

Appendix A - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this switch.

802.1X

Log Description	Severity
<p>Event description: 802.1X Authentication failure.</p> <p>Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>)</p> <p>Parameters description:</p> <p>reason: The reason for the failed authentication. The possible reason may be:</p> <ul style="list-style-type: none"> (1) user authentication failure. (2) no server(s) responding. (3) no servers configured. (4) no resources. (5) user timeout expired. <p>username: The user that is being authenticated..</p> <p>interface-id: The switch interface number.</p> <p>mac-address: The MAC address of the authenticated device.</p>	Critical
<p>Event description:802.1X fails to work due to H/W ACL resource is exhausted.</p> <p>Log Message: 802.1X cannot work correctly because ACL rule resource is not available.</p>	Alert
<p>Event description: 802.1X Authentication successful.</p> <p>Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>)</p> <p>Parameters description:</p> <p>username: The user that is being authenticated.</p> <p>interface-id: The interface name.</p> <p>mac-address: The MAC address of the authenticated device.</p>	Informational

AAA

Log Description	Severity
<p>Event description: This log will be generated when AAA global state is enabled or disabled.</p> <p>Log Message: AAA is <status>.</p> <p>Parameters description:</p> <p>status: The status indicates the AAA enabled or disabled.</p>	Informational
<p>Event description: This log will be generated when login successfully.</p> <p>Log Message: Successful login through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p>	Informational

<p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: none, local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>Username: It indicates the username for authentication.</p>	
<p>Event description: This log will be generated when login failure.</p> <p>Log Message: Login failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Warning
<p>Event description: This log will be generated when the remote server does not respond to the login authentication request.</p> <p>Log Message: Login failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>server-ip: It indicates the AAA server IP address.</p> <p>username: It indicates the username for authentication.</p>	Warning
<p>Event description: This log will be generated when enable privilege successfully.</p> <p>Log Message: Successful enable privilege through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: none, local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>Username: It indicates the username for authentication.</p>	Informational
<p>Event description: This log will be generated when enable privilege failure.</p> <p>Log Message: Enable privilege failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>).</p> <p>Parameters description:</p> <p>exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).</p> <p>client-ip: It indicates the client's IP address if valid through IP protocol.</p> <p>aaa-method: It indicates the authentication method, e.g.: local, server.</p> <p>server-ip: It indicates the AAA server IP address if authentication method is remote server.</p> <p>username: It indicates the username for authentication.</p>	Warning

<p>Event description: This log will be generated when the remote server does not respond to the enable password authentication request.</p> <p>Log Message: Enable privilege failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>).</p> <p>Parameters description:</p> <ul style="list-style-type: none"> exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address. username: It indicates the username for authentication. 	Warning
<p>Event description: This log will be generated when RADIUS assigned a valid VLAN ID attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> server-ip: It indicates the RADIUS server IP address. vid: The assign VLAN ID that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. Username: It indicates the username for authentication. 	Informational
<p>Event description: This log will be generated when RADIUS assigned a valid bandwidth attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface -id> (Username: <username>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> server-ip: It indicates the RADIUS server IP address. Direction: It indicates the direction for bandwidth control, e.g.: ingress or egress. Threshold: The assign threshold of bandwidth that authorized by from RADIUS server. Interface-id: It indicates the port number of the client authenticated. Username: It indicates the username for authentication. 	Informational
<p>Event description: This log will be generated when RADIUS assigned a valid priority attributes.</p> <p>Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port < interface -id> (Username: <username>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> server-ip: It indicates the RADIUS server IP address. priority: The assign priority that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. Username: It indicates the username for authentication. 	Informational
<p>Event description: This log will be generated when RADIUS assigned ACL script but fails to apply to the system due to insufficient resource.</p> <p>Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port < interface -id> (<acl-script>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> server-ip: It indicates the RADIUS server IP address. username: It indicates the username for authentication. interface-id: It indicates the port number of the client authenticated. acl-script: The assign ACL script that authorized by from RADIUS server. 	Warning

Auto Surveillance VLAN

Log Description	Severity
<p>Event description: When a new surveillance device is detected on an interface.</p> <p>Log Message: New surveillance device detected (<interface-id>, MAC: < mac-address >)</p> <p>Parameters description:</p> <p> interface-id: Interface name.</p> <p> mac-address: Surveillance device MAC address.</p>	Informational
<p>Event description: When an interface which is enabled surveillance VLAN joins the surveillance VLAN automatically.</p> <p>Log Message: <interface-id> add into surveillance VLAN <vid ></p> <p>Parameters description:</p> <p> interface-id: Interface name.</p> <p> vid:VLAN ID</p>	Informational
<p>Event description: When an interface leaves the surveillance VLAN and at the same time, no surveillance device is detected in the aging interval for that interface, the log message will be sent.</p> <p>Log Message: <interface-id> remove from surveillance VLAN <vid ></p> <p>Parameters description:</p> <p> interface-id: Interface name.</p> <p> vid:VLAN ID</p>	Informational

Configuration/Firmware

Log Description	Severity
<p>Event description: Firmware upgraded successfully.</p> <p>Log Message: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p> unitID: The unit ID.</p> <p> session: The user's session.</p> <p> username: Represent current login user.</p> <p> ipaddr: Represent client IP address.</p> <p> macaddr : Represent client MAC address.</p> <p> serverIP: Server IP address.</p> <p> pathFile: Path and file name on server.</p>	Informational
<p>Event description: Firmware upgraded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description:</p> <p> unitID: The unit ID.</p> <p> session: The user's session.</p> <p> username: Represent current login user.</p> <p> ipaddr: Represent client IP address.</p>	Warning

<p>macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.</p>	
<p>Event description: Firmware uploaded successfully.</p> <p>Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.</p>	Informational
<p>Event description: Firmware uploaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.</p>	Warning
<p>Event description: Configuration downloaded successfully.</p> <p>Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.</p>	Informational
<p>Event description: Configuration downloaded unsuccessfully.</p> <p>Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)</p> <p>Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.</p>	Warning

serverIP: Server IP address. pathFile: Path and file name on server.	
Event description: Configuration uploaded successfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event description: Configuration uploaded unsuccessfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning

DAI

Log Description	Severity
Event description: This log will be generated when DAI detect invalid ARP packet. Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). Parameters description: type: The type of ARP packet, it indicates that ARP packet is request or ARP response.	Warning
Event description: This log will be generated when DAI detect valid ARP packet. Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). Parameters description: type: The type of ARP packet, it indicates that ARP packet is request or ARP response.	Informational

DDM

Log Description	Severity
Event description: when the any of SFP parameters exceeds from the warning	Warning

threshold.

Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded.

Parameters description:

interface-id: port interface ID.

component: DDM threshold type. It can be one of the following types:

temperature

supply voltage

bias current

TX power

RX power

high-low: High or low threshold.

Event description: when the any of SFP parameters exceeds from the alarm threshold. Critical

Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded.

Parameters description:

interface-id: port interface ID.

component: DDM threshold type. It can be one of the following types:

temperature

supply voltage

bias current

TX power

RX power

high-low: High or low threshold.

Event description: when the any of SFP parameters recovers from the warning threshold. Warning

Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeding back to normal.

Parameters description:

interface-id: port interface ID.

component: DDM threshold type. It can be one of the following types:

temperature

supply voltage

bias current

TX power

RX power

high-low: High or low threshold.

Event description: when the any of SFP parameters recovers from the alarm threshold. Critical

Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeding back to normal.

Parameters description:

interface-id: port interface ID.

component: DDM threshold type. It can be one of the following types:

temperature

supply voltage

bias current

TX power

RX power
high-low: High or low threshold.

DHCPv6 Client

Log Description	Severity
<p>Event description: DHCPv6 client interface administrator state changed.</p> <p>Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled disabled].</p> <p>Parameters description: <ipif-name>: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: DHCPv6 client obtains an ipv6 address from a DHCPv6 server.</p> <p>Log Message: DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name>.</p> <p>Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The ipv6 address obtained from a DHCPv6 server starts renewing.</p> <p>Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts renewing.</p> <p>Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The ipv6 address obtained from a DHCPv6 server renews success.</p> <p>Log Message: The IPv6 address < ipv6address > on interface <ipif-name> renews success.</p> <p>Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The ipv6 address obtained from a DHCPv6 server starts rebinding</p> <p>Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding.</p> <p>Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The ipv6 address obtained from a DHCPv6 server rebinds success</p> <p>Log Message: The IPv6 address < ipv6address > on interface <ipif-name> rebinds success.</p> <p>Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.</p>	Informational
<p>Event description: The ipv6 address from a DHCPv6 server was deleted.</p> <p>Log Message: The IPv6 address < ipv6address > on interface <ipif-name> was deleted.</p>	Informational

Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	
Event description: DHCPv6 client PD interface administrator state changed. Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled disabled> Parameters description: intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: DHCPv6 client PD obtains an IPv6 prefix from a delegation router. Log Message: DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> Parameters description: ipv6networkaddr: ipv6 preifx obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router starts renewing. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing. Parameters description: ipv6networkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router renews success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success. Parameters description: ipv6anetworkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD nterface.	Informational
Event description: The IPv6 prefix obtained from a delegation router starts rebinding. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router rebinds success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix from a delegation router was deleted. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational

DHCPv6 Relay

Log Description	Severity
<p>Event description: DHCPv6 relay on a specify interface's administrator state changed</p> <p>Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled]</p> <p>Parameters description: <ipif-name>: Name of the DHCPv6 relay agent interface.</p>	Informational

DNS Resolver

Log Description	Severity
<p>Event description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted</p> <p>Log Message: [DNS_RESOLVER(1);]Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr></p> <p>Parameters description: domainname: the domain name string. ipaddr: IP address.</p>	Informational

DOS Prevention

Log Description	Severity
<p>Event description: Detect DOS attack.</p> <p>Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>).</p> <p>Parameters description: dos-type: DOS attack type ip-address: IP address. interface-id: Interface name</p>	Notice

Interface

Log Description	Severity
<p>Event description: When port is down</p> <p>Log Message: Port <port-type>< interface-id> link down</p> <p>Parameters description: port-type: port type interface-id: Interface name</p>	Informational
<p>Event description: When port is up</p> <p>Log Message: Port <port-type>< interface-id> link up, <link-speed></p> <p>Parameters description: port-type: port type interface-id: Interface name link-speed: port link speed.</p>	Informational

JWAC

Log Description	Severity
<p>Event description: when a host has passed the authentication.</p> <p>Log Message: JWAC host login success (Username: <string>, IP: <ipaddr ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>).</p> <p>Parameters description:</p> <p> Username: The host username.</p> <p> IP: The host IP address</p> <p> mac-address: The host MAC addresses.</p> <p> interface-id: The interface on which the host is authenticated.</p> <p> vlan-id: The VLAN ID on which the host exists</p>	Informational
<p>Event description: When a host fail to pass the authentication.</p> <p>Log Message: JWAC host login fail (Username: <string>, IP: <ipaddr ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>)</p> <p>Parameters description:</p> <p> Username: The host username.</p> <p> IP: The host IP address</p> <p> mac-address: The host MAC addresses..</p> <p> interface-id: The interface on which the host is authenticated.</p> <p> vlan-id: The VLAN ID on which the host exists</p>	Critical
<p>Event description: when the authorized user number on the whole device has reached the maximum user limit.</p> <p>Log Message: JWAC enters stop learning state.</p>	Warning
<p>Event description: when the authorized user number on the whole device is below the maximum user limit in a time interval.</p> <p>Log Message: JWAC recovers from stop learning state.</p>	Warning

LACP

Log Description	Severity
<p>Event description: Link Aggregation Group link up.</p> <p>Log Message: Link Aggregation Group < group_id > link up.</p> <p>Parameters description:</p> <p> group_id: The group id of the link down aggregation group.</p>	Informational
<p>Event description: Link Aggregation Group link down.</p> <p>Log Message: Link Aggregation Group < group_id > link down.</p> <p>Parameters description:</p> <p> group_id: The group id of the link down aggregation group.</p>	Informational
<p>Event description: Member port attach to Link Aggregation Group.</p> <p>Log Message: <ifname> attach to Link Aggregation Group <group_id>.</p> <p>Parameters description:</p> <p> ifname: The interface name of the port that attach to aggregation group.</p> <p> group_id: The group id of the aggregation group that port attach to.</p>	Informational
<p>Event description: Member port detach from Link Aggregation Group.</p> <p>Log Message: <ifname> detach from Link Aggregation Group <group_id>.</p>	Informational

Parameters description:

ifname: The interface name of the port that detach from aggregation group.

group_id: The group id of the aggregation group that port detach from.

LBD

Log Description	Severity
Event description: Record the event when an interface detect loop. Log Message: <interface-id> LBD loop occurred. Parameters description: interface-id: Interface on which loop is detected.	Critical
Event description: Record the event when an interface detect loop. Log Message: <interface-id > VLAN <vlan-id> LBD loop occurred. Parameters description: interface-id: Interface on which loop is detected. vlan-id: VLAN on which loop is detected.	Critical
Event description: Record the event when an interface loop recovered Log Message: <interface-id> LBD loop recovered. Parameters description: interface-id: Interface on which loop is detected.	Critical
Event description: Record the event when an interface loop recovered. Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered. Parameters description: interface-id: Interface on which loop is detected. vlan-id: VLAN on which loop is detected.	Critical
Event description: Record the event when the number of VLANs that loop back has occurred exceeds a reserved number. Log Message: Loop VLAN numbers overflow.	Critical

LLDP-MED

Log Description	Severity
Event description: LLDP-MED topology change detected Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6)	Notice

7. local(7)
 chassisID: chassis ID.
 portType: port ID subtype.
 Value list:
 1. interfaceAlias(1)
 2. portComponent(2)
 3. macAddress(3)
 4. networkAddress(4)
 5. interfaceName(5)
 6. agentCircuitId(6)
 7. local(7)
 portID: port ID.
 deviceClass: LLDP-MED device type.

Event description: Conflict LLDP-MED device type detected Notice

Log Message: Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)

Parameters description:

portNum: The port number.
 chassisType: chassis ID subtype.
 Value list:
 1. chassisComponent(1)
 2. interfaceAlias(2)
 3. portComponent(3)
 4. macAddress(4)
 5. networkAddress(5)
 6. interfaceName(6)
 7. local(7)
 chassisID: chassis ID.
 portType: port ID subtype.
 Value list:
 1. interfaceAlias(1)
 2. portComponent(2)
 3. macAddress(3)
 4. networkAddress(4)
 5. interfaceName(5)
 6. agentCircuitId(6)
 7. local(7)
 portID: port ID.
 deviceClass: LLDP-MED device type.

Event description: Incompatible LLDP-MED TLV set detected Notice

Log Message: Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)

Parameters description:

portNum: The port number.
 chassisType: chassis ID subtype.
 Value list:

1. chassisComponent(1)
 2. interfaceAlias(2)
 3. portComponent(3)
 4. macAddress(4)
 5. networkAddress(5)
 6. interfaceName(6)
 7. local(7)
 chassisID: chassis ID.
 portType: port ID subtype.
 Value list:
 1. interfaceAlias(1)
 2. portComponent(2)
 3. macAddress(3)
 4. networkAddress(4)
 5. interfaceName(5)
 6. agentCircuitId(6)
 7. local(7)
 portID: port ID.
 deviceClass: LLDP-MED device type.

Login/Logout CLI

Log Description	Severity
Event description: Login through console successfully. Log Message: [Unit <unitID>,]Successful login through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Login through console unsuccessfully. Log Message: [Unit <unitID>,] Login failed through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Warning
Event description: Console session timed out. Log Message: [Unit <unitID>,] Console session timed out (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Logout through console. Log Message: [Unit <unitID>,] Logout through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Login through telnet successfully.	Informational

<p>Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: Represent current login user. ipaddr: Represent client IP address. 	
<p>Event description: Login through telnet unsuccessfully.</p> <p>Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: Represent current login user. ipaddr: Represent client IP address. 	Warning
<p>Event description: Telnet session timed out.</p> <p>Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: Represent current login user. ipaddr: Represent client IP address. 	Informational
<p>Event description: Logout through telnet.</p> <p>Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: Represent current login user. ipaddr: Represent client IP address. 	Informational
<p>Event description: Login through SSH successfully.</p> <p>Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: Represent current login user. ipaddr: Represent client IP address. 	Informational
<p>Event description: Login through SSH unsuccessfully.</p> <p>Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: Represent current login user. ipaddr: Represent client IP address. 	Critical
<p>Event description: SSH session timed out.</p> <p>Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: Represent current login user. ipaddr: Represent client IP address. 	Informational
<p>Event description: Logout through SSH.</p> <p>Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>)</p> <p>Parameters description:</p> <ul style="list-style-type: none"> username: Represent current login user. ipaddr: Represent client IP address. 	Informational

MAC-based Access Control

Log Description	Severity
Event description: A host has passed the authentication.	Informational

<p>Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>).</p> <p>Parameters description:</p> <ul style="list-style-type: none"> mac-address: The host MAC address interface-id: The interface on which the host is authenticated vlan-id: The VLAN ID on which the host exists 	
<p>Event description: A host has aged out.</p> <p>Log Message: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>).</p> <p>Parameters description:</p> <ul style="list-style-type: none"> mac-address: The host MAC address interface-id: The interface on which the host is authenticated vlan-id: The VLAN ID on which the host exists 	Informational
<p>Event description: A host failed to pass the authentication.</p> <p>Log Message: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>).</p> <p>Parameters description:</p> <ul style="list-style-type: none"> mac-address: The host MAC address interface-id: The interface on which the host is authenticated vlan-id: The VLAN ID on which the host exists 	Critical
<p>Event description: The authorized user number on the whole device has reached the maximum user limit.</p> <p>Log Message: MAC-based Access Control enters stop learning state.</p>	Warning
<p>Event description: The authorized user number on the whole device is below the maximum user limit in a time interval.</p> <p>Log Message: MAC-based Access Control recovers from stop learning state.</p>	Warning
<p>Event description: The authorized user number on an interface has reached the maximum user limit.</p> <p>Log Message: <interface-id> enters MAC-based Access Control stop learning state.</p> <p>Parameters description:</p> <ul style="list-style-type: none"> interface-id: The interface on which the host is authenticated 	Warning
<p>Event description: The authorized user number on a interface is below the maximum user limit in a time interval.</p> <p>Log Message: <interface-id> recovers from MAC-based Access Control stop learning state.</p> <p>Parameters description:</p> <ul style="list-style-type: none"> interface-id: The interface on which the host is authenticated 	Warning

MSTP Debug Enhancement

Log Description	Severity
<p>Event description: Used to record the event that Spanning Tree Protocol is enabled.</p> <p>Log Message: Spanning Tree Protocol is enabled</p>	Informational
<p>Event description: Used to record the event that Spanning Tree Protocol is disabled</p> <p>Log Message: Spanning Tree Protocol is disabled.</p>	Informational

<p>Event description: Used to record MSTP instance topology change event.</p> <p>Log Message: Topology changed (Instance : < Instance-id >,<interface_id>, MAC:<macaddr>)</p> <p>Parameters description:</p> <p>Instance-id: MST instance id. Instance 0 represents for default instance, CIST.</p> <p>interface_id: The port number which detect or reive topochange information.</p> <p>macaddr: The system of bridge mac address.</p>	Notice
<p>Event description: Used to record MSTP instance new root bridge selected.</p> <p>Log Message: [CIST CIST Regional MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :< priority>)</p> <p>Parameters description:</p> <p>Instance-id: MST instance id. Instance 0 represents for default instance, CIST.</p> <p>macaddr: The system of bridge mac address.</p> <p>priority: The bridge priority value must be divisible by 4096</p>	Informational
<p>Event description: Used to record MSTP instance new root port selected.</p> <p>Log Message: New root port selected (Instance:<Instance-id >, <interface_id >)</p> <p>Parameters description:</p> <p>Instance-id: MST instance id. Instance 0 represents for default instance, CIST.</p> <p>interface_id: The port number which detect or rereive topochange information.</p>	Notice
<p>Event description: Used to record MSTP instance port state change event.</p> <p>Log Message: Spanning Tree port status change (Instance :< Instance-id >, <interface_id>) <old_status> -> <new_status></p> <p>Parameters description:</p> <p>Instance-id: MST instance id. Instance 0 represents for default instance, CIST.</p> <p>interface_id: The port number which detect or rereive topochange information.</p> <p>old status:</p> <p>new status:</p> <p>The port of STP state.The value may be Disable, Discarding, Learning, Forwarding</p>	Notice
<p>Event description: Used to record MSTP instance port role change event.</p> <p>Log Message: Spanning Tree port role change (Instance :< Instance-id >, <interface_id>) <old_role> -> <new_role></p> <p>Parameters description:</p> <p>Instance-id: MST instance id. Instance 0 represents for default instance, CIST.</p> <p>Interface_id: The port number which detect or rereive topochange information.</p> <p>old role:</p> <p>new role :</p> <p>The port role of stp.The value may be Disable, Alternate, Backup, Root, Designated</p>	Informational
<p>Event description: Use to record action to create an MST instance.</p> <p>Log Message: Spanning Tree instance created (Instance :< Instance-id >)</p>	Informational

Parameters description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
Event description: Use to record action to delete an MST instance. Log Message: Spanning Tree instance deleted (Instance :< Instance-id >)	Informational
Parameters description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	
Event description: Use to record action to change the STP version. Log Message: Spanning Tree version change (new version :< new_version>)	Informational
Parameters description: new_version: Running under which version of STP.	
Event description: Spanning Tree MST configuration ID name and revision level change (name :< name>, revision level <revision_level>). Log Message: Used to record the configuration name and revision level changed in the MST Configuration Identification.	Informational
Parameters description: name: The name given for a specified MST region. revision_level: Switches using the same given name but with a different revision level are considered members of different MST regions.	
Event description: Use to record action to maps a VLAN(s) to an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> add vlan <startvlanid> [- <endvlanid>])	Informational
Parameters description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. startvlanid: The start vid of add vlan range. endvlanid: The end vid of add vlan range.	
Event description: Use to record action to delete a VLAN(s) from an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> delete vlan <startvlanid> [- <endvlanid>])	Informational
Parameters description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. startvlanid: The start vid of add vlan range. endvlanid: The end vid of add vlan range.	
Event description: Used to record the event that port role change to alternate due to guard root. Log Message: Spanning Tree port role change (Instance :< instance-id >, <interface-id>) to alternate port due to the guard root	
Parameters description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. Interface_id: The port number which detect the event.	

Peripheral

Log Description	Severity
-----------------	----------

<p>Event description: Fan Recovered.</p> <p>Log Message: Unit <id>, <fan-descr> back to normal.</p> <p>Parameters description: Unit <id>: The unit ID. fan-descr: The FAN ID and position.</p>	Critical
<p>Event description: Fan Fail</p> <p>Log Message: Unit <id> <fan-descr> failed</p> <p>Parameters description: Unit <id>: The unit ID. fan-descr: The FAN ID and position.</p>	Critical
<p>Event description: Temperature sensor enters alarm state.</p> <p>Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree></p> <p>Parameters description: unitID: The unit ID. thermal-sensor-descr: The sensor ID and position. degree: The current temperature.</p>	Critical
<p>Event description: Temperature recovers to normal.</p> <p>Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal</p> <p>Parameters description: unitID: The unit ID. thermal-sensor-descr: The sensor ID and position.</p>	Critical
<p>Event description: Power failed.</p> <p>Log Message: Unit <unit-id> <power-descr> failed</p> <p>Parameters description: unitID: The unit ID. power-descr: The power position and ID.</p>	Critical
<p>Event description: Power is recovered.</p> <p>Log Message: Unit <unit-id> <power-descr> back to normal</p> <p>Parameters description: unitID: The unit ID. power-descr: The power position and ID.</p>	Critical
<p>Event description: Press the factory reset button.</p> <p>Log Message: Unit <unit-id> factory reset button pressed.</p> <p>Parameters description: unitID: The unit ID.</p>	Critical

PoE

Log Description	Severity
<p>Event description: Total power usage threshold is exceeded</p> <p>Log Message: Unit <unit-id> usage threshold <percentage> is exceeded</p> <p>Parameters description: unit-id : box id percentage : usage threshold</p>	Warning
<p>Event description: Total power usage threshold is recovered.</p>	Warning

Log Message: Unit <unit-id> usage threshold <percentage> is recovered

Parameters description:

unit-id : box id

percentage : usage threshold

Port Security

Log Description	Severity
Event description: Address full on a port Log Message: MAC address <macaddr> causes port security violation on <interface-id>. Parameters description: macaddr: The violation MAC address. interface-id: The interface name.	Warning
Event description: Address full on system Log Message: Limit on system entry number has been exceeded.	Warning

Safeguard

Log Description	Severity
Event description: the host enters the mode of exhausted. Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. Parameters description: unit-id: The Unit ID	Warning
Event description: the host enters the mode of normal. Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode. Parameters description: unit-id: The Unit ID	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string Log Message: SNMP request received from <ipaddr> with invalid community string. Parameters Description: ipaddr: The IP address.	Informational

SSH

Log Description	Severity
Event description: SSH server is enabled. Log Message: SSH server is enabled	Informational
Event description: SSH server is disabled.	Informational

Log Message: SSH server is disabled	
Event description: Login failed through SSH.	Critical
Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr ipv6address>).	
Parameters description:	
username: User name which logs in fail.	
ipaddr: IP address of host from which the user logged in.	
ipv6address: IPv6 address of host from which the user logged in.	

Stacking

Log Description	Severity
Event description: Hot insertion. Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion. Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
Event description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal. Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
Event description: Stacking topology change. Log Message: Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>). Parameters description: Stack_TP_TYPE: The stacking topology type is one of the following: 1. Ring, 2. Chain. unitID: Box ID. Macaddr: MAC address.	Informational
Event description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
Event description: Slave changed to master Log Message: Slave changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
Event description: Box ID conflict. Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>). Parameters description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	Critical

Storm Control

Log Description	Severity
<p>Event description: Storm occurrence.</p> <p>Log Message: <Broadcast Multicast Unicast> storm is occurring on <interface-id>.</p> <p>Parameters description:</p> <p>Broadcast: Storm is resulted by broadcast packets(DA = FF:FF:FF:FF:FF:FF).</p> <p>Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast and known IP multicast.</p> <p>Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets</p> <p>interface-id: The interface ID on which a storm is occurring.</p>	Warning
<p>Event description: Storm cleared.</p> <p>Log Message: <Broadcast Multicast Unicast> storm is cleared on <interface-id>.</p> <p>Parameters description:</p> <p>Broadcast: Broadcast storm is cleared.</p> <p>Multicast: Multicast storm is cleared.</p> <p>Unicast: Unicast storm (including both known and unknown unicast packets) is cleared.</p> <p>interface-id: The interface ID on which a storm is cleared.</p>	Informational
<p>Event description: Port shut down due to a packet storm</p> <p>Log Message: <interface-id> is currently shut down due to the <Broadcast Multicast Unicast> storm.</p> <p>Parameters description:</p> <p>interface-id: The interface ID on which is error-disabled by storm.</p> <p>Broadcast: The interface is disabled by broadcast storm.</p> <p>Multicast: The interface is disabled by multicast storm.</p> <p>Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).</p>	Warning

Voice-VLAN

Log Description	Severity
<p>Event description: When a new voice device is detected on an interface.</p> <p>Log Message: New voice device detected (<interface-id>, MAC: < mac-address >)</p> <p>Parameters description:</p> <p>interface-id: Interface name.</p> <p>mac-address: Voice device MAC address</p>	Informational
<p>Event description: When an interface which is in auto voice VLAN mode joins the voice VLAN</p> <p>Log Message: < interface-id > add into voice VLAN <vid ></p> <p>Parameters description:</p> <p>interface-id: Interface name.</p> <p>vid:VLAN ID</p>	Informational

Event description: When an interface leaves the voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent. Informational

Log Message: < interface-id > remove from voice VLAN <vid >

Parameters description:

interface-id: Interface name.

vid:VLAN ID

Web

Log Description	Severity
<p>Event description: Successful login through Web.</p> <p>Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>).</p> <p>Parameters description:</p> <p>username: The use name that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational
<p>Event description: Login failed through Web.</p> <p>Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>).</p> <p>Parameters description:</p> <p>username: The use name that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Warning
<p>Event description: Web session timed out.</p> <p>Log Message: Web session timed out (Username: <usname>, IP: <ipaddr>).</p> <p>Parameters description:</p> <p>username: The use name that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational
<p>Event description: Logout through Web.</p> <p>Log Message: Logout through Web (Username: %S, IP: %S).</p> <p>Parameters description:</p> <p>username: The use name that used to login HTTP server.</p> <p>ipaddr: The IP address of HTTP client.</p>	Informational

Web-Authentication

Log Description	Severity
<p>Event description: When a host has passed the authentication.</p> <p>Log Message: Web-Authentication host login success (Username: <string>, IP: <ipaddr ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>)</p> <p>Parameters description:</p> <p>Username: The host username.</p> <p>IP: The host IP address</p> <p>mac-address: The host MAC addresses.</p> <p>interface-id: The interface on which the host is authenticated.</p> <p>vlan-id: The VLAN ID on which the host exists</p>	Informational
<p>Event description: When a host fail to pass the authentication.</p>	Critical

Log Message: Web-Authentication host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>).

Parameters description:

Username: The host username.

IP: The host IP address

mac-address: The host MAC addresses..

interface-id: The interface on which the host is authenticated.

vlan-id: The VLAN ID on which the host exists

Event description: when the authorized user number on the whole device has reached the maximum user limit. Warning

Log Message: Web-Authentication enters stop learning state.

Event description: when the authorized user number on the whole device is below the maximum user limit in a time interval. Warning

Log Message: Web-Authentication recovers from stop learning state.
