipv6-address*	* }
Clears the statistics on sent and received packets after the DHCPv6 relay is enabled on the current device.	**clear ipv6 dhcp relay statistics**

Displaying

Description	Command
Displays the DUID of a device.	**show ipv6 dhcp**
Displays address bindings on the DHCPv6 server.	**show ipv6 dhcp binding** [*ipv6-address*]
Displays DHCPv6 interface.	**show ipv6 dhcp interface** [*interface-name*]

Displays DHCPv6 pool.	**show ipv6 dhcp pool** [*poolname*]
Displays conflicted DHCPv6 addresses.	**show ipv6 dhcp conflict**
Displays the statistics on the DHCPv6 server.	**show ipv6 dhcp server statistics**
Displays the destination address of the DHCPv6 relay agent.	**show ipv6 dhcp relay destination** { **all** | *interface-type interface-number* }
Displays the statistics on sent and received packets after the DHCPv6 relay is enabled on a device.	**show ipv6 dhcp relay statistics**
Displays the local IPv6 prefix pool.	**show ipv6 local pool** [*poolname*]

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs DHCPv6.	**debug ipv6 dhcp [detail]**

6   CONFIGURING DNS

6.1   Overview

A Domain Name System (DNS) is a distributed database containing mappings between domain names and IP addresses on the Internet, which facilitate users to access the Internet without remembering IP strings that can be directly accessed by computers. The process of obtaining an IP address through the corresponding host name is called domain name resolution (or host name resolution).

Protocols and Standards

- RFC1034: DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

6.2   Applications

Application	Description
Static Domain Name Resolution	Performs domain name resolution directly based on the mapping between a domain name and an IP address on a device.
Dynamic Domain Name Resolution	Obtains the IP address mapped to a domain name dynamically from a DNS server on the network.

6.2.1   Static Domain Name Resolution

Scenario

- Preset the mapping between a domain name and an IP address on a device.
- When you perform domain name operations (such as Ping and Telnet) through application programs, the system can resolve the IP address without being connected to a server on the network.

Deployment

- Preset the mapping between a domain name and an IP address on a device.

6.2.2   Dynamic Domain Name Resolution

Scenario

- DNS Server is deployed on the network to provide the domain name service.
- Domain name "host.com" is deployed on the network.
- Device-A applies to DNS Server for domain name "host.com".

Figure 6-1 Dynamic Domain Name Resolution
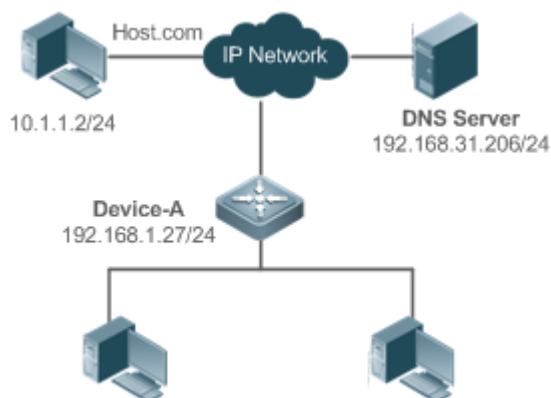
Deployment

- Deploy DNS Server as the DNS server of Device-A.

6.3 Features

Basic Concepts

DNS

The DNS consists of a resolver and a DNS server. The DNS server stores the mappings between domain names and IP addresses of all hosts on the network, and implements mutual conversion between the domain names and IP addresses. Both the TCP and UDP port IDs of DNS are 53, and generally a UDP port is used.

Features

Feature	Description
Domain Name Resolution	IP addresses are obtained based on domain names from a DNS server or a local database.

6.3.1 Domain Name Resolution

Working Principle

Static Domain Name Resolution

Static domain name resolution means that a user presets the mapping between a domain name and an IP address on a device. When you perform domain name operations (such as Ping and Telnet) through application programs, the system can resolve the IP address without being connected to a server on the network.

Dynamic Domain Name Resolution

Dynamic domain name resolution means that when a user perform domain name operations through application programs, the DNS resolver of the system queries an external DNS server for the IP address mapped to the domain name.

The procedure of dynamic domain name resolution is as follows:

1. A user application program (such as Ping or Telnet) requests the IP address mapped to a . domain name from the DNS resolver of the system.

2.The DNS resolver queries the dynamic cache at first. If the domain name on the dynamic cache does not expire, the DNS resolver returns the domain name to the application program.

3. If all domain names expire, the DNS resolver initiates a request for domain name-IP address conversion to the external DNS server.

4. After receiving a response from the DNS server, the DNS resolver caches and transfers the response to the application program.

Related Configuration

Enabling Domain Name Resolution

▪ By default, domain name resolution is enabled.
▪ Run the **ip domain-lookup** command to enable domain name resolution.

Configuring the IP Address Mapped to a Static Domain Name

▪ By default, no mapping between a domain name and an IP address is configured.
▪ Run the **ip host** command to specify the IPv4 address mapped to a domain name.

Configuring a DNS Server

▪ By default, no DNS server is configured.
▪ Run the **ip name-server** command to configure a DNS server.

6.4   Configuration

Configuration	Description and Command	
Configuring Static Domain Name Resolution	⚠ Optional.	
	ip domain-lookup [**oob** [**via** *mgmt-name*] | **vrf** *vrf-name*]	Enables domain name resolution.

	ip host [**oob** [**via** *mgmt-name***]** | **vrf** *vrf-name*]	Configures the IPv4 address mapped to a domain name.
[Configuring Dynamic Domain Name Resolution](#)	⚠ Optional.	
	ip domain-lookup [**oob** [**via** *mgmt-name***]** | **vrf** *vrf-name* **]**	Enables domain name resolution.
	ip name-server [**oob** [**via** *mgmt-name*] | **vrf** *vrf-name*]	Configures a DNS server.

6.4.1 Configuring Static Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name on a local device.

Configuration Steps

Enabling Domain Name Resolution

- The domain name resolution function is enabled by default.
- If this function is disabled, static domain name resolution does not take effect.

Configuring the IPv4 Address Mapped to a Domain Name

- (Mandatory) Domain names to be used must be configured with mapped IP addresses.

Verification

- Run the **show run** command to check the configuration.
- Run the **show hosts** [**oob** [**via** *mgmt-name*] \| **vrf** *vrf-name*] command to check the mapping between the domain name and the IP address.

Related Commands

Configuring the IPv4 Address Mapped to a Domain Name

Command	**ip host [oob | vrf** *vrf-name* **]** *host-name ip-address* **[via** *mgmt-name* **]**

| Parameter Description | vrf *vrf-name*: specifies the name of a VRF instance. If this parameter is not specified, it indicates the public network.
oob: enables the out-band channel. It must be set when MGMT is specified as the source port.
via: configures MGMT port.
mgmt-name: specifies the MGMT port in oob mode.
host-name: indicates a domain name.
ip-address: indicates a mapped IPv4 address. |
|---|---|
| Command Mode | Global configuration mode |
| Usage Guide | N/A |

Configuration Example

Configuring Static Domain Name Resolution

| Configuration Steps | ▪ **Set the IP address of static domain name www.test.com to 192.168.1.1 on the VRFM.**
▪ **Set the IP address of static domain name www.test.com to 192.168.1.1 on MGMT port.** |
|---|---|
| | QTECH #configure terminal
QTECH (config)# ip host vrf VRFM www.test.com 192.168.1.1
QTECH (config)# ip oob host www.test.com 192.168.1.1
QTECH (config)# exit |
| Verification | Run the **show hosts vrf VRFM** command to check whether the static domain name entry is configured.
Run the **show hosts oob** command to check whether the static domain name entry is configured.
Run the **show hosts** command to check whether the static domain name entry is configured. |
| | QTECH #show hosts vrf VRFM |

QTECH МИР ДОСТУПНЕЕ   www.qtech.ru

```
Name servers are:


Host            type   Address      TTL(sec)
www.test.com        static  192.168.1.1     ---


QTECH #show hosts oob
Name servers are:


Host            type   Address      TTL(sec)
www.test.com        static  192.168.1.1     ---

QTECH #show hosts
Name servers are:


Host            type   Address      TTL(sec)
www.test.com        static  192.168.1.1     ---
```

6.4.2   Configuring Dynamic Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name through a DNS server.

Configuration Steps

Enabling Domain Name Resolution

- Domain name resolution is enabled by default.
- If this function is disabled, dynamic domain name resolution does not take effect.

Configuring a DNS Server

- (Mandatory) To use dynamic domain name resolution, you must configure an external DNS server.

Verification

- Run the **show run** command to check the configuration.

Related Commands

Configuring a DNS Server

Command	ip name-server [oob	vrf *vrf-name*] { *ip-address* } [via *mgmt-name*]
Parameter Description	oob: indicates that the DNS server supports an out-of-band management interface (interface of mgmt). vrf *vrf-name*: specifies the name of a VRF instance. If this parameter is not specified, it indicates the public network. *ip-address*: indicates the IPv4 address of the DNS server. *via:* configures an egress management interface. *mgmt-name:* specifies the egress management interface for packets in oob mode.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Dynamic Domain Name Resolution

Scenario Figure 6-2	
	Device resolves the domain name through the DNS server (192.168.10.1) on the network.
Configuration Steps	Set the IP address of the DNS server to 192.168.10.1 on the device. Set the IP address of the DNS server to 192.168.10.1 on MGMT port. Set the IP address of the DNS server to 192.168.10.1 on the VRFM.

<table>
<tr><td></td><td>

```
DEVICE#configure terminal
DEVICE(config)# ip name-server oob 192.168.10.1
DEVICE(config)# ip name-server vrf VRFM 192.168.10.1
DEVICE(config)# ip name-server 192.168.10.1
DEVICE(config)# exit
```

</td></tr>
<tr><td>Verification</td><td>

Run the **show hosts** command to check whether the DNS server is specified.

Run the **show hosts oob** command to check whether the DNS server is specified.

Run the **show hosts vrf VRFM** command to check whether the DNS server is specified.

</td></tr>
<tr><td></td><td>

QTECH (config)#show hosts

Name servers are:

192.168.10.1 static

2001::1 static

Host   type   Address   TTL(sec)

QTECH (config)#show hosts oob

Name servers are:

192.168.10.1 static

2001::1 static

Host   type   Address   TTL(sec)

QTECH (config)#show hosts vrf VRFM

Name servers are:

192.168.10.1 static

2001::1 static

Host   type   Address   TTL(sec)

</td></tr>
</table>

6.4.3 Configuring the Source IP Address for DNS Query

**Configur
ation
Effect**

The prime IP address of the interface is configured as the source IP address of DNS query.

Configuring the Source IP Address for DNS Query

▪ (Optional) You can configure the source IP address of DNS query.
▪ By default, no source IP address is specified for DNS query.

▪ Run the **show run** command to check the configuration.

Configuring the Source IP Address for DNS Query

Command	ip domain-lookup [oob [via *mgmt-name*]	vrf *vrf-name*] [source { *interface*	ip *ip-address* }]
Parameter Description	**oob**: indicates that the DNS server supports an out-of-band management interface (interface of mgmt). *via:* configures an egress management interface. *mgmt-name:* specifies the egress management interface for packets in oob mode. **vrf** *vrf-name*: specifies the name of a VRF instance. If this parameter is not specified, it indicates the public network. *interface*: indicates a Layer 3 interface. *ip-address*: indicates the IPv4 address of the DNS server.
Command Mode	Global configuration mode
Usage Guide	By default, no source IP address of DNS query is configured, so the source IP address of DNS query is decided through the routing process. If the *interface* parameter is specified, when IPv4 DNS query is sent, its source address is the prime IPv4 address of the source interface.

QTECH МИР ДОСТУПНЕЕ   www.qtech.ru

Configuration Example

Configuring the Source IP Address for DNS Query

Scenario Figure 6-3	
	The source address configured on the device is10.1.1.1.
Configuration Steps	Set 10.1.1.1 as the source IP address for DNS query on the device. Set 10.1.1.1 as the source IP address for DNS query on MGMT port. Set 10.1.1.1 as the source IP address for DNS query on the VRFM.
	DEVICE#configure terminal DEVICE(config)# ip domain-lookup source ip 10.1.1.1 DEVICE(config)# exit DEVICE#configure terminal DEVICE(config)# ip domain-lookup oob source ip 10.1.1.1 DEVICE(config)# exit DEVICE#configure terminal DEVICE(config)# ip domain-lookup vrf VRFM source ip 10.1.1.1 DEVICE(config)# exit
Verification	Run the **show run** command to check whether the source IP address is specified.
	QTECH (config)#show run | include domain-lookup ip domain-lookup source ip 10.1.1.1 ip domain-lookup oob source ip 10.1.1.1 ip domain-lookup vrf VRFM source ip 10.1.1.1

6.5 Monitoring

Clearing

⚠ Running the **clear** command during device operation may cause data loss or even interrupt services.

Description	Command
Clears the dynamic host name cache table.	clear host [*host-name*]

Displaying

Description	Command
Displays DNS parameters.	show hosts [oob [via *mgmt-name*] | vrf *vrf-name*] [*host-name*]

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the DNS function.	debug ip dns

7   CONFIGURING FTP SERVER

7.1   Overview

The File Transfer Protocol (FTP) server function enables a device to serve as an FTP server. In this way, a user can connect an FTP client to the FTP server and upload files to and download files from the FTP server through FTP.

A user can use the FTP server function to easily obtain files such as syslog files from a device and copy files to the file system of the device through FTP.

Protocols and Standards

- RFC959: FILE TRANSFER PROTOCOL (FTP)
- RFC3659: Extensions to FTP
- RFC2228: FTP Security Extensions
- RFC2428: FTP Extensions for IPv6 and NATs
- RFC1635: How to Use Anonymous FTP

7.2   Applications

Application	Description
Providing FTP Services in a LAN	Provides the uploading and downloading services for a user in a Local Area Network (LAN).

7.2.1   Providing FTP Services in a LAN

Scenario

Provide the uploading and downloading services for a user in a LAN.

As shown in Figure 7-1, enable the FTP server function only in a LAN.

- G and S are enabled with the FTP server function and layer-2 transparent transmission function respectively.
- A user initiates a request for FTP uploading and downloading services.

Figure 7-1

Remarks	G is an egress gateway device. S is an access device.

**Deploym
ent**

- G is enabled with the FTP server function.
- As a layer-2 switch, S provides the function of layer-2 transparent transmission.

7.3 Features

**Basic
Concept
s**

FTP

FTP is a standard protocol defined by the IETF Network Working Group. It implements file transfer based on the Transmission Control Protocol (TCP). FTP enables a user to transfer files between two networked computers and is the most important approach to transferring files on the Internet. A user can obtain abundant Internet for free through anonymous FTP. In addition, FTP provides functions such as login, directory query, file operation, and other session control. Among the TCP/IP protocol family, FTP is an application-layer protocol and uses TCP ports 20 and 21 for transmission. Port 20 is used to transmit data and port 21 is used to transmit control messages. Basic operations of FTP are described in RFC959.

User Authorization

To connect an FTP client to an FTP server, you should have an account authorized by the FTP server. That is, a user can enjoy services provided by the FTP server after logging in to the FTP server with a user name and password. A maximum of 10 accounts can be configured, a maximum of 2 connections are allowed for each account, and a maximum of 10 connections are supported by the server.

FTP File Transmission Modes

FTP provides two file transmission modes:

- Text transmission mode (ASCII mode): It is used to transfer text files (such as .txt, .bat, and .cfg files). This mode is different from the binary mode in carriage return and line feed processing. In ASCII mode, carriage return and line feed are changed to local CRC characters, for example, \n in Unix, \r\n in Windows, and \r in Mac. Assume that a file being copied contains ASCII text. If a remote computer does not run Unix, FTP automatically converts the file format to suit the remote computer.
- Binary transmission mode: It is used to transfer program files (for example, .app, .bin and .btm files), including executable files, compressed files and image files without processing data. Therefore, Binary mode facilitates faster transfer of all files and more reliable transfer of ASCII files.

FTP Working Modes

FTP provides two working modes:

Figure 7-2
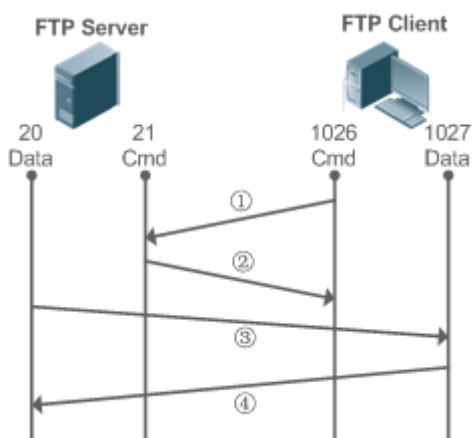
Figure 7-3
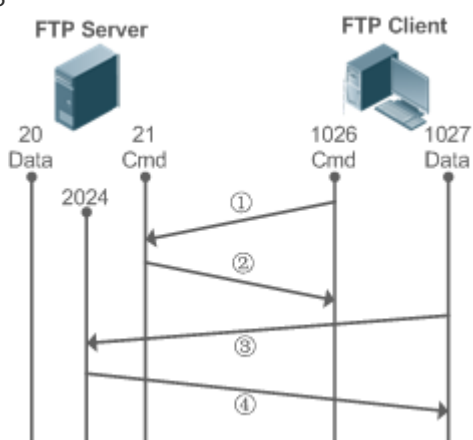
- Figure 7-2 shows the active (PORT) mode. The FTP client uses port 1026 to connect to the FTP server through port 21. The client sends commands through this channel. Before receiving data, the client sends the **PORT** command on this channel. The **PORT** command contains information on the channel port (1027) of the client for receiving data. The server uses port 20 to connect to the client through port 1027 for establishing a data channel to receive and transmit data. The FTP server must establish a new connection with the client for data transmission.

- Figure 7-3 shows the passive (PASV) mode. The process for establishing a control channel is similar to that in the PORT mode. However, after the connection is established, the client sends the **PASV** command rather than the **PORT** command. After receiving the **PASV** command, the FTP server enables a high-end port (2024) at random and notifies the client that data will be transmitted on this port. The client uses port 1027 to connect the FTP server through port 2024. Then, the client and server can transmit and receive data on this channel. In this case, the FTP server does not need to establish a new connection with the client.

Supported FTP Commands

After receiving an FTP connection request, the FTP server requires the client to provide the user name and password for authentication.

If the client passes the authentication, the FTP client commands can be executed for operations. The available FTP client commands are listed as follows:

ascii	delete	mdelete	mput	quit	send
bin	dir	mdir	nlist	recv	size
bye		mget		rename	system
cd	get	mkdir	passive		type
cdup		mls	put	rmdir	user
close	ls		pwd		

For usage of these FTP client commands, please refer to your FTP client software document. In addition, many FTP client tools (such as CuteFTP and FlashFXP) provide the graphic user interface. These tools facilitate operations by freeing users from configuring FTP commands.

Overview

Feature	Description
Enabling the FTP Server Function	Provides the functions of uploading, downloading, displaying, creating and deleting files for an FTP client.

7.3.1 Enabling the FTP Server Function

Working Principle

The basic working principle is described in the previous chapter. QTECH devices provide FTP services after the user name, password, and top-level directory are configured.

Related Configuration

Enabling the FTP Server Function Globally

The FTP server function is disabled by default.

Run the **ftp-server enable** command to enable the FTP server function.

You must enable the FTP server function globally before using it.

Configuring a User Name, Password, and Top-Level Directory

There is no authorized user or top-level directory by default.

Run the **ftp-server username** and **ftp-server topdir** commands to set an authorized user and top-level directory.

The three configurations above are mandatory; otherwise, the FTP server function cannot be enabled.

7.4   Configuration

Configuration	Description and Command	
Configuring Basic Functions	⚠ (Mandatory) It is used to enable an FTP server.	
	ftp-server enable	Enables the FTP server function.
	ftp-server login timeout	Configures Login timeout for an FTP session.
	ftp-server login times	Configures the valid login count.
	ftp-server topdir	Configures the top-level directory of the FTP server.
	ftp-server username *username*	Configures a user name.
	ftp-server password [*type*] *password*	Configures a password.
	ftp-server timeout	Configures the idle timeout of an FTP session.

7.4.1   Configuring Basic Functions

Configuration Effect

- Create an FTP server to provide FTP services for an FTP client.

Notes

- The user name, password, and top-level directory need to be configured.
- To enable the server to close an abnormal session within a limited period, you need to configure the idle timeout of a session.

Configuration Steps

Enabling the FTP Server Function

- Mandatory.
- Unless otherwise noted, enable the FTP server function on every router.

Configuring a Top-Level Directory

- Mandatory.
- Unless otherwise noted, configure the top-level directory as the root directory on every router.

Configuring a User Name and Password for Login

- Mandatory.
- The lengths of the user name and password are restricted.

Configuring the Login Timeout for an FTP Session

- Optional.
- When the client is disconnected from the server due to an error or other abnormal causes, the FTP server may not know that the user is disconnected and continues to keep the connection. Consequently, the FTP connection is occupied for a long time and the server cannot respond to the login requests of other users. This configuration can ensure that other users can connect to the FTP server within a period of time upon an error.

Verification

Connect an FTP client to the FTP server.

- Check whether the client is connected.
- Check whether operations on the client are normal.

Related Commands

Enabling the FTP Server Function

Command	ftp-server enable
Parameter Description	-
Command Mode	Global configuration mode

| Usage Guide | The client cannot access the FTP server unless the top-level directory, user name and password are configured. Therefore, it is recommended that you configure the top-level directory, user name and password for login by referring to the subsequent chapters before enabling the service for the first time. |

Configuring the Valid Login Count

Command	ftp-server login times*times*
Parameter Description	*times:* Indicates the valid login count, ranging from 1 to 10.
Command Mode	Global configuration mode
Usage Guide	The valid login count refers to the number of times you can perform account verification during an FTP session. The default value is 3, which means that your session will be terminated if you enter an incorrect user name or password for three times and other users can go online.

Configuring the Login Timeout for an FTP Session

Command	ftp-server login timeout*timeout*
Parameter Description	*timeout*: Indicates the login timeout, ranging from 1 to 30 minutes.
Command Mode	Global configuration mode
Usage Guide	The login timeout refers to the maximum duration that the session lasts since being established. If you do not pass the password verification again during the login timeout, the session will be terminated to ensure that other users can log in.

Configuring the Top-Level Directory of the FTP Server

Command	**ftp-servertopdir*directory***
Parameter Description	*directory:* Indicates the user access path.

Command Mode	Global configuration mode
Usage Guide	If the top-level directory of the server is set to "/syslog", the FTP client can access only the files and directories in the "/syslog" directory on the device after login. Due to restriction on the top-level directory, the client cannot return to the upper directory of "/syslog".

Configuring a User Name and Password for Server Login

Command	ftp-server username *username* password [*type*] *password*
Parameter Description	*username*: Indicates a user name. *type*: 0 or 7. 0 indicates that the password is not encrypted (plaintext) and 7 indicates that the password is encrypted (cipher text). **password**: Indicates a password.
Command Mode	Global configuration mode
Usage Guide	The FTP server does not support anonymous login; therefore, a user name must be configured. A user name consists of up to 64 characters including letters, half-width digits and symbols without spaces. A password consists of only letters or digits. Spaces at the beginning and end of the password are ignored. Spaces inside the password are viewed as part of the password. A plaintext password consists of 1 to 25 characters. A cipher text password consists of 4 to 52 characters. User names and passwords must match. A maximum of 10 users can be configured.

Configuring the Idle Timeout for an FTP Session

Command	ftp-server timeout *time*
Parameter Description	*time*: Indicates the idle timeout, ranging from 1 to 3,600 minutes.

Command Mode	Global configuration mode
Usage Guide	The idle timeout of a session refers to the duration from the end of an FTP operation to the start of the next FTP operation in an FTP session. After the server responds to an FTP client command operation (for example, after a file is completely transferred), the server starts to count the idle time again, and stops when the next FTP client command operation arrives. Therefore, the configuration of the idle timeout has no effect on some time-consuming file transfer operations.

Displaying Server Status

Command	show ftp-server
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display FTP server status.

Debugging

Command	debug ftp-server pro/err
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to debug message/error events of the FTP server.

Configuration Example

Creating an FTP Server on an IPv4 Network

Configuration Steps	**A TCP connection is established for transmission from a server to a client.** **Configure the top-level directory/syslog.** **Set the user name user and password to password.** **Set the session idle timeout to 5 minutes.**
	QTECH (config)#ftp-server username user QTECH (config)#ftp-server password password QTECH (config)#ftp-server timeout 5 QTECH (config)#ftp-server topdir / QTECH (config)#ftp-server enable
Verification	Run the show ftp-server command to check whether the configuration takes effect.

	QTECH #show ftp-server
	
	  ftp-server information
	
	=================================
	
	enable : Y
	
	topdir : tmp:/
	
	timeout: 10min
	
	username:aaaa password:(PLAINT)bbbb connect num[2]
	
	  [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21]
	
	               client IP:192.168.21.26[3927]
	
	  [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21]
	
	               client IP:192.168.21.26[3929]
	
	username:a1 password:(PLAINT)bbbb connect num[0]
	
	username:a2 password:(PLAINT)bbbb connect num[0]
	
	username:a3 password:(PLAINT)bbbb connect num[0]
	
	username:a4 password:(PLAINT)bbbb connect num[0]
	
	username:a5 password:(PLAINT)bbbb connect num[0]
	
	username:a6 password:(PLAINT)bbbb connect num[0]
	
	username:a7 password:(PLAINT)bbbb connect num[0]
	
	username:a8 password:(PLAINT)bbbb connect num[0]
	
	username:a9 password:(PLAINT)bbbb connect num[0]

Commo n Errors

- No user name is configured.
- No password is configured.
- No top-level directory is configured.

7.5 Monitoring

Displayi ng

Description	Command
Displays the FTP server configuration.	show ftp-server

Debuggi ng

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the FTP server error events.	**debug ftp-server err**
Debugs the FTP server message events.	**debug ftp-server pro**

8 CONFIGURING FTP CLIENT

8.1 Overview

The File Transfer Protocol (FTP) is an application of TCP/IP. By establishing a connection-oriented and reliable TCP connection between the FTP client and server, a user can access a remote computer that runs the FTP server program.

An FTP client enables file transfer between a device and the FTP server over the FTP protocol. A user uses the client to send a command to the server. The server responds to the command and sends the execution result to the client. By means of command interaction, the user can view files in the server directory, copy files from a remote computer to a local computer, or transfer local files to a remote computer.

FTP is intended to facilitate sharing of program/data files and encourage remote operation (by using programs). Users do not need to be concerned with differences of different files systems on different hosts. Data is transmitted in an efficient and reliable manner. FTP enables remote file operation securely.

QTECH FTP clients are different from standard FTP clients that run interactive commands. Instead, you enter the **copy** command in CLI to perform control-connection instructions such as **open**, **user**, and **pass**. After a control connection is established, the file transfer process starts, and then a data connection is established to upload or download files.

> ⓘ Old devices support TFTP. However, TFTP is used to transfer small files whereas FTP is used to transfer large files. Implementing FTP on a device enables the file transfer between the local device and other clients or servers.

Protocols and Standards

- RFC959: FILE TRANSFER PROTOCOL (FTP)

8.2 Applications

Application	Description
Uploading a Local File to a Remote Server	Local and remote files need to be shared, for example, uploading a local file to a remote server.
Downloading a File from a Remote Server to a Local Device	Local and remote files need to be shared, for example, downloading a file from a remote server to a local device.

8.2.1 Uploading a Local File to a Remote Server

Scenario

Local and remote files need to be shared, for example, uploading a local file to a remote server.

As shown in Figure 8-1, resources are shared only on the Intranet.

Figure 8-1

Deployment

- Implement only communication on the Intranet.
- Enable file uploading on the FTP client.
- Enable file uploading on the FTP server.

8.2.2 Downloading a File from a Remote Server to a Local Device

Scenario

Local and remote files need to be shared, for example, downloading a file from a remote server to a local device.

As shown in Figure 8-2, resources are shared only on the Intranet.

Figure 8-2

Deployment

- Implement only communication on the Intranet.
- Enable file downloading on the FTP client.
- Enable file downloading on the FTP server.

8.3 Features

Basic Concepts

Uploading FTP Files

Upload files from an FTP client to an FTP server.

Downloading FTP Files

Download files from an FTP server to an FTP client.

FTP Connection Mode

An FTP client and an FTP server can be connected in the active or passive mode.

FTP Transmission Mode

The transmission between an FTP client and an FTP server is available in two modes, namely, text (ASCII) and binary (Binary).

Specifying the Source Interface IP Address for FTP Transmission

An FTP client is configured with a source IP address for communication with an FTP server.

Overview

Feature	Description
Uploading FTP Files	Uploads files from an FTP client to an FTP server.
Downloading FTP Files	Downloads files from an FTP server to an FTP client.
FTP Connection Mode	Specifies the connection mode between an FTP client and an FTP server.
FTP Transmission Mode	Specifies the transmission mode between an FTP client and an FTP server.
Specifying the Source Interface IP Address for FTP Transmission	Configures a source IP address of an FTP client for communication with an FTP server.

8.3.1 Uploading FTP Files

FTP enables file uploading. Start the FTP client and FTP server simultaneously, and upload files from the FTP client to the FTP server.

8.3.2 Downloading FTP Files

FTP enables file downloading. Start the FTP client and FTP server simultaneously, and download files from the FTP server to the FTP client.

8.3.3 FTP Connection Mode

FTP needs to use two TCP connections: one is a control link (command link) that is used to transfer commands between the FTP client and server; the other one is a data link that is used to upload or download data.

1. Control connection: Some simple sessions are enabled with the control connection only. A client sends a command to a server. After receiving the command, the server sends a response. The process is shown in Figure 8-3.

Figure 8-3 Control Connection
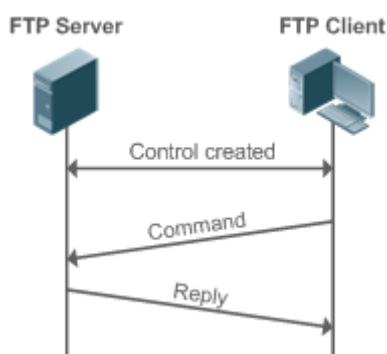
2. Control connection and data connection: When a client sends a command for uploading or downloading data, both the control connection and data connection need to be established.

FTP supports two data connection modes: active (PORT) and passive (PASC). The two modes are different in establishing a data connection.

▪ Active mode

In this mode, an FTP server connects to an FTP client actively when a data connection is established. This mode comprises four steps:

1. The client uses source port 5150 to communicate with the server through port 21 as shown in Figure 1-1 to send a connection request and tell the server that the port to be used is port 5151.
2. After receiving the request, the server sends a response OK(ACK). The client and server exchanges control signaling by console ports.
3. The server enables port 20 as the source port to send data to port 5151 of the client.
4. The client sends a response. Data transmission ends.

Figure 8-4 Active (PORT) Mode
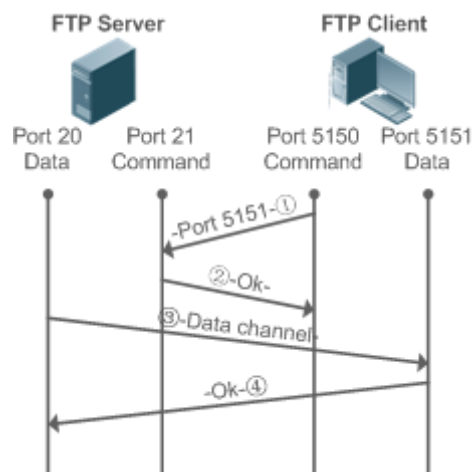
▪ Passive mode

Figure 8-5 Passive (PASV) Mode
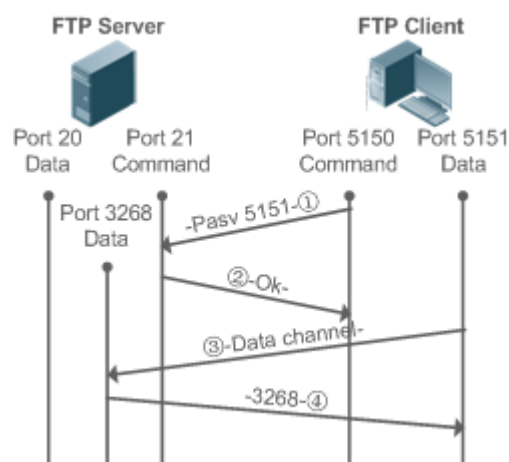
This mode is often set by the **passive** command. When a data connection is established, the FTP server is connected to the FPT client passively. This mode comprises four steps:

1. In the passive mode, the client initializes the control signaling connection. The client uses source port 5150 to connect to the server through port 21 as shown in Figure 1-5, and runs the **passive** command to request the server to enter the PASV mode.

2. The server agrees to enter the PASV mode, selects a port number greater than 1024 at random, and tells the port number to the client.

3. After receiving the message, the client uses port 5151 as shown in Figure 1-5 to communicate with the server through port 3268. Here, port 5151 is the source port and port 3268 is the destination port.

4. After receiving the message, the server sends data and responds an ACK(OK) response.

After the data connection is established, you can perform file uploading and downloading. Besides, you can perform some operations on the server file from the client.

> ⓘ The control connection for command and feedback transmission is always present whereas the data connection is established as required. Only an FTP client has the right to select and set the PASV or PORT mode. The FTP client sends a command to establish a data connection. QTECH FTP clients use the PASV mode by default.

8.3.4 FTP Transmission Mode

FTP provides two transmission modes: text (ASCII) and binary (Binary). At present, QTECH FTP clients support both the ASCII and Binary modes and use the BINARY mode by default.

- ASCII mode

The difference between the ASCII and Binary modes lies in carriage return and line feed processing. In ASCII mode, carriage return and line feed are changed to a local Carriage Return Character (CRC), for example, \n in Unix, \r\n in Windows, and \r in Mac.

- Binary mode

The Binary mode can be used to transfer executable files, compressed files and image files without processing data. For example, a text file needs to be transferred from Unix to Windows. When the Binary mode is used, the line breaks in Unix will not be converted from \r to \r\n; therefore in Windows, this file has no line feeds and displays many black squares. Therefore, Binary mode facilitates faster transfer of all files and more reliable transfer of ASCII files.

8.3.5 Specifying the Source Interface IP Address for FTP Transmission

An FTP client is configured with a source IP address for communication with an FTP server. In this way, the FTP client connects to the server and shares files with the server through the specified source IP address.

8.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	⚠ (Mandatory) It is used to configure the functions of an FTP client.	
	copy flash	Uploads a file.
	copy ftp	Downloads a file.
Configuring Optional Functions	⚠ (Optional) It is used to configure the working mode of the FTP client.	
	ftp-client port	Sets the connection mode to active (port).

	ftp-client ascii	Sets the transmission mode to ASCII.
	ftp-client source-address	Configures the source IP address of the FTP client.
	default ftp-client	Restores the default settings, namely, connection mode set to passive (PASV), transmission mode to Binary and source IP address removed.

8.4.1 Configuring Basic Functions

Configuration Effect

- Implement file uploading and downloading.

Notes

- Pay attention to the command formats for uploading and downloading.

Configuration Steps

Uploading a File

- This configuration is mandatory when a file needs to be uploaded.
- Configure the FTP URL as the destination address of **copy** in Privileged EXEC mode.

Downloading a File

- This configuration is mandatory when a file needs to be downloaded.
- Configure the FTP URL as the source address of **copy** in Privileged EXEC mode.

Verification

- Check whether the uploaded file exists on the FTP server.
- Check whether the downloaded file exists at the destination address.

Related Commands

Uploading a File

Command	copy flash:[local-directory/]local-file
	ftp: //username:password@dest-address[/remote-directory]/remote-file
Parameter Description	*local-directory:* Specifies a directory on the local device. If it is not specified, it indicates the current directory.
	local-file: Specifies a local file to be uploaded.
	username: Specifies a user name for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as /, :, @ and space. This parameter is mandatory.
	password: Specifies a password for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as /, :, @ and space. This parameter is mandatory.
	dest-address: Specifies an IP address for the FTP server.
	remote-directory: Specifies a directory on the server.
	remote-file: Renames the file on the server.
	⚠ The directory specified by the *local-directory* field must have been created on the device. This command will not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	Run this command to upload a file from the flash of a local device to an FTP server.

Downloading an FTP File

Command	copy ftp://username:password@dest-address[/remote-directory]/remote-file
	flash:[local-directory/]local-file
Parameter Description	*username*: Specifies a user name for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as /, :, @ and space. This parameter is mandatory.
	password: Specifies a password for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as /, :, @ and space. This parameter is mandatory.
	dest-address: Specifies an IP address for the FTP server.
	remote-directory: Specifies a directory on the server.

	remote-file: Specifies a file to be downloaded.
	local-directory: Specifies a directory on the local device. If it is not specified, it indicates the current directory.
	local-file: Renames the file in the local flash.
	⚠ The directory specified by the *local-directory* field must have been created on the device. This command will not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	Run this command to download a file from an FTP server to the flash of a local device.

Configuration Example

Uploading a File

Configuration Steps	**Upload the local-file file in the home directory of a device to the root directory of an FTP server whose user name is user, password is pass and IP address is 192.168.23.69 and name the file as remote-file.**
	QTECH # copy flash: home/local-file ftp://user:pass@192.168.23.69/root/remote-file
Verification	Check whether the remote-file file exists on the FTP server.

Downloading a File

Configuration Steps	**Download the remote-file file from the root directory of an FTP server whose user name is user, password is pass and IP address is 192.168.23.69 to the home directory of a device and save the file as local-file.**
	QTECH # copy ftp://user:pass@192.168.23.69/root/remote-file flash: home/local-file
Verificatio	Check whether the **remote-file** file exists in the **home** directory of the flash.

n	

Common Errors

- The command formats for uploading and downloading are incorrect.
- The user name or password is incorrect.

8.4.2 Configuring Optional Functions

Configuration Effect

- Set the connection and transmission modes and configure a source IP address of the client for file uploading and download.

Notes

- If an FTP client needs to be configured based on VRF, specify a VRF first.

Configuration Steps

Setting the Connection Mode to Active (Port)

- Optional.
- Configure the connection mode of FTP.

Setting the Transmission Mode to ASCII

- Optional.
- Configure the transmission mode of FTP.

Configuring the Source IP Address of the FTP Client

- Optional.
- Configure the source IP address of the FTP client.

Restoring the Default Settings

- Optional.
- Restore the default settings of the FTP client.

Verification

Run the **show run** command to check whether the configuration takes effect.

Related Commands

Setting the Connection Mode to Active (Port)

Command	ftp-client [vrf *vrf-name*] port
Parameter Description	vrf *vrf-name*: Specifies a VRF.
Command Mode	Global configuration mode
Usage Guide	Run this command to set the connection mode to active (port). The default connection mode is passive (PASV).

Configuring the Source IP Address of the FTP Client

Command	ftp-client [vrf *vrfname*] source-address {*ip-address* | *ipv6-address*}
Parameter Description	**vrf** *vrf-name*: Specifies a VRF. *ip-address:* Specifies the IPv4 address of a local interface. *ipv6-address:* Specifies the IPv6 address of a local interface.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an interface IP address of the client for connection to the server. By default, the client is not configured with a local IP address. Instead, the route selects an IP address for the client.

Setting the Transmission Mode to ASCII

Command	ftp-client [vrf *vrf-name*] ascii
Parameter Description	**vrf** *vrf-name*: Specifies a VRF.
Command Mode	Global configuration mode
Usage	Run this command to set the transmission mode to ASCII. The default

Guide	transmission mode is Binary.

Restoring the Default Settings

Command	default ftp-client [vrf *vrf-name*]
Parameter Description	**vrf** *vrf-name*: Specifies a VRF.
Command Mode	Global configuration mode
Usage Guide	Run this command to restore the default settings, namely, connection mode set to passive (PASV), transmission mode to Binary and source IP address removed.

Configuration Example

Configuring Optional Functions

Configuration Steps	- Set the connection mode of FTP to port. - Set the transmission mode to ASCII. - Set the source IP address to 192.168.23.167. - Set the connection mode of vrf 123 to port. - Set the transmission mode of vrf 123 to ASCII.
	QTECH # configure terminal QTECH (config)# ftp-client ascii QTECH (config)# ftp-client port QTECH (config)# ftp-client source-address 192.168.23.167 QTECH (config)# ftp-client vrf 123 port QTECH (config)# ftp-client vrf 123 ascii QTECH (config)# end
Verification	Run the **show run** command on the device to check whether the configuration takes effect. QTECH # show run

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

```
!
ftp-client ascii
ftp-client port
ftp-client source-address 192.168.23.167
!
```

Common Errors

- The source IP address is not a local IP address.
- Before configuring the **ftp-client vrf** command, configure the **vrf** command.

8.5 Monitoring

Displaying

Description	Command
Displays the FTP client configuration.	**show run**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the FTP Client.	**debug ftp-client**

9 CONFIGURING TUNNEL INTERFACES

9.1 Overview

Tunnel interfaces are virtual interfaces used to implement tunneling. A tunnel interface provides a standard transmission link and you do not need to specify a transport protocol or payload protocol. Each tunnel interface represents a transmission link.

Tunneling function includes the following parts:

- Payload protocol: Is used to encapsulate the data transmitted in tunnels. For example, the IPv4 and IPv6 protocols work as payload protocols. Generic routing encapsulation (GRE) tunnels can carry IPv4 or IPv6 data.
- Bearer protocol: Is used for secondary encapsulation and identification of the data to be transmitted. Among the tunnels described in this document, only the GRE tunnel uses a bearer protocol, that is, the GRE protocol. The other tunnels use the IPv4 and IPv6 protocols. Packets are encapsulated with outer IPv4 and IPv6 headers.
- Transport protocol: Is used to transmit the data encapsulated for the second time through a bearer protocol. QTECH products use the widely applied IPv4 and IPv6 protocols as transport protocols.

The tunnel mode can be used to set up communication between two private networks running the same protocol through a heterogeneous public network.

Tunneling is applicable to the following scenarios:

- Because tunneling supports different payload protocols, it allows the communication between local networks running non-IP protocols through a single network (IP network). Because tunneling operates on routes running transport protocols (IP protocols), it allows wider application of the protocols with hop limit.
- Tunneling allows discrete subnets to be connected through a single network (IP network).
- Tunneling allows the virtual private network (VPN) feature to be enabled on wide area networks (WANs).

Encapsulated data is transmitted through tunnels, which is a complex process. In some cases, you need to pay attention to the following changes:

- Because a tunnel is a logical link, it appears to be a single hop in routing. However, actually its path cost may be more than one hop. When you use a tunnel for transmission, note that the route of the tunnel link is different from the actual route.
- When you configure a firewall or an access control list (ACL), take the tunnel configuration into consideration. The transmission bandwidth and maximum transmission unit (MTU) allowed by payload protocols are smaller than the theoretical values.

Protocols and Standards

- RFC2784: Generic Routing Encapsulation (GRE)

- RFC2890: Key and Sequence Number Extensions to GRE
- RFC3056: Connection of IPv6 Domains via IPv4 Clouds
- RFC3068: An Anycast Prefix for 6to4 Relay Routers
- RFC3964: Security Considerations for 6to4
- RFC4023: Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
- RFC4087: IP Tunnel MIB
- RFC4213: Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC4797: Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks
- RFC5158: 6to4 Reverse DNS Delegation Specification
- RFC5214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- RFC5332: MPLS Multicast Encapsulations
- RFC5579: Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Interfaces
- RFC5845: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC6245: Generic Routing Encapsulation (GRE) Key Extension for Mobile IPv4
- RFC6343: Advisory Guidelines for 6to4 Deployment
- RFC6372: 6to4 Provider Managed Tunnels
- draft-zhou-dhc-gre-option-00 DHCPv4 and DHCPv6 options for GRE
- draft-templin-v6ops-isops-18 Operational Guidance for IPv6 Deployment in IPv4 Sites using ISATAP

9.2   Applications

Application	Description
Accessing the IPv6 Sites on a Campus Network	Accesses the IPv6 sites on a campus network.
Connecting a Campus Network to an IPv6 Backbone Network	Connects a campus network to an IPv6 backbone network.

9.2.1   Accessing the IPv6 Sites on a Campus Network

Scenario

IPv6 servers are deployed on some campus networks, and PCs need to access the servers. The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) can be used to realize the access.

Figure 9-1
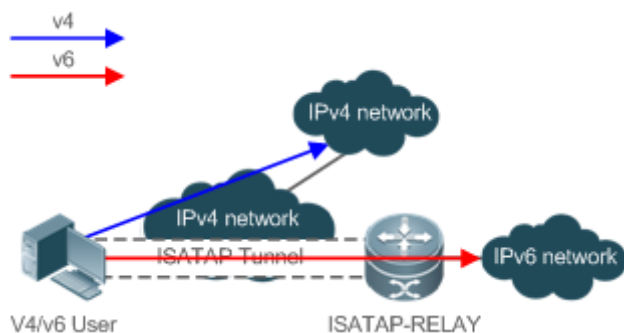
Remarks	ISATAP-RELAY supports tunneling. Users on the campus network can access IPv4 servers directly through the IPv4 network, but need to access IPv6 servers through the ISATAP tunnel.

Deployment

- IPv4 and IPv6 users access the IPv4 network by using IPv4 addresses.
- IPv4 and IPv6 users access the IPv6 network through the ISATAP tunnel.
- The ISATAP tunnel is established between PCs and the ISATAP-RELAY router.

9.3　Configuration

Configuration	Description and Command	
Configuring Tunnel Interfaces	⚠️ (Mandatory) It is used to create tunnels.	
	Interface tunnel	Creates a tunnel interface.
	tunnel source	Configures the local address of a tunnel.
Configuring a Tunnel Mode	⚠️ (Optional) It is used to configure a tunnel mode.	
	tunnel mode	Configures a tunnel encapsulation mode.
Configuring a Local Address	⚠️ (Optional) It is used to configure the local address of a tunnel.	
	tunnel source	Configures the address of a tunnel.

Configuring a Peer Address	⚠️ (Optional) It is used to configure the peer address of a tunnel.	
	tunnel destination	Configures the peer address of a tunnel.
Configuring the TOS of a Tunnel	⚠️ (Optional) It is used to configure the type of service (TOS) of a tunnel.	
	tunnel tos	Configures the TOS of a tunnel.
Configuring the TTL of a Tunnel	⚠️ (Optional) It is used to configure the time to live (TTL) of a tunnel.	
	tunnel ttl	Configures the TTL of a tunnel.

9.3.1 Configuring Tunnel Interfaces

Configuration Effect

- Create a tunnel interface.

Configuration Steps

Creating a Tunnel Interface

- Run the **interfaces tunnel** *number* command in global configuration mode to create a tunnel interface.
- The tunneling service is available only after a tunnel interface is created.

Verification

- Run the **show interfaces tunnel** *number* command to check whether the tunnel interface is created successfully.

Related Commands

Configuring a Tunnel Interface

Command	interface tunnel *number*

Parameter Description	*number*: Indicates the number of a tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Checking the Tunnel Configuration

Command	**show interfaces tunnel** *number*
Parameter Description	*number*: Indicates the number of a tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Configur ation Example

Creating a Tunnel Interface

Configurati on Steps	Create a tunnel interface.
	QTECH # configure terminal
	QTECH (config)# interface tunnel 1
	QTECH (config-if-Tunnel 1)# end
Verificatio n	Check the configuration of the tunnel interface.
	QTECH # show interfaces tunnel 1
	……

	Tunnel attributes: ...... Tunnel protocol/transport is gre ip

Common Errors

- A tunnel interface cannot be created due to memory deficiency.
- A tunnel interface cannot be created due to insufficient hardware resource deficiency.

9.3.2 Configuring a Tunnel Mode

Configuration Effect

- Configure a tunnel encapsulation mode in tunnel interface configuration mode when you need to use a tunnel in non-default encapsulation mode.

Configuration Steps

Configuring a Tunnel Mode

- Optional.
- The default encapsulation mode for switches is tunnel mode ipv6ip.
- To change the default encapsulation mode, run the **tunnel mode** command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** *number* command to check whether the tunnel encapsulation mode is configured.

Related Commands

Configuring a Tunnel Mode

Command	tunnel mode { gre {ip | ipv6} | ipv6 | ipip | ipv6ip [6to4 | isatap] }
Parameter Description	Each mode corresponds to different encapsulation format of the packets sent out by the tunnel interface. **gre ip** indicates that a packet is encapsulated with a GRE header and an IPv4

	header in sequence and then is transmitted over a new IPv4 network. **gre ipv6** indicates that a packet is encapsulated with a GRE header and an IPv6 header in sequence and then is transmitted over a new IPv6 network. **ipv6** indicates that a packet sent out by the tunnel interface is encapsulated with an IPv6 header and then transmitted over a new IPv6 network. **ipip** indicates that the tunnel interface carries only IPv4 packets and a packet sent out by the tunnel interface is encapsulated with an IPv4 header and then transmitted over a new IPv4 network. **ipv6ip** indicates that the tunnel interface carries only IPv6 packets and a packet sent out by the tunnel interface is encapsulated with an IPv4 header and then transmitted over a new IPv4 network. The preceding tunnels are manual tunnels, whereas IPv6IP, 6to4, and ISATAP are automatic tunnels. During packet encapsulation, the destination IPv4 address is mapped from the destination IPv6 address.
Command Mode	Interface configuration mode
Usage Guide	Both ends of a tunnel must be configured with the same encapsulation mode. Otherwise, the tunnel cannot work.

Configuration Example

Configuring the IPv4 over IPv4 Encapsulation Mode

Configuration Steps	▪ **Configure the IPv4 over IPv4 encapsulation mode on a tunnel interface.**
	QTECH # configure terminal QTECH (config)# interface tunnel 1 QTECH (config-if-Tunnel 1)# tunnel mode ipip QTECH (config)# end
Verification	▪ Check the configuration of the tunnel interface.
	QTECH # show interfaces tunnel 1

> ......
>
> Tunnel attributes:
>
> ......
>
>   Tunnel protocol/transport is ipv6ip

Common Errors

- A 6to4 tunnel or ISATAP tunnel is configured for a virtual routing and forwarding (VRF) instance that is already configured with a 6to4/ISATAP tunnel.

9.3.3 Configuring a Local Address

Configuration Effect

- Configure the local address of a tunnel.

Notes

- The local address of a tunnel must match the transport protocol used by the tunnel. Otherwise, the tunnel interface will not be up (be disabled).
- When the local address is specified indirectly by configuring another interface, the local address is the primary IPv4 address or the first global public IPv6 address of IPv6.

Configuration Steps

Configuring a Local Address

- Mandatory.
- Run the **tunnel source** command in tunnel interface configuration mode to specify the local address of a tunnel.

Verification

- Run the **show interfaces tunnel** *number* command to display the local address of the tunnel.

Related Commands

Configuring a Local Address

Command	tunnel source { *ip-address* | *interface-name interface-number* }
Parameter Description	**ip-address**: Indicates an IPv4 or IPv6 address. *Interface-name interface-number*: Indicates a Layer-3 interface.
Command Mode	Interface configuration mode
Usage Guide	If you specify an IPv4 or IPv6 address directly, you need to configure the address of the device.

Configuration Example

Configuring a Local Address

Configuration Steps	▪ **Configure the local address of a tunnel as 1.1.1.1.**
	QTECH # configure terminal QTECH (config)# interface tunnel 1 QTECH (config-if-Tunnel 1)# tunnel mode ipv6ip QTECH (config-if-Tunnel 1)# tunnel source 1.1.1.1
Verification	▪ Check the configuration of the tunnel interface.

	QTECH # show interfaces tunnel 1
	……
	Tunnel attributes:
	  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
	  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
	  Tunnel config nested limit is 0, current nested number is 0
	  Tunnel protocol/transport ipv6ip
	  Tunnel transport VPN is no set
	……

9.3.4 Configuring a Peer Address

Configuration Effect

- A manual tunnel can be used (the tunnel interface is up) only after its peer address is configured.

Notes

- Peer addresses cannot be configured for automatic tunnels.

Configuration Steps

Configuring a Peer Address

- The peer addresses must be configured for all tunnels except 6to4, and ISATAP tunnels.
- Run the **tunnel destination** command in interface configuration mode to configure the peer address of a tunnel.

Verification

- Run the **show interfaces tunnel** command to check whether the destination address is configured.

Related Commands

Configuring a Peer Address

Command	tunnel destination { *ip-address* }
Parameter Description	*ip-address*: Indicates an IPv4 or IPv6 address.
Command Mode	Interface configuration mode
Usage Guide	The peer address of a manual tunnel must be configured. The protocol suite type of the configured peer address must be consistent with the transport protocol used by the tunnel. If they are not consistent, the tunnel interface will be disabled (down).

Configuring a Peer Address

Configurati on Steps	Configure the peer address of a tunnel as 2.2.2.2.
	QTECH # configure terminal QTECH (config)# interface tunnel 1 QTECH (config-if-Tunnel 1)# tunnel mode ipv6ip QTECH (config-if-Tunnel 1)# tunnel destination 2.2.2.2
Verificatio n	Check the configuration of the tunnel interface.

	QTECH # show interfaces tunnel 1
	
	 ……
	
	 Tunnel attributes:
	
	   Tunnel source: UNKNOWN, destination 2.2.2.2, unrouteable
	
	   Tunnel TOS/Traffic Class not set, Tunnel TTL 254
	
	   Tunnel config nested limit is 0, current nested number is 0
	
	   Tunnel protocol/transport ipv6ip
	
	   ……

Commo n Errors

- A peer address is configured for an automatic tunnel.
- The peer address configured for a tunnel is the same as that of another tunnel.

9.3.5 Configuring the TOS of a Tunnel

**Configur
ation
Effect**

- Specify the TOS or Traffic Class field in the transport protocol header.

Notes

- ▪ If the TOS or Traffic Class field in the transport protocol header is not specified, the TOS or Traffic Class field of the protocol is copied to the header.

Configuration Steps

Configuring the TOS of a Tunnel

- ▪ Optional.
- ▪ To change the priority of tunnel data on a network, run the **tunnel tos** command in interface configuration mode.

Verification

- ▪ Run the **show interfaces tunnel** command to check whether the TOS is configured.

Related Commands

Configuring the TOS of a Tunnel

Command	tunnel tos *number*
Parameter Description	*number*: Indicates the TOS of a tunnel.
Command Mode	Interface configuration mode
Usage Guide	By default, if the IPv4 protocol is used for the inner bearer and outer encapsulation in a tunnel, the TOS bytes in the inner IPv4 header are copied to the outer IPv4 header. If the IPv6 protocol is used for the inner bearer and outer encapsulation in a tunnel, the Traffic Class 8 bit in the inner IPv6 header is copied to the outer IPv6 header. In other cases, the TOS field in the outer IPv4 header and the Traffic Class field in the IPv6 header are 0.

Configuration Example

Configuring the TOS of a Tunnel

Configuration Steps	▪ Configure the TOS of a tunnel.

	QTECH # configure terminal QTECH (config)# interface tunnel 1 QTECH (config-if-Tunnel 1)# tunnel mode ipv6ip QTECH (config-if-Tunnel 1)# tunnel tos 2
Verification	▪ Check the configuration of the tunnel interface.

	QTECH # show interfaces tunnel 1
	……
	Tunnel attributes:
	  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
	  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 254
	  Tunnel config nested limit is 0, current nested number is 0
	  Tunnel protocol/transport ipv6ip
	  Tunnel transport VPN is VPN1
	……

9.3.6   Configuring the TTL of a Tunnel

Configuration Effect

▪ Specify the TTL or hop limit of tunnel encapsulation protocol headers.

Configuration Steps

Configuring the TTL of a Tunnel

▪ Optional.
▪ By default, the TTL is 254.
▪ To specify the tunnel link length limit, run the **tunnel ttl** command.

Verification

▪ Run the **show interfaces tunnel** command to check whether the TTL is configured.

Related Commands

Configuring the TTL of a Tunnel

Command	tunnel ttl *hop-limit*
Parameter Description	*hop-limit*: Indicates the hop limit of a tunnel.
Command Mode	Global configuration mode
Usage Guide	The hop limit specifies the maximum number of routers that a packet can pass through. The default value is 254. This command is used to specify the hop quantity limit.

Configuration Example

Configuring the TTL of a Tunnel

Configuration Steps	▪ Configure the TTL of a tunnel.
	QTECH # configure terminal QTECH (config)# interface tunnel 1 QTECH (config-if-Tunnel 1)# tunnel mode ipv6ip QTECH (config-if-Tunnel 1)# tunnel ttl 3
Verification	▪ Check the configuration of the tunnel interface.

	QTECH # show interfaces tunnel 1
	……
	Tunnel attributes:
	  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
	  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3

	Tunnel config nested limit is 0, current nested number is 0
	Tunnel protocol/transport ipv6ip
	Tunnel transport VPN is VPN1

9.4   Monitoring

Displaying

Description	Command
Displays the information about a tunnel interface.	**show interfaces tunnel** *number*

Debugging

⚠️ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables tunnel interface debugging.	**debug tunnel**

10 CONFIGURING NETWORK COMMUNICATION TEST TOOLS

10.1 Overview

Network communication test tools can be used to check the connectivity of a network and helps you analyze and locate network faults. Network communication test tools include Packet Internet Groper (PING) and Traceroute. Ping is used to check the connectivity and delay of a network. A greater delay indicates a slower network speed. Traceroute helps you learn about the topology of physical and logical links and transmission rate. On a network device, you can run the **ping** and **traceroute** commands to use the two tools respectively.

Protocols and Standards

- RFC792: Internet Control Message Protocol
- RFC4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

10.2 Applications

Application	Description
End-to-End Connectivity Test	Both the network device and the destination host are connected to the IP network and configured with IP addresses.
Host Route Test	Both the network device and the destination host are connected to the IP network and configured with IP addresses.

10.2.1 End-to-End Connectivity Test

Scenario

As shown in Figure 10-1, Network Device A and Target Host B are connected to the IP network.

If both the network device and the target host are connected to the IP network, the end-to-end connectivity test aims to check whether IP packets can be transmitted between the two ends. The target host can be the network device itself. In this case, the connectivity test aims to check the network interface and TCP/IP configurations on the device.

Figure 10-1

**Deploym
ent**

Execute the ping function on the network device.

10.2.2 Host Route Test

Scenario

As shown in Figure 10-2, Network Device A and Target Host B are connected to the IP network.

If both the network device and the target host are connected to the IP network, the host route test aims to check gateways (or routers) that IP packets pass through between the two ends. Generally, the target host is not within the same IP network segment as the network device.

Figure 10-2

**Deploym
ent**

Execute the traceroute function on the network device.

10.3 Features

**Overvie
w**

Feature	Description
Ping Test	Test whether the specified IPv4 or IPv6 address is reachable and display the related information.
Traceroute Test	Display the gateways that IPv4 or IPv6 packets pass through when transmitted from the source to the destination.

10.3.1 Ping Test

**Working
Principle**

The ping tool sends an Internet Control Message Protocol (ICMP) Request message to the destination host to request the for an ICMP Echo Reply message. In this way, the ping tool determines the delay and the connectivity between the two network devices.

Related Configuration

- Run the **ping** command.

10.3.2 Traceroute Test

Working Principle

The traceroute tool uses the Time To Live (TTL) field in the headers of the ICMP and IP messages for the test First, the traceroute tool on the network device sends an ICMP Request message with TTL 1 to the destination host. After receiving the message, the first router on the path decreases the TTL by 1. As the TTL becomes 0, the router drops the packets and returns an ICMP time exceeded message to the network device. After receiving this message, the traceroute tool learns that this router exists on this path, and then sends an ICMP Request packet with TTL 2 to the destination host to discover the second router. Each time the traceroute tool increases the TTL in the ICMP Request message by 1 to discover one more router. This process is repeated until a data packet reaches the destination host. After the packet reaches the destination host, the host returns an ICMP Echo message instead of an ICMP time exceeded message to the network device. Then, the traceroute tool finishes the test and displays the path from the network device to the destination host.

Related Configuration

- Run the **traceroute** command.

10.4 Configuration

Configuration	Description and Command	
Ping Test	⚠ (Optional) It is used to check whether an IPv4 or IPv6 address is reachable.	
	ping	Executes the Ping function.
Traceroute Test	⚠ (Optional) It is used to display the gateways that IPv4 or IPv6 packets pass through when transmitted from the source to the destination.	
	traceroute	Executes the traceroute function.

10.4.1 Ping Test

Configuration Effect

After conducting a ping test on a network device, you can learn whether the network device is connected to the destination host and whether packets can be transmitted between the network device and the destination host.

Notes

The network device must be configured with an IP address.

Configuration Steps

- To check whether an IPv4 address is reachable, use the **ping IPv4** command.
- To check whether an IPv6 address is reachable, use the **ping IPv6** command.

Verification

Run the **ping** command to display related information on the command line interface (CLI) window.

Related Commands

Ping IPv4

Command	ping [oob | vrf *vrf-name* | ip] [*address* [via *mgmt-name*] [length *length*] [ntimes *times*] [timeout *seconds*] [data *data*] [source *source*] [df-bit] [validate] [detail] [interval millisecond]]
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as the source port. *vrf-name*: Indicates the VPN routing and forwarding (VRF) name. *address*: Specifies the destination IPv4 address or domain name. *mgmt-name:* Specifies the MGMT port in OOB mode. *length*: Specifies the length of the data packet. The value ranges from 36 to 18, 024. The default length is 100. *times*: Specifies the number of probes. The value ranges from 1 to 4, 294, 967, 295

	seconds: Specifies the timeout. The value ranges from 1s to 10s. *data*: Specifies the data in the packet. The data is a string of 1 to 255 bytes. By default, the string is "abcd". *source*: Specifies the source IPv4 address or source port of the packet. The loopback interface address, for example, 127.0.0.1, cannot be used as the source address. **df-bit**: Configures the DF bit of the IP address. When the DF bit is set to 1, the packet is not fragmented. By default, the DF bit is 0. **validate**: Configures whether to verify the response packet. **detail**: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed. millisecond: Specifies the interval at which the ping packet is sent. The value ranges from 10 ms to 300,000 ms. The default interval is 100 ms.
Command Mode	In User EXEC mode, you can execute only the basic ping function. In Privileged EXEC mode, you can execute the extended ping function. In other configuration modes, you can run the **do** command to execute the extended ping function. For details about the configuration, see the description about the **do** command.
Configuration Usage	When the ping function is executed, information about the response (if any) will be displayed, and then related statistics will be output. Using the extended ping function, you can specify the number, length and timeout of packets to be sent. Like the basic ping function, related statistics will be output. To use the domain name, you must first configure the domain name server (DNS). For details about the configuration, see *Configuring DNS*.

Ping IPv6

Command	**ping [vrf *vrf-name*	[oob] ipv6]** [*address* [via *mgmt-name*] [length *length*] [ntimes *times*] [timeout *seconds*] [data *data*] [source *source*] [detail] [interval millisecond] [out-interface interface]]
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as the source port. *vrf-name*: Indicates the VRF name. *address*: Specifies the destination IPv6 address or domain name. *mgmt-name:* Specifies the MGMT port in OOB mode.

	length: Specifies the length of data packet. The value ranges from 16 to 18, 024. The default length is 100.
	times: Specifies the number of probes. The value ranges from 1 to 4, 294, 967, 295.
	seconds: Specifies the timeout. The value ranges from 1s to 10s.
	data: Specifies the data in the packet. The data is a string of 1 to 255 bytes.
	source: Specifies the source IPv6 address or source port of the packet. The loopback interface address, for example, ::1, cannot be used as the source address.
	detail: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed.
	millisecond: Specifies the interval at which the ping packet is sent. The value ranges from 10 ms to 300,000 ms. The default interval is 100 ms.
Command Mode	In User EXEC mode, you can execute only the basic ping IPv6 function. In Privileged EXEC mode, you can execute the extended ping IPv6 function. In other configuration modes, you can run the **do** command to execute the extended ping function. For details about the configuration, see the description about the **do** command.
Configuration Usage	When the ping IPv6 function is executed, information about the response (if any) will be displayed, and then related statistics will be output. Using the extended ping IPv6 function, you can specify the number, length and timeout of packets to be sent. Like the basic ping IPv6 function, related statistics will be output. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Configuration Example

Executing the Common Ping Function

Configuration Steps	**In Privileged EXEC mode, run the ping 192.168.21.26 command.**
	Common ping command:

	QTECH # ping 192.168.21.26
	Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
	< press Ctrl+C to break >
	!!!!!
	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
	Detailed ping command:
	QTECH #ping 192.168.21.26 detail
	Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
	< press Ctrl+C to break >
	Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
	Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
	Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
Verificatio n	Send five 100-byte packets to the specified IP address, and the response information will be displayed in the specified time (2s by default). Finally the statistics is output.

Executing the Extended Ping Function

Configurati on Steps	In Privileged EXEC mode, run the ping 192.168.21.26 command. In addition, specify the length, number, and timeout of the packets.
	Common ping command:
	QTECH # ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3
	Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
	< press Ctrl+C to break >
	!!!
	Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms

	Detailed ping command:
	ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail
	Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
	< press Ctrl+C to break >
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
	Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms.
Verification	Send twenty 1500-byte packets to the specified IP address, and the response information (if any) will be displayed in the specified time (3s by default). Finally the statistics is output.

Executing the Common Ping IPv6 Function

Configuration Steps	In Privileged EXEC mode, run the ping ipv6 2001::1 command.
	Common ping command: QTECH # ping ipv6 2001::1 Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms Detailed ping command: QTECH #ping 2001::1 detail Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
Verification	Send five 100-byte packets to the specified IP address, and the response information will be displayed in the specified time (2s by default). Finally the statistics is output.

Executing the Extended Ping IPv6 Function

Configuration Steps	In Privileged EXEC mode, run the ping ipv6 2001::5 command. In addition, specify the length, number, and timeout of the packets.

	Common ping command:
	QTECH # ping ipv6 2001::5 length 1500 ntimes 100 data ffff source 2001::9 timeout 3
	Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds:
	< press Ctrl+C to break >
	!!!
	Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
	Detailed ping command:
	QTECH #ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3
	Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds:
	< press Ctrl+C to break >
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Reply from 2001::5: bytes=1500 time=1ms
	Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.
Verification	Send one hundred 1500-byte packets to the specified IPv6 address, and the response information (if any) will be displayed in the specified time (3s by default). Finally the statistics is output.

10.4.2 Traceroute Test

Configuration Effect

After conducting a traceroute test on a network device, you can learn about the routing topology between the network device and the destination host, and the gateways through which packets are sent from the network device to the destination host.

Notes

The network device must be configured with an IP address.

Configuration Steps

- To trace the route an IPv4 packet would follow to the destination host, run the **traceroute IPv4** command.
- To trace the route an IPv6 packet would follow to the destination host, run the **traceroute IPv6** command.

Verification

Run the **traceroute** command to display related information on the CLI window.

Related Commands

Traceroute IPv4

Command	traceroute [oob | vrf *vrf-name* | ip] [*adress* [via *mgmt-name*] [probe *number*] [source *source*] [timeout *seconds*] [ttl *minimum maximum*]]
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as the source port. *vrf-name*: Indicates the VRF name. *address*: Specifies the destination IPv4 address or domain name. *mgmt-name:* Specifies the MGMT port in OOB mode. *number*: Specifies the number of probes. The value ranges from 1 to 255. *source*: Specifies the source IPv4 address or source port of the packet. The loopback interface address, for example, 127.0.0.1, cannot be used as the source address. *seconds*: Specifies the timeout. The value ranges from 1s to 10s. *minimum maximum*: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255.

Command Mode	In User EXEC mode, you can execute only the basic traceroute function. In privileged EXEC mode, you can execute the extended traceroute function.
Configuration Usage	The **traceroute** command is used to test the network connectivity and accurately locate a fault when the fault occurs. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Traceroute IPv6

Command	traceroute [vrf *vrf-name*	[oob] ipv6] [*address* [via *mgmt-name*] [probe *number*] [timeout *seconds*] [ttl *minimum maximum*]
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as a source port.
	vrf-name: Indicates the VRF name.
	address: Specifies the destination IPv6 address or domain name.
	mgmt-name: Specifies the MGMT port in OOB mode.
	number: Specifies the number of probes. The value ranges from 1 to 255.
	seconds: Specifies the timeout. The value ranges from 1s to 10s.
	minimum maximum: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255.
Command Mode	In User EXEC mode, you can execute only the basic traceroute IPv6 function. In privileged EXEC mode, you can execute the extended traceroute IPv6 function.
Configuration Usage	The traceroute IPv6 command is used to test the network connectivity and accurately locate a fault when the fault occurs. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Configuration Example

Executing the Traceroute Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the traceroute ipv6 3004::1 command.
	QTECH #

QTECH # traceroute ipv6 3004::1

 < press Ctrl+C to break >

Tracing the route to 3004::1

1	3000::1	0 msec	0 msec	0 msec
2	3001::1	4 msec	4 msec	4 msec
3	3002::1	8 msec	8 msec	4 msec

The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1–3. In addition, the time required to reach each gateway is displayed.

Executing the Traceroute Function on a Faulty Network

Configuration Steps	In Privileged EXEC mode, run the traceroute 5.134.219.3 command.
	QTECH # traceroute 202.108.37.42 < press Ctrl+C to break > Tracing the route to 202.108.37.42 1 192.168.12.1 0 msec 0 msec 0 msec 2 192.168.9.2 0 msec 4 msec 4 msec 3 192.168.110.1 16 msec 12 msec 16 msec 4 * * * 5 5.134.219.3 12 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 5.134.219.3 by transmitting packets through gateways 1–5, and Gateway 4 is faulty.

Executing the Traceroute IPv6 Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the traceroute ipv6 3004::1 command.
	QTECH # traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1

	1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 3004::1 4 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1-4. In addition, the time required to reach each gateway is displayed.

Executing the Traceroute IPv6 Function on a Faulty Network

Configuration Steps	In Privileged EXEC mode, run the traceroute ipv6 3004::1 command.
	QTECH # traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 * * * 5 3004::1 4 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1–5, and Gateway 4 is faulty.

www.qtech.ru

11 CONFIGURING TCP

11.1 Overview

The Transmission Control Protocol (TCP) is a transport-layer protocol providing reliable connection-oriented and IP-based services to for the application layer.

Internetwork data flows in 8-bit bytes are sent from the application layer to the TCP layer, and then fragmented into packet segments of a proper length via the TCP. The Maximum Segment Size (MSS) is usually limited by the Maximum Transmission Unit (MTU) of the data link layer. After that, the packets are sent to the IP layer and then to the TCP layer of a receiver through the network.

To prevent packet loss, every byte is identified by a sequence number via the TCP, and this ensures that packets destined for the peer are received in order. Then, the receiver responds with a TCP ACK packet upon receiving a packet. If the sender does not receive ACK packets in a reasonable Round-Trip Time (RTT), the corresponding packets (assumed lost) will be retransmitted.

- TCP uses the checksum function to check data integrity. Besides, MD5-based authentication can be used to verify data.
- Timeout retransmission and piggyback mechanism are adopted to ensure reliability.
- The Sliding Window Protocol is adopted to control flows. As documented in the Protocol, unidentified groups in a window should be retransmitted.

Protocols and Standards

- RFC 793: Transmission Control Protocol
- RFC 1122: Requirements for Internet Hosts -- Communication Layers
- RFC 1191: Path MTU Discovery
- RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
- RFC 2385: Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 4022: Management Information Base for the Transmission Control Protocol (TCP)

11.2 Applications

Application	Description
Optimizing TCP Performance	To avoid TCP packet fragmentation on a link with a small MTU, Path MTU Discovery (PMTUD) is enabled.
Detecting TCP Connection	TCP checks whether the peer works normally.

Exception	

11.2.1 Optimizing TCP Performance

Scenario

For example, TCP connection is established between A and D, as shown in the following figure. The MTU of the link between A and B is 1500 bytes, 1300 bytes between B and C, and 1500 bytes between C and D. To optimize TCP transmission performance, packet fragmentation should be avoided between B and C.

Figure 11-1

Remarks:	A, B, C and D are routers.

Deployment

- Enable PMTUD on A and D.

11.2.2 Detecting TCP Connection Exception

Scenario

For example, in the following figure, User logs in to A through telnet but is shut down abnormally, as shown in the following figure. In case of TCP retransmission timeout, the User's TCP connection remains for a long period. Therefore, TCP keepalive can be used to rapidly detect TCP connection exception.

Figure 11-2
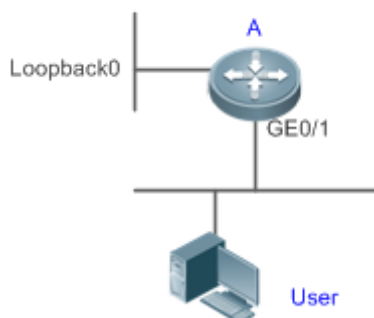
Remark s:	A is a router.

Deploym ent

- Enable TCP keepalive on A.

11.3 Features

Basic Concept s

TCP Header Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Acknowledgment Number                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                               |
| Offset| Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
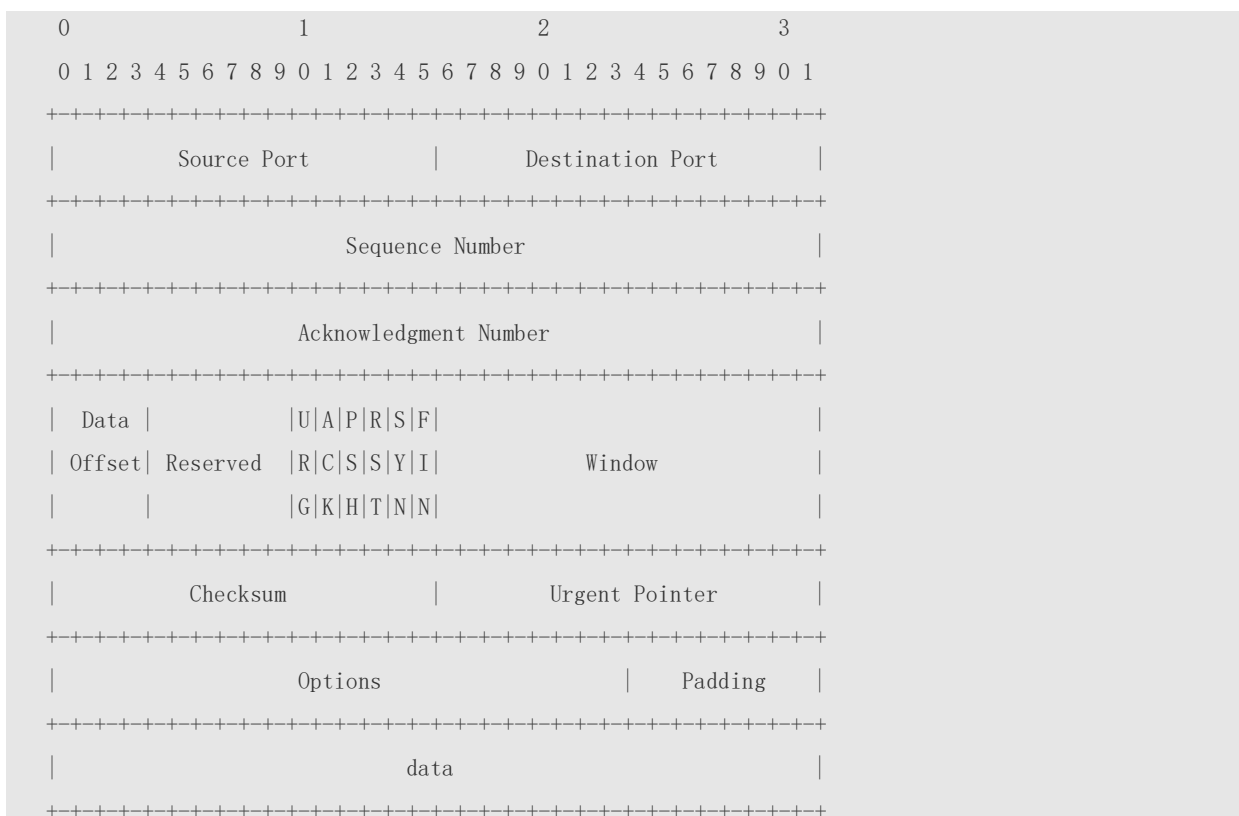
- **Source Port** is a 16-bit source port number.
- **Destination Port** is a 16-bit destination port number.
- **Sequence Number** is a 32-bit sequence number.
- **Acknowledgment Number** is a 32-bit number that identifies the next sequence number that the receiver is expecting to receive.
- **Data Offset** is a 4-bit number that indicates the total number of bytes in the TCP header (option included) divided by 4.

- A flag bit is 6-bit. URG: the urgent pointer field is significant; ACK: the acknowledgment field is significant; PSH: indicates the push function; RST: resets TCP connection; SYN: synchronizes the sequence number (establishing a TCP connection); FIN: no more data from the sender (closing a TCP connection).
- A 16-bit Window value is used to control flows. It specifies the amount of data that may be transmitted from the peer between ACK packets.
- **Checksum** is a 16-bit checksum.
- **Urgent Pointer** is 16-bit and shows the end of the urgent data so that interrupted data flows can continue. When the URG bit is set, the data is given priority over other data flows.

TCP Three-Way Handshake

- The process of TCP three-way handshake is as follows:
1. A client sends a SYN packet to the server.
2. The server receives the SYN packet and responds with a SYN ACK packet.
3. The client receives the SYN packet from the server and responds with an ACK packet.
- After the three-way handshake, the client and server are connected successfully and ready for data transmission.

Overview

Feature	Description
Configuring SYN Timeout	Configure a timeout waiting for a response packet after an SYN or SYN ACK packet is sent.
Configuring Window Size	Configure a window size.
Configuring Reset Packet Sending	Configure the sending of TCP reset packets after receiving port unreachable messages.
Configuring MSS	Configure an MSS for TCP connection.
Path MTU Discovery	Discover the smallest MTU on TCP transmission path, and adjust the size of TCP packets based on this MTU to avoid fragmentation.
TCP Keepalive	Check whether the peer works normally.

11.3.1 Configuring SYN Timeout

Working Principle

A TCP connection is established after three-way handshake: The sender sends an SYN packet, the receiver replies with a SYN ACK packet, and then the sender replies with an ACK packet.

- If the receiver does not reply with a SYN ACK packet after the sender sends an SYN packet, the sender keeps retransmitting the SYN packet for certain times or until timeout period expires.
- If the receiver replies with a SYN ACK packet after the sender sends an SYN packet but the sender does not reply with an ACK packet, the receiver keeps retransmitting the SYN ACK packet for certain times or until timeout period expires. (This occurs in the case of SYN flooding.)

Related Configuration

Configuring TCP SYN Timeout

- The default TCP SYN timeout is 20 seconds.
- Run the ip tcp synwait-time seconds command in global configuration mode to configure an SYN timeout ranging from 5 to 300 seconds.
- In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time. You may prolong SYN timeout properly on a poor network.

ℹ️ In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

11.3.2 Configuring Window Size

Working Principle

Data from the peer is cached in the TCP receiving buffer and subsequently read by applications. The TCP window size indicates the size of free space of the receiving buffer. For wide-bandwidth bulk-data connection, enlarging the window size dramatically promotes TCP transmission performance.

Related Configuration

Configuring Window Size

- Run the ip tcp window-size size command in global configuration mode to configure a window size ranging from 128 to (65535<< 14) bytes. The default is 65535 bytes. If the window size is greater than 65535 bytes, window enlarging will be enabled automatically.
- The window size advertised to the peer is the smaller value between the configured window size and the free space of the receiving buffer.

ℹ️ In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

11.3.3 Configuring Reset Packet Sending

**Working
Principle**

When TCP packets are distributed to applications, if the TCP connection a packet belongs to cannot be identified, the local end sends a reset packet to the peer to terminate the TCP connection. Attackers may use port unreachable messages to attack the device.

**Related
Configur
ation**

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Run the **no ip tcp send-reset** command in global configuration mode to disable TCP reset packet sending upon receiving port unreachable messages.

After this function is enabled, attackers may use port unreachable messages to attack the device.

ℹ️ In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

11.3.4 Configuring MSS

**Working
Principle**

The MSS refers to the total amount of data contained in a TCP segment t excluding TCP options.

Three-way handshake is implemented through MSS negotiation. Both parties add the MSS option to SYN packets, indicating the largest amount of data that the local end can handle, namely, the amount of data allowed from the peer. Both parties take the smaller MSS between them as the advertised MSS.

The MSS value is calculated as follows:

- IPv4 TCP: MSS = Outgoing interface MTU –IP header size (20-byte)–TCP header size (20-byte).
- IPv6 TCP: MSS = IPv6 Path MTU –IPv6 header size (40-byte)–TCP header size (20-byte).

ℹ️ In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

ℹ️ The effective MSS is the smaller one between the calculated MSS and the configured MSS.

ℹ️ If a connection supports certain options, the option length (with **data offset** taken into consideration) should be deducted from an MSS value. For example, 20 bytes for MD5 digest (with **data offset** taken into consideration) should be subtracted from the MSS.

Configuring MSS

▪ Run the **ip tcp mss** *max-segment-size* command in global configuration mode to set an MSS. It ranges from 68 to 1000 bytes. By default, the MSS is calculated based on MTU. If an MSS is configured, the effective MSS is the smaller one between the calculated MSS and the configured MSS.

▪ An excessively small MSS reduces transmission performance. You can promote TCP transmission by increasing the MSS. Choose an MSS value by referring to the interface MTU. If the former is bigger, TCP packets will be fragmented and transmission performance will be reduced.

11.3.5 Path MTU Discovery

The Path MTU Discovery f stipulated in RFC1191 is used to discover the smallest MTU in a TCP path to avoid fragmentation, enhancing network bandwidth utilization. The process of TCPv4 Path MTU Discovery is described as follows:

1. The source sends TCP packets with the Don't Fragment (DF) bit set in the outer IP header.
2. If the outgoing interface MTU value of a router in the TCP path is smaller than the IP packet length, the packet will be discarded and an ICMP error packet carrying this MTU will be sent to the source.
3. Through parsing the ICMP error packet, the source knows the smallest MTU in the path (path MTU) is.
4. The size of subsequent data segments sent by the source will not surpass the MSS, which is calculated as follows: TCP MSS = Path MTU – IP header size – TCP header size.

Enabling Path MTU Discovery

By default, Path MTU Discovery is disabled.

Run the **ip tcp path-mtu-discovery** command to enable PMTUD in global configuration mode.

ⓘ In version 11.0 or later, it applies to only IPv4 TCP. TCPv6 PMTUD is enabled permanently and cannot be disabled.

11.3.6 TCP Keepalive

You may enable TCP keepalive to check whether the peer works normally. If a TCP end does not send packets to the other end for a period of time (namely idle period), the latter starts sending keepalive packets successively to the former for several times. If no response packet is received, the TCP connection is considered inactive and then closed.

Related Configuration

Enabling Keepalive

▪ By default, TCP keepalive is disabled.
▪ Run the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command to in global configuration mode to enable TCP keepalive. See **Configuration** for parameter description.

ⓘ In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

ⓘ This command applies to both TCP server and client.

11.4 Configuration

Configuration	Description and Command	
Optimizing TCP Performance	⚠ (Optional) It is used to optimize TCP connection performance.	
	ip tcp synwait-time	Configures a timeout for TCP connection.
	ip tcp window-size	Configures a TCP window size.
	ip tcp send-reset	Configures the sending of TCP reset packets after receiving port unreachable messages.
	ip tcp mss	Configures an MSS for TCP connection.
	ip tcp path-mtu-discovery	Enables Path MTU Discovery.
Detecting TCP Connection Exception	⚠ (Optional) It is used to detect whether the peer works normally.	
	ip tcp keepalive	Enables TCP keepalive.

11.4.1 Optimizing TCP Performance

Configuration Effect

- Ensure optimal TCP performance and prevent fragmentation.

Notes

N/A

Configuration Steps

Configuring SYN Timeout

- Optional.
- Configure this on the both ends of TCP connection.

Configuring TCP Window Size

- Optional.
- Configure this on the both ends of TCP connection.

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages.

- Optional.
- Configure this on the both ends of TCP connection.

Configuring MSS

- Optional.
- Configure this on the both ends of TCP connection.

Enabling Path MTU Discovery

- Optional.
- Configure this on the both ends of TCP connection.

Verification

N/A

Related Commands

Configuring SYN Timeout

Command	ip tcp synwait-time *seconds*
Parameter	*seconds*: Indicates SYN packet timeout. It ranges from 5 to 300 seconds. The

Description	default is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time. You may prolong SYN timeout properly on a poor network.

Configuring TCP Window Size

Command	**ip tcp window-size** *size*
Parameter Description	*size*: Indicates a TCP window size. It ranges from 128 to (65535 << 14) bytes. The default is 65535 bytes.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

Command	**ip tcp send-reset**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Configuring MSS

Command	**ip tcp mss** *max-segment-size*
Parameter	*max-segment-size*: Indicates the maximum segment size. It ranges from 68 to

Description	10000 bytes. By default, the MSS is calculated based on MTU.
Command Mode	Global configuration mode
Usage Guide	This command defines the MSS for a TCP communication to be established. The negotiated MSS for a new connection should be smaller than this MSS. If you want to reduce the MSS, run this command. Otherwise, do not perform the configuration.

Configuring Path MTU Discovery

Command	ip tcp path-mtu-discovery [age-timer *minutes* | age-timer infinite]
Parameter Description	**age-timer** *minutes*: Indicates the interval for a new probe after a path MTU is discovered. It ranges from 10 to 30 minutes. The default is 10 minutes. **age-timer infinite**: No probe is implemented after a path MTU is discovered.
Command Mode	Global configuration mode
Usage Guide	The PMTUD is an algorithm documented in RFC1191 aimed to improve bandwidth utilization. When the TCP is applied to bulk data transmission, this function may facilitate transmission performance. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The age timer is a time interval for how often TCP estimates the path MTU with a larger MSS. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You may turn off the timer by setting it to **infinite**.

Configuration Example

Enabling Path MTU Discovery

Configuration Steps	Enable PMTUD for a TCP connection. Adopt the default age timer settings.

www.qtech.ru

	QTECH # configure terminal QTECH (config)# ip tcp path-mtu-discovery QTECH (config)# end
Verification	Run the show tcp pmtu command to display the IPv4 TCP PMTU.
	QTECH # show tcp pmtu Number Local Address Foreign Address PMTU 1 192.168.195.212.23 192.168.195.112.13560 1440
	Run the show ipv6 tcp pmtu command to display the IPv6 TCP PMTU.
	QTECH # show ipv6 tcp pmtu Number Local Address Foreign Address PMTU 1 1000::1:23 1000::2.13560 1440

Common Errors

N/A

11.4.2 Detecting TCP Connection Exception

Configuration Effect

▪ Check whether the peer works normally.

Notes

N/A

Configuration Steps

Enabling TCP Keepalive

▪ Optional.

Verification

N/A

Enabling TCP Keepalive

Command	ip tcp keepalive [interval *num1*] [times *num2*] [idle-period *num3*]
Parameter Description	**interval** *num1*: Indicates the interval to send keepalive packets. Ranging from 1 to120 seconds. The default is 75 seconds.
	times *num2*: Indicates the maximum times for sending keepalive packets. It ranges from 1 to 10. The default is 6.
	idle-period *num3*: Indicates the time when the peer sends no packets to the local end, It ranges from 60 to 1800 seconds. The default is15 minutes.
Command Mode	Global configuration mode
Usage Guide	You may enable TCP keepalive to check whether the peer works normally. The function is disabled by default.
	Suppose a user enables TCP keepalive function with the default interval, times and idle period settings. The user does not receive packets from the other end within 15 minutes and then starts sending Keepalive packets every 75 seconds for 6 times. If the user receives no TCP packets, the TCP connection is considered inactive and then closed.

Enabling TCP Keepalive

Configuration Steps	**Enable TCP keepalive on a device with interval and idle-period set to 3 minutes and 60 seconds respectively. If the user receives no TCP packets from the other end after sending keepalive packets four times, the TCP connection is considered inactive.**
	QTECH # configure terminal QTECH (config)# ip tcp keepalive interval 60 times 4 idle-period 180 QTECH (config)# end

Verificatio n	A user logs in to a device through telnet, and then shuts down the local device. Run the **show tcp connect** command on the remote device to observe when IPv4 TCP connection is deleted.

Commo n Errors

N/A

11.5 Monitoring

Displayi ng

Description	Command
Displays basic information on IPv4 TCP connection.	**show tcp connect** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP connection statistics.	**show tcp connect statistics**
Displays IPv4 TCP PMTU.	**show tcp pmtu** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP port information.	**show tcp port** [*num*]
Displays IPv4 TCP parameters.	**show tcp parameter**
Displays IPv4 TCP statistics.	**show tcp statistics**
Displays basic information on IPv6 TCP connection.	**show ipv6 tcp connect** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Displays IPv6 TCP connection statistics.	**show ipv6 tcp connect statistics**
Displays IPv6 TCP PMTU.	**show ipv6 tcp pmtu** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]

| Displays IPv6 TCP port information. | **show ipv6 tcp port** [*num*] |

Debugging

⚠️ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Displays the debugging information on IPv4 TCP packets.	**debug ip tcp packet** [**in** | **out**] [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**global** | **vrf** *vrf-name*] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv4 TCP connection.	**debug ip tcp transactions** [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]
Displays the debugging information on IPv6 TCP packets.	**debug ipv6 tcp packet** [**in** | **out**] [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**global** | **vrf** *vrf-name*] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv6 TCP connection.	**debug ipv6 tcp transactions** [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-port** *num*]

12 CONFIGURING IPV4/IPV6 REF

12.1 Overview

On products incapable of hardware-based forwarding, IPv4/IPv6 packets are forwarded through the software. To optimize the software-based forwarding performance, QTECH introduces IPv4/IPv6 express forwarding through software (QTECH Express Forwarding, namely REF).

REF maintains two tables: forwarding table and adjacency table. The forwarding table is used to store route information. The adjacency table is derived from the ARP table and IPv6 neighbor table, and it contains Layer 2 rewrite(MAC) information for the next hop..

REF is used to actively resolve next hops and implement load balancing.

Protocols and Standards

N/A

12.2 Applications

Application	Description
Load Balancing	During network routing, when a route prefix is associated with multiple next hops, REF can implement load balancing among the multiple next hops.

12.2.1 Load Balancing

Scenario

As shown in Figure12-1, a route prefix is associated with three next hops on router A, namely, link 1, link 2, and link 3. By default, REF implements load balancing based on the destination IP address. Load balancing can be implemented based on the source IP address and destination IP address as well.

Figure 122-1
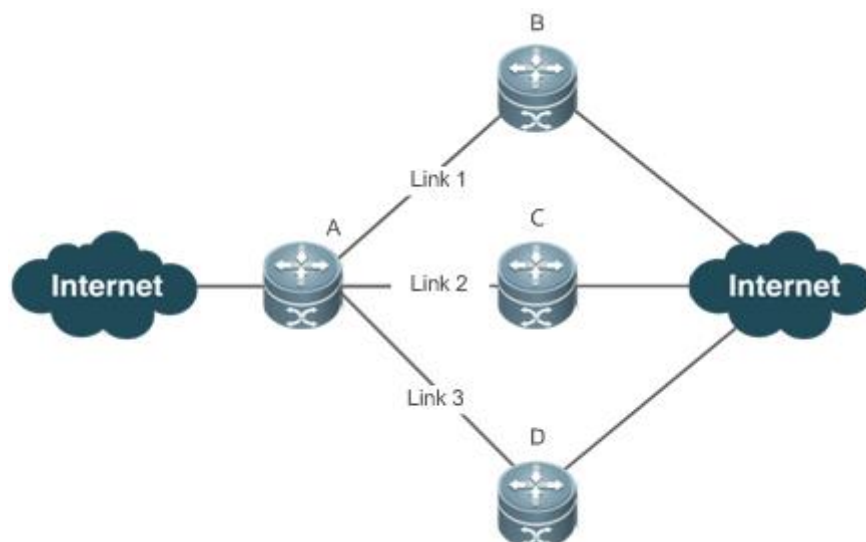
Remarks	A is a router that runs REF.
	B, C and D are forwarding devices.

Deployment

- Run REF on router A.

12.3 Features

Basic Concepts

IPv4/IPv6 REF involves the following basic concepts:

Routing table

An IPv4/IPv6 routing table stores routes to the specific destinations and contains the topology information. During packet forwarding, IPv4/IPv6 REF selects packet transmission paths based on the routing table.

Adjacent node

An adjacent node contains output interface information about routed packets, for example, the next hop, the next component to be processed, and the link layer encapsulation. When a packet is matched with an adjacent node, the packet is directly encapsulated and then forwarded. For the sake of query and update, an adjacent node table is often organized into a hash table. To support routing load balancing, the next hop information is organized into a load balance entry. An adjacent node may not contain next hop information. It may contain indexes of next components (such as other line cards and multi-service cards) to be processed.

Active resolution

REF supports next hop resolution. If the MAC address of the next hop is unknown, REF will actively resolve the next hop. IPv4 REF requests the ARP module for next hop resolution while IPv6 REF applies the ND module to resolution.

Packet forwarding path

Packets are forwarded based on their IPv4/IPv6 addresses. If the source and destination IPv4/IPv6 addresses of a packet are specified, the forwarding path of this packet is determined.

12.3.1 Load Balancing Policies

Load balancing is configured to distribute traffic load among multiple network links.

Working Principle

So far, the switch supports the load balancing policies based on destination IP addresses. In the REF model, a route prefix is associated with multiple next hops, in other words, it is a multi-path route. The route will be associated with a load balance table and implement weight-based load balancing. When an IPv4/IPv6 packet is matched with a load balance entry based on the longest prefix match, REF performs hash calculation based on the IPv4/IPv6 address of the packet and selects a path to forward the packet.

12.4 Configuration

By default, the switch supports destination address-based load balancing. Run the following commands for monitoring.

Displaying REF Packet Statistics

REF packet statistics includes the number of forwarded packets and the number of packets discarded due to various causes. You can determine whether packets are forwarded as expected by displaying and clearing REF packet statistics.

Command	Description
show ip ref packet statistics	Displays IPv4 REF packet statistics.
clear ip ref packet statistics	Clears IPv4 REF packet statistics.
show ipv6 ref packet statistics	Displays IPv6 REF packet statistics.
clear ipv6 ref packet statistics	Clears IPv6 REF packet statistics.

Displaying Adjacency Information

You can run the following commands to display adjacency information:

Command	Description
show ip ref adjacency [glean | local | *ip-address* | {interface *interface_type interface_number*) | discard | statistics]	Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes in IPv4 REF.
show ipv6 ref adjacency [glean | local | *ipv6-address* | (interface *interface_type interface_number*) | discard | statistics]	Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IPv6 address, adjacencies associated with a specified interface, and all adjacent nodes in IPv6 REF.

Displaying Active Resolution Information

You can run the following commands to display next hops to be resolved:

Command	Description
show ip ref resolve-list	Displays the next hop to be resolved .
show ipv6 ref resolve-list	Displays the next hop to be resolved.

Displaying Packet Forwarding Path

Information

Packets are forwarded based on their IPv4/IPv6 addresses. If the source and destination IPv4/IPv6 addresses of a packet are specified, the forwarding path of this packet is determined. Run the following commands and specify the IPv4/IPv6 source and destination addresses of a packet. The forwarding path of the packet is displayed, for example, the packet is discarded, submitted to a CPU, or forwarded. Furthermore, the interface that forwards the packet is displayed.

Command	Description
show ip ref exact-route [**oob** | **vrf** *vrf_name*] *source-ipaddress dest_ipaddress*	Displays the forwarding path of a packet. oob indicates out-of-band management network.
show ipv6 ref exact-route [**oob** | **vrf** *vrf-name*] *src-ipv6-address dst-ipv6-address*	Displays the forwarding path of an IPv6 packet. oob indicates out-of-band, management network.

Displaying Route Information in an REF Table

Run the following commands to display the route information in an REF table:

Command	Description
show ip ref route [**oob** | **vrf** *vrf_name*] [**default** | {*ip mask*}| **statistics**]	Displays route information in the IPv4 REF table. The parameter **default** indicates a default route. oob indicates out-of-band management network.
show ipv6 ref route [**oob** | **vrf** *vrf-name*] [**default** | **statistics** | *prefix/len*]	Displays route information in the IPv6 REF table. The parameter **default** indicates a default route. oob indicates out-of-band management network.