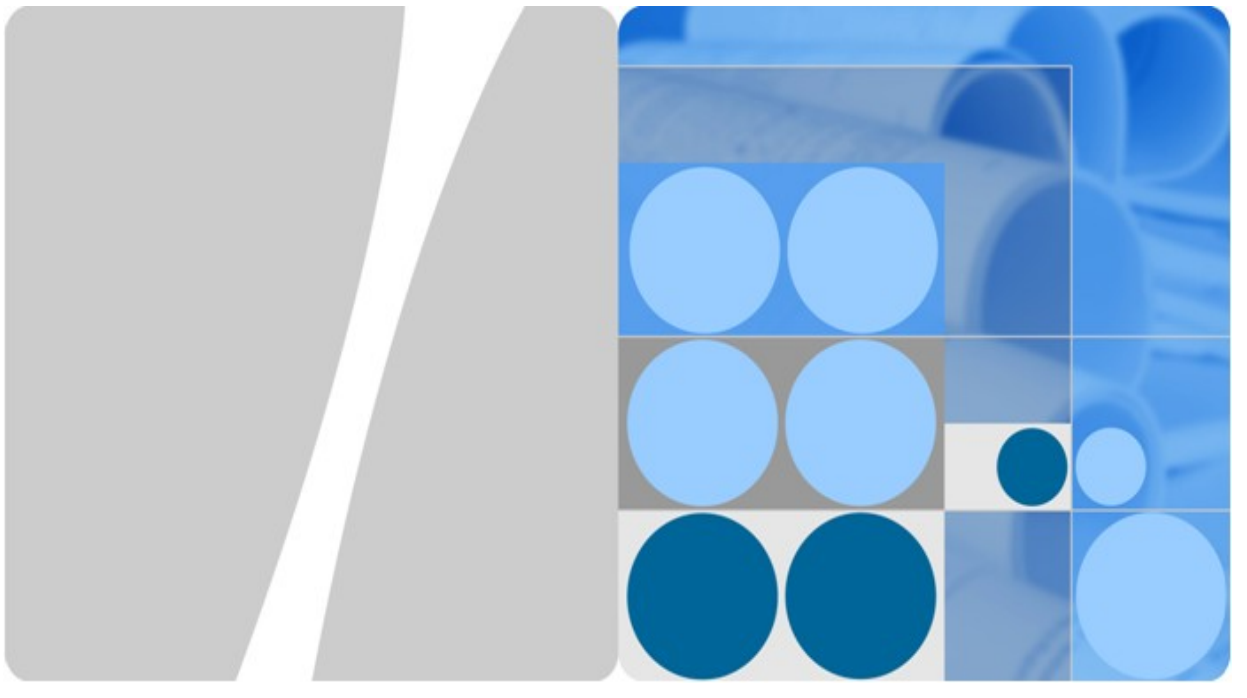

Huawei AR G3 Feature List(V200R005C00)

Date **2013/7/19**

HUAWEI TECHNOLOGIES CO., LTD.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
NAT				
	Basic NAT			
		NAT standards	Y	RFC 1631, RFC 2663, RFC 2993, RFC 3022, RFC 3235, RFC 4787
		PAT (address pool mode)	Y	For the connections initiated by private network hosts to public network hosts, AR routers translate private addresses into public addresses using an address pool and perform port mapping.
		NOPAT (address pool mode)	Y	AR routers support TCP, UDP, and ICMP connections. For the connections initiated by private network hosts to public network hosts, AR routers only translate private addresses into public addresses using an address pool, but do not perform port mapping.
		Easy IP	Y	AR routers support TCP, UDP, and ICMP connections. They use the public address of an interface as the translated source address.
		Static NAT-PAT	Y	AR routers support network segment translation, and TCP and UDP connections.Support use the address from address pool. Both private network hosts and public network hosts can initiate NAT connections. AR routers perform static address translation and port mapping on these connections.
		Static NAT-NOPAT	Y	AR routers support network segment translation, and TCP, UDP, and ICMP connections.Support use the address from address pool. Both private network hosts and public network hosts can initiate NAT connections. AR routers only perform static address translation, but do not perform port mapping on these connections.
		Overlapping NAT	Y	AR routers can translate both source and destination IP addresses. They map overlapping addresses to a unique temporary address. AR routers support TCP, UDP, ICMP connections, and other special protocol connections. Only private network hosts can initiate NAT connections to public network hosts.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		NAT session aging time	Y	AR routers can set aging time for NAT sessions based on protocol types, including TCP, UDP, ICMP, HTTP, FTP, DNS, SIP, and RTSP.
		Packet fragment NAT	Y	AR routers support TCP, UDP, and ICMP connections. They perform NAT-PAT on the initial fragment of TCP and UDP connections, perform NAT-NOPAT for the initial fragment of ICMP connections, and perform NAT-NOPAT for other fragments.
		Endpoint-independent mapping	Y	AR routers support the mapping from the same internal IP addresses and ports to the same ports. The mapping is irrelevant to external IP addresses and ports.
		Endpoint-independent filtering	Y	Before the NAT mapping entry between internal hosts and ports (X:x) and external hosts is aged out, any external host can initiate connections to the internal hosts and match the IP addresses, port IDs, and protocol type (TCP or UDP) of the destination hosts.
		Address-dependent filtering	Y	A host (Y:any) can transmit packets to an internal host (X:x) only after this internal host has transmitted packets to the host before. In addition, the protocol type (TCP or UDP) is matched.
		Address and port-dependent filtering	Y	An external host (Y:y) can transmit packets to an internal host (X:x) only after this internal host has transmitted packets to the external host before. In addition, the protocol type (TCP or UDP) is matched.
		Inbound NAT	Y	AR routers translate addresses for the connections from public network to private network.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		NAT multi-instance	Y	Each instance is associated with a VPN. An ACL is specified if NAT outbound addresses are configured for interfaces. ACL rules can be bound to a VPN. A VPN is specified if the NAT server or NAT static address is configured for an interface.
		PAT port range	Y	Port range: 10240-51199; NAT ALG: 51200-61199 (Easy IP)/51200-65534 (NAT address)
		NAT aging time	Y	
		Clearing the NAT session table when the link is Down		AR routers support the clearing of the NAT session table when the link is Down
		VRRP binding	Y	Support to bind VRRP instance,only the VRRP state is main to response the ARP request of the NAT address in the address pool.
		Address translation on a specified loopback interface		Address translation can be performed on a specified loopback interface.
		Tanduay Report (TR) 069		AR routers support the configuration of TR069.
		Supported interface types	Y	Interfaces that support NAT include GigabitEthernet interface, cellular interface, dialer interface, serial interface, async interface, ATM interface, BRI interface, PON interface, Eth-Trunk interface, virtual-template interface, virtual-ethernet interface, tunnel interface, MP-group interface, MFR interface, and Ethernet interface.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	NAT ALG			
		DNS	Y	
		DNS mapping	Y	AR routers support DNS mapping during DNS packet parsing. Using DNS mapping, private network addresses of internal servers can be advertised to internal hosts.
		FTP	Y	AR routers support the following functions: Private network hosts access the FTP servers on the public network in PORT mode. Private network hosts access the FTP servers on the public network in PASV mode. Public network hosts access the FTP servers on the private network in PORT mode. Public network hosts access the FTP servers on the private network in PASV mode.
		ICMP	Y	AR routers support these ICMP packets: Destination Unreachable, Time Exceeded, Parameter Problem, Source Quench, Redirect, Echo Request/Reply, Timestamp/Timestamp Reply, Information Request/Information Reply, Address mask Request/Reply, Router Advertisement, Router Solicitation
		RTSP	Y	AR routers support the following functions: Private network hosts access the RTSP servers on the public network. Public network hosts access the RTSP servers on the private network.
		PPTP	Y	Private network PPTP Client call public network PPTP Server Public network PPTP Client call private network PPTP Server
		TFTP	Y	Private network hosts access the TFTP servers on the public network. (TFTP server need not to process inter private network,only config NAT Static/Server.)
		SIP	Y	AR routers support SIP servers only in the following scenarios in the public network: three-party audio and video services, call hold, and call transfer. Support SIP servers on the private network after V2R3C01 and V2R5C00.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	Log			
		Log recording mode	Y	Logs are uploaded to the log server or recorded in a CF card.
		Log format	Y	Binary and text
		Session logs	Y	Session logs record the addresses, port IDs, protocols, NAT information, time, and number of bytes of user sessions.
		Syslog	Y	Syslogs record the addresses, port numbers, protocols, NAT information, time, and number of bytes of user sessions.
	SIP ALG CAC			
		Enable SIP ALG CAC and bandwidth configuration	Y	Enable SIP ALG CAC Config the SIP call bandwidth,then must config limitative bandwidth,otherwise does not limit bandwidth.
		SIP call bandwidth	Y	Support bandwidth statistics to the call that be used SIP and ALG(statistics by the maximum encoding type in the negotiation signaling packet),reject call in that the bandwidth exceed limit.
		QOS process to netstream	Y	Put down call number and netstream address/port/protocol(RTCP) three unit team,when user hook(BYE) or flow table aging to notice QOS recover resources.
NetStream				
	Traffic sampling			
		Traffic analysis interface	Y	AR routers analyze traffic between WAN ports, from LAN ports to WAN ports, and from WAN ports to LAN ports, but do not support traffic analysis between LAN ports.
		Fixed-packet sampling ratio	Y	1-65535
		Random-packet sampling ratio	Y	1-65535
		Fixed-time sampling ratio	Y	5-30000 ms
		Random-time sampling ratio	Y	3-6136 ms
		Maximum processing capability of sampled traffic	Y	All sampled traffic can be processed successfully if the fixed-packet sampling ratio is greater than or equal to 100.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	Original stream			
		RFC3917	Y	IPFIX-Requirements for IP Flow Information
		IPv4 unicast original stream	Y	An IPv4-based unicast original stream can be set up based on the following conditions: Protocol type, ToS, source IP address and port, destination IP address and port, inbound interface index and outbound interface index.
		IPv4 multicast original stream	Y	An IPv4-based unicast original stream can be set up based on the following conditions: Protocol type, ToS, source IP address and port, destination IP address and port, inbound interface index and outbound interface index.
		Flow table setup speed	Y	1.2K/s
		IPv4 original flow specification	Y	AR1200 4K AR2200 16K AR3200 32K
	Flexible NetStream			
		IPv4 flexible NetStream	Y	An IPv4-based flexible stream can be set up based on the following conditions: Layer 3 protocol ID, ToS, destination port, source port, destination IP address, and source IP address.
		Exporting flexible stream statistics	Y	The following information can be set for flexible stream statistics: inbound interface index and outbound interface index, packet quantity, and byte quantity.
		Flexible stream support export DPI information	Y	Set Flexible stream statistics export packet is or not DPI application name and ID.
		Flow table setup speed	Y	1.2 K/s
		IPv4 flexible flow specification	Y	AR1200 4K AR2200 16K AR3200 32K
		Flexible stream template quantity	Y	16

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	Aggregated stream			
		Aggregation based on the AS	Y	AR routers aggregate streams based on source and destination AS IDs.
		Aggregation based on the AS and ToS	Y	AR routers aggregate streams based on source AS ID, destination AS ID, and ToS value.
		Aggregation based on the destination address prefix	Y	AR routers aggregate streams based on destination address prefixes.
		Aggregation based on the destination address prefix and ToS	Y	AR routers aggregate streams based on destination address prefixes and ToS.
		Aggregation based on the source address prefix	Y	AR routers aggregate streams based on source address prefixes.
		Aggregation based on the source address prefix and ToS	Y	AR routers aggregate streams based on source address prefixes and ToS.
		Aggregation based on the source and destination address prefixes	Y	AR routers aggregate streams based on source and destination address prefixes.
		Aggregation based on the address prefixes and ToS	Y	AR routers aggregate streams based on source and destination address prefixes and ToS.
		Aggregation based on the protocol type and port IDs	Y	AR routers aggregate streams based on protocol types and port IDs.
		Aggregation based on the protocol type, port IDs, and ToS	Y	AR routers aggregate streams based on source and destination port IDs, protocol types and ToS.
		Flow table setup speed	Y	It will be tested later.
		IPv4 aggregation stream table size	Y	AR1200 2K AR2200 8K AR3200 16K
	Stream aging			
		Active aging of original streams including flexible streams	Y	1-60 minutes
		Active aging of aggregated streams	Y	1-60 minutes
		Inactive aging of original streams including flexible streams	Y	10-600 seconds
		Inactive aging of aggregated streams	Y	10-600 seconds
		Overflow aging	Y	Aging occurs when the packet size reaches 3.9 GB.
		Original stream aging due to TCP termination	Y	
		Original stream aging speed	Y	1.2K/s

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	Statistics output			
		RFC5101&RFC5102	Y	RFC IPFIX standard,AR routers can export statistics on original streams, aggregated streams, and flexible streams.
		Standards compliance	Y	RFC3954: Cisco Systems NetFlow Services Export Version 9 AR routers can export statistics on original streams, aggregated streams, and flexible streams.
		Cisco NetFlow Export V5	Y	This is a Cisco netflow statistics output format for exporting statistics on IPv4 original streams.
		Cisco NetFlow Export V8	Y	This is a Cisco netflow statistics output format for exporting statistics on IPv4 aggregated streams.
		Exporting IPv4 original stream statistics packets	Y	V5 and V9
		Exporting IPv4 flexible stream statistics packets	Y	V9
		Exporting IPv4 aggregated stream statistics packets	Y	V8 and V9
		Exporting statistics packets to multiple NSCs or NDAs	Y	At most two NDAs
	Maintainability			
		Netstream table cache information	Y	Display information include： 1）Active aging time of streams 2）Inactive aging time of streams 3）Active number of streams 4）Inactive number of streams 5）The time of reset statistics 6）Packet length distribution 7）Protocol packets statistics 8）The ip information of active streams
		Logs and alarms	Y	A trap is transmitted and a log is generated if the number of entries in stream table reaches the maximum number.
		Accelerated stream table aging	Y	The idle aging time is 2/3 of the preset aging time if the number of stream tables reaches 70% of the maximum number. The idle aging time is 1/2 of the preset aging time if the number of stream tables reaches 75% of the maximum number. The idle aging time is 0 if the number of stream tables reaches 80% of the maximum number.
		Key information query	Y	AR routers support NetStream information query. They support query for original streams, aggregated streams, flexible streams, and resource usage in group-based key mode. AR routers support query for statistics on streams that are discarded due to the failure to set up stream tables.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
ARP				
	Basic ARP			
		RFC826	Y	Ethernet Address Resolution Protocol
		Broadcasting ARP Request packets	Y	1. The AR broadcasts ARP Request packets if an ARP Miss message is reported. 2. The AR broadcasts gratuitous ARP Request packets. 3. The AR broadcasts ARP Request packets in ARP probe.
		Unicasting ARP Request packets	Y	The AR unicasts ARP Request packets in ARP aging detection using commands.
		Unicasting ARP Reply packets	Y	The AR unicasts ARP Reply packets after receiving an ARP Request packet with the destination IP address as a gateway address.
		Broadcasting ARP Reply packets	Y	The AR broadcasts a gratuitous ARP Reply packet after receiving a gratuitous ARP Request packet with the destination IP address as a gateway address. Note: Currently, gratuitous ARP Reply packet are broadcast in V5.
		Gratuitous ARP packets	Y	A gratuitous ARP packet has the same source and destination IP addresses.
		Address conflict detection by means of gratuitous ARP packets	Y	The AR broadcasts a gratuitous ARP Reply packet after receiving a gratuitous ARP Request packet with the destination IP address as a gateway address.
		Sending gratuitous ARP packets upon a VRRP active/standby switchover	Y	After a VRRP active/standby switchover is performed, the master device broadcasts a gratuitous ARP packet, requesting devices in the broadcast domain to update ports in ARP entries.
		Learning ARP Request packets	Y	ARP entries are updated regardless of whether destination IP addresses in ARP packets are gateway addresses.
		Learning gratuitous ARP packets	Y	The AR learns and updates ARP entries when receiving ARP Request packets from the same network segment.
		Learning ARP Reply packets	Y	1. The AR learns ARP Reply packets after transmitting ARP Request packets. 2. The AR learns ARP entries only when the destination IP address in ARP Reply
		ARP aging mechanism	Y	By default, an ARP probe packet is transmitted for three times consecutively every 5 seconds and after an ARP entry is
		ARP aging time	Y	The default aging time is 20 minutes and

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Number of ARP probe times	Y	1. The default number of ARP probe times is three. 2. The number of ARP probe times is adjustable. 3. If the number of ARP probe times is, an ARP entry is aged out immediately.
		ARP probe mode	Y	1. ARP probe packets can be unicasted by means of commands.
		Static ARP configuration	Y	A static ARP entry specifies the mapping between the IP address and the MAC address.
		Static ARP entries on the main interface	Y	IP addresses and MAC addresses must be specified in static ARP entries on the main interface.
		Static ARP entries on a VLANIF interface	Y	1. IP addresses, MAC addresses, VLAN IDs, and outbound interfaces must be specified in static ARP entries on a VLANIF interface. 2. Static ARP entries on a VLANIF interface must contain the outbound interface
		Static ARP entries on a dot1q termination interface	Y	1. IP addresses, MAC addresses, VLAN IDs, and outbound interfaces must be specified in static ARP entries on a dot1q termination interface. 2. A sub-interface configured with dot1q
		Static ARP entries in a VPN instance	Y	1. The **arp static 60.0.0.2 1-1-1 vpn-instance vpna** command can be run on the Layer 3 interface. 2. A VPN instance does not need to be specified if the outbound interface is specified. 3. On dot1q and VLANIF interfaces,
		Deleting static ARP entries	Y	1. Static ARP entries in the system can be deleted. 2. Static ARP entries can be deleted based on the specified IP address.
		Deleting dynamic ARP entries	Y	1. Dynamic ARP entries in the system can be deleted. 2. Dynamic ARP entries can be deleted based on the specified Layer 3 interface. 3. A dynamic ARP entry can be deleted based on the specified IP address and interface number.
		Deleting all ARP entries	Y	The system deletes all ARP entries,
		Deleting ARP entries on logical interfaces	Y	If Layer 3 logical interfaces such as the Eth-Trunk, VLANIF, VE, and dot1q interfaces are deleted, their ARP entries are deleted accordingly.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Address conflict detection	Y	1. ARP address conflict detection must be enabled. 2. After receiving ARP Request packets about address conflicts, the system reports an address conflict message and transmits a gratuitous ARP Reply packet. 3. After receiving ARP Reply packets about address conflicts, the system reports an address conflict message but does not transmit a gratuitous ARP Reply packet.
		Address conflict timer	Y	1. The AR starts the address conflict timer and transmits a gratuitous ARP Request packets 5 seconds later after detecting address conflicts. 2. The address conflict timer transmits the
		Address conflict detection log	Y	The AR records address conflict information
		ARP entry query	Y	The system displays ARP entries in the system, on a specified interface, in a specified VPN instance, or based on the specified wildcard.
		ARP entry display	Y	1. ARP entries are displayed as follows: IP ADDRESS, MAC ADDRESS, EXPIRE(M), TYPE, INTERFAce [PVC], VPN-INSTANce, [VLAN/ceVLAN] 2. EXPIRE(M): indicates the validity period of ARP entries, in minutes. 3. TYPE VLAN/ceVLAN: indicates the entry type. The options are as follows: D: dynamic
		ARP packet statistics	Y	You can view the ARP packet statistics in the system.
		ARP entry statistics	Y	
		ARP-related functions in a L3VPN	Y	1. ARP entries are associated with VPN instances. 2. The AR supports all ARP-related functions after an AR interface is bound to a
		Sending gratuitous ARP packets if the VLANIF interface is in the up state	Y	The AR sends gratuitous ARP packets if the VLANIF interface is in the up state.
		Layer 2 topology detection	Y	Layer 2 topology detection enables the system to update all the ARP entries in the VLAN that a Layer 2 interface belongs to when the Layer 2 interface status changes from Down to Up.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	ARP Proxy			
		ARP proxy anti-attack	Y	The proxy gateway does not learn ARP entries directly. It sends ARP requests to the source address to learn ARP entries only after the destination address returns an ICMP response. This mechanism helps protect the gateway from attacks.
		Routing gateway proxy	Y	If the destination address is reachable and the outbound port is not the local port, AR router returns a response as a proxy.
		Intra-VLAN proxy	Y	Requirements: The destination address and gateway address are in the same network segment. If the destination ARP entry already exists, a response is returned directly. If the destination ARP entry does not exist, a packet is broadcast in the VLAN, and a response is returned after the destination ARP entry is learned; no response is returned if the destination ARP fails to be learned. Intra-VLAN proxy is supported by VLANIF interfaces and super VLANs, but is not supported by Ethernet sub-interfaces and Eth-trunk member interfaces.
		Inter-VLAN proxy	Y	Requirements: The destination address and gateway address are in the same network segment. If the destination ARP entry already exists, a response is returned directly. If the destination ARP entry does not exist, a packet is broadcast in sub-VLANs except the local VLAN, and a response is returned after the destination ARP entry is learned; no response is returned if the destination ARP fails to be learned. Inter-VLAN proxy is supported by super VLANs and VLANIF interfaces.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	ARP Ping			
		ARP Ping ip	Y	Check whether an IP address is used by another device on the network. If so, the MAC address of that device is obtained.
		ARP Ping mac	Y	Check whether a MAC address is used by another device on the network. If so, the IP address of that device is obtained.
IPv4 protocol suite				
	IPV4 forwarding			
		Interface address	Y	1. Only class A, class B, and class C addresses can be configured. 2. The length of subnet masks (except for natural subnet masks) is configurable. 3. IP addresses with 32-bit subnet mask can be configured for the loopback interface.
		Primary address and secondary address	Y	
		Address negotiation on an interface	Y	An interface can obtain IP address using DHCP. An interface can obtain IP address using BOOTP. An interface can obtain IP address using PPP.
		IP address unnumbered	Y	
		Address overlapping between VPNs	Y	Each VRF is configured with an address space.
		The IP address with a 31-bit mask can be set for the interface.	Y	
		The IP address with a 32-bit mask can be set for the interface.	Y	
		Fragment reassemble timeout interval	Y	30s
		Fragment reassemble queue length	Y	1000
		Number of fragment reassemble queues	Y	400
	IP options			
		Source Route option	Y	
		Strict source route option	Y	
		Loose source route option	Y	
		Timestamp option	Y	
		Route Alert option	Y	
		Option length	Y	40 bytes
		Controlling the processing of source route options for IP packets	Y	

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	ICMP			
		RFC 792	Y	
		RFC 950	Y	
		RFC1256	Y	
		Processing ICMP error packets	Y	
		Processing ICMP request packets	Y	
		Processing ICMP redirection packets	Y	
	TCP			
		TCP	Y	RFC793 Transmission Control Protocol
	UDP			
		UDP	Y	RFC768 User Datagram Protocol
	Socket			
		Standard APIs	Y	
		Multi-instance	Y	
	PING			
		IP PING	Y	The IP ping function is configured by means of commands. AR routers transmit ping packets to check network connectivity and host connectivity.
		Ping parameters	Y	You can specify the domain name of the target host.□ You can specify the destination IP address.□ -a: indicates the source IP address. -c: indicates the number of times packets are sent,□ -d: sets the socket in debug mode. -f: indicates that packets are not fragmented when they are sent. -h: indicates the TTL value of the request packet. -i: indicates the outbound interface.□ -m: specifies the waiting time for sending the next Request packet. -n: Uses the value of *host* as the IP
		VRF PING	Y	
		Response PING fast	Y	Response echo request fast

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	TRACERT			
		IP TRACERT	Y	The IP tracert function is configured by means of commands. AR routers transmit tracert packets to check network connectivity and locate network faults.
		Parameters	Y	You can specify the domain name of the target host. You can specify the destination IP address. -a: indicates the source address. -f: indicates the initial TTL value. -m: indicates the maximum TTL value. -name: indicates the host name of each hop. -p: indicates the port number. -q: indicates the number of packets. -w: indicates the timeout interval.
		VRF tracert	Y	A VRF name can be specified in the tracert command.
	IP source address check			
		Packets with invalid source addresses are discarded	Y	The validity of source addresses in packets is checked during packet receiving. The following source addresses are considered as invalid addresses: 1. IP addresses with all 0s (the destination IP address is not all 1s) or 1s 2. Multicast addresses (class D addresses) and class E addresses 3. Loopback addresses (format: 127.x.x.x) not generated by the local device 4. Class A, B, and C broadcast addresses 5. Broadcast address in the same subnet as the address of the inbound interface
		Statistics on packets with invalid source IP addresses	Y	You can run the display ip interface command to display statistics on packets with invalid source addresses, and run the reset ip statistics command to clear the statistics.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	Broadcast packet forwarding			
		Controlling broadcast packet forwarding on a specified interface	Y	A packet is forwarded and a response is returned to the local device when the following conditions are met: (1) The packet is a broadcast packet of the outbound interface and is not sent by the local device. (2) The ip forward-broadcast command is run and the packet matches the ACL. If the packet does not match the ACL, the packet is not forwarded and a response is returned to the local device. If the ip forward-broadcast command is not run, the packet is not forwarded.
		Statistics on broadcast packets	Y	You can run the **display ip interface** command to view directed broadcast packets that are received, transmitted, forwarded, and discarded by interfaces, and run the reset ip statistics command to clear statistics.
	Load balancing			
		Using CLI to globally configure the load balancing algorithm for IP packet forwarding	Y	Based on flows or number of packets
		Unequal-Cost Multiple Path (UCMP)	Y	Interfaces supporting UCMP: Layer 3 Ethernet interface, synchronous/asynchronous serial interface, ATM interface, BRI interface, 3G interface, dialer interface, VLANIF interface, Layer 3 Eth-Trunk, VE interface, MP-group, and MFR. This function is not supported by all types of sub-interfaces.
	DF flag clearance			
		Forcible packet fragment on outbound interface	Y	Packets are fragmented and the DF flag is cleared if the following conditions are met: (1) The DF is 1. (2) The packet length exceeds the MTU of the outbound interface. If the DF of packets is 1 but the packet length does not exceed the MTU of the outbound interface, the packets are not fragmented.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	Policy-based routing			
		Selecting routes based on policies	Y	(1) Based on packet length; (2) Based on ACL
		Actions in routing policy	Y	(1) Set packet priority. (2) Specify the next hop. (3) Specify the outbound interface.
		Default actions in routing policy	Y	(1) Specify the default next hop. (2) Specify the default outbound interface.
		Local policy-based routing	Y	Only applied to locally sent packets.
		Policy-based load balancing	Y	A policy can contain multiple apply clauses.
		Specifying accessible VPN instances	Y	
		Number of policy routes	Y	The number should be within 100 for the sake of query efficiency.
		Node quantity for each policy route	Y	The node quantity should be within 20 for the sake of query efficiency.
DNS				
	DNS Client			
		RFC1034	Y	Domain Names--Concepts and Facilities
		RFC1035	Y	Domain Names--Implementation and
		Static DNS	Y	The mapping between domain names and IP addresses is set up manually in the static DNS resolution table. The functions of this table are similar to those of the hosts file on Windows 9x. If a client requires the IP address corresponding to a domain name, the client obtains the IP address from the static DNS resolution table.
		Adding domain name suffixes automatically	Y	AR routers support the function of resolving the list of dynamic domain suffixes. You can set certain domain name suffixes in the list in advance. When a domain name is resolved, you need to enter only some fields of the domain name and the system automatically adds different suffixes for resolution.
		Transmitting query packets of type A	Y	AR routers can transmit DNS query packets of type A.
		Receiving and parsing query responses	Y	AR routers can monitor and receive responses from the DNS server and resolve them correctly.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Querying information in the dynamic cache	Y	If the TTL of the responses is greater than 1 and the cache is not full, AR routers record query results. If the cache is full, they overwrite the earlier record with the latest record. If the same information is queried, AR routers do not need to query the information in the DNS server but return the required IP address to the query program.
		Timed aging of cached information	Y	The TTL of cached information indicates how long query results can be cached on the client. The unit is 3 seconds. That is, the TTL value is reduced by three every second. The cached information is deleted if its TTL value is reduced to zero.
		Client can send source IP address of DNS packet	Y	
		Reverse resolution function, that is, PTR-type query (query for domain names based on IP addresses)	Y	
		SRV query	Y	
		NAPTR query	Y	
		Static DNS server	Y	
		Dynamic DNS server	Y	1. DNS server can be obtained by using PPP client. 2. DNS server can be obtained by using DHCP client.
		Querying domain names based on priorities in descending order using voice	Y	The AR supports the query of domain names based on priorities in descending order using voice.
		Serial and parallel query	Y	Support serial and parallel query mode，default mode is parallel query，send request to the configure servers，select the priority echo.
	DNS PROXY/RELAY			
		Forwarding query packets	Y	Query packets include the packets of type A, PTR type, SRV type, and NAPTR type
		Setting aging time of forwarding entries	Y	
		The DNS proxy searches for query packets of type A and PTR type in the DNS cache, and constructs a response.	Y	
		The DNS relay only forwards query packets	Y	
		Giving a DNS spoofing response to query packets of type A	Y	An IP address is configured.
		Query multiple domain names in a single query request	Y	
		Send overtime and times of a query request to IPV4 DNS servers	Y	support send overtime and times of a query request to IPV4 DNS servers
		Insert local voice server for the local phone DNS query	Y	Suppoert insert local voice server address for the local phone DNS query

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	DDNS			
		DDNS client	Y	
		DDNS policy applied on an interface	Y	
		Configurable interval for refreshing policies	Y	
		Communicating with service providers over HTTP	Y	Currently, routers can communicate with only 3322 DDNS service providers.
		Communicating with service providers over TCP	Y	Currently, routers can only communicate with Oray DDNS service provider.
		Heartbeat mechanism	Y	
		Manually triggering DDNS policy refresh	Y	
		Manually triggering interface-based DDNS policy refresh	Y	
	DNS6 Client			
		IPv6 static DNS entry	Y	You can manually establish the mappings between domain names and IPv6 addresses in the IPv6 static DNS resolution table. The client can find the required IPv6 address by checking the domain name in the table.
		AAAA query on suffix adding	Y	You can pre-configure some suffixes of domain names in the dynamic DNS resolution table. You need to input only part of the domain name, and the system automatically displays the complete domain name with different suffixes for resolution.
		Configuring the source IPv6 address of the DNS packet to be sent	Y	The source IPv6 address specified for the DNS packet to be sent to the IPv6 DNS server.
		Sending Class-AAAA query packets	Y	The AR can send Class-AAAA query packets.
		IPv6 RARP	Y	The AR supports query from IPv6 addresses to domain names.
		Requesting query results from the IPv6 DNS server.	Y	The AR can request query results from the IPv6 DNS server.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		IPv6 dynamic query on the buffer	Y	When the buffer is not full, the query result of the Response packet with the TTL value greater than 1 is recorded in the buffer. If the buffer is full, the query result of the Response packet with the TTL value greater than 1 overwrites the oldest entry in the buffer. In this way, to query the same information, the AR responses the IP address to the program without query on the DNS server.
		Aging of IPv6 information in the buffer	Y	The TTL value in the buffer indicates the lifetime of the information. The unit is 3 seconds. The TTL value deduces 3 every second. When the TTL value is 0, the information is deleted from the buffer.
		Static IPv6 DNS server	Y	You can configure the IP address of the IPv6 DNS server using command lines.
		Domain name suffixes in ND packets	Y	DNS modules can use dynamic domain name suffixes in ND packets.
		IPv6 dynamic DNS server addresses in ND packets	Y	DNS modules can use the IPv6 dynamic DNS server addresses in ND packets.
		IPv6 dynamic DNS server addresses in DHCPv6 messages	Y	DNS modules can use the IPv6 dynamic DNS server addresses in DHCPv6 messages.
		Aging of DNS domain name suffixes and IPv6 DNS server addresses	Y	DNS domain name suffixes and IPv6 DNS server addresses in ND packets have lifetime. The TTL value indicates the lifetime of DNS domain name suffixes and IPv6 DNS server addresses. The unit is 3 seconds. The TTL value deduces 3 every second. When the TTL value is 0, the DNS domain name suffixes and IPv6 DNS server addresses are deleted from the buffer.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	DNS6 PROXY/RELAY			
		DNS proxy query mode: 1. AAAA query 2. A6 query 3. IPv6 PTR query	Y	The DNS proxy supports AAAA, A6, and IPv6 PTR query. Reply packets are buffered and can be used to reply user requests.
		Query request forwarding	Y	On an IPv6 network, the DNS relay agent forwards query requests from users, but does not query the buffer or buffer query results.
		Spoofing users in AAAA and A6 query	Y	When DNS is not enabled or no route can reach the DNS server, a configured IPv6 address can be used in AAAA and A6 query to spoof users.
		Specifying the source IPv6 address for query packets in forwarding	Y	The source IPv6 address can be specified for query packets when the DNS proxy/relay forwards query packets.
		Receiving DNS query requests from clients with IPv6 addresses	Y	The AR can process DNS query requests from clients with IPv6 addresses
		Requesting query results from the IPv6 DNS server	Y	The AR can request DNS queries from the IPv6 DNS server. If failing to request from the IPv6 DNS server, the AR request from the IPv4 DNS server.
VRRP				
	VRRP4			
		RFC3768	Y	Virtual Router Redundancy Protocol
		Master/Backup VRRP	Y	1. The AR supports VRRP backup groups formed by virtual routers. A VRRP backup group consists of one master router and several backup routers. 2. All upstream service flows are transmitted by the master router. When the master router fails, a backup router takes over traffic. 3. Downstream service flows can be transmitted by either the master router or backup routers as required by the upstream router. 4. When changing its VRRP status to Master, an interface sends gratuitous ARP packets to request the devices in broadcast domain to update MAC address entries and ARP entries, and deletes ARP entries corresponding to local virtual MAC addresses.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Load balancing	Y	1. If multiple VRRP groups are created on multiple devices and the master routers of these VRRP groups are deployed on different routers, traffic is load balanced. 2. If different VRRP groups are configured on the same interface, traffic is load balanced on the same interface.
		VRRP status switchover	Y	VRRP defines three status types: Master, Backup, and Initial.
		VRRP group priority	Y	The default VRRP priority is 100. The VRRP priority can be adjusted within the value range. The greater the value, the higher the priority.
		VRRP preemption	Y	Preemption/non-preemption/delay preemption
		Interval for sending VRRP packets	Y	The interval for sending VRRP packets can be adjusted based on the VRRP virtual router ID. By default, the interval is 1s. The interval can be set within the value range. Note: VRRP packets are sent by the master router. Backup routers only receive VRRP packets.
		Learning the interval for sending VRRP packets	Y	By default, the device is enabled to learn the interval for sending VRRP packets. If the timers on the master and backup routers are different, the backup router adjusts the timer value based on the timer on the master router.
		VRRP packet encapsulation	Y	1. The destination MAC address is 01-00-5E-00-00-12. 2. The source MAC address is the virtual MAC address 00-00-5E-00-01-{VRID} (in hexadecimal) 3. The source IP address is the IP address of the interface (the primary IP address). 4. The destination IP address is a multicast address 224.0.0.18. 5. Fields in the VRRP packets are filled based on the configuration.
		Processing VRRP error packets	Y	When receiving a VRRP packet, an interface checks the following items to determine whether the packet is an error packet: 1. The TTL value is 255. 2. The Version value is 2. 3. The VRID is the same as the local VRID and the local port is not the IP address owner. 4. Authentication mode and parameters are the same as the local authentication mode and parameters. 5. Timer negotiation is performed. Note: 1. Devices of some vendors do not send TTL based on RFC. You can disable TTL detection on the interface. 2. After the undo timer-advertise learning command is executed, if the timers on the master and backup routers are different, negotiation fails.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Authentication	Y	By default, a VRRP group uses non-authentication. The simple authentication and MD5 authentication are supported.
		Pinging virtual addresses	Y	1. By default, a VRRP virtual IP address advertises 32-bit routes. VRRP virtual IP addresses can be pinged successfully. 2. The pinging virtual IP address function can be disabled using command lines.
		Broadcasting gratuitous ARP packets	Y	When changing its VRRP status to Master, an interface sends gratuitous ARP packets to request the devices in broadcast domain to update MAC address entries and ARP entries, and deletes ARP entries corresponding to local virtual MAC addresses.
		VRRP version switchover	Y	VRRPv2 and VRRPv3 can be switched globally or based on VRID. The default VRRP version is VRRPv2.
		VRRPv3 Advertisement packet sending	Y	1. The mode in which VRRPv3 Advertisement packets are sent can be configured globally. The router can send only VRRPv2 Advertisement packets, only VRRPv3 Advertisement packets, or both VRRPv2 and VRRPv3 Advertisement. 2. The mode in which VRRPv3 Advertisement packets are sent can be configured based on the VRID. The router can send only VRRPv2 Advertisement packets, only VRRPv3 Advertisement packets, or both VRRPv2 and VRRPv3 Advertisement. 3. Configurations based on the VRID take preference over the global configurations. 4. By default, the router running VRRPv3 sends VRRPv3 Advertisement packets.
		VRRPv3 compatibility with VRRPv2	Y	If a router runs VRRPv3, it is compatible with VRRPv2.
		VRRP on an L3VPN	Y	An interface bound to an L3VPN supports all VRRP basic functions.
		VRRP in a super-VLAN	Y	
		Multiple VRID in different interface	Y	1、Support multiple VRID in different interface 2、Support multiple physical interface/sub interface in a interface

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	VRRP4 association			
		Association between VRRP and BFD sessions	Y	BFD is used to detect the link between the master and backup VRRP routers and notifies the VRRP group if a fault occurs on the link. Then the backup VRRP router increases its priority and fast switchover is performed.
		Association between VRRP and NQA	Y	VRRP tracks the NQA status.
		Association between VRRP and IP routes	Y	VRRP tracks the reachability of a single IP route.
		Association between VRRP and interfaces	Y	When the uplink interface that is tracked by VRRP goes Up or Down, the priority of the router automatically changes by a certain value (can be configured). Routers in the VRRP group detect faults on the uplink interface and then the VRRP routers re-compete with each other to be the master router.
		VRRP flapping suppression	Y	1. VRRP flapping suppression is performed on flapping that can be detected by VRRP on the interface or track interface. VRRP responds fast when the interface goes Down and slowly when the interface goes Up. By default, VRRP flapping suppression is disabled. Messages can be suppressed within 1s. 2. VRRP responds for a certain delay when the interface goes Up. During the period, VRRP does not respond to other Up events. If a Down event is received, the Up event is cancelled. 3. After the delay expires, if the last event is an Up event, an Up message is simulated for processing; if the last event is a Down event, no processing is performed.
		Priority of the IP route associated with VRRP	Y	When the router is not the master router in the VRRP backup group, the cost of the direct route on the route must be adjusted.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	VRRP6			
		Master/Backup VRRP6	Y	Same as VRRP4
		Load balancing	Y	Same as VRRP4
		VRRP6 status switchover	Y	Same as VRRP4
		Setting priorities	Y	Same as VRRP4
		VRRP6 preemption	Y	Same as VRRP4
		Interval for sending VRRP6 packets	Y	Same as VRRP4
		Pinging virtual addresses	Y	Same as VRRP4
		Broadcasting ND packets	Y	1. ND packets are sent during VRRP6 switchover to request devices in the broadcast domain to update ND entries and MAC address entries. 2. Periodical sending of ND packets can be enabled or disabled using the command which is also used to send gratuitous ARP packets.
		VRRP Version 3	Y	VRRP6 is implemented on VRRPv3 draft. Therefore, VRRP6 cannot be switched to VRRPv2 and is compatible with VRRPv2. VRRPv2 Advertisement packets are discarded on the router running VRRP6.
	VRRP6 association			
		VRRP track interface	Y	Note: VRRP6 is associated with IPv4 protocol status, not IPv6 protocol status.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
BFD				
	Basic BFD			
		Static BFD	Y	1. Static BFD session with the session ID specified manually 2. Static BFD session with the negotiated session ID
		Dynamic BFD	Y	Dynamic BFD session triggered by protocol packets
		BFD in asynchronous mode	Y	
		BFD for single-hop link	Y	
		BFD for multi-hop link	Y	
		Dynamically modifying BFD parameters	Y	The parameters of a BFD session can be modified, including expected receiving interval, expected sending interval, local detection multiplier, and WTR.
		BFD session creation after a delay	Y	A BFD session is set up after a delay if the router restarts or the board associated with the BFD session is hot swapped.
		Port number of multi-hop BFD session	Y	Option: 3784, 4784
		Multicast BFD	Y	
		BFD echo	Y	
		BFD packets sent by hardware	Y	Multi-core CPU forwarding engine is used to send BFD packets.
	BFD application			
		BFD for interface	Y	Association between the BFD session status and interface status is supported.
		BFD for VRRP	Y	Association between VRRP track and automatically negotiated BFD session is supported.
		BFD for VRF	Y	BFD can be bound to VPN4, and BFD packets are sent on a specified VPN.
		BFD for interface backup	Y	Association between interface backup track and automatically negotiated BFD session is supported.
		BFD for static routes	Y	Association between static track and automatically negotiated BFD session is supported.
		BFD for RIP	Y	Static BFD for RIP is supported. Dynamic BFD for RIP is supported.
		BFD echo function	Y	BFD echo function is supported.
		BFD for OSPF	Y	Dynamic BFD for OSPF is supported.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		BFD for IS-IS	Y	Static BFD for IS-IS is supported. Dynamic BFD for IS-IS is supported.
		BFD for BGP	Y	Dynamic BFD for BGP is supported.
		BFD for PIM (IPv4)	Y	Dynamic BFD for PIM is supported.
		Dynamic BFD for RSVP-TE	Y	Dynamic BFD for RSVP-TE is supported.
		Static BFD for static LSP	Y	Static LSP can be bound to BFD.
		Static BFD for LDP LSP	Y	BFD sessions can be bound to LDP LSP.
		Static BFD for CR LSP	Y	Static BFD detects static CR LSPs or RSVP CR-LSP.
		Static BFD for TE tunnel	Y	BFD detects the MPLS TE tunnel.
		Dynamic BFD for LDP LSP	Y	LDP LSPs can dynamically set up, delete, or update BFD sessions.
		Dynamic BFD for CR-LSP	Y	RSVP CR LSPs can dynamically set up, delete, or update BFD sessions. Static CR LSPs can dynamically set up, delete, or update BFD sessions.
		BFD for PST	Y	When a BFD session detects a fault, the interface status in the port state table (PST) is changed, which triggers FRR switchover.
NQA				
	NQA version			
		Support Software NQA	Y	Send and response NQA detect packet in the control plane
		Support Hardware NQA	Y	Send and response NQA detect packet in the data plane
		Support IP SLA Responser	Y	Support send response for Cisco IP SLA detect packet
	NQA association			
		NQA associated with VRRP	Y	VRRP monitors NQA status
		NQA associated with interface backup	Y	NQA is associated with interface backup.
		NQA associated with policy-based routing	Y	NQA is associated with policy-based routing.
		NQA associated with static routes	Y	NQA is associated with static routes.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	ICMP test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 3s.
		Setting the interval at which probe packets are sent	Y	Value range: 1-60s The default value is 4s.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	Value range: 1-15 The default value is 3.
		Destination IP address (ipaddress)	Y	IPv4
		Destination IPv6 address	Y	
		Size of the data field in detection packets (datasize)	Y	Value range: 0-8100 The default value 0 indicates that the size of the data field is not set.
		Service type of packets (tos)	Y	
		VPN instance name (L3VPN)	Y	
		Source interface for transmitting packets	Y	
		Not querying routes in routing entries	Y	Only IPv4 addresses support this function. By default, this function is not set.
		Adopting forcible IP forwarding for the head	Y	By default, the function is not supported. IP forwarding and VPN ping are not supported for TE tunnel outbound interfaces and BGP-matched routes.
		Initiating tests for an outbound interface that is a trunk member port	Y	You can run the source-interface command to configure the function. The Layer 3 IP trunk or Ethernet trunk member ports of direct links can be tested. 1. You need to run the trunk member-port-inspect command to enable the trunk member port to respond to echo packets at the destination. 2. Layer 2 trunk ports and their member ports are not tested. 3. This test is applicable only to IPv4 addresses.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	UDP test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 3s.
		Setting the interval at which probe packets are sent	Y	Value range: 1-60s The default value is 4s.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	Value range: 1-15 The default value is 3.
		Destination IP address (ipaddress)	Y	IPv4
		Destination port (port)	Y	Value range: 1-50000
		Size of the data field in detection packets (datasize)	Y	Value range: 0-8100. Default: 0, indicating not configured.
		Service type of packets (tos)	Y	
		VPN instance name (L3VPN)	Y	
		Viewing UDP test results (delays in both directions) through the CLI and MIB	Y	
	SNMP test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 3s.
		Setting the interval at which probe packets are sent	Y	Value range: 1-60s The default value is 4s.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	Value range: 1-15 The default value is 3.
		Destination IP address (ipaddress)	Y	IPv4
		VPN instance name (L3VPN)	Y	
	TCP test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 3s.
		Setting the interval at which probe packets are sent	Y	Value range: 1-60s The default value is 4s.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	Value range: 1-15 The default value is 3.
		Destination IP address (ipaddress)	Y	IPv4
		Destination port (port)	Y	Value range: 1-50000
		Service type of packets (tos)	Y	
		VPN instance name (L3vnp)	Y	
		Viewing TCP test results (connection delay) through the CLI and MIB	Y	

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	UDP jitter test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		Jitter packet version	Y	The size of jitter packets in earlier version is 68, 100, or 172. It can communicate with the NQA servers running either of the two versions. The size of a jitter packet in later version ranges from 20 to 8100. When the jitter test of later version is used, the device can communicate with only the NQA server running the later version. The device running the later version can communicate with H3C devices running the later version. The size of a jitter packet in earlier version is the same as the size of the HWPING jitter packet. The jitter packet version can be configured using MIB or CLI. The value 1 indicates the earlier version. The value 2 indicates the later version.
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 3s.
		Setting the interval at which probe packets are sent	Y	Value range: 20-60000 ms The default value is 20 ms.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	Value range: 1-15 The default value is 3.
		Setting the number of test packets sent in each probe of	Y	Value range: 1-3000 The default value is 20 and test instance 1 is not supported.
		Destination IPv6 address	Y	The destination IPv6 address cannot be a broadcast address or link-local address.
		Destination IP address (ipaddress)	Y	IPv4
		Destination port (port)	Y	Value range: 1-50000
		Size of the data field in detection packets (datasize)	Y	Value range: 0-8100. Default: 0, indicating not configured.
		Service type of packets (tos)	Y	
		VPN instance name (L3VPN)	Y	
		Number of packets that can be transmitted consecutively in a single test instance (3000)	Y	The packets are the traffic of simulated voice service. Packets are transmitted by the control board. Router performance is affected if the packet quantity exceeds 3000.
		Viewing UDP jitter historical records through the CLI and MIB	Y	The historical table records only packets that are transmitted successfully.
		Viewing UDP jitter test results through the CLI and MIB	Y	Statistics on the unidirectional packet loss (including the SD, DS, and unknown direction) and on the unidirectional delay threshold are supported in a jitter test in V500R003C08 and V500R003C07B200.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Viewing UDP jitter accumulated test results through the CLI and MIB	Y	The results of jitter tests are accumulated.
		Transmitting packets by an interface board	Y	By default, packets are transmitted by software. You can run the hardware-based enable command to enable an interface board to transmit packets.
		Statistics on 1588v2 time stamps	Y	The default unit is ms. You can run the timestamp-unit command to set the time stamp unit.
		Initiating tests for an outbound interface that is a trunk member port	Y	You can run the source-interface command to configure the function. The Layer 3 IP trunk or Ethernet trunk member ports of direct links can be tested. 1. You need to run the trunk member-port-inspect command to enable the trunk member port to respond to echo packets at the destination. 2. Layer 2 trunk ports and member ports are not tested. 3. This test is applicable only to IPv4 addresses.
	FTP test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		FTP test type	Y	get, put
		FTP user name	Y	
		FTP password	Y	
		FTP file path	Y	
		FTP file size	Y	Value range: 1-10000 KB. Default: 1000 KB
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 15s.
		Setting the interval at which probe packets are sent	Y	The value cannot be set.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	The value cannot be set.
		Destination IP address (ipaddress)	Y	IPv4
		VPN instance name (L3VPN)	Y	
		FTP get operation specification	Y	FTP get: indicates that a client downloads a file from the server but not save it. The
		FTP put operation specification	Y	FTP put: indicates that a client uploads a file to the server is the specified file exists or uploads a created file to the server if the specified file does not exist. This operation saves segments. The upload time and file
		Viewing FTP test results (FTP control connection time, data connection time, total time, and size of transferred files) through the CLI and MIB	Y	

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	HTTP test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		HTTP test type	Y	get, post
		HTTP URL	Y	
		HTTP version number	Y	V1.0/V1.1 (V1.1 for VRP V5R3R3B03D051)
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 3s.
		Setting the interval at which probe packets are sent	Y	The value cannot be set.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	Value range: 1-15 The default value is 3.
		Timeout duration of detection packets (timeout)	Y	IPv4, URL
		Interval for transmitting detection packets (interval)	Y	
		VPN instance name (L3vnp)	Y	
	DHCP test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 15s.
		Setting the interval at which probe packets are sent	Y	The value cannot be set.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	Value range: 1-15 The default value is 3.
		Outbound interface	Y	
		Source interface for transmitting packets	Y	
		Viewing DHCP test results (delays in both directions) through the CLI and MIB	Y	
	Trace test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 3s.
		Setting the interval at which probe packets are sent	Y	The value cannot be set.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	Value range: 1-10 The default value is 3.
		Destination IP address (ipaddress)	Y	IPv4
		Destination IPv6 address	Y	The destination IPv6 address cannot be a broadcast address or link-local address.
		Initial TTL value	Y	Value range: 1-255. Default: 1
		Viewing trace test results (delays in both directions of each hop) through the CLI and MIB	Y	
		VPN instance name (L3VPN)	Y	

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Fragmentation settings	Y	Only IPv4 addresses support this function. By default, this function is not set.
		Skipping routing entries	Y	Only IPv4 addresses support this function. By default, this function is not set.
		Specifying the pipe mode for initiating tests	Y	You can run the ttl-copymode command to configure the test. In the L3VPN scenario, the pipe mode is specified in an NQA trace test and the TTL value of the MPLS label for transmitted packets is 255.
	DNS test			
		CLI configuration mode	Y	
		MIB configuration mode	Y	
		Setting the timeout interval of	Y	Value range: 1-60s The default value is 3s.
		Setting the interval at which probe packets are sent	Y	The value cannot be set.
		Setting the probe frequency	Y	Value range: 1-604800s The default value is 0.
		Setting the probe count	Y	The value cannot be set.
		Destination IP address (ipaddress)	Y	URL
		Viewing DNS test results (DNS resolution time) through the CLI and MIB	Y	
	Storage of NQA client test results			
		Storing NQA test results on the FTP server over FTP	Y	AR routers send test results to the NQA FTP module for transmitting test results after one test instance is complete. The NQA FTP module buffers the test results. When the number of test results to be delivered reaches the threshold or timeout occurs, the NQA FTP module starts an FTP connection and sends test results to the FTP server to save as .txt files. The files are named as follows: specified file name+yyyymmdd+hhmmss. If the number of transmitted test results reaches the preset threshold, another file is created to store test results. If an FTP connection fails to be started and the buffer is full, the latest test result overwrites the earliest test result.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	Scheduling of NQA test instances			
		Start mode of a test instance: immediate	Y	
		Start mode of a test instance: scheduled	Y	
		Start mode of a test instance: restart	Y	
		Stop mode of a test instance: immediate	Y	
		Stop mode of a test instance: scheduled	Y	
		Deletion mode of a test instance: deleting a single test that is not in the running state	Y	
		Deletion mode of a test instance: deleting all test instances	Y	
		Deletion mode of a test instance: setting aging time of the test instance	Y	
		Automatic delay feature applied to all test instances (except test groups)	Y	Tests of certain types cannot be performed concurrently because the NMS does not support group tests and the system processing mechanism is defective. Automatic delay processing is added to ensure the scheduling performance and configuration tests. Nevertheless, it incurs certain issues, such as unstable periodical tests and uneven scheduling of test instances.
		Calculating the number of packets transmitted per second based on the packet transmission interval. If the number exceeds the upper threshold, the automatic delay mechanism is started, and the test is started when the number of transmitted packets meets execution requirements of the test instance.	Y	
	NQA Server			
		NQA server type	Y	UDP, TCP, and ICMP
		Creating a server	Y	AR routers create the monitoring service at the NQA UDP receiver or at the NQA TCP receiver through the CLI and MBI, to respond to test instances at the transmitter.
		Deleting a server	Y	AR routers delete a single NQA UDP/TCP receiver through the CLI and MIB. Routers delete all NQA TCP receivers through the CLI.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
UDP Helper				
		Enabling and disabling UDP helper	Y	After UDP helper is enabled, the AR forwards the broadcast packets with UDP port numbers 37, 49, 53, 69, 137, and 138 by default. After UDP helper is disabled, all the destination server addresses and UDP port numbers forwarded by the AR are deleted.
		Configuration of UDP interfaces in UDP helper	Y	Ports with numbers 1 to 65535, except 67 and 68 are supported.
		Forwarding packets to specified servers based on interfaces	Y	The IP address of the destination server can be a unicast address or a subnet broadcast address, but cannot be 255.255.255.255.
IPv6 protocol stack				
	IPv6 address management			
		Manually setting link-local addresses	Y	
		Automatically creating link-local addresses	Y	Create a link-local address based on the interface number.
		Setting link-local addresses based on the complete addresses or prefixes	Y	
		Setting global addresses based on the complete addresses or prefixes	Y	1. The mask length of the global address cannot be 128. 2. Different interfaces must be configured with different global addresses.3. The mask length cannot be 128 and the loopback mask length can be 128.4. In the format of X:X:X:X:X:X:X:X, a 128-bit IP address is divided into eight groups. The 16 bits of each group are represented by four hexadecimal characters, that is, 0 to 9, and A to F. Groups are separated by colons. Every "X" represents a group of hexadecimal numbers
		Configuring global unicast addresses or site-local unicast addresses using EUI-64	Y	Only the network bit needs to be specified EUI-64. The host bit is converted from the interface MAC address (insert fffe in the sixth bit of the MAC address). For example, the host bit is 1234::00E0:82FF:FEDA:DBA8, subnet is 1234::/64. The prefix length of the network bits of an EUI-64 address cannot be more than 64 bits.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		IPv4-compatible IPv6 address	Y	1. The format of an IPv4-compatible IPv6 address is 0:0:0:0:0:0:IPv4-address. The high-order 96 bits are all 0s, and the low-order 32 bits specify an IPv4 address. This IPv4 address must be reachable on the IPv4 network, and cannot be a multicast address, a broadcast address, a loopback address, or an unspecified address (0.0.0.0). 2. This address is used on the tunnel interface on the IPv6 over IPv4 tunnel.
		Multiple global unicast addresses on the same interface	Y	
		Automatically creating link-local addresses	Y	Th automatically configured local-link address starts with FE80 and is created with the interface ID.
		Configuring anycast addresses	Y	DAD is not performed and responded by anycast addresses. Anycast addresses cannot be used as the source address of the packet. Address conflict detection is performed on anycast addresses.
		Address change with the interface number change	Y	The link-local addresses configured automatically and using EUI-64 change with the interface ID.
		DAD on IPv6 addresses	Y	
		Specifying the source IP address when sending a packet	Y	1. Select the same source address based on the destination address. 2. Select a proper address type (link-local address or global address) based on the destination address. 3. Match the longest prefix to the IPv6 source address policy table based on the destination address. 4. Select the source address using the address with the largest bits. 6. If no entries can be matched, select any address of the same type on the interface.
		Specifying the destination IP address when sending a packet	N	Currently not supported
		Configuring the address policy table	Y	IPv6 default source address policy table Prefix PrefixLen precedence Label ::1 128 50 0 :: 0 40 1 2002:: 16 30 2 :ffff:0:0 96 10 4 fc00::

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	IPv6 forwarding			
		Enabling IPv6 on the interface	Y	IPv6 configurations can be performed on an interface only after IPv6 is enabled on the interface. By default, IPv6 is not enabled on the interface (except the inloopback interface and Null0 interface) when the system starts with zero configuration.
		Processing IPv6 extended headers in compliant mode	Y	The IPv6 extended headers in compliant mode include the hop-by-hop options header, ~~routing options header, fragment header, and destination options header~~.
		Processing packets whose destination IP addresses are unicast addresses	Y	
		Processing packets whose destination IP addresses are multicast addresses	N	
		Checking the destination IPv6 address of the packet to be forwarded	Y	
		Fragmentation and reassembly on packets sent by the local AR	Y	
		Fragmentation and reassembly on forwarded packets	N	
		Statistics on IPv6 packets	Y	
		IPv6 flow-based load balancing	Y	
		IPV6 flow forwarding:	N	
	TCP6			
		Processing TCP6 packets	Y	
		Adjusting the MSS size based on IPv6 PMTU	Y	
		MD5 options	Y	
		Enhanced Authentication Option	Y	
	UDP6			
		Processing UDP6 packets	Y	
		Processing changes of PMTUs notified by the socket layer	Y	

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	RawIP6			
		Processing RawIP6 packets	Y	
		Processing changes of PMTUs notified by the socket layer	Y	
	ICMP6			
		Receiving ICMPv6 Error messages	Y	The Error messages include the following types: 1. Destination Unreachable 2. Packet Too Big 3. Time Exceeded 4. Parameter Problem
		Receiving ICMPv6 Request messages	Y	
		Receiving ICMPv6 Response messages	Y	
		Receiving neighbor discovery packets	Y	
	Socket6			
		Providing standard APIs	Y	
		Notifying the upper layer (TCP6/UDP6/RAWIP6) of MTUs obtained from the PMTUs	Y	
	IPV6 PMTU			
		Dynamic PMTU learning	Y	
		Notifying the upper layer of processing PMTU changes	Y	
		Configuring PMTU based on a single destination address	Y	
		Aging of dynamic entries	Y	
		Setting the aging time	Y	
		Setting the IPv6 MTU	Y	The IPv6 MTU must be greater than or equal to 1280 bytes. By default, the IPv6 MTU is 1500 bytes.
	Ping6			
		Ping based on IPv6 addresses	Y	
		Ping based on host names	Y	
		Ping with options	Y	The AR supports ping with the following options: 1. Source address 2. Size of the packet 3. Time 4. Number of sent packets 5. Source interface

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	Tracert6			
		TraceRoute with a specified IPv6 address	Y	
		TraceRoute with a specified host name	Y	
		TraceRoute with options	Y	The AR supports TraceRoute with the following options: 1. First TTL 2. Maximum TTL 3. UDP port number 4. Number of detection packets 5. Timeout period
IPv6 Transition Technology				
	6 over 4 tunnel			
		6 over 4 manual tunnel	Y	The AR supports RIPng, OSPFv3, ISISv6, and BGP4+.
		6 over 4 GRE tunnel	Y	The AR supports RIPng, OSPFv3, ISISv6, and BGP4+.
		IPv4-compatible IPv6 address tunnel	Y	
		6 to 4 tunnel	Y	The AR supports BGP4+.
		6 to 4 relay	Y	
		ISTAP tunnel	Y	
	4 over 6 tunnel			
		4 over 6 tunnel	Y	The AR supports the manual configuration of an IPv4 over IPv6 tunnel. Not support ISIS protocol
		Setting the traffic identifier of the tunnel	Y	
		Setting the hop threshold for the tunnel	Y	
		Setting the traffic level of the tunnel	Y	
		Setting the threshold for the number of packets encapsulated in the tunnel	Y	

Sub-system	Item	Specification	Version V200R005C00	Specification Description
ND				
	Basic ND			
		Periodically sending RA packets with default or configured parameters	Y	
		Sending an RA packet when parameters in the RA packet changes	Y	
		Setting the value of valid lifetime in the prefix option	Y	The default value is 2592000, in seconds.
		Setting the value of preferred lifetime in the prefix option	Y	The default value is 604800, in seconds.
		Configuring the M flag in an RA packet	Y	
		Setting the configuration and management on the O flag	Y	
		Setting the configuration and management on the reachable time	Y	
		Setting the configuration and management on the hop limit	Y	
		Setting the configuration and management on the default lifetime	Y	
		Configuring the default router priority in an RA packet	Y	
		Configuring routing information in an RA packet	Y	
		Setting the maximum interval for route advertisement	Y	
		Setting the minimum interval for route advertisement	Y	
		Configuring advertisements on route suppression	Y	
		IPv6 neighbor address resolution	Y	
		IPv6 neighbor reachability detection	Y	
		Static neighbor entry	Y	

Sub-system	Item	Specification	Version V200R005C00	Specification Description
DHCP				
	DHCP Client			
		RFC951	Y	Bootstrap Protocol (BOOTP), BOOTP Client supports BOOTP Options 1 (Subnet mask Option), 3 (Router Option), 6 (Domain Name Server Option), 12 (Host Name Option), and 43 (Vendor Specific Information).
		RFC2131	Y	Dynamic Host Configuration Protocol
		DHCP Option	Y	The DHCP server supports DHCP Options 1, 3, 6, 12, 43, 50, 51, 53, 54, 55, 58, 59, 60, 61, 67, 120, 141 to 147, and 150.
		IP address application, lease extension, and release	Y	The DHCP server supports IP address application, lease extension, and release using DHCP.
		VPN	Y	The DHCP server function supports VPN.
		Configuring IP address lease	Y	The expected IP address lease of the DHCP client can be configured.
		Gateway detection	Y	When functioning as the DHCP client to obtain IP addresses from different IP address pools of the DHCP server through two uplinks, the AR quickly detects whether the Relay gateway being used is faulty and determines whether to switch to another Relay gateway to request a new IP address.
		Default gateway router dynamic delivery	Y	After DHCP Client get address,AR issue or update default gateway router,and set the priority of the default gateway router.
		Service debugging	Y	DHCP client request、relet addressand so on
		Log	Y	When check the address conflict and log it.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	DHCP Relay			
		RFC 951	Y	Bootstrap Protocol (BOOTP)
		RFC3046	Y	DHCP Relay Agent Information Option
		RFC2131	Y	Dynamic Host Configuration Protocol
		DHCP servers in VPN	Y	Currently, all servers in a DHCP server group must be in the same VPN.
		Manual and forcible IP address release	Y	The DHCP Relay agent sends a DHCP Release message to the DHCP server to release the DHCP Client IP address.
		Log	Y	Incorrect formats of Giaddr fields or incorrect source MAC addresses (for example, a broadcast or multicast MAC address) are recorded in the log.
		TR069	Y	The TR069-compliant DHCP relay is supported.
		DHCP Option 82	Y	DHCP Option 82 is supported.
		Trusting Option 82	Y	If the DHCP relay agent receives a DHCP message with Option 82 but the gateway address is all-0, the message is discarded by default. If the switch between the DHCP client and the DHCP relay agent inserts an Option 82 field in the DHCP message, the message is discarded by the DHCP relay agent. This function can be changed through configurations.
		DHCP relay agent gateway switchover	Y	The DHCP relay agent supports gateway switchover.
		MIB objects for IP address of relayed DHCP servers	Y	The DHCP relay agent supports MIB objects for IP address of relayed DHCP servers.
		MIB objects for IP address assignment mode of DHCP servers	Y	The DHCP relay agent supports MIB objects for IP address assignment mode of DHCP servers.
		Log	Y	Log when Giaddr check failing 、Chaddr address error (for example broadcast)
		DHCP server round robin	Y	After turn on it, the different address request are sent to different server according the round robin.If turn off it,the request of client will be sent to all servers.
		Service debugging	Y	Forword address request、relet address between DHCP client and server.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	DHCP Server			
		RFC 951	Y	Bootstrap Protocol (BOOTP) The BOOTP server supports the following options: 1 (Subnet mask Option) 3 (Router Option) 6 (Domain Name Server Option) 12 (Host Name Option) 43 (Vendor Specific Information)
		RFC2131	Y	Dynamic Host Configuration Protocol
		DHCP server based on the global address pool	Y	The DHCP server assigns IP addresses and configurations to a client from the global address pool.
		Assigning dynamic IP addresses to clients from the IP address pool	Y	The DHCP server randomly assigns IP addresses and configurations to a client from the global address pool or interface address pool.
		Assigning fixed IP addresses to clients from the IP address pool	Y	Static IP addresses can be bound to MAC addresses in the global or interface address pool so that the DHCP server can assign fixed IP addresses to specified clients from the global or interface address pool.
		Removing IP addresses that cannot be assigned from the global address pool	Y	The DHCP server reserves special IP address and does not assign them to the clients.
		Assigning gateway addresses from the global address pool	Y	The DHCP server assigns a gateway address to a client from the global address pool.
		Assigning the lease of the address pool	Y	The DHCP server assigns IP addresses with lease information to a client from the global address pool or interface address pool.
		Assigning DNS domain names in the address pool	Y	The DHCP server assigns DNS domain names to a client from the global address pool or interface address pool.
		Assigning DNS server addresses in the IP address pool	Y	The DHCP server assigns DNS server addresses to a client from the global address pool or interface address pool.
		Assigning NetBIOS server addresses in the IP address pool	Y	The DHCP server assigns NetBIOS server addresses to a client from the global address pool or interface address pool.
		Configuring the NetBIOS type for the DHCP client in the IP address pool.	Y	When a DHCP client uses the NetBIOS protocol for communication on the WAN, host names must be mapped to IP addresses. Based on the modes of obtaining mapping, NetBIOS nodes are classified into the following types: b node: A node that obtains mappings in broadcast mode. b node: A node that obtains mappings by communicating with the NetBIOS server. m node: A node that has some broadcast features. h node: A b-type node enabled with the end-to-end communication mechanism.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Configuring DHCP user-defined options in the IP address pool	Y	The DHCP server supports the configuration of DHCP user-defined options in the global address pool or interface address pool and encapsulation of the options in the DHCP Reply message. The options can be strings, hexadecimal or IP addresses.
		Set bootfile and sname option in the address pool	Y	The bootfile field log the startup configuration file name of the client,the sname field log the startup configuration file name of the server,client select startup configuration file according the file name from the server.
		Preventing repetitive IP address assignment	Y	Repetitive IP address assignment may cause IP address conflicts. To solve this problem, before assigning an IP address to a client, the DHCP server needs to send ping packets to check whether the IP address is in use. If there is no response within a certain period of time, the DHCP server continues to send ping packets to this address until the number of ping packets reaches the maximum value. If there is still no response, the IP address is not in use. This ensures that the IP address assigned to the client is unique.
		Reuse of conflict addresses	Y	If the DHCP address pool has no available IP address, the DHCP server searches the expired IP addresses and conflicting IP addresses, and then assigns a valid IP address to the client.
		TR069	Y	TR069 nodes support the following attributes: DHCPServerConfigurable, DHCPServerEnable, MinAddress, MaxAddress, ReservedAddresses, SubnetMask, DNSServers, DomainName, IPRouters, IPAddress, AddressSource, and LeaseTimeRemaining.
		DHCP Option	Y	The AR supports Options 1, 3, 6, 12, 15, 33, 43, 44, 46, 50, 51, 53 to 55, 58 to 61, and 141 to 150.
		IP address pool saving	Y	The AR supports IP address pool saving.
		Assigning configurations to users	N	The DHCP Inform message only contains DNS configurations but does not IP addresses. This is called stateless DHCP.
		DHCP server IP address	Y	The AR supports configurations and dynamic delivery of the next server IP address in the DHCP Offer messages and ACK messages.
		Trusting Option 82	Y	If the DHCP relay agent inserts Option 82 to a message but does not set the Giaddr field, you can configure the DHCP server to trust Option 82 inserted by the DHCP relay agent and prevent the server from discarding the message.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		DHCP server with DHCP relay	Y	IP addresses are assigned from the local server. If this fails, the request is relayed to the remote DHCP server for addresses.
		MIB objects for the global address pool	Y	The MIB objects for the global address pool are supported.
		MIB objects for the interface address pool	Y	The MIB objects for the interface address pool are supported.
		MIB objects for assigned addresses	Y	The MIB objects for assigned addresses are supported.
		MIB objects for locked addresses	Y	The MIB objects for locked addresses are supported.
		MIB objects for conflict IP addresses	Y	The MIB objects for conflict IP addresses are supported.
		Option response forcible	Y	The addess request packet of some client don't take the option,but hope the DHCP server reply the option which config under the address pool.In order to be compatible with the nonstandard client,when the DHCP server reply the client,reply the specified option information forcibly.
		Service debugging	Y	DHCP server distribute 、relet address
	DHCP snooping			
		Rate limit on all the DHCP messages in the system	Y	The rate of DHCP messages that are sent to the host is limited globally.
		Rate limit on all the DHCP messages on the interface	Y	The rate of DHCP messages that are sent to the host is limited based on the interface.
		Rate limit on all the DHCP messages in the VLAN	Y	The rate of DHCP messages that are sent to the host is limited based on the VLAN.
		Detection of bogus DHCP servers	Y	DHCP Reply messages from untrusted interfaces on the DHCP server are discarded and IP addresses of bogus DHCP servers are recorded.
		Dynamic rate limit on DHCP messages	Y	The processing rate of DHCP messages is dynamically adjusted based on the current CPU usage and memory usage.
		Preventing attacks from IP packets	Y	IP packets whose actual lengths are different from the length field in the packets are discarded.
		Log	Y	Record the log when discover the other DHCP server、exceed the packet limit rate.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
DHCPv6				
	DHCPv6 Client			
		Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	Y	RFC3315
		RFC 4075	Y	SNTP Configuration Option for DHCPv6
		RFC 4242	Y	Information Refresh Time Option for DHCPv6
		Process of address allocation through DHCPv6 exchange involving four messages	Y	The DHCPv6 client obtains its IPv6 address and configurations through DHCPv6 exchange involving four messages.
		Process of address allocation through DHCPv6 exchange involving two messages	Y	The DHCPv6 client obtains its IPv6 address and configurations through DHCPv6 exchange involving two messages.
		Stateful DHCPv6 mode	Y	The DHCPv6 client obtains its IPv6 address and configurations through DHCPv6 exchange involving two or four messages.
		Stateless DHCPv6 mode	Y	The DHCPv6 client obtains configurations through DHCPv6 exchange involving two messages.
		Extending IP address lease	Y	IP address leases are extended using the **renew** or **rebind** command.
		IP address release	Y	The IP address is released when the interface is Down or in other situations.
		IP addresses conflict	Y	The server is notified of conflicts detected by DAD.
		Randomly sending messages for a delay period	Y	The DHCPv6 client randomly sends messages for a delay period.
		Checking whether DHCPv6 messages are valid	Y	The DHCPv6 client checks whether DHCPv6 messages are valid based on RFC3315.
		Reliability of sending DHCPv6 messages	Y	Packets are retransmitted based on retransmission policies.
		Log recording on address conflicts	Y	Logs are recorded when the DHCPv6 client detects address conflicts.
		Maximum number of supported clients	Y	32
		Process of IPv6 prefix allocation through DHCPv6 exchange involving four messages	Y	The DHCPv6 client obtains its IPv6 address prefix and configurations through DHCPv6 exchange involving four messages.
		Process of IPv6 prefix allocation through DHCPv6 exchange involving two messages	Y	The DHCPv6 client obtains its IPv6 address prefix and configurations through DHCPv6 exchange involving two messages.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Extending IP address prefix lease	Y	IPv6 address prefix leases are extended using the **renew** or **rebind** command.
		Releasing IPv6 address prefixes	Y	IPv6 prefixes can be released.
		Obtaining IPv6 prefixes using stateful DHCPv6	Y	IPv6 prefixes and configurations are obtained using stateful DHCPv6, including IP address, DNS server name/IP address, TFTP server name/IP address, and configuration file name.
		Querying the requested IPv6 prefix information	Y	IPv6 prefix information can be obtained using the prefix name.
		Querying information about interfaces on the DHCPv6 client	Y	Information about interfaces on the DHCPv6 client includes the DHCPv6 server address, DHCPv6 server DUID, DHCPv6 server priority, and whether Rapid-Commit is supported.
		Querying information about DHCPv6 client address	Y	Information about DHCPv6 client address includes the address, address lifetime, address lease, and DNS server.
		Querying statistics on packets	Y	Statistics on packets includes the number of each type of packets, number of packets successfully sent, and number of packets failed to be sent.
		ND prefix delegation	Y	The DHCPv6 client obtains prefixes and associates the prefix with the router on the local link. The router periodically sends RA packets and assigns addresses to other clients on the link in stateless mode.
		DHCPv6 standard Option	Y	RFC 3315（DHCPv6）standard option:1（Client Identifier）、3（IA_NA）、5（IA Address）、6（Option Request）、7（Preference）、8（Elapsed Time）、14（Rapid Commit）。
		DHCPv6 Option16	Y	The vendor class option is used to mark DHCPv6 client，generally is company code and hardware address.
		DHCPv6 Option31	Y	SNTP servers option is used to carry address of the SNTP server.DHCPv6 client get address of the SNTP server according to resolve the option of the packet from DHCP server .AR synchronize on time with the server.
		DHCPv6 Option32	Y	The DHCPv6 server notice DHCPv6 client to refresh the upper limit time on the DHCPv6 server accoding to information refresh time option.DHCPv6 client must request option32 in the Information-Request packet.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	DHCPv6 Relay			
		DHCPv6 Option 37	Y	The DHCPv6 relay agent can insert the remote ID in Relay-Forward messages to replace the original remote ID of the Relay-Reply messages before forwarding them.
		DHCPv6 Option 18	Y	The **Interface-id** option is a standard option defined in DHCPv6 and is used to identify the interface that receives a message of a DHCPv6 client, that is, the interface through which the DHCPv6 relay agent sends a response message to a DHCPv6 client. The DHCPv6 relay agent can insert the remote ID to a Relay-Forward message.
		Statistics on DHCPv6 messages forwarded by the interface on the DHCPv6 Relay agent	Y	Statistics on DHCPv6 messages forwarded by the interface on the DHCPv6 Relay agent are provided.
		Advertising routes with PD prefixes	Y	Routes with PD prefixes can be advertised.
	DHCPv6 Server			
		Process of address allocation through DHCPv6 exchange involving two messages	Y	A DHCPv6 client multicasts a Solicit message to locate the DHCPv6 server that can allocate addresses and configuration parameters. After receiving the Solicit message, the DHCPv6 server responds with a Reply message carrying allocated addresses and configuration parameters allocated to the DHCPv6 client.
		Process of address allocation through DHCPv6 exchange involving four messages	Y	A DHCPv6 client first locates DHCPv6 servers that can provide the DHCPv6 service for the DHCPv6 client by multicasting a Solicit message. After receiving Advertise messages from multiple DHCPv6 servers, the DHCPv6 client selects one of the DHCPv6 servers according to priorities of DHCPv6 servers. Then the DHCPv6 client and the DHCPv6 server complete address application and allocation through exchange of Request and Reply messages.
		Stateful DHCPv6 mode	Y	The DHCP server can assign IP addresses and configurations to the client, including DNS server, SIP server, NIS server, and SNTP server.
		Stateless DHCPv6 mode	Y	The DHCP server can assign IP addresses and configurations to the client, including DNS server, SIP server, NIS server, and SNTP server.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Extending IP address lease	Y	The IP address assigned to the client has lifetime and time to extend the lease (T1 and T2 of an IA). To extend the valid and preferred lifetimes for the addresses associated with an IA, a DHCPv6 client sends a Renew message to the DHCPv6 server at T1. In the Renew message, the IA option carries the addresses whose leases need to be extended. If the DHCPv6 client does not receive a response message, the DHCPv6 client sends a Rebind message at T2 to the DHCPv6 server to continue to extend the address lease.
		IP address release	Y	When a DHCPv6 client does not use one or more IP addresses, the client sends a DHCP Release message to request the DHCPv6 server to release the address. In the DHCP Release message, the IA option carries the IA whose address needs to be released.
		IP addresses conflict	Y	After the DHCPv6 client receives the address allocated by the server, DAD is performed using ND. If address conflicts are detected, the client needs to notify the server.
		IP address acknowledgment	Y	When a DHCPv6 client moves to a new link, the old address may not be used on the new link. When the link that the client accesses changes, the client needs to send an ACK message to the DHCPv6 server to confirm whether the old address can be used on the new link.
		IP address lease management	Y	The DHCPv6 server needs to manage the lease of the assigned IP addresses and release the addresses when the valid lifetime of the addresses expires.
		IPv6 address prefix lease management	Y	The DHCPv6 server needs to manage the lease of the assigned IPv6 prefixes and release the prefixes when the valid lifetime of the prefixes expires.
		IP address reservation	Y	The DHCPv6 server reserves some special addresses using command lines.
		Static IP address allocation	Y	Some clients, such as VIPs, must use the same IP addresses each time. Therefore, the DHCPv6 server provides command lines to assign fixed IP addresses for clients with specified DUIDs.
		Manual IP address release	Y	The DHCPv6 server provides command lines to manually release IPv6 addresses that clients do not use.
		IP address pool locking	Y	The DHCPv6 server provides command lines to lock specified IP address pools so that IP addresses in this pool cannot be assigned.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Process of IPv6 address prefix allocation through DHCPv6 exchange involving two messages	Y	A DHCPv6 client multicasts a Solicit message to locate the DHCPv6 server that can allocate addresses and configuration parameters. After receiving the Solicit message, the DHCPv6 server responds with a Reply message carrying allocated prefixes allocated to the DHCPv6 client.
		Process of IPv6 address prefix allocation through DHCPv6 exchange involving four messages	Y	A DHCPv6 client first locates DHCPv6 servers that can provide the DHCPv6 service for the DHCPv6 client by multicasting a Solicit message. After receiving Advertise messages from multiple DHCPv6 servers, the DHCPv6 client selects one of the DHCPv6 servers according to priorities of DHCPv6 servers. Then the DHCPv6 client and the DHCPv6 server complete prefix application and allocation through exchange of Request and Reply messages.
		Extending IPv6 address prefix lease	Y	The prefix assigned to the client has lifetime and time to extend the lease (T1 and T2 of an IA). To extend the valid and preferred lifetimes for the prefixes associated with an IA, a PD client sends a Renew message to the PD server at T1. In the Renew message, the IA option carries the prefixes whose leases need to be extended. If the PD client does not receive a response message, the PD client sends a Rebind message at T2 to the PD server to continue to extend the prefix lease.
		IPv6 address prefix release	Y	When a PD client does not use one or more prefixes, the client sends a Release message to request the server to release the prefix. In the Release message, the IA option carries the IA whose prefix needs to be released.
		Static IPv6 address prefix allocation	Y	Customer Premise Equipment (CPE) locates between the client network and carrier network as a router to request IPv6 prefixes. To ensure stability of the client network, the client requests the CPE to obtain the same prefix. In dynamic prefix allocation, the client cannot obtain the same prefix each time. The DHCPv6 server provides command lines to statically assign fixed prefixes to the client.
		Manual IPv6 address prefix release	Y	The DHCPv6 server provides command lines to manually release prefixes that clients do not use.
		Local database proxy	Y	To prevent the client addresses or prefixes from losing when the AR restarts, the DHCPv6 server can be enabled to automatically save the address or prefixes that have been assigned in the local database.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
		Preferred assignment of addresses that the client requests	Y	The DHCPv6 server preferentially assigns the address that the client requests.
		Preferred assignment of prefixes that the client requests	Y	The DHCPv6 server preferentially assigns the prefix that the client requests.
		DHCPv6 server with DHCPv6 snooping	Y	When the DHCPv6 server functions as the first-hop Layer 3 device, the DHCPv6 server function can be used with DHCPv6 snooping.
		Displaying address pool information	Y	The address pool information can be displayed.
		Displaying address binding information	Y	The address binding information can be displayed.
		Displaying information about an interface on the server	Y	The information about an interface on the server can be displayed.
		Packet statistics and checking	Y	Packet statistics can be displayed.
		DHCPv6 standard Option	Y	RFC 3315（DHCPv6）standard option:2（Server Identifier）、3（IA_NA）、5（IA Address）、6（Option Request）、7（Preference）、9（Relay Message）、12（Server Unicast）、13（Status Code）、14（Rapid Commit）、17（Vendor-specific Information option.
		DHCPv6 Option21	Y	SIP Servers Domain Name List option，take the domain name list of the SIP(Session Initiation Protocol) server.
		DHCPv6 Option22	Y	SIP Servers IPv6 Address List option，tack the address list of the SIP (Session Initiation Protocol) server.
		DHCPv6 Option23	Y	DNS Recursive Name Server option，take the adress of the DNS server.
		DHCPv6 Option24	Y	Domain Search List option,take the domain name search list when users are resolving DNS domain name.
		DHCPv6 Option27	Y	Network Information Service (NIS) Servers option,take the address of the NIS server.
		DHCPv6 Option28	Y	Network Information Service V2 (NIS+) Servers option,take the address of the NIS+server.
		DHCPv6 Option29	Y	Network Information Service (NIS) Domain Name option,take the NIS domain name.
		DHCPv6 Option30	Y	Network Information Service V2 (NIS+) Domain Name option,take the NIS+ domain name .
		DHCPv6 Option31	Y	SNTP servers option,take the address of the SNTP server.
		DHCPv6 Option32	Y	information refresh time option,DHCPv6 server notice DHCPv6 client refresh the high limit of time on the DHCPv6 server according to the option.

Sub-system	Item	Specification	Version V200R005C00	Specification Description
IP Accounting				
		Statistics on IP packets	Y	This function can be enabled on the interface on both incoming and outgoing packets. The statistics include the source IP address, destination IP address, protocol type, number of packets, and number of bytes.
		Statistics on IP packet priorities	Y	Statistics are collected based on IP priorities. The statistics include the direction, priority, number, and bytes of IP packets.
		Statistics on IP packets based on filtering policies	Y	A maximum of 32 policies can be defined in the filtering list based on IP addresses.
		Clearing statistics on IP accounting	Y	Statistics on IP packets and IP priorities can be cleared.
		Aging of IP accounting entries	Y	The accounting table supports aging time. By default, the aging time is 720 minutes and the minimum time is 60 minutes.
		Displaying 32 entries with the largest traffic in the IP accounting table	Y	Statistics on traffic can be arranged in descending order and the 32 entries with the largest traffic are displayed in the IP accounting table.
		IP accounting entry	Y	AR150/200 series: 1K AR1220 series: 4K AR2220 series: 8K AR3200 series: 16K
IP Unicast Policy-based Routing				
	Local IPv4 PBR			
		PBR packet matching rule	Y	Y
		PBR action	Y	Y
		Default PBR action	Y	Y
		Local PBR	Y	Y
		PBR load balancing	Y	Y
		Specifying accessible VPN instances	Y	Y
		PBR number	Y	Y
		PBR node number	Y	Y
	IPv4 Interface Policy-based Routing			
		PBR packet matching rule	Y	Y
		Specifying the next hop to forward the packet	Y	Y
		Specifying the next hop to trace NQA	Y	Y
		Specifying the next hop to trace ip-route	Y	
		Specifying outbound interface to forward the packet	Y	Y

Sub-system	Item	Specification	Version V200R005C00	Specification Description
	IPv6 Interface Policy-based Routing			
		PBR packet matching rule	Y	Y
		Specifying the next hop to forward the packet	Y	Y
		Specifying outbound interface to forward the packet	Y	Y
	SPR			
		Selecting the optimal link from links that meet the service requirement in the link group	Y	Y
		Selecting the optimal link when no link meets the service requirement in the link group	Y	Y
		Best-effort link	Y	Y
		Setting the switching interval	Y	Y
		Setting the flapping suppression interval	Y	Y
		Alarms on link faults	Y	Y
		Interface types supported by the SPR	Y	Y
		Checking jitter, delay, and packet loss ratio using NQA	Y	Y