Chapter 19: L3 Base Function

Table of Contents

Chapter 19 L3 Base Function

19.1 L3 Base Function Overview

Switch is a 10-Gigabit intelligent routing Switch Switch based on the application specific integrated circuit (ASIC) technology and supports layer 2 (L2) and layer 3 (L3) forwarding. It performs L2 forwarding when hosts in the same virtual local area network (VLAN) access eachother and L3 forwarding when hosts in different VLANs access each other.

19.2 Configure L3 Base Function

19.2.1 L3 Base Function Configuration List

Configuration Task	Description	Detailed Configuration
Planning VLANs and creating L3 interfaces	Required	19.2.2
Configure the forwarding mode	Optional	19.2.3
Creating VLAN interfaces for common VLANs	Optional	19.2.4
Creating superVLAN interfaces and adding VLANs to the superVLAN	Required	19.2.5
Configure IP addresses for VLAN or superVLAN interfaces	Required	19.2.6
Configure an IP address range for VLAN or superVLAN interfaces	Required	19.2.7
Configure the Address Resolution Protocol (ARP) proxy	Optional	19.2.8
Display interface configurations	Optional	19.2.9
Configure unicast reverse path forwarding (URPF)	Optional	19.2.10
Disabling the function of sending Internet Control Message Protocol (ICMP) packets with an unreachable destination host on interfaces	Optional	19.2.11

19.2.2 Planning VLANs and Creating L3 Interfaces

For details about VLAN planning, see VLAN configurations.

L3 interfaces are classified into common VLAN interfaces and superVLAN interfaces. Common VLAN interfaces are created on VLANs and superVLAN interfaces on superVLANs (superVLANs do not exist or contain any port).

19.2.3 Configure the Forwarding Mode

The L3 Switch supports stream forwarding and network topology-based forwarding. In stream forwarding mode, The L3 Switch identifies the failed route or the unreachable destination host route and sends packets to the CPU for further processing. In network topology-basedforwarding mode, The L3 Switch directly discards the packets. By default, The L3 Switch worksin stream forwarding mode.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Set the packet forwarding mode in the system to stream forwarding.	**ip def cpu**	
Set the packet forwarding mode in the system to network topology-based forwarding.	**undo ip def cpu**	
Display the configured packet forwarding mode.	**display ip def cpu**	

19.2.4 Creating VLAN Interfaces for Common VLANs

A VLAN interface needs to be configured for each VLAN that performs L3 forwarding or theVLAN needs to be added to the superVLAN

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	

Create a VLAN interface with the VLAN ID being **vid** and enter the VLAN interface configuration mode.	**interface vlan-interface** *vid*	
Return to the global configuration mode.	**quit**	
Delete the VLAN interface with the VLAN ID being vid.	undo interface vlan-interface vid	

19.2.5 Creating SuperVLAN Interfaces and Adding VLANs to the SuperVLAN

SuperVLAN interfaces are used for communication between hosts in different VLANs in thesame network segment. SuperVLAN interfaces are implemented through the ARP proxy.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Create a superVLAN interface with the interface ID being **vid** and enter the superVLAN interface configuration mode.	**interface supervlan-interface** *vid*	
Return to the global configuration mode.	**quit**	
Delete the superVLAN interface with the interface ID being **vid**.	**undo interface supervlan-interface** *vid*	
Configure sub VLANs for the superVLAN interface.	**subvlan** *vid*	
Delete the sub VLANs configured for	**undo subvlan** *vid*	
the superVLAN interface.		

19.2.6 Configure IP Addresses for VLAN or SuperVLAN Interfaces

Each VLAN or superVLAN interface can be configured with a maximum of 32 IP addresses and the IP addresses of VLAN or superVLAN interfaces cannot be in the same network segment. The first IP address of an interface will be automatically selected as the primary IP address. When the primary IP address is deleted, the interface automatically selects another IP address as the primary IP address or a configured IP address can be manually specified asthe primary IP address. For example, if the IP address of VLAN interface 1 is 10.11.0.1/16, theIP addresses of other interfaces must not be in the 10.11.0.0/16 network segment (such as 10.11.1.1/24).

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Configure an IP address and a mask for the interface.	**ip address** *ipaddress ipaddress mask*	
Delete all IP addresses of the interface.	**undo ip address**	
Delete the specified IP address of	**undo ip address** *ipaddress ipaddress mask*	
the interface.		
Configure the primary IP address for the interface.	ip address primary ipaddress	

19.2.7 Configure an IP Address Range for VLAN or SuperVLAN Interfaces

Each VLAN or superVLAN interface can be configured with a maximum of eight IP address ranges. After an IP address range is configured, only the ARP entries within this range can be learnt so as to restrict user access. When a VLAN or superVLAN interface is deleted, relevant

configurations are automatically deleted.

For superVLAN interfaces, sub VLANs can be specified at the same time so that the set address range is applicable only to these sub VLANs.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Configure the IP address range supported by this interface, ranging from **startip** to **endip**.	**ip address range** *startip endip*	
Delete all IP address ranges supported by the interface.	**undo ip address range**	
Delete the specified IP address ranges supported by the interface.	undo ip address range startip endip	
Configure the IP address range for sub VLANs of the superVLAN.	ip address range startip endip vlan vlanid	
Delete the IP address ranges of the sub VLANs of the superVLAN.	undo ip address range startip endip vlan vlanid	

19.2.8 Configure the ARP Proxy

ARP request packets are broadcast packets and cannot pass through VLANs. If the ARP proxy function is enabled, ARP interaction is supported between hosts in sub VLANs of the same superVLAN. When the ARP proxy is disabled, the hosts of the sub VLANs in the superVLAN interface cannot communicate with each other.

By default, the ARP request packets from all sub VLANs are processed in the preceding manner.

Operation	Command	Remarks
Enter the VLAN configuration mode.	**interface vlan-interface** *vlan-id*	
Enable the arp-proxy function for the VLAN.	**local-arp-proxy**	
Disable the arp-proxy function for the VLAN.	undo local-arp-proxy	
Enable the arp-proxy broadcast function for the VLAN.	local-arp-proxy broadcast	
Disable the arp-proxy broadcast function for the VLAN.	undo local-arp-proxy broadcast	
Display the information about the ARP proxy configured in the system.	display local-arp-proxy	
Display information about the ARP proxy broadcast function configured in the system.	display local-arp-proxy broadcast	

In addition, relevant commands can be used to prevent the ARP request packets froma sub VLAN from being broadcast to other sub VLANs when they are processed by the ARP proxy.

19.2.9 Display VLAN and SuperVLAN Interface Information

The L3 Switch integrates VLAN interface information and superVLAN interface information.They can be viewed by running a unified display command.

Operation	Command	Remarks
Display information about the VLAN and superVLAN interfaces currently configured in the system.	**display ip interface** [[**vlan-interface** *vlanid*] | [**supervlan-interface** *supervlanid*]]	

19.2.10 Configure URPF

URPF aims to prevent network attack behaviors based on source address spoofing. URPF obtains the source address and ingress interface of a packet and uses the source address as the destination address to query the routing table for the matching route. The packet is forwarded if it meets conditions and discarded if it does not meet conditions. Two URPF modesare supported:

Strict mode: In this mode, the source address must exist in the routing table and the egress interface of the source address of the packet is the same as the ingress interface of the packet.

Loose mode: In this mode, the system only checks whether the source address of the packetexists in the unicast routing table. If yes, the packet is forwarded.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Enable URPF for this interface and specify the URPF mode.	**urpf** { **loose** | **strict** }	
Disable URPF for this interface.	**undo urpf**	
Display URPF information in the system.	**display urpf**	

19.2.11 Disabling the Function of Sending ICMP Packets with an Unreachable Destination Host on interfaces

To avoid attacks from address scanning software similar to ip-scan, users can disable thefunction of sending ICMP packets with an unreachable host on interfaces.

Operation	Command	Remarks
Enter the global configuration mode.	**system-view**	
Enter the VLAN or superVLAN interface configuration mode.	**interface vlan-interface** *vid* **interface supervlan-interface** *vid*	
Enable the function of this interface for sending ICMP packets with an unreachable destination	**ip icmp unreachable**	
Disable the function of this interface for sending ICMP packets with an unreachable destination	**undo ip icmp unreachable**	
Display the configuration of the function of sending ICMP packets with an unreachable destination	**display ip icmp unreachable**	