H18EDD-0402C Ethernet Demarcation Access Device

Product Description

Beijing Huahuan Electronics Co.,Ltd.

H18EDD-0402C

Ethernet Demarcation Access Device

Product Description

Beijing Huahuan Electronics Co., Ltd.
June.2019

Copyright Notice

The intellectual property rights of all parts of this product, including accessories etc., are owned by Beijing Huahuan Electronics Co., Ltd. (Beijing Huahuan for short). Without prior written consent of Beijing Huahuan, no part of this document may be reproduced or transmitted in any form or by any means. The information in this document, including product specifications and information, is subject to change without notice. For information related, please consult Beijing Huahuan.

Product Name: H18EDD-0402C Ethernet Demarcation Access Device

Version: 1.0

Release Date: June. 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

Contents i
List of Figures iii
List of Tables iv
1 Overview 1
1.1 Features 1
1.2 Ordering Information 2
2 Typical Application 4
3 Functional Properties 5
3.1 VLAN 5
3.2 QinQ 6
3.3 MAC 7
3.4 LLDP 8
3.5 Loop Detection 9
3.6 Interface Mirror 9
3.7 LACP 9
3.8 DHCP 10
3.9 QoS 11
3.9.1 Port Speed Limit 11
3.9.2 Port Mirror 11
3.9.3 Priority Trust 11
3.9.4 Traffic Classification 11
3.9.5 Traffic Behavior 12
3.9.6 Traffic Policy 12
3.9.7 Priority Mapping 12

3.9.8 Queue Scheduling 13
3.9.9 Congestion Avoidance 13
3.9.10 Traffic Statistics 13
3.9.11 ACL 13
3.10 AAA 13
3.11 EFM 15
3.12 CFD 17
3.13 IEEE RFC 2544 19
3.14 ITU-T Y.1564 20
3.15 SLA 20
3.16 ERPS 20
3.17 ELPS 20
3.18 Clock 21
3.19 Storm Control 22
3.20 IGMP 22
3.21 BFD 23
3.22 DDM 23
3.23 RMON 24
4 Device Management 24
5 Appendix Terms and Abbreviations 27

List of Figures

Figure 2-1 Typical application diagram..4

List of Tables

Table 1-1 Card ordering information of H18EDD-0402C device 3

Table 3-1 Interface link types and packet forwarding 6

Table 3-2 General link events 16

Table 3-3 Critical link events..17

1 Overview

Thank you for choosing H18EDD-0402C Ethernet Demarcation Access Devices from Beijing Huahuan Electronics Co., Ltd. For the best service from this product, please read this manual carefully.

H18EDD-0402C device helps operators improve network broadband and deployment efficiency, so as to reduce operation and maintenance costs. It supports 2 GE optical interfaces, 2 GE electrical interfaces and 2 1000M COMBO interfaces. You can customize the device with 4 optical interfaces+2 electrical interfaces or 2 optical interfaces+4 electrical interfaces. It supports L2/L3 protocol and builds reliable carrier-level packet switching network

1.1 Features

- Multiple service types, including E-Line service, E-LAN service, E-Tree service, E-Access and CES service.
- MAC functions (static MAC TAB, dynamic MAC learning, display dynamic MAC, clear dynamic MAC, MAC global configuration);
- VLAN and Q-in-Q;
- Ethernet port management (including SFP DDM);
- Ethernet port speed limit;
- Port mirror;

- Carrier-class reliability: Manual LAG and static LACP; ELPS (Ethernet Linear Protection Switching); ERPS (Ethernet Ring Protection Switching); loopback detection etc;
- Storm control;
- 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;
- Power failure and fiber break alarm;
- SLA network performance detection, such as statistics of response time, network jitter, delay, packet loss rate, throughput and another network information;
- DHCP zero-touch configuration;
- RMON performance statistics;
- LLDP;
- IEEE 1588v2 (PTP) and NTP;
- QoS management;
- ACL (Access Control List)
- AAA management mechanism, providing three security functions: Authentication, Authorization and Accounting;
- MTU and Jumbo frame settings (at least 9600 bytes);
- Switching capacity: 6Gbps;
- EzView, SSH, SNMP, CLI.

1.2 Ordering Information

Table 1-1 lists card ordering information of H18EDD-0402C device.

Table 1-1 Card ordering information of H18EDD-0402C device

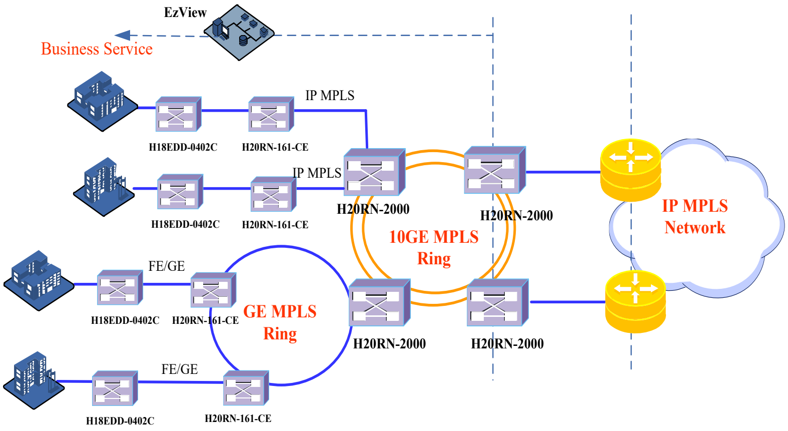
Equipment model	Descriptions
H18EDD-0402C	• 2GE optical interfaces • 2GE electrical interfaces • 2 1000M COMBO interfaces • AC~220V or DC-48V

2 Typical Application

Typical application diagrams of H18EDD-0402C devices are shown in Figure 2-1 错误!未找到引用源。.

H18EDD-0402C Ethernet Demarcation Access Device is accessed into the station from FE/GE ports, and then the data of the station is transmitted through the GE ring network composed of H20RN-161-CE devices.

Figure 2-1 Typical application diagram



3 Functional Properties

3.1 VLAN

The device supports 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 device supports 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

3.2 QinQ

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

H18EDD-0402C device supports 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 series 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 MAC

H18EDD-0402C device supports MAC address forwarding.

MAC Address Forwarding Table Entries

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 forwarding table entries include the following information:

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

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

MAC Address Table Entries Classification

H18EDD-0402C device supports 2 MAC address entries: static, and dynamic.

- 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. H18EDD-0402C device supports setting dynamic MAC address table entries and manually clearing dynamic MAC address table entries. For the specific range and default parameters, refer to *H18EDD-0402C Ethernet Demarcation Access Device Command Reference*.

MAC Ageing Time

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

3.4 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.

3.5 Loop Detection

In H18EDD 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.

3.6 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.

3.7 LACP

H18EDD-0402C 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.

H18EDD-0402C supports following load sharing algorithms: source MAC, destination MAC, source MAC and destination MAC, source port and destination port. The default is source MAC.

NOTE

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.

3.8 DHCP

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.

3.9 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.

3.9.1 Port Speed Limit

H18EDD-0402C device offers port speed limit, which will discard the excess flow. The limit granularity is 8Kbps.

- Based on port
- Based on ACL

3.9.2 Port Mirror

H18EDD-0402C device offers mirror function based on port, i.e. copying packet from a specific port to mirror port for analysis and monitoring.

3.9.3 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 H18EDD-0402C device are:

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

3.9.4 Traffic Classification

Users can classify traffic according to layer-2, layer-3 information carried by the packet, and then relate traffic classification to some traffic behavior, and deal with the packet within traffic classification.

H18EDD-0402C device supports traffic classification by the following methods:

- Based on port
- IP packet based DSCP priority
- IP packet based ToS priority
- VLAN packet based CoS priority
- VLAN packet based VLAN ID
- 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

3.9.5 Traffic Behavior

Traffic behaviors supported by H18EDD-0402C device are as follows:

- 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.

- CAR (Commit Access Rate)

CAR supports sending cir parameters under car template parameters, supports acl flow speed limit by using car template.

3.9.6 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.

3.9.7 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.

H18EDD-0402C device supports priority mappings of IP packet based ToS, DSCP priority or VLAN packet based CoS priority.

3.9.8 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.

3.9.9 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.

3.9.10 Traffic Statistics

H18EDD 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.

3.9.11 ACL

H18EDD-0402C device supports 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.

H18EDD-0402C ACL function only supports matching vlan, vlan priority, untag; Protocol types only support matching: any and 0x0800.

3.10 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/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 exCPEt 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.

3.11 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 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

3.12 CFD

CFD (Connectivity Fault Detection) follows IEEE 802.1ag-compliant CFM (Connectivity Fault Management) protocol and ITUT Y.1731 protocol. It is an end-to-end OAM mechanism based on VLAN on the L2 link, which is mainly used to detect link connectivity, confirm faults and determine the location of faults in the L2 network.

CFM

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

CFM consists of MD (Maintenance Domain), MA (Maintenance Association), MEP (Maintenance associations End Point), MIP (Maintenance association Intermediate Point), and MP (Maintenance Point).

CFM can provide the following OAM functions:

- Continuity Check function (CC)

Continuity check function means to check the continuity of EVC by CC (continuity check) protocol and confirm connection status between MP (Maintenance Point). This function is implemented by periodically sending CCM (Continuity Check Message) through MEP. The other MEPs in the same service entity receive the message and ascertain the status of RMEP (Remote Maintenance associations End Point). If device fault occurs or link configuration error occurs, MEP will not normally receive and process CCM sent by RMEP. If MEP does not receive remote CCM message in 3.5 CCM periods, link fault occurs and alarm will be sent according to alarm priority configuration.

- Loopback function (LB)

Loopback function is used to confirm the connection status between the local device and the remote device. This function is to ascertain the connectivity between two MPs by sending LBM (Loopback Message) from source MEP to destination MP and sending LBR (Loopback Reply) from destination MP to source MEP. Source MEP sends LBM to MP that requires fault ascertainment. When this MP receives LBM message, it sends an LBR to source MEP. If source MEP receives this LBR, the path is connected. If source MEP does not receive LBR, connectivity fault exists.

- 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.

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, frame delay/delay variation, 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.

3.13 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.

3.14 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.

3.15 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.

3.16 ERPS

H18EDD-0402C device is support ERPS (Ethernet Ring Protection Switching). ERPS is a link layer protocol specially used for Ethernet ring. Through defining different roles for nodes in the ring network, this protocol utilizes VLAN for Ethernet ring to send ring control information under normal circumstances and prevent loop broadcast storm. When link or node fault occurs, ERPS can switch the network to backup link, so as to implement loop-removing, fault protection switching, automatic fault restoration, etc. ERPS protocol is simple, reliable, and convenient for maintenance. It has high switching performance and flexible topology. All in all, ERPS can greatly facilitate planning and management of network. H18EDD-0402C supports three networking methods: single ring, intersecting rings and tangent rings.

3.17 ELPS

H18EDD-0402C device is support ELPS (Ethernet Linear Protection Switching). ELPS is used to protect an Ethernet connection, which is an end-to-end protection technology. H18EDD-0402C support 1:1 bidirectional switching. 1:1 means that each working path is allocated with one protection path, normally, flow is transmitted through the working path, the protection path is a backup, but when failure occurs to the working path, negotiation will be conducted via APS protocol so that both the source and sink ends can switch to the backup path at the same time; bidirectional switching means that when link failure occurs, even if only one direction fails, the two ends will switch to the backup link simultaneously via APS protocol negotiation, and the result is that both connected by ELPS choose the same link for sending and receiving.

ELPS provides three methods to detect faults:

- Detecting faults based on physical interface status: it learns link faults and switch fast, applicable between adjacent equipment.
- Detecting faults based on CFM: suitable for unidirectional detection or detection crossing multiple devices.
- Detecting faults based on physical interface and CFM: any fault detected through physical link or CFM will be reported.

H18EDD-0402C's ELPS supports revertive mode and non-revertive mode, under revertive mode, when the failure of the working link recovers, the flow will switched back to the working link from the protection link, which will not under non-revertive mode. Under revertive mode, if WTR timer is configured, the flow will not switch back to the working path until the timeout of WTR timer. This can avoid frequent switches caused by unstable working path. By default WTR timer is 5 minutes.

Tip: The related CFM configurations should be finished before the fault detection becomes effective if it is failure detection based on CFM

3.18 Clock

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.
H18EDD-0402C device supports NTP client mode, and can synchronize time with NTP server.

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.

3.19 Storm Control

H18EDD-0402C can limit the broadcast traffic generated in the network, and can suppress the broadcast storm when the broadcast traffic surges, so as to ensure the normal forwarding of ordinary unicast.

H18EDD-0402C supports bandwidth limits for the following three types of broadcast traffic. The upper limit of the limited bandwidth is 50000kbit/s.

- Unknown unicast traffic: destination MAC is unknown unicast traffic, which is broadcast by the device.
- Unknown multicast traffic: destination MAC is unknown multicast traffic, which is broadcast by the device.
- Broadcast traffic: destination MAC is broadcast traffic, which is broadcast by the device.

3.20 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

3.21 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.

3.22 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.

3.23 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.

4 Device Management

NM and CONSOLE ports on the front panel of H18EDD-0402C device are management ports, which support EzView, SNMP, and CLI.

The default IP address of the device hiso system is 192.192.4.2; the IP address mask is

255.255.255.0. The default IP address of the device Linux system is 192.192.4.3; the IP address mask is 255.255.255.0.

H18EDD-0402C device supports 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 password is “Admin123”, the username is admin. The protocols used by hyper terminal are: baud rate: 115200bps; data bit: 8; parity bit: none; stop bit: 1.
2. SNMP: supports SNMP V1, SNMP V2c, SNMPv3 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 H18EDD-0402C device 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 series 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.

D

DHCP (Dynamic Host Configuration Protocol)

DHCP is a technology which can assign IP address dynamically in the network. It can automatically assign IP address for all clients in the network to reduce the workload of the administrator, realizing the centralized management of IP address.

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.

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

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.

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

BITS	Building Integrated Timing Supply System
BPDU	Bridge Protocol Data Unit

C

CAR	Committed Access Rate
CBS	Committed Burst Size
CIR	Committed Information Rate
CoS	Class of Service

D

DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
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

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

N

NTP	Network Time Protocol

O

OAM	Operation， Administration and Management

Q

QoS	Quality of Service

R

RH	Relative Humidity
RADIUS	Remote Authentication Dial In User Service

S

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

T

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service

TPID	Tag Protocol Identifier

V

VLAN	Virtual Local Area Network