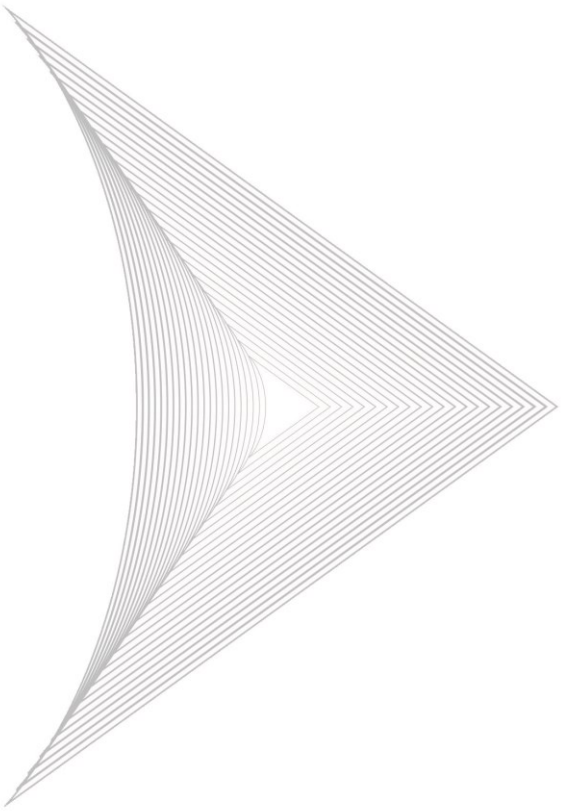
Huahuan

H20RN-2000.V2 Series IP/MPLS Aggregation Platforms

Product Description



Beijing Huahuan Electronics Co.,Ltd.

H20RN-2000.V2 Series
IP/MPLS Aggregation Platforms

Product Description

Beijing Huahuan Electronics Co., Ltd.
Oct.2019

Copyright Notice

Product Name: H20RN-2000.V2 Series IP/MPLS Aggregation Platforms

Version: 1.4

Release Date: Oct. 2019

BEIJING HUAHUAN ELECTRONICS Co., LTD.

Address: No.26, Shangdi 6th Street, Haidian District, Beijing, 100085
P.R. China

Tel: +86-400-810-8580, +86-10-52046188

Fax: +86-10-52046288

Website: www.huahuan.com

E-mail: support@huahuan.com

Contents

List of Figures

List of Tables

1 Overview

H20RN-2000.V2 Series IP/MPLS Aggregation Platforms use routing architecture, solve the network smooth evolution, equipment interconnection and interoperability, and realize the end-to-end clock scheme. They support L2/L3 IP protocol, and build reliable carrier-level packet switching network.

H20RN-2000.V2 series platforms include H20RN-2000.V2 and H20RN-2000L.V2.

H20RN-2000.V2 series platforms are composed of aggregation cards and tributary cards, H20RN-2000.V2 and H20RN-2000L.V2 respectively use 2U/1U chassis. Aggregation cards include dual-power card, network management aggregation card, and fan card; tributary cards include 16E1 interface card, 10GE interface card, STM-1 interface emulation card and 8GE interface card.

For the appearance structure, hardware specifications, and device installation, refer to the *H20RN-2000.V2 Series IP/MPLS Aggregation Platforms Hardware Description* and the *H20RN-2000.V2 Series IP/MPLS Aggregation Platforms Quick Installation Guide*.

1.1 Features

- PW over GRE encapsulation;
- IP over GRE encapsulation;
- Ethernet interface IEEE 802.1p;
- PW redundancy protection;
- LDP, RVSP-TE label distribution, dynamic tunnel;

- STM-1 interface emulation function, MSP 1+1 protection;
- CES synchronization ACR/DCR recovered clock;
- System management, interface management, network management;
- Ethernet functions, including VLAN, QinQ, MAC address forwarding, Link Layer Disco very Protocol (LLDP), and other functions;
- Carrier-class reliability: Manual LAG and static LACP; ITU-T G.8031 ELPS (Ethernet Linear Protection Switching); ITU-T G.8032 ERPS (Ethernet Ring Protection Switching); loopback detection etc;
- L3 routing protocol, including routing management, RIP, ISIS, OSPF and BGP;
- L2 IP service, including ARP, DHCP, NDP and IP Ping;
- MPLS-TP technology and static LSP, MPLS L2VPN;
- QoS management, including port speed limit, priority trust, flow classification, flow behavior, flow policy;
- Access Control List (ACL);
- AAA management mechanism, providing three security functions: Authentication, Authorization and Accounting.
- Ethernet OAM protocols, including IEEE 802.3ah, IEEE 802.1ag and ITU-T Y.1731; standard OAM active mode and passive mode, OAM link discovery, OAM remote loopback and OAM link event;
- Jumbo frame setting (at least 9600 bytes);
- Switching capacity: 56Gbps;
- Clock function, SyncE and NTP;
- Multiple service types, including E-Line service, E-LAN service, E-Tree service, E-Access and CES service.
- EzView NMS, SNMP and SSH CLI;
- Upgrade software through TFTP;
- Pluggable fan, speed control function, high temperature alarm.

1.2 Ordering Information

Table 1-1 lists card ordering information of H20RN-2000.V2 series platforms.

Table 1-1 Card ordering information of H20RN-2000.V2 series platforms

Cards	Models	Descriptions
NM+PX card	MX01/PXM01	• Master-control switching card, 1 NM port and 1 CONSOLE port; • 1 external clock input/output port, supporting 2MHz, 2Mbit/s clock mode, 1 1PPS+TOD port
2×10GE card	XGE02	2 10GE optical signal transmission
2×10GE card	TU02	2 10GE optical signal transmission
2×10GE card	XGE02G	• 2 10GE optical signal transmission • GRE encapsulation
8GE card	GE08	8GE optical signal transmission
8GE card	GU08	8GE optical signal transmission
8GE card	GE08G	• 8GE optical signal transmission • GRE encapsulation
8GE card	GE08E	8GE electrical signal transmission
8GE card	GU08E	8GE electrical signal transmission

Cards	Models	Descriptions
STM-1 interface emulation card	SC01QE	4 STM-1 interfaces
16E1 emulation card	EC16	• 16E1 signal transmission
-48V power card	PWR48150/ PWR48	• Used in H20RN-2000.V2 device • Provides power supply and fan power for each card • 1+1 protection • Output power 150W
-48V power card	PWR4875	• Used in H20RN-2000L.V2 device • Provides power supply and fan power for each card • 1+1 protection • Output power 150W
220V power card	PWR22150/ PWR22	• Used in H20RN-2000.V2 device • Provides power supply and fan power for each card • 1+1 protection • Output power 150W

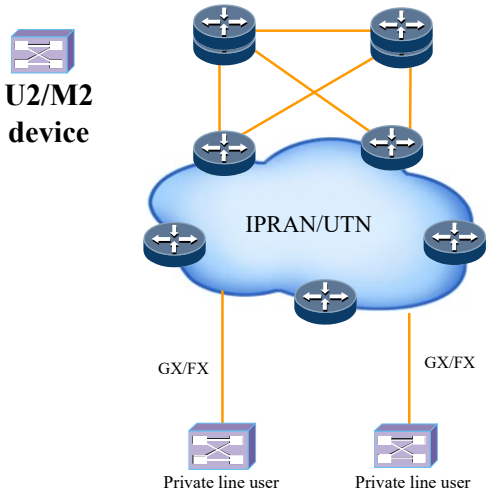
Cards	Models	Descriptions
220V power card	PWR2275	• Used in H20RN-2000L.V2 device • Provides power supply and fan power for each card • 1+1 protection • Output power 150W
Fan card	FAN02/FAN	Pluggable fan, speed detection

2 Typical Application

Typical application diagram of H20RN-2000.V2 series platforms is shown in Figure 2-1.

Used as the private line users, H20RN-2000.V2 series IP/MPLS aggregation platforms are accessed into the Carrier equipment for data transmitting.

Figure 2-1 Typical application diagram



3 Functional Properties

NOTE

This chapter introduces the main features supported by the H20RN-2000.V2 series platforms. For specific service configurations and function examples, refer to the *H20RN Intelligent Packet Device Configuration Guide (CLI)* manual.

3.1 System Management

H20RN-2000.V2 series equipment system management includes user management, configuration management, file management, device management, log management and alarm management.

3.2 Interface Management

Configure and manage the interface's enabling/disabling, data statistics and other information. Device interface includes Ethernet interface, Tunnel interface, Lookback interface, TRUNK interface, VLANIF interface, TDM interface, etc.

3.3 Ethernet

3.3.1 VLAN

H20RN-2000.V2 series platforms support IEEE 802.1Q based VLAN (Virtual Local Network)

division. IEEE 802.1Q tag can be identified and processed, and VLAN ID (1~4094) and IEEE 802.1p priority can be configured (up to 4094 entries are supported). The devices support port-based VLAN division. The interface link types include Hybrid, Access, and Trunk. See details in Table 3-1.

Table 3-1 Interface link types and packet forwarding

Port type	Process of untagged packets	Process of tagged packet	Process of sending frames
Trunk	➢ Tagged with PVID, and when PVID is in the VLAN ID list that permits to pass through, receive the packet ➢ Tagged with PVID, and when PVID is not in the VLAN ID list that permits to pass through, discard the packet	➢ When VLAN ID is in the VLAN ID list that permits to pass through, receive the packet ➢ When VLAN ID is not in the VLAN ID list that permits to pass through, discard the packet	➢ When VLAN ID is the same with PVID, strip the tag and send the packet ➢ When VLAN ID is different from PVID, and is a VLAN ID that permits to pass through by the interface, keep the tag and send the packet
Access	Receive the packet and tag with PVID	➢ When VLAN ID is the same with PVID, receive the packet ➢ When VLAN ID is different from PVID, discard the packet	Strip PVID Tag of the frame first and then send it
Hybrid	The same with trunk mode	The same with trunk mode	Untagged/tagged can be used to set whether to carry tag or not when sending packets

3.3.2 QinQ

QinQ technology is an extension of IEEE 802.1Q, is a layer-2 VPN tunnel technology defined in IEEE 802.1ad.

H20RN-2000.V2 series platforms support basic QinQ and flexible QinQ.

Basic QinQ

Basic QinQ is a simple layer-2 VPN technology, which seals outer VLAN tag for user packet from private network through the operator's access end, and then the packet brings two VLAN Tags to pass through the operator's backbone network (public network). In public network, packets are transmitted according to their outer VLAN tags only (public network VLAN tags), so user private net VLAN tags are transmitted as part of the data of packets.

Flexible QinQ

Flexible QinQ (VLAN stacking) is an enhanced application of basic QinQ. In addition to the realization of all the functions of basic QinQ, flexible QinQ can do different things to the packets received by the same interface according to different VLAN tags and add different outer VLAN ID for different inner VLAN ID. By configuring inner and outer Tag mapping rules, the user can encapsulate different outer Tags for packets with different inner Tags according to the mapping rules.

3.3.3 MAC

H20RN-2000.V2 series platforms support MAC address forwarding.

MAC Address Forwarding Table

Ethernet devices forward Ethernet packets through fast forwarding through MAC address forwarding rules. Each device has a MAC address and a forwarding table for each interface. This is the MAC address forwarding table. All inbound interface packets are forwarded according to the MAC address forwarding table, which is the basis for the Ethernet device to implement Layer 2 packet forwarding.

MAC address table entries include the following information:

- Destination MAC address
- Destination MAC address corresponding to forwarding port
- VLAN ID which the port belongs to

- Flag

We can view the MAC address table information based on the device, interface, and VLAN.

MAC Address Table Classification

H20RN-2000.V2 series platforms support 2 MAC address entries: static MAC address entries and dynamic address entries.

- Static MAC address table entry

MAC address table is added and deleted by users, and it does not age.

- Dynamic MAC address table entry

MAC address table is created by learning source MAC addresses of the received packets automatically. Dynamic MAC address table is stored in the device's cache, which is not saved after resetting the device. H20RN-2000.V2 series platformss support setting dynamic MAC address table entries and setting MAC aging time. They support manually removal of dynamic MAC address table entries. For the specific range and default parameters, refer to H20RN Intelligent Packet Devices Command Reference.

MAC Address Learning Number Limit

MAC address learning number limit is mainly used to limit MAC address entries, when the number of the accessed users exceeds the limit value, the MAC addresses of newly accessed users will not be learned. New user packets can be configured to discard or forward. MAC address learning number limit only limits dynamic MAC address learning.
H20RN-2000.V2 series platforms support MAC address learning number limit based on global, port and VLAN.

- Port based MAC address learning number limit

It learns the packets source MAC addresses which access into the VLAN that the port belongs to; when the learned number reaches the threshold value, it won't learn MAC address. At this time if the source MAC address of the input packet is unknown, i.e. not included in the learned MAC address table, the interface will not learn this MAC and this MAC packet will be configured to discard or forward.

- Global based MAC address learning number limit

  The device can globally configure the MAC address learning limit, and when the learning threshold is reached, MAC address learning is no longer

performed. New user packets that exceed the limit can be configured to forward or discard.

- VLAN based MAC address learning number limit

It learns the packets source MAC addresses of the specified VLAN; when the learned number reaches the threshold value, MAC address learning of the VLAN will be stopped.

MAC Aging Time

The MAC address forwarding table is limited in capacity. To make the full use of the address forwarding table resources, the aging mechanism is used to update the MAC address forwarding table. That is, the system starts an aging timer while dynamically creating an entry. If the packets from this MAC address are not received again within the aging time, the device will delete this MAC address table entry.

3.3.4 LACP

Device supports link aggregation which aggregates multiple physical Ethernet interfaces to form a logical aggregation group, and treat multiple physical links in the same aggregation group as one logical link, so as to implement link protection and load sharing between devices, and enhance the reliability of service between devices.

The device supports manual LACP and static LACP modes. Both aggregations support load sharing and main/standby modes. In the load sharing mode, all member ports can forward traffic. In the main/standby mode, only the main link forwards the traffic, and the standby link is used as a backup of the main link, not forwarding the traffic. Only when the main link fails, the standby link will forward the traffic.

In the both manual LACP and static LACP modes, we need to manually create the aggregation group and add the aggregate group member interface. The difference is that manual LACP in the load sharing mode, all interfaces are in a forwarding state, to share the load flow, without the participation of LACP protocol packets, but the static LACP in load sharing mode, LACP protocol packets are used to negotiate member ports, the ports passing negotiation are in a forwarding state, while the ports not passing negotiation cannot forward the traffic

H20RN-2000.V2 series platforms support six load sharing algorithms: S-MAC, D-MAC, S-MAC or D-MAC, S-IP, D-IP and S-IP or D-IP. The default is S-MAC or D-MAC.

Tip:

In the same link aggregation group, the interfaces sharing load must have consistent configurations. The configuration includes six aspects: STP, QoS, QinQ, VLAN, interface

attributes, and MAC address learning:

3.3.5 LLDP

LLDP (Link Layer Discovery Protocol) is an IEEE 802.1ab compliant protocol. Through this protocol, NMS can quickly master topology and changing conditions of layer-2 network. LLDP organizes information of local device into different TLVs (Type Length Value) and encapsulates them to LLDPDU (Link Layer Discovery Protocol Data Unit), so as to send to directly connected neighbor. At the same time, LLDP saves information from the neighbor in standard MIB (Management Information Base), for the NMS to query and judge the link communication conditions.

Device count information includes: port packet-sending count, port packet-receiving count, frame loss count, frame error count, TLV error count, TLV unrecognized count and neighbor aging count.

3.3.6 Loop Detection

In H20RN-2000.V2 series platforms, the function of interface loop detection is to overcome the influence of loops on network and improve the self-checking, fault tolerance, and robustness of network.

The processes of loop detection are as follows:

- Each port of the device periodically sends Loopback-detection packets (the interval can be set and generally is 1s by default).
- The device checks the source MAC field of the loop detection packet received by interfaces. If the MAC of this device is saved in source MAC field, interfaces loops of this device will be detected, or it will be discarded.
- If the serial numbers of packet-sending and receiving interfaces are the same, this interface will be closed.
- If the serial numbers of packet-sending and receiving interfaces are different, the interface with the smaller number will be closed and other interfaces will be kept at Up state.

3.3.7 Interface Mirror

The interface mirror function refers to mirroring the packets of specified source interface to the specified destination interface, without affecting the normal packet forwarding. The

switching device user uses this feature to monitor the packets receiving and sending of an interface, and to analyze the network status, or the failure situation

The device supports the data flow mirroring based on the ingress and egress. After the mirror function takes effect, the ingress and egress mirroring packets will be copied to the monitoring interface. The monitor interface cannot be the same interface as the mirror interface.

3.4 IP Routing

The L3 interface is the VLAN-based virtual interface. It is configured to the situation in which the device needs to be managed through network, or multiple devices need to be connected through routing. For the VLAN which needs to be configured with the IP, you can relate an L3 interface to it, each L3 interface is corresponding to an IP and relates to at least one VLAN.

Routing is used when devices with different VLANs communicate. Routing is the behavior that transfers packets through the network to the destination, using routing tables to forward the packets.

There are three ways to implement the routing function:

- The default router, it will send the packet whose destination address cannot be found to a specified default router.
- The static router, which is a manually configured route that forwards the packets through a pre-specified interface. It is applied to networks with simpler topologies.
- The dynamic router, which dynamically learns routes through routing protocols, can dynamically calculate the optimal route for packet forwarding. In the calculation process, more bandwidth and network resources are required. There are two types of dynamic routing protocols:
  - RIP (Routing Information Protocol): each device maintains a vector table, which lists the best distance known to other target devices and the path it passes. By exchanging information between neighbor devices, devices continuously update their internal vector tables.
  - OSPF (Open Shortest Path First): the link state database is established by announcing the state of the network interface

between devices. The database contains every link state directly connected to all devices. All devices will have a common network topology, but each device will independently determine the best path to every node in the network topology. Link state protocol can respond to topology changes quickly, but it needs more bandwidth and resources compared with RIP.

Routing Management

Routing management is used to manage the routing tables, static routing and various dynamic routing protocols.

RIP

RIP (Routing Information Protocol) is a simple Distance-Vector based IGP, (Interior Gateway Protocol).

There are two versions for RIP: RIPv1 and RIPv2.

- RIPv1 is a routing protocol with categories, which only supports releasing the protocol packet through broadcast.
- RIPv2 is a routing protocol without categories.

Each device running the RIP protocol manages a routing database that contains routing items to all reachable destinations, including destination address; next hop address, egress interface, measurement value, and routing time. RIP protocol is a routing protocol based on distance vector algorithm. Because it tells neighbors about its entire routing table, there is the possibility of routing loop. In order to improve the performance, RIP protocol also supports counting to infinity, horizontal segmentation, toxicity reversal and trigger update mechanism, so as to prevent the generation of routing loop. For the configuration and application of related functions, please refer to the H20RN Intelligent Packet Device Configuration Guide (CLI).

OSPF

OSPF (Open Shortest Path First) is a dynamic routing protocol based on link state. The OSPF of this device refers to the OSPFv2 used for the IPv4 protocol.

OSPF protocol packets are as follows:

- Hello packet: It is sent periodically and used to discover and maintain the OSPF neighbor relationship. The contents include time values of some timers, DR, BDR, priority and known neighbor information.
- DD (Database Description) packet: it describes the summary information of every LSA (Link State Advertisement) in local LSDB, that is, the LSA packet header, used in two routing devices for database synchronization.
- LSR (Link State Request) packet: it requests the required LSA from peer end. After two routing devices exchange DD packets to learn what LSA is missing from local LSDB, it is necessary to send a LSR packet to the peer end for the required LSA. It requests the required LSA summary.
- LSU (Link State Update) packet: it sends the required LSA to the peer end. It sends a collection of multiple LSA.
- LSAck (Link-State Acknowledge) packet: it is used to confirm the received LSA. It acknowledges the LSA header (A packet can confirm multiple LSA).

ISIS

ISIS (Intermediate System to Intermediate System) is one of the inner gateway protocols used by telecom operators. The IS-IS protocol only supports two types of networks: broadcast network and point-to-point network.

IS-IS uses a hierarchical structure of two levels within the routing domain. A large routing domain is usually divided into multiple areas. The device supports three instance area types of Level-1, Level-2, and Level-1-2. The Level-1 router is deployed in the area, the Level-2 router is deployed between the areas, and the Level-1-2 router is deployed between the Level-1 router and the Level-2 router. The device supports the deployment of Level-1 router, Level-1-2 router and Level-2 router. Through the IS-IS routing penetration function (Level-2 to Level-1), the Level-2 routing information and the Level-1 routing information of other areas can be penetrated into the Level-1 area.

By controlling the IS-IS routing penetration (level-1 to level-2), you can control IS-IS routing information in the Level-1 area not to permeate to Level-2, and effectively control the routing information in Level-2 level. For the ISIS basic functions, specific routing penetration and

information control methods, please refer to the IP routing chapter ISIS related content of H20RN Intelligent Packet Devices Configuration Guide (CLI).

BGP

BGP (Border Gateway Protocol) is a dynamic routing protocol that can be used between different ASs (Autonomous Systems) and within the same AS. It is not focus on finding and calculating routes, but on controlling the propagation of routes and choosing the best route. According to the AS where the peer resides, it can be divided into an IBGP peer (the peer and the local router are located in the same AS) and an EBGP peer (the peer is located in a different AS from the local router). The device supports the two peers. The device supports route aggregation and route attenuation.

- Route aggregation

Route aggregation is actually the process of merging multiple routes. In this way, when BGP advertises routes to its peers, it can advertise only the aggregated routes instead of advertising all the specific routes. Currently, the H20RN-2000.V2 series devices software system supports automatic aggregation and manual aggregation. Using manual aggregation also controls the attributes of the aggregated route and determines whether to advertise specific routes.

- Route attenuation

When a route changes, the routing protocol will advertise a route update to the neighbors. The router that receives the route update needs to recalculate the route and modify the route table. The route attenuation can suppress unstable BGP route information. The device supports the route attenuation function but does not add such routes to the BGP routing table, nor advertise such routes to other BGP peers.

For detailed configuration examples, configuration prerequisites, and methods of BGP, refer to the IP Routing section of the *H20RN Series Configuration Guide (CLI)*.

3.5 IP Service

3.5.1 DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol which can assign IP address dynamically in the TCP/IP network. It is based on BOOTP (Bootstrap Protocol), and adds more

functions on it, such as automatic allocation of available network addresses, Network address reuse and other extension configuration options.

DHCP uses client/server model, the client sends configuration application to the server (including IP address, subnet mask, default gateway), and then the server returns the IP address assigned to the client and other corresponding configuration information, so as to realize dynamic configuration of things like IP address.

H20RN-2000.V2 series platforms support DHCP Client/Server and DHCP Relay functions. After the DHCP client obtains an IP address from the DHCP server, it cannot use the IP address obtained by the DHCP server permanently. Instead, it has a fixed lifetime, which is called the lease time. The length of the time can be specified by the user, and the IP address will be recycled after lease time becoming the due. For the lease time range that can be configured on the device, refer to the *H20RN Series Command Reference*.

Generally, we use the DHCP Server to complete the IP address allocation in the following occasions:

- With a large scale of networks, manual configuration requires a lot of work and it is difficult to centrally manage the entire network.
- The number of hosts in the network is greater than the number of IP addresses supported by the network. Each host cannot be assigned a fixed IP address, and there are restrictions on the number of users accessing the network at the same time.
- A large number of users must dynamically obtain their own IP address through the DHCP server.
- Only a few hosts in the network need a fixed IP address, and most hosts do not have a fixed IP address requirement.

The device also supports DHCP Relay function, which enables relay services between DHCP clients and DHCP servers on different network segments, and relays DHCP protocol packets across the network segment to the destination DHCP server. DHCP clients on different network segments can use the same DHCP server. For specific DHCP configuration examples, refer to the IP Services section of the H20RN Intelligent Packet Devices Configuration Guide (CLI).

Zero-touch Configuration

H18EDD-0402C supports zero-touch configuration function, it means that remote device can realize auto-discovery, Plug and Manage, no need to configure management VLAN and management IP, as long as the NMS service path of the PTN Network is unblocked, the correct configuration needed by management can be generated automatically and the communication with NMS server will be established. Note that zero-touch configuration realizes zero configuration of NMS channel; the configuration relating to services still needs manual configuration.

If the device had been configured with management VLAN, and then been moved, there are two methods to realize zero-touch configurations when management VLAN changed: method 1---you can restore manufacturer defaults through command lines at CONSOLE port. After rebooting the device, management VLAN will be detected automatically, but all the previous configurations of the device will be restored to factory state; method 2--- configure the management VLAN through command lines at CONSOLE port and save the configuration; when connecting to the network, the device will be shown in the NMS. This method can ensure that the previous configuration of the device will not be changed.

3.5.2 ARP

ARP (Address Resolution Protocol) is a protocol used to resolve the IP address to Ethernet MAC address (or physical address).

In a network, when the host or other network device has data to be sent to another host or device, it must know its network layer address (that is, the IP address). But it is not enough to have an IP address, because the IP datagram must be encapsulated into a frame can be sent through the physical network, so the sending station must also have a physical address of the terminal, so need a mapping from IP addresses to physical addresses. ARP is the protocol to implement this feature.

Device ARP address mapping entries include the following two types:

- Static entry: A static entry is a static binding of an IP address and a MAC address to prevent ARP dynamic learning from spoofing.
  - Static ARP address entries need to be manually added and manually deleted.
  - Static ARP address is not aged

- Dynamic entry: MAC address learned automatically by the device through ARP.
  - Dynamic table entries are generated automatically by the switch and do not require manual configuration. You can adjust some parameters of dynamic ARP.
  - If not used, the aging time will be aged.

For dynamic ARP aging time and dynamic ARP limit, refer to the *H20RN Series Command Reference*.

3.5.3 NDP

Using the NDP (neighbor discovery protocol) on IPv6 devices of the same link can discover each other's existence, determine each other's MAC address and maintain neighbor device information.

The NDP obtains the link layer address (the MAC address) of the neighbor device on the same link through the Neighbor Solicitation message NS and the Neighbor Advertisement message NA.

Through the use of ICMPv6 messages, the IPv6 Neighbor Discovery Protocol can also be used to verify neighbor reachability, duplicate address detection, routing device discovery/prefix discovery, address auto-configuration, and redirection. Refer to the *H20RN Series Configuration Guide (CLI)* for the detailed configuration of this device.

3.5.4 Ping

The device supports the Ping function for troubleshooting and excluding commands. The ping function is generally implemented with ICMP Echo packets. If the network runs normally, it will return a set of response packets.

3.6 Multicast

IGMP

Internet Group Management Protocol (IGMP) manages the membership of hosts and routing devices in multicast groups. IP hosts use IGMP to report their multicast group memberships to any neighboring multicast routing devices. Multicast routing devices use IGMP to learn, for each of their attached physical networks, which groups have members.

IGMPv3, defined in RFC 3376, adds support for Source-Specific Multicasting (SSM) and source filtering. Source filtering enables a multicast receiver host to signal from which groups it wants to receive multicast traffic, and from which sources this traffic is expected. That information may be used by multicast routing protocols to avoid delivering multicast packets from specific sources to networks where there are no interested receivers. Two filter modes in IGMPv3 source filtering are INCLUDE mode and EXCLUDE mode.

IGMP snooping is a multicast constraint mechanism running on layer 2 devices, which is used to manage and control multicast groups. By analyzing the received IGMP message, the layer-2 device running IGMP snooping establishes the mapping relationship between the port and the MAC multicast address, and forwards the multicast data according to the mapping relationship.

IGMP Proxy is similar with IGMP snooping, but it is to establish multicast table by intercepting IGMP messages between users and routers. The upper port of the proxy device performs the role of host, and the lower port performs the role of router.

3.7 MPLS-TP

Based on MPLS, MPLS-TP (Multiprotocol Label Switching-Transport Profile) expands packet forwarding, network protection, network management, control plane and OAM technologies to meet more requirements for carrier-transmission network.

GRE

GRE (Generic Routing Encapsulation) is a kind of generic protocol that multiple network protocol packets can be encapsulated as IP packets and transmitted over IP networks. GRE can be used as a third layer Tunnel protocol for VPN, using Tunnel technology between the protocol layers. Tunnel is a virtual point-to-point connection, the connection is established through a logical tunnel interface, and this interface provides a pathway, making the encapsulated data packets transmit on the channel, and encapsulate data packets at both ends of a tunnel.

Static LSP

MPLS needs to pre-assign labels for the packet, sets up a LSP, and then can conduct packet forwarding. LSP is divided into a static LSP and a dynamic

LSP. Static LSP is configured manually by the administrator, while dynamic LSP is established dynamically by routing protocol and the label released protocol.

NOTE

- Assigning labels manually needs to follow the principle: the output label value of the previous node is the input label value of the next node.
- As for static LSP, each LSR can't rely on awareness to get the whole LSP situation, so the static LSP is a local concept.

L2VPN

MPLS L2VPN provides layer-2 VPN service based on MPLS network, so that the operator can provide layer-2 VPN based on different data link layer protocols on the unified MPLS network, including ATM, FR, VLAN, Ethernet, PPP etc. Simply, MPLS L2VPN transfers user's layer-2 data transparently in MPLS network.

H20RN-2000.V2 series platforms support the following two L2VPN services:

- VPWS (Virtual Pseudo Wire Service) provides point-to-point layer-2 data link frame transmission, mainly used in bearing Ethernet layer-2 service.
- VPLS (Virtual Private LAN Services) provides similar LAN technology in wide area network range, integrating a plurality of local area networks in wide area range into a network, and provides virtual Ethernet LAN services for users.

Based on VPWS and VPLS, H20RN-2000.V2 series platforms can realize L2VPN services in following three types.

- E-Line service (EPL, EVPL) L2VPN (VPWS);
- E-LAN service (EP-LAN, EVP-LAN) L2VPN (VPLS);
- E-Tree service (EP-Tree, EVP-Tree) L2VPN (root node is VPLS, Leaf node is VPWS);
- E-Access service (Access EPL, Access EVPL) L2VPN, wholesale access service.

PW Redundancy Protection

If there is only one PW between the two CE, when the fault occurs to the PE node, the link between PE and CE, or PW between PE nodes, the communication between CE will be broken. The PW redundant protection function is implemented by deploying the master and standby PWs, the flow will be switched to backup PW immediately when the fault occurs to the master PW, so that the flow can be forwarded normally.

L3VPN

MPLS L3VPN is a Layer 3 VPN technology. It uses BGP to advertise the private routes of user sites on service provider backbones, and uses MPLS to forward private network packets between user sites on service provider backbones, so as to realize the user sites belong to the same VPN and in different geographic locations through provider's backbone network connections.

For detailed MPLS-TP related service configuration and service examples, refer to the H20RN Intelligent Packet Devices Configuration Guide (CLI). Specific application scenarios, configuration prerequisites, and data preparation are included in this manual.

3.8 QoS

QoS (Quality of Service) can ensure the timeliness and integrity of important service during network overload or congestion and the highly efficient running of the entire network.

3.8.1 Port Speed Limit

H20RN-2000.V2 series platforms offer port speed limit, which will discard the excess flow. The limit granularity is 8Kbps.

- Based on port
- Based on Tunnel VC
- Based on Policy

3.8.2 Priority Trust

Priority trust is a subsequent QoS management operation of packet classified by its own priority. Generally, the larger the priority field value of the packet is, the higher its priority will be.

The trusted priorities of H20RN-2000.V2 series platforms are:

- IP packet based DSCP (Differentiated Services Code Point) priority
- VLAN packet based CoS (Class of Service) priority
- LSP based EXP priority

3.8.3 Traffic Classification

Users can classify traffic according to layer-2, layer-3 information carried by the packet, or with the help of ACL (Access Control List), and then relate traffic classification to some traffic behavior, and deal with the packet within traffic classification correspondingly.

H20RN-2000.V2 series platforms support traffic classification by the following methods:

- Based on port
- DSCP priority based on IP packet
- ToS priority based on IP packet
- CoS priority based on VLAN packet
- VLAN ID based on VLAN packet
- Based on ACL (Access Control List) rules
- Based on source or destination MAC
- Based on source or destination IP
- Based on source or destination TCP/UDP port number
- Based on MPLS LSP or PW tag
- Based on MPLS LSP or PW EXP

3.8.4 Traffic Behavior

Traffic classification is to provide services differently, which makes sense only when associates with some traffic control or resource allocation behavior.

Traffic behaviors supported by H20RN-2000.V2 series platforms are traffic rate limit, re-direction and re-tagging.

The device supports retagging the following fields of the packet:

- ToS priority of IP packet
- DSCP priority of IP packet
- CoS priority of VLAN packet

- VLAN ID of VLAN packet

- Mirroring

Mirroring based on flow means that the device copies the packets which comply with specified rules to a specified port for network supervision and troubleshooting.

- Commit access rate

CAR (Commit Access Rate) limits packet flow rate through setting CIR, CBS, PIR, PBS and other CAR parameters, and sets actions towards packet with different PHB (Per-Hop Behavior) colors, such as discarding, retagging colors, retagging service levels, and so on.

3.8.5 Traffic Policy

Traffic policy is a complete QoS policy formed after the association of traffic classification and traffic behavior. The user can bind a specified class to a traffic behavior via traffic policy for convenient QoS control.

3.8.6 Priority Mapping

Priority mapping is to send ingress packets to packet queues of different internal priorities according to the preset mapping relation between external priorities and internal priorities, so as to schedule different queues in output direction.

H20RN-2000.V2 series platforms support priority mappings of IP packet based DSCP priority or VLAN packet based CoS priority and LSP based EXP priority.

3.8.7 Queue Scheduling

When delay-sensitive service requires QoS service of higher quality than non-delay-sensitive, and congestion occurs intermittently in the network, queue scheduling will be needed.

The supported queue scheduling algorithms include SP (Strict-Priority), WRR (Weight Round Robin), DRR (Deficit Round Robin), SP+WRR and SP+DRR. Each scheduling algorithm is to solve certain network flow problems and has different influences on allocation, delay, and jitter of bandwidth resource.

3.8.8 Congestion Avoidance

Congestion avoidance refers to discard packets actively when congestion occurs or worsens by monitoring the usage of network resources (like queues or memory buffers). It is a flow control mechanism relieving network overload by adjusting the network flow.

H20RN-2000.V2 series platforms support the configuration of RED for congestion avoidance.

WRED (Weighted Random Early Detection) technology is to avoid TCP global synchronization by discarding packets randomly, but its random discarding parameters are queue-based, which distinguishes among discarding polices by the queue of the packets and its color and take the interests of packets in high-priority queues into consideration, making their probability of being discarded relatively small.

3.8.9 Traffic Shaping

Traffic shaping is to control the packet rate, therefore packets can be sent at a uniform rate. Traffic shaping is usually for the match between the packet rate and the downstream device, to avoid unnecessary packet discard and congestion.

H20RN-2000.V2 series platforms support queue–based traffic shaping; first the queue where the traffic is in must be confirmed, then traffic shaping parameters must be configured to it, including committed rate and committed burst size. For the packets that exceed the committed burst size, they will be cached and delayed to send out.

3.8.10 Traffic Statistics

H20RN-2000.V2 series platforms support traffic statistics. Traffic statistics based on flow is to use QoS to classify packets and then make traffic statistics. They can help users to make a statistical analysis of interested packets.

3.8.11 Port Mirror

H20RN-2000.V2 series device offers mirror function based on port, i.e. copying packet from a specific port to mirror port for analysis and monitoring.

3.8.12 ACL

H20RN-2000.V2 series platforms support port-based ACL (Access Control List). In the network, to control the illegal packet's influence, a series of rules on the device is required to be configured to determine what types of data packets can pass. These rules are defined through ACL.

ACL has the following types:

- IPv4 ACL: making classification rules according to the source or destination addresses carried by data packet IP head and the used TCP or UDP port number.

- IPv6 ACL: making classification rules according to the source or destination addresses carried by data packet IPv6 head, the used TCP or UDP port number and the tag value.
- MAC ACL: making classification rules according to the source MAC address, destination MAC address, IEEE 802.1p priority, layer-2 protocol type, and other layer-2 information carried by data packet layer-2 frame head of data packet.

3.8.13 CPU Protection

When the device is in a complex network environment, it is likely to be attacked by various types of packets, such as ARP packets, BPDU packets, and ICMP packets. If the device receives a large number of attack packets within a short period of time, the CPU runs at full capacity and the utilization rate reaches 100%, device's functions will not run normally.

The CPU protection function is to prevent such packets from attacking. The principle is to monitor the packet statistics of certain types of packets in real time. When a certain number of packets received on the interface exceed the discard threshold within a certain interval, the interface discards the packets and does not send them to the CPU, through which, the CPU is protected. If the number of received packets on the interface is smaller than the normal threshold, the packets entering the interface will not be discarded.

3.9 AAA

AAA (Authentication, Authorization, Accounting) is a network security management mechanism, providing authentication, authorization, and accounting security functions.

The device supports basic AAA functions, RADIUS authentication, accounting functions, TACACS+ authentication, and accounting functions.

- Authentication is used to verify the identity of the remote user accessing the network and determine whether the visitor is a legitimate web user.
- Authorization is used to give different permissions to different users, limit the services users can use. For example, office users who are authorized by administrators can access the server and print files, while, other temporary visitor does not have the permission.

- Accounting is used to record all operations in the process of user accessing to network services, including the service types, starting time, data flow, etc. It is also used to collect and record the usage of network resources, and can realize the accounting requirements for time and traffic, as well as network monitoring.

RADIUS

RADIUS (Remote Authentication Dial In User Service) is a standard communication protocol for authenticating and authorizing dial-up users. RADIUS authentication function

RADIUS is a client/server protocol. Remote users dial into the access server, and the access server sends authentication requests to the RADIUS server. The RADIUS server authenticates users and authorizes access to internal network resources. Remote users are clients to the access server and the access server is a client to the RADIUS server. The user and the access server exchange authentication information. In this way, you can control the user accessing to equipment and network, improve the network security.

The communication between the client and the RADIUS server is identified by the use of the Shared key, which is not transmitted over the network. In addition, any user password that is sent between the client and the RADIUS server requires an encryption process to avoid the user's password being obtained by sniffing out a non-secure network.

- RADIUS accounting function

The RADIUS accounting refers to the ability of RADIUS to gather information about user sessions that can be processed for billing and network analysis. It is mainly aimed at users who are authenticated by RADIUS. When a user logs in, he sends a start billing message to RADIUS billing server, and then, sends billing update message to the RADIUS billing server according to the billing strategy during login, after logging out, sends the stop billing message to RADIUS billing server, this message contains the user login time. With these messages, the RADIUS billing server can record each user's access time and actions.

TACACS+

TACACS+ (Terminal Access Controller Access Control System) is a kind of network access authentication protocol, which is similar to the RADIUS. The differences are:

- TACACS+ uses TCP port 49, while RADIUS uses UDP port, so TACACS+ has higher transmission reliability;

- TACACS+ encrypts the whole data packet except TACACS+ head, while RADIUS only encrypts the user password, TACACS+ has higher security;
- TACACS+'s authentication function is separated from the authorization and accounting functions, and the deployment is more flexible.

3.10 OAM

3.10.1 BFD

BFD (Bidirectional Forwarding Detection) is a common and standardized fast fault detection mechanism, which has nothing to do with the medium or protocol. It is used to detect link connection condition of IP network, ensure that the communication fault between the devices can be quickly detected, so as to take measures timely to ensure the continuous operation of the services.

BFD can quickly detect the failure of the bidirectional forwarding path between two devices for various upper level protocols, such as routing protocol, MPLS, etc. The upper layer protocol usually uses the Hello packet mechanism to detect the failure, and the required time is second, while BFD can provide a millisecond level detection.

In practice, BFD can be used for single-hop and multi-hop detection:

- Single-hop detection refers to the IP connectivity detection of two direct connected devices. The "single-hop" is a hop of IP.
- Multi-hop detection：BFD can detect the link of any path between two devices that can span a lot of hops.

3.10.2 MPLS OAM

H20RN-2000.V2 series platforms support MPLS-TP OAM function. In MPLS-TP network, using GACH (Generic Associated Channel, a general correlation channel) defined in RFC5586 as control channel of the PW layer (VC+Tunnel), LSP layer and Section layer (physical link) to encapsulate and transfer the related packets of OAM technology defined in Y.1731 through the GACH, and then can realize the OAM function based on MPLS-TP.

MPLS-TP OAM mainly achieves the following functions:

- Detect, identify and locate the MPLS user's fault.

- Measure the utilization of the network and the network performance.

3.10.3 CFM

CFM (Connectivity Fault Management) is an end-to-end OAM protocol, which is used to conduct an active fault diagnosis for EVC (Ethernet Virtual Connection) and reduce network maintenance cost through fault management to increase Ethernet maintainability.

This equipment provides fault management functions compatible with ITU-T Y.1731 and IEEE 802.1ag standards, and performance monitoring functions defined in Y.1731, collectively referred to as Y.1731 functions. Includes the following features:

- Fault Detection function

Fault detection function means to check the continuity of EVC by CC (continuity check) protocol and confirm connection state between MPs (Maintenance Point).

- Loopback function (LB)

Loopback function is used to confirm the connection state between the local device and the remote device. This function is to ascertain the connectivity between two MPs by sending LBM (Loop Back Message) from source MEP to destination MP and sending LBR (Loop Back Reply) from destination MP to source MEP.

- Link Trace function (LT)

Link trace function is used to confirm the path from source MEP to destination MP. This function requires source MEP to send LTM (Link Trace Message) to destination MP. Every MP device in the LTM transmission path will send back LTR (Link Trace Reply) to source MEP. Through noting effective LTR and LTM the path between MP will be finally confirmed.

- Performance Monitoring

ITU-T Y.1731 defines the measurement of frame loss rate, frame delay and frame delay variation for point-to-point Ethernet connection.

3.10.4 Y.1731

The CFM part of Y.1731 is basically the same as IEEE 802.1ag, and ETH-AIS, ETH-LCK, PM and other functions are added.

- ETH-AIS (Ethernet-alarm indication signal)

Alarm indication signal is used to reduce the reported amount of fault alarms. If a MEP fails to receive the remote CCM message within 3.5 CCM periods, it will be considered as link fault, and AIS message (Alarm Indication Signal) will be sent periodically. After receiving AIS message,

MP will suppress the local fault alarm and continue to send AIS message. AIS message will be stopped to be sent when each MP can receive CCM message again.

- ETH-LCK (Ethernet lock signal)

Ethernet lock signal (ETH-LCK) function is used to communicate the administrative locking and the subsequent interruption of data traffic, enabling the MEP that receives ETH-LCK information to differentiate between a defect condition and an administrative locking of a server (sub-) layer MEP.

- ETH-RDI (Ethernet Remote Defect Indication)

Ethernet remote defect indication (ETH-RDI) is used to indicate the local defect to its peer MEP.

- ETH-Test (Ethernet Test Signal)

Ethernet test signal (ETH-Test) can perform a one-way online or offline diagnostic test as required, including verifying bandwidth throughput, frame loss, BIT ERR and etc.

- PM (Performance Monitoring)

It defines the measurement of throughput, frame loss rate, frame delay and frame delay variation for point-to-point Ethernet connection.

3.10.5 EFM

IEEE 802.3ah-compliant EFM (Ethernet in the First Mile) is a link-level Ethernet OAM technology. It focuses on link between two directly connected H18EDD-0402C devices and provides link connectivity check, link fault monitoring, remote fault notification, and other functions. EFM is mainly applied in Ethernet link of user access network edge.

OAM Mode and OAM Discovery

H18EDD-0402C device supports two modes for Ethernet OAM connection: active mode and passive mode. Active OAM entity can initiate Ethernet OAM connection, while passive OAM entity can respond to it.

After Ethernet OAM connection is built, the OAM entities at both ends keep connection through sending Information OAMPDU. If there is no Information OAMPDU from link partner OAM entity received in five seconds, connection will be expired and OAM connection will be rebuilt.

Tip: Link aggregation logical ports do not support IEEE802.3ah OAM, but link

aggregation member ports support IEEE802.3ah OAM.

OAM Remote Loopback

When the Ethernet OAM connection is built, active OAM entity initiates remote loopback command and the link partner entity corresponds to it.

Under remote loopback state, active OAM entity sends all the other packets except OAMPDU to the link partner (the remote end); the link partner will return them the local end after receiving them. It can be used to locate link failure and detect link quality: network administrators can judge link performance (including packet loss rate, delay, jitter and etc.) by observing the returned state of non-OAMPDU packets.

OAM Link Event

Link events include general link events and critical link events, the former is used for link performance monitoring while the latter is used for remote failure detection. The supported general and critical link events are respectively shown in Table 3-2 and Table 3-3.

Table 3-2 General link events

Event type	Description
Errored Symbol Period Event	The number of errored symbol exceeds the defined threshold per unit time
Errored Frame Event	The number of errored frame exceeds the threshold per unit time
Errored Frame Period Event	The number of errored frame exceeds the threshold within the time of receiving specified number of frames
Errored Frame Seconds Summary Event	The number of errored frame seconds exceed the threshold within the specified time

Table 3-3 Critical link events

Event type	Description
Link Fault	Remote link signal loss
Dying Gasp	Unpredictable local failure occurs, such as power interruption
Critical Event	Undefined critical event occurs, such as the temperature is too high or too low

3.11 IEEE RFC 2544

RFC2544 protocol is an international standard proposed by RFC organization for evaluating network interconnection equipment (firewall, IDS, Switch, etc.). It mainly specifies the specific test method and the form of result submission of performance evaluation parameters defined in RFC1242.

RFC2544 provides a number of parameters for testing different network devices. The following is a brief introduction of the four most important parameters:

- Throughput

Throughput reflects the maximum data flow that the device under test can handle (without losing packets).

- Frame Loss

Frame loss can reflect the ability of the device under test to bear a specific load.

- Latency

Send a certain number of packets, record the time T1 when the intermediate packets are sent and the time T2 when they arrive at the receiving port after being forwarded by the test device, and then calculate according to the following formula:

For storage/bit forwarding devices: Latency = T2-T1

Latency can reflect the speed of processing packets by the device under test.

- Back-to-Back

Back-to-Back reflects the ability of the device under test to deal with burst data (data cache ability), that is, the maximum data packet processed per second.

3.11.1 ITU-T Y.1564

Prior to Y.1564, the most widely used testing tool to assess the Ethernet performance, was RFC 2544. However, RFC 2544 does not include all required measurements such as throughput, frame loss, packet jitter, latency, QoS measurement and multiple concurrent service levels.

Y.1564 supports current service providers' offerings, which typically consist of multi-services. It allows them to simultaneously test all services and measure if they qualify to the committed SLA attributes. Y.1564 defines test streams (or "flows") with service attributes and these test flows can be classified using various mechanisms, such as 802.1q VLAN, 802.1ad, DSCP and class of service (CoS) profiles.

3.11.2 SLA

SLA is a real-time network performance detection and statistics technology. It can count network information such as response time, network jitter, delay, and packet loss rate. The SLA of the device can be used to monitor different job-related metrics by selecting different jobs for different applications.

3.11.3 DDM

H18EDD-0402C supports DDM (Digital Diagnosis Monitoring) function defined in SFF-8472, which is used to real-time monitoring optical port connection status&quality, real-time monitoring of intelligent optical module's emission optical power, reception optical power, temperature, work voltage, laser offset current, and other parameters. Through analyzing monitoring data of optical module, you can predict its service life, isolate system fault, and authenticate the compatibility of optical module in on-site installation.

3.11.4 RMON

RMON (Remote Network Monitoring) is a standard of network data monitoring through different network Agent and NMS, which is established by IETF (Internet Engineering Task Force). RMON mainly realizes functions of statistics and alarm, is an extension of SNMP, but it monitors the remote device more actively and effectively than SNMP, making network administrators track failures occurring to the network, segment and device more quickly.

Users can configure the devices' RMON event group, RMON alarm group, RMON statistics group, RMON history group and etc.

- Statistics group: responsible for collecting statistical information of an interface, including the statistics of the count and size;
- History group: similar to statistics group, but it collects statistical

information in a specified detection period;

- Alarm group: monitor a specified Management Information Base (MIB) object within a time interval, and set the rising threshold and the falling threshold, if the monitored object reaches the threshold, an event will be triggered;
- Event group: work with alarm group, when an alarm triggers an event, it will record the corresponding event information, such as sending Trap information and writing to log.

3.12 Network Management

3.12.1 SNMP

SNMP (Simple Network Management Protocol) is a network management standard protocol which is used to solve the management in network devices.

Currently, the SNMP protocol has three versions: v1, v2c and v3.

- SNMPv1 uses a Community Name authentication mechanism. The community name is used to define the relationship between the SNMP network management system and the SNMP agent and acts like a password to limit the access of the SNMP network management system to the SNMP agent. If the community name carried in the SNMP packet does not pass the authentication on the device, the packet will be discarded.
- SNMPv2c also uses a community name authentication mechanism. It is compatible with SNMPv1 while expanding the functionality of SNMPv1: it supports more types of operations, data types and error codes, and can distinguish the error more accurately.
- SNMP v3 uses USM (user-based security model) and VACM (view-based access control model) security mechanisms. The user can set the authentication and encryption functions. Through the combination of authentication and encryption, the user can provide higher security for communication between the SNMP network management system and the SNMP agent. Authentication is used to verify the legitimacy of the sender of the packet and avoid accessing

by unauthorized users. Encryption is to encrypt the transmission packet between the NMS and the agent to avoid eavesdropping.

The device supports SNMP versions v1, v2c, and v3.

3.13 Clock

SyncE

H20RN-2000.V2 series platforms support Synchronous Ethernet (SyncE).

Synchronous Ethernet (SyncE) means that devices in the network extract clock signals from physical links or external BITS interfaces, and choose the one of the signals with the highest quality as the local clock from multiple clock signals and send it to the downstream devices through other interfaces, thus the concatenation relationship between the upstream clock and the downstream clock will be produced, so as to realize clock synchronization among the devices in the Ethernet transmission network.

SyncE technology can perform clock synchronization in packet transport network, as it only supports clock frequency synchronization instead of clock phase synchronization, so it is suitable for base stations, fixed network TDM relay, dedicated clock network relay, GSM (Global System for Mobile Communications) that has no requirements for clock phase synchronization, WCDMA (Wideband Code Division Multiple Access) wireless base station and etc.

H20RN-2000.V2 series platforms support three clock source types:

- External clock source

  Access 2MHz, 2Mbit/s clock signal form external clock-source devices through BITS interfaces provided by the devices.

- Ethernet line clock source

  Extract clock signal from the optical port.

- Local clock source

  Provide clock signal from the crystal oscillator inside the device.

H20RN-2000.V2 series platforms can choose the best clock source automatically according to G.781 protocol, as well as choose the specified clock source manually.

NOTE

- Clock synchronization system of SyncE is mature and reliable, which meets timing interface specifications of ITU-T G.823. It is not affected by the changes of network load, but as the transmission of clock are link-based, therefore SyncE technology requires that all the devices in the clock link have SyncE feature.

NTP

NTP (Network Time Protocol) is a time synchronization protocol defined by RFC1305, which is used for the time synchronization between distributed time server and client.

IEEE 1588v2

The IEEE 1588-2008 Precision Time Protocol (PTP) is designed to distribute sub-microsecond timing accuracy to slave nodes in packet-based transport environment. The most suitable domain for PTP is a local area network where timing distribution is limited to a few intermediate nodes with each step inevitably introduces some degradation to the accuracy.

3.14 CES

H20RN-2000.V2 series platforms support CES (Circuit Emulation Service, circuit emulation service) function, which is implemented based on PWE3 (Pseudo Wire Emulation Edge to Edge) protocol frame work, using SAToP (Structure-Agnostic TDM over Packet) encapsulation type, E1 service is used as a serial data bit stream to segment and encapsulate. After that, transfer E1 service on PW line through MPLS, IP and MEF encapsulating formats, pass through the PSN network, Tunnel, reach the PW exit, and then de-capsulate it, finally, reconstruct E1 service flow. EC16 card of H20RN-2000.V2 series platforms supports 16 channels of E1 services.

Clock Synchronization

The clock working modes at the receiving end of H20RN-2000.V2 series platforms are as follows:

- Adaptive timing mode (ACR)

  The adaptive timing model is that the receiver reconstructs timing mode over E1 stream transferred from peer end.

- Loopback timing mode

  Loop timing mode refers to extracting clock from E1 input port signal to reconstruct E1 output bit stream. The memorizer inside the network absorbs the drift formed by the network transmission completely. Once the loss of input signal occurs, loop timing mode will switch to the adaptive timing automatically.

- Differentiated timing mode (DCR)

  Differentiated clock mode refers to both the sending terminal and the receiving terminal devices are provided with a reference clock. Sending terminal device codes the difference between source clock and the reference clock and then transfers it. The receiving terminal device compares the difference between the receiver clock and the reference clock according to the difference sent by the sending terminal device, so as to adjust clock.

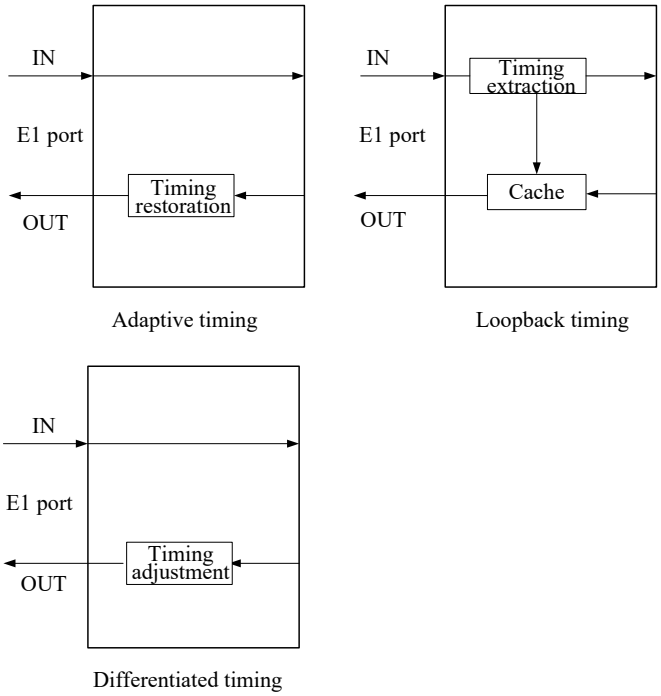
- Restoration timing mode in physical layer signal

  The clock reference source can be IEEE 1588, synchronous Ethernet or GPS.

- Local clock source

  The local oscillator (internal free oscillation clock)

Figure 3-1 Timing mode diagram



The clock working modes at the transmitting end of H20RN-2000.V2 series platforms are as follows:

- Loopback clock

  Loopback timing mode refers to extracting clock from E1 input port signal to reconstruct E1 output bit stream.

- External clock synchronization port (2MHz, 2Mbit/s)

  Access 2MHz, 2Mbit/s clock signal form external clock-source devices through BITS interfaces provided by the device.

- Internal free oscillation clock

  The local oscillator (internal free oscillation clock)

Delay Jitter Cache

H20RN-2000.V2 series platforms support RTP (Real-time Transport Protocol), which is used to define the E1 timestamp (removing jitter and realizing the synchronous). It can realize the

jitter absorption cache.

3.15 STM-1 Interface Emulation

H20RN-2000.V2 series devices support STM-1 interface emulation card (SC01QE), which can work with remote H20RN-161E device. The remote E1 is emulated by PWE3, and multiplexed to STM-1 at CO. Working mode can be configured to un-channelized STM-1 interface emulation card and channelized STM-1 interface emulation card.

NOTE

SC01QE card defaults to E1 emulation, you can use **switch emulation-image (e1 | stm-1) slot <1-32>** under **config** node to switch its working mode.

SC01QE supports LAS (laser automatic shutdown) function. It supports SDH service, including standard SDH frame structure, SDH frame demarcation, clock recovery, processing of segment layer overhead, alarm and performance statistics, and PWE3 service encapsulation load.

At E1 emulation mode: SC01QE supports 126-channel SAToP compliant E1 circuit emulation, and can work with H20RN-161E device. SDH clock supports synchronization to local clock, to external clock and to clock at STM-1 optical port. The E1 clock recovery function supports local clock, port loop-back clock, adaptive timing and differential timing, and the differential algorithm reference source supports external clock or synchronous Ethernet.

AT STM-1 emulation mode: supports 4-channel SOP compliant STM-1 interface emulation. SDH clock supports synchronization to clock at STM-1 optical port. When the physical layer synchronous clock is used to restore timing, the physical layer clock reference source supports external clock or synchronous Ethernet.

SC01QE supports MSP 1+1 protection, fixed at port 1 and port 2, port 3 and 4 for mutual protection. Port 1 (protection port 2) has 63 VC12; corresponding to CES emulation interface 1-63, it can be used only when there is no protection. Port 3 (protection port 4) has 63 VC12; corresponding to CES emulation interface 64-126, it can be used only when there is no protection.

4 Device Management

NM and CONSOLE ports on the front panel of H20RN-2000.V2 series platforms are management ports, which support EzView NMS, SNMP, and CLI command line.

The default hios system IP address of H20RN-2000.V2 series platforms is 192.192.4.2; the IP address mask is 255.255.255.0.

H20RN-2000.V2 series platforms support the following management methods:

1. CLI: uses hyper terminal through CONSOLE port to log in CLI; or use Telnet through NM port to log in CLI. Telnet command format: Telnet IP, e.g. Telnet 192.192.4.2. The username is admin and password is Admin123. The protocols used by hyper terminal are: baud rate: 115200bps; data bit: 8; parity bit: none; stop bit: 1.
2. SNMP: supports SNMP V1 and SNMP V2c and uses community based access control. The SNMP packet which does not comply with community recognized by device will be discarded. Different communities can have Read-Only access authority or Read-Write access authority. The Read-Write authority can query device information and configure the device, while Read-Only authority can only query device information. By default, the system has created a community with Read-Only authority named Public and a community with Read-Write authority named Private. The default configuration cannot be deleted or modified. You can create new communities if required. It supports Trap. Trap means that the device automatically sends unrequested information to NMS, to report urgent events.
3. EzView NMS: For details, please refer to the online help of the software.

Remote in-band IP address can be used to implement remote in-band monitoring function. One device in network is configured as Master node, and other devices are configured as Slave nodes. Only one Master node can exist in the network. At in-band mode, Master node should be configured to route or bridge, and configuration of Slave nodes is ineffective. If remote in-band IP address and management IP are not in the same subnet, in-band mode is route; if they are in the same subnet; in-band mode is the bridge. In addition, in-band management port should be configured. Master node and Slave nodes are connected through in-band management port, which is usually NNI port.

CAUTION

For security reasons, you are recommended to modify the password when using H20RN-2000.V2 series platforms for the first time.

5 Appendix Terms and Abbreviations

This chapter introduces terms and abbreviations involved in this user's manual.

- Terms
- Abbreviations

Terms

A

ACL (Access Control List)	ACL is a of sequential rules composed by permit | deny statements. Based on these rules, the device determines which data packets can be received and which must be denied.
APS (Automatic Protection Switched)	Automatic protection switched technology can conduct real-time monitoring towards transmission path and automatic analysis of alarm information, to timely detect the fault and hidden dangers. In the event of a serious fault, it can automatically switch the working channel to the spare channel, so as to recover the communication in time and complete the rapid response to failure and recovery mechanism.

Auto-Negotiation	Two interconnected Ethernet interfaces automatically select interface rate and duplex mode according to negotiation result.
DHCP (Dynamic Host Configuration Protocol)	DHCP is a technique for dynamically assigning IP addresses in the network. It can automatically assign IP addresses to all clients in the network, thereby reducing the workload of administrators and enabling centralized management of IP addresses.

E

EFM (Ethernet in the First Mile)	EFM that complies with IEEE 802.3ah is a link-level Ethernet OAM technology. It focuses on link between two directly connected devices and provides link connectivity check, link fault monitoring, remote fault notification, and other functions. EFM is mainly applied in Ethernet link of user access network edge.

F

Full-duplex	In a communication link, both parties can receive and send data concurrently

H

Half-duplex	In a communication link, only one party can send data at a time. One party is receiving information, while the other party is sending information

I

IEEE (Institute of Electrical and Electronics Engineers)	IEEE is an international electronic technology and information science and engineer association, which is also one of the world's largest professional technical organizations (number of members).

L

Label	Label is the Identification for cable, chassis and alarm.
LACP (Link Aggregation Control Protocol)	LACP is a protocol used to implement the link dynamic aggregation. LACP uses LACPDU (Link Aggregation Control Protocol Data Unit) to exchange information with remote side.
Link Aggregation	One logical aggregation group is formed through aggregating multiple physical Ethernet interfaces and the physical links in the same aggregation group is seen as one logical link, so as to implement link protection and load sharing between devices, greatly enhance reliability of service between devices, and enhance the bandwidth without upgrading the hardware.

M

Multi-mode Fiber	Multi-mode can be transmitted in one fiber

N

NTP (Network Time Protocol)	NTP is a time synchronization protocol defined by RFC1305, which is used for the time synchronization between distributed time server and client. The purpose of using NTP is to conduct fast clock synchronization to all devices which have clocks in the network, so that the device can provide different application based on the unified time. At the same time, NTP can guarantee high accuracy (error is about 10ms).
P	
Protection Ground Wire	Protection ground wire is used to connect device with the protection ground. Usually, it is a yellow-green coaxial wire.
Q	
QoS (Quality of Service)	QoS is a network security mechanism used to solve the network delay and congestion problems. It can ensure the timeliness and integrity of important service during network overload or congestion and the highly efficient running of the entire network.
QinQ (Stacked VLAN or Double VLAN)	QinQ is extended from 802.1Q, defined by IEEE 802.1ad recommendation. In carrier backbone network (public network), the packets take double VLAN Tag passing through trunk network (public network): public network VLAN Tag and private network VLAN Tag. In public network, the private VLAN Tag is transmitted as data in packets. QinQ supports basic QinQ and flexible QinQ

R

RSTP (Rapid Spanning Tree Protocol)	RSTP is developed to make up slow convergence for the STP (Spanning Tree Protocol). Based on STP, RSTP is improved a lot, which implements fast convergence for network topology.

S

SNMP (Simple Network Management Protocol)	SNMP is a protocol which is promoted by IETF (Internet Engineering Task Force) to solve the management in network devices. SNMP can make a NMS remote manage all SNMP supported network devices, including monitoring network status, modifying the network device configuration, and receiving network event alarm etc. It is the most popular network management protocol used in TCP/IP network.
SNTP (Simple Network Time Protocol)	SNTP is mainly used in the device time of synchronization network.
STP (Spanning Tree Protocol)	STP can remove loopback in a LAN and backup data links. Thus it can logically block loopback and avoid the generation of broadcast storm. When the unblocked link fails, the blocked link will be activated and serve as a backup line.

V

VLAN (Virtual Local Area Network)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segment logically rather than physically, thus implementing virtual work groups which are based on Layer 2 isolation and do not affect each other.

Abbreviations

A

AC	Alternating Current
ACL	Access Control List
ARP	Address Resolution Protocol
APS	Automatic Protection Switching

B

BC	Boundary Clock
BITS	Building Integrated Timing Supply System
BPDU	Bridge Protocol Data Unit

C

CAR	Committed Access Rate
CBS	Committed Burst Size
CE	Customer Edge
CIR	Committed Information Rate

CoS	Class of Service

D

DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DRR	Deficit Round Robin
DS	Differentiated Services

E

EFM	Ethernet in the First Mile
ERPS	Ethernet Ring Protection Switching
ESD	Electro Static Discharge
EVC	Ethernet Virtual Connection

F

FE	Fast Ethernet

G

GE	Gigabit Ethernet
GRE	Generic Routing Encapsulation

I

IEC	International Electro technical Commission

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

M

MAC	Medium Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface cross-over
MIB	Management Information Base

N

NTP	Network Time Protocol
NDP	Neighbor Discovery Protocol

O

OAM	Operation，Administration and Management
OC	Ordinary Clock
OSPF	Open Shortest Path First

P

P2P	Point-to-Point
PE	Provider Edge
PPP	Point to Point Protocol
PTP	Precision Time Protocol

Q

QoS	Quality of Service

R

RH	Relative Humidity
RADIUS	Remote Authentication Dial In User Service
RSTP	Rapid Spanning Tree Protocol

S

SFP	Small Form-factor Pluggable
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SP	Strict-Priority

STP	Spanning Tree Protocol

T

TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier

U

UNI	User Network Interface

V

VLAN	Virtual Local Area Network

W

WRR	Weight Round Robin