ISW-168XX PoE Switch Software Release Notes

Model:

ISW 8GbP, 4-SFP, PoE Switch (GE)

ISW 4GbP, 2GbT, 2-SFP, PoE Switch (GE)

ISW 8-10/100P, 4-SFP, PoE Switch (FE)

ISW 4-10/100P, 2-10/100T, 2-SFP, PoE Switch (FE)

FW Release Version: v01.01.04.0002 (for all models)

Documentation Date: 2024/01/05

[New Release: v01.01.04.0002]

The release note includes all feature changes and fixed bugs since previous release v01.01.04.0001. (v01.01.04.0001 is for new feature & bug fixing.)

<Release Information>

File Name	File Size(kb)	File Type	Checksum(md5)
ISW-TLN-12PORT_V01.01.04.0002.dat	5989853	dat	181dba1d2c2d0504e780516afbfd244d
ISW-TLN-8PORT_V01.01.04.0002.dat	5986725	dat	0809df21521fb870c621233064daf5f2

<Software Date>

Software Build Date: 2024/01/05

<Software Base>

MSCC VSC7429, VSC7425 Compatible

OS: eCos Operating System

Version 3.65 CE Service

<New Features>

None

<Feature update>

1. CLI/WEB/MIB implementation to report the Serial No. of the ISW switch.

    CLI: Serial number display at command "show version"

WEB: Serial number display at page of Monitor/System/Information

System Information

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-05-65-a0-0a-00
Serial Number	2401-GT0034
Chip ID	VSC7429
Time	
System Date	2000-01-01T00:30:23+00:00
System Uptime	0d 00:30:24
Software	
Software Version	V01.01.04.0002
Software Date	2024-01-05T11:57:42+08:00
Acknowledgments	Details

SNMP: Serial number display with standard MIB OID and proprietary MIB OID.

- Standard MIB OID: 1.3.6.1.2.1.47.1.1.1.1.11
- Proprietary MIB OID: 1.3.6.1.4.1.5833.1916.2.1.6

2. Enable loop protect with RingV2

The following cases all can work, the access ports and the ring ports can enable at the same time and work with physical loop.
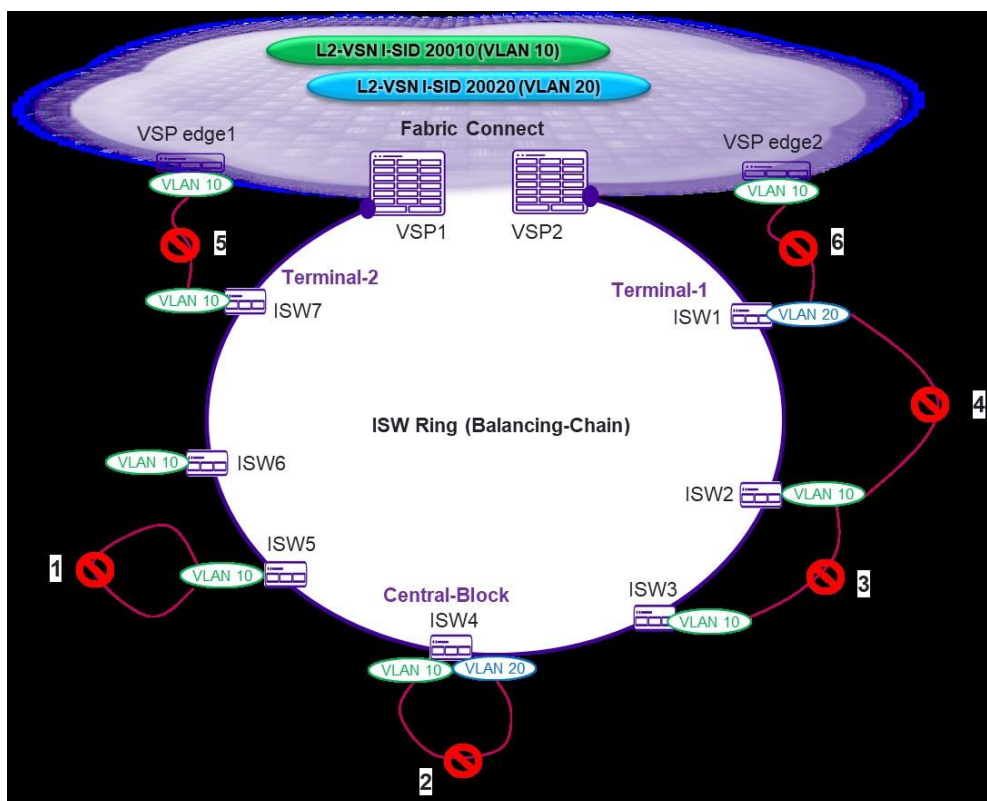
Description:

Case 1: Loop protect can work when the access ports with loop protect enable in the same VLAN and the same device.

Case 2: Loop protect can work when the access ports with loop protect enable in different VLAN and the same device.

Case 3: Loop protect can work when the access ports with loop protect enable in the same VLAN and the different device.

Case 4: Loop protect can work when the access ports with loop protect enable in the different VLAN and different device.

Case 5: Loop protect can work when the access ports with loop protect enable connected to other vendor's device in the same VLAN.

Case 6: Loop protect can work when the access ports with loop protect enable connected to other vendor's device in the different VLAN.

Case 1 ~ case 6 applied the same configuration.

Configuration by WEBGUI:

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)	
1	Disable	Ring(Slave)	Forward Port :	Port-1
			Forward Port :	Port-2
2	Disable	Ring(Slave)	Forward Port :	Port-3
			Forward Port :	Port-4
3	Enable	Chain(Member)	Member Port :	Port-9
			Member Port :	Port-10

Save Reset

Loop Protection Configuration

General Settings

Global Configuration		
Enable Loop Protection	Enable	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Log Only	Enable
10	☑	Log Only	Enable
11	☑	Shutdown Port	Enable
12	☑	Shutdown Port	Enable

Save Reset

Note-1: Ring ports should configure loop protect action with log only not shutdown port

Note-2: In case 6, the fabric connect network, VSP should forward the loop protect

control packets back to ISW.

3. RingV2 can work with spanning tree

    There is no restriction when the ring port enable, the other access ports can be enable with spanning tree function, the ring ports is not available for enable spanning tree function.

4. PoE controller firmware version advance and can upgrade PoE firmware depend on the PoE chipset, use command "poe firmware upgrade" to upgrade to latest version.
    - PD69200 can upgrade to version 211
    - PD69210 can upgrade to version 223
    - PD69220 can upgrade to version 224

<Fixed Bugs>

1. TSS5484: Switches crash when running a vulnerability scan from Tenable
    - Root cause: When the tenable use the format of SSH-9.9-OpenSSH_5.0 to attack device will let the device crash and reboot automatically.
    - Solution: When the format of SSH is different with ISW, will skip it and prevent the device crash.

2. TSS 5512: ISW 16804 switch cannot route packets via management interface 1292
    - Root cause: When the startup-config is "no ip address", the interface VLAN will be changed to "ip address dhcp" by LLDP TLV of management VLAN.
    - Solution: Not changed the interface VLAN config when the startup-config is "no ip address".

3. TSS 5513: ISW 16801 switch, removing an authenticated client removes the configured vlan from the running configuration
    - Root cause: When the client disconnected, it will remove the PVLAN of that access port, but also remove other ports' PVLAN that is not the uplink ports connected to FA server.
    - Solution: When the client disconnected, it will not affect other ports which is not the

uplink ports connected to FA server.

4. TSS 5515: ISW Switch POE Status Failure - Changing between different states
   - Root cause: The specific PD device let the PoE controller work abnormal exchanged the information between PoE controller and main chip.
   - Solution: To let the communication between PoE controller and main chip success.

5. TSS 5517: Connecting ISW to VSP7400 cluster via a LAG the management subnet on ISW becomes unreachable
   - Root cause: When the fiber ports config as LAG ports with aggregation spanning tree is disable, after bootup, the management interface will be always down and not work, it can be recovered by re-connected the cables of LAG ports.
   - Solution: After the bootup completed, the fiber ports status can work normal with LAG and aggregation spanning tree disable to trigger the management interface up.

6. TSS 5518: ISW + 5320 FA Auto-Sense Issue
   - Root cause: When the LLDP packets has some TLV in the first LLDP packet will cause fabric attach communication stop working, and the TLV is caused by the VPS config with auto-sense VOICE i-sid enable.
   - Solution: The communication of fabric attach will be success and skip some unknown TLV in the first LLDP packet.

7. TSS 5531: AP PEAP not moving to RADIUS assigned VLAN
   - Root cause: The attribute of PVLAN from RADIUS server not work in port-based mode, single mode, and port-based of sense mode.
   - Solution: To support the attribute of PVLAN from RADIUS server in port-based mode, single mode and port-based of sense mode, when the authorization got success, the port VLAN will be changed as the attribute of PVALN from RADIUS server.

Release History
[v01.01.04.0001]
The release note includes all feature changes and fixed bugs since previous release
v01.01.03.0014. (v01.01.03.0015 is for bug fixing, v01.01.04.0001 is for new feature & bug fixing.)

<Software Date>

Software Build Date: 2022/02/24

<Software Base>

MSCC VSC7429, VSC7425 Compatible

OS: eCos Operating System

Version 3.65 CE Service

<New Features>

1. Support Dual Ring (Ring/Chain with LAG)

   →Support this feature in all of Ring/Chian/Coupling/Dual-homing/Balancing Chain technologies).

   ● Restrictions of Dual Ring
     - Each LAG Ring node only support 2 ports of LAG
     - Don't make Ring topologies mixed with STP when enable LAG Ring nodes. (Recovery time is bad)
     - Not support LACP (Only support Static LAG)

- Supported topologies:

Average recovery time are same as original Ring technologies (Almost same as without LAG). The recovery time is less than 50ms.
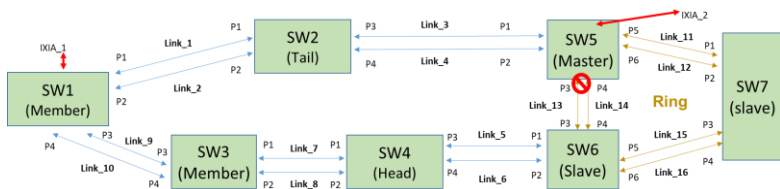
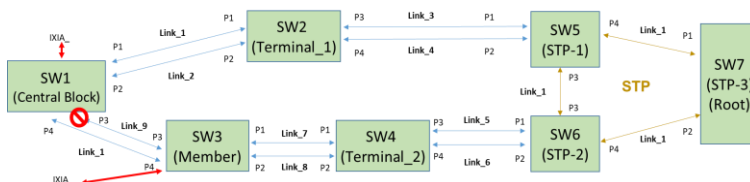 ■ Ring with LAG
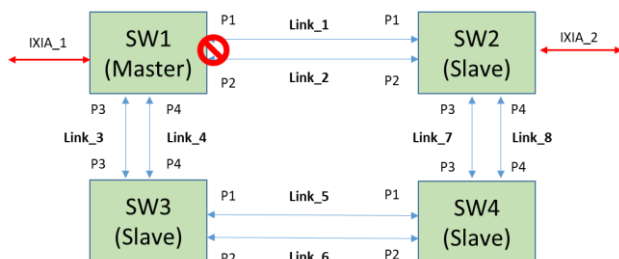
  ■ Balancing Chain with LAG
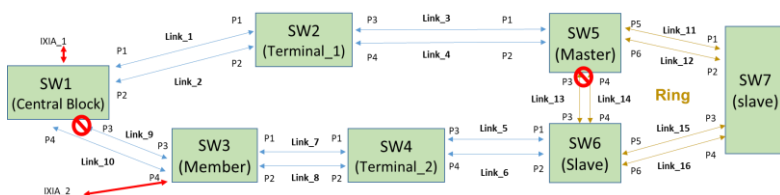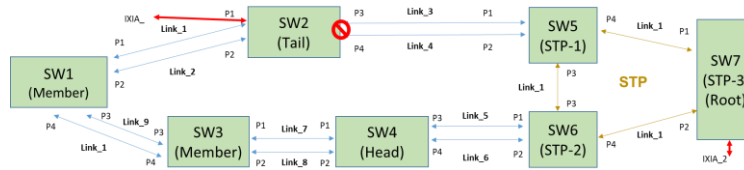

  ■ Chain with LAG

- Supported topologies but not support to use due to bad recovery time.

  ■ Balancing Chain with LAG + STP

Bad recovery time on Link_3, Link_4, Link_5 and Link_6.

■ Chain with LAG + STP

Bad recovery time on Link_5 and Link_6.

● Web (Support LAG port be configured for Ring Port(s))

● CLI commands

Support LAG port can be configured for Ring node1 & node2.

(config-ringv2-group1)#

(config-ringv2-group1)#node1 aggregation group <LAG group ID>
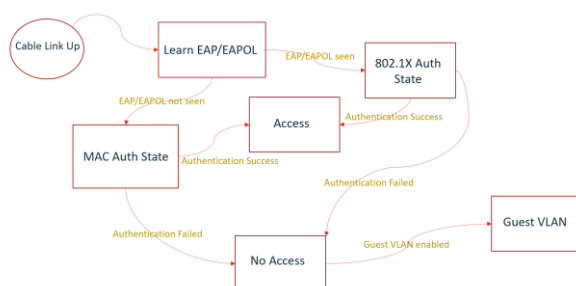
(config-ringv2-group1)#node2 aggregation group <LAG group ID>

2. Support "Enable both MAC and 802.1X auth on same port"
→802.1X/MAC Auth auto sense mode.

- Mode States
  - Try to authenticate through 802.1X else
  - Try to authenticate through MAC else
  - Provide Guest VLAN access (if Guest VLAN is enabled) else
  - No Access

State chart of 802.1X/MAC auto sense mode

- New timer parameter: Sense Period
  Used to identify if the client enabled 802.1X. Identification method is to learning if the port received EAP/EAPOL packets, the first learnt packet will be EAPOL start normally after port is linked up.

  - CLI:
    (config)#dot1x timeout sense-period <10-255>, default: 10 seconds

- New mode of port control: dot1x port-control sense
  To support enable both MAC and 802.1X auth on same port.

  - CLI:
    (config-if)# dot1x port-control sense

● Web design for Sense Period and port-control mode.

<Feature update>

5. Support TLS1.2 for HTTPs connection.

6. Enable HTTPs and HTTPs redirect by default. (By default, all of HTTP session will be redirected to HTTPs)

7. ISW SNMP performance improvement (OID:1.3.6.1.2.1.31 and for 1.3.6.1.2.1.2.2) Modify the snmp response for 1.3.6.1.2.1.31 and for 1.3.6.1.2.1.2.2 to report only existing VLANs = do not report non-existing VLANs (Previous version will response 1~4095 VLANs if one of the port is enabled Trunk mode.)

<Fixed Bugs>

8. TSS5406: Switch reboots when I enable dot1x authentication

[v01.01.03.0015]

The release note includes all feature changes and fixed bugs since previous release v01.01.03.0014.

<Software Date>

Software Build Date: 2022/02/17

<Software Base>

MSCC VSC7429, VSC7425 Compatible

OS: eCos Operating System

Version 3.65 CE Service

<New Features>

None.

<Feature update>

1. Support TLS1.2 for HTTPs connection.
2. Enable HTTPs and HTTPs redirect by default. (By default, all of HTTP session will be redirected to HTTPs)
3. ISW SNMP performance improvement (OID:1.3.6.1.2.1.31 and for 1.3.6.1.2.1.2.2) Modify the snmp response for 1.3.6.1.2.1.31 and for 1.3.6.1.2.1.2.2 to report only existing VLANs = do not report non-existing VLANs (Previous version will response 1~4095 VLANs if one of the port is enabled Trunk mode.)

<Fixed Bugs>

9. TSS5406: Switch reboots when I enable dot1x authentication

[v01.01.03.0014]

The release note includes all feature changes and fixed bugs since previous release v01.01.03.0013.

<Software Date>

Software Build Date: 2021/10/24

<Software Base>

MSCC VSC7429, VSC7425 Compatible

OS: eCos Operating System

Version 3.65 CE Service

<New Features>

1. IP address configuration for interface vlan 1 will be changed to default dhcp client enable with fallback ip address is 192.0.2.1.

    When dhcp client can't get IP address from DHCP server, it will fallback the IP address to 192.0.2.1 after 60 seconds.

    Interface vlan 1

    Ip address dhcp fallback 192.0.2.1 255.255.255.0 timeout 60

<Feature update>

4. SSH default setting is changed. Add CLI and WEB commands to enable/disable CBC ciphers and HMACs item by item.

    Raw issue

    TSS 5372: Request For Information: Changing Key Exchange Alg. And Parameters?
    Disable weak CBC ciphers and HMAC/Hashing Message Authentication Code.

SSH / TELNET Configuration

SSH Mode	Enabled ⌄
Key Exchange Algorithms	
	☑ curve25519-sha256
	☑ ecdh-sha2-nistp521
	☑ ecdh-sha2-nistp384
	☑ ecdh-sha2-nistp256
	☑ diffie-hellman-group14-sha1
	☑ diffie-hellman-group1-sha1
	☑ kexguess2
HMAC	
	☐ hmac-sha1-96
	☑ hmac-sha1
	☑ hmac-sha2-256
	☑ hmac-sha2-512
	☐ hmac-md5
Cipher	
	☑ aes128-ctr
	☑ aes256-ctr
	☑ 3des-ctr
	☐ aes128-cbc
	☐ aes256-cbc
	☐ twofish256-cbc
	☐ twofish-cbc
	☐ twofish128-cbc
	☐ 3des-cbc
	☐ blowfish-cbc
Hostkey Status	Normal
TELNET Mode	Enabled ⌄

Default setting of Ciphers and HMAC/Hashing Message Authentication Code are list in following table.

Weak CBC Ciphers are disabled by default. Weak HMAC are disabled by default.

No	Type	Default Setting
1	hmac-sha1-96	*Disabled*
2	hmac-sha1	Enabled
3	hmac-sha2-256	Enabled
4	hmac-sha2-512	Enabled
5	hmac-md5	*Disabled*
6	aes128-ctr	Enabled
7	aes256-ctr	Enabled
8	3des-ctr	Enabled

9	aes128-cbc	*Disabled*
10	aes256-cbc	*Disabled*
11	twofish256-cbc	*Disabled*
12	twofish-cbc	*Disabled*
13	twofish128-cbc	*Disabled*
14	3des-cbc	*Disabled*
15	blowfish-cbc	*Disabled*

<Fixed Bugs>

10. TSS 5432: Process crash when running 'show ip ssh public-key'

11. TSS 5403: Flow stops working after sFlow configuration timeout

    Support sflow commands in show running-config and configuration saving.

    Change the behavior of "timeout" parameter:

    - If timeout is not 0, the sflow will be enabled.

      <u>Timeout will not count down to 0 to keep sflow working</u>.

    - If timeout is 0, the sflow will be disabled/released.

      <u>Only manually setting can change timeout to 0</u>.

    - Timeout value still can access through SNMP and Timeout will not be decreased.

[v01.01.03.0013]

The release note includes all feature changes and fixed bugs since previous release v01.01.03.0012.

\<Software Date\>

Software Build Date: 2021/4/30

\<Software Base\>
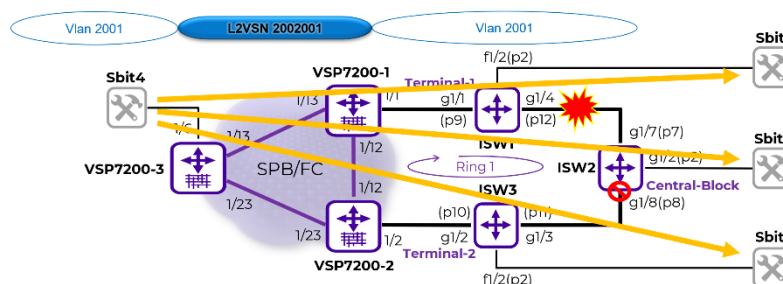
    MSCC VSC7429, VSC7425 Compatible

    OS: eCos Operating System

    Version 3.65 CE Service

\<New Features\>

1. TCN (topology change notification) of MSTP.
    ISW Ringv2(Chain/Balancing Chain) support MSTP/RSTP TCN BPDU for fast (less than 100ms) network redundancy recovery time.

- Ring Cut (64 millisecs interruption)

Signature Frames Sent	0	0	0	0	0	0	238,194	0	Sbit1	Sbit2	Sbit3
Signature Frames Received	79,398	0	79,334	0	79,398	0	0	0	0	64	0

- Ring Restore (65 millisecs interruption)

Signature Frames Sent	0	0	0	0	0	0	124,711	0	Sbit1	Sbit2	Sbit3
Signature Frames Received	41,571	0	41,505	0	41,570	0	0	0	-1	65	0

Verified: ISW of TCN BDUs for fast aging of MACs on Fabric Core whenever ISW ring is cut or restored. (Less than 100ms)

2. Support "show tech-support" CLI command.
3. Support SSH Key Exchange Algorithms configuration in CLI/WEB/SNMP.

\<Feature update\>

1. Providing TELNET enable/disable configuration in CLI and Web. (Default is enable)

2. LLDP management ip address

TSS 5386: Query relating to LLDP displaying IP address for untagged vlans as opposed to or not for tagged vlans.

3. Remove CPU drop packet counter from "Rx packet drops"

TSS 5355: Rx packet drops seen on port

<Fixed Bugs>

1. Mantis 6298: System Hang (no reboot) when fail to login switch with SSH.command is applied.
   Whenever "unsupported" SSH KEX (encryption algorithm) is used to login switch, and failed for 3 times, first ip interface malfunction, then system hang. (Console, TELNET, SSH, Web all malfunction)

2. Mantis 6305: SSH disable cause system's cpu to 100%.

3. Mantis 6311: The format of SSH WEBGUI display inconsistent (alignment).

SSH / TELNET Configuration

SSH Mode	Enabled ∨
Key Exchange Algorithms	
	☑ curve25519-sha256
	☑ ecdh-sha2-nistp521
	☑ ecdh-sha2-nistp384
	☑ ecdh-sha2-nistp256
	☑ diffie-hellman-group14-sha1
	☑ diffie-hellman-group1-sha1
	☑ kexguess2
TELNET Mode	Enabled ∨
Hostkey Status	Normal

Alignment incorrect in previous version

Improved in v01.01.03.0013

4. TSS5386: Query relating to LLDP displaying IP address for untagged vlans as opposed to or not for tagged vlans.

5. TSS5398: ISW 10/100 ISW 4-10/100P || Version: ISW-TLN-8PORT_V01.01.03.0012.dat || Fast Ethernet interfaces changed to Gigabit

Special notes: When upgrade to software version 01.01.03.0012 or later, the FE models (ISW 4-10/100P, 2-10/100T, 2-SFP and ISW 8-10/100P, 4-SFP) will change to GE models.

Root cause: The firmware size is bigger in newer version and cause FE/GE model customization database overlapped with firmware partition. The issue is triggered by firmware upgrade with 01.01.03.0012 or later version.

Workaround solution for solving this issue:
- Login to ISW
- Type following commands to re-format GE/FE model customization database. In v01.01.03.0013, the new customization information moves to a safe location.

  platform debug allow
  configure terminal
  debug default interface fe

- Reboot ISW

6. Mantis 6314: Use CLI to show poe firmware version is 0.

[v01.01.03.0012]

The release note includes all feature changes and fixed bugs since previous release
v01.01.03.0011.

<Software Base>

MSCC VSC7429, VSC7425 Compatible

OS: eCos Operating System

Version 3.65 CE Service

<New Features>

None

<Feature update>

When a FA upstream switch is selected, ISW will set 'QoS trust tag' of uplink ports
automatically:

- In the case of no link aggregation, ISW will set 'QoS trust tag' of the uplink port.
- In the case of static LAG or LACP, ISW will set 'QoS trust tag' of all ports of the
  aggregation group.

<Fixed Bugs>

None

[v01.01.03.0011]

Model:

ISW 8GbP, 4-SFP, PoE Switch (GE)

ISW 4GbP, 2GbT, 2-SFP, PoE Switch (GE)

ISW 8-10/100P, 4-SFP, PoE Switch (FE)

ISW 4-10/100P, 2-10/100T, 2-SFP, PoE Switch (FE)

FW Release Version: v01.01.03.0011 (for all models)

Documentation Date: 2020/9/28

This is ISW release to add Fabric Attach Client Features. The release note includes all feature changes and fixed bugs since previous release v01.01.02.0010.

<Software Base>

MSCC VSC7429, VSC7425 Compatible

OS: eCos Operating System

Version 3.65 CE Service

<New Features>

Fabric Attach Client features are added in this release (V01.01.03.0011).

<Feature update>

None

<Fixed Bugs>

Default config is wrong on FE models (bug found during test of Fabric Attach Client feature)

[v01.01.02.0010]

Model:

ISW 8GbP, 4-SFP, PoE Switch (GE)

ISW 4GbP, 2GbT, 2-SFP, PoE Switch (GE)

ISW 8-10/100P, 4-SFP, PoE Switch (FE)

ISW 4-10/100P, 2-10/100T, 2-SFP, PoE Switch (FE)

FW Release Version: v01.01.02.0010 (for all models)

Documentation Date: 2020/7/23

This is formal release for production. The release note includes all feature changes and fixed bugs since previous production release v01.01.02.0005.

<Software Base>

MSCC VSC7429, VSC7425 Compatible

OS: eCos Operating System

Version 3.65 CE Service

<New Features>

Support sFTP client, for firmware upgrade and configuration import/export in v01.01.02.0008 or later version.

Example command:

"*firmware upgrade sftp://grace:grace@192.168.7.82/image/ISW-TLN-8PORT_V01.01.02.0008.dat*"

"*copy running-config sftp://test:123@172.16.9.136/abc.txt*"

Note:

sFTP usually is spending time for file transferring due to encoding/decoding of data.

While SFTP file transferring is proceeding, another new SSH session will interrupt the SFTP file transfer.

<Features Updated>

1. SSH (dropbear) is upgraded to 2017.75 in v01.01.02.0007 or later versions.

2. PSE (PoE Chipset) firmware upgrade function is available in normal mode in v01.01.02.0008 or later version.

    Detail: PoE firmware v211 is bundled in side. New CLI command for PoE firmware update ***"poe firmware upgrade"*** CLI command is available for upgrade poe firmware manually. ***"show poe firmware"*** CLI command is available for show poe firmware version.

<Fixed bugs>

TSS 4720: PoE configuration shows "PoE not available - No PoE chip found"

TSS 4926: Customer is having an issue power a license plate camera created by Vigilant Solutions
Details: PoE AF/AT/POH 3 mode are available in this release. To support Vigilant Solutions IPCAM, PoE should operate in POH mode.

TSS 4966: Dropbear SSH Server < 2016.72 Multiple Vulnerabilities

TSS 4986: No PoE Chip found in three switches

TSS 4987: High CPU in most of the network switches

TSS 5035: Unable to provide POE to an MR62e Controller
Details: PoE firmware v211 bundled in this release to solve MR62e Controller issue. Please use CLI command "poe firmware upgrade" to upgrade PoE firmware after upgrade ISW to V01.01.02.0008 or later version
Notes: ISW PoE firmware should be upgraded to v211 to solve this issue. ISW with the production release will included PoE firmware v211 and not required PoE firmware upgrade.

TSS 5067: SNMPv3 does not work when NTP is configured

TSS 5093: The ISW switch or NTP server calculated the wrong time causing SNMPv3 to stop working

TSS 5138: Do ISW switches support writeable SNMP values for these MIB entries - ifXEntry.ifAlias & ifEntry.ifDescr?
Details:
ifXEntry.ifAlias is writable now, but ifEntry.ifDescr is still read-only because it is standard MIB. "Port Description" has been added to switch, switch returns value to ifXEntry.ifAlias as per this new field of each port.
Configurable in CLI/Web. Web page "Configuration/Port", support length 255 char, however, ifAlias length is defined as 64 octets(char). Manager have to make "reload default" or "reload default keep-ip" to load default "Port Description" of each port.

CLI example as below:
===
(config)# interface g 1/1

(config-if)# description ?
<line255>   Port description
(config-if)# description Port-1
SNMPWalk result by default:
***** SNMP QUERY STARTED *****
1: ifAlias.1000001 (octet string) Port-1 [50.6F.72.74.2D.31 (hex)]
2: ifAlias.1000002 (octet string) Port-2 [50.6F.72.74.2D.32 (hex)]
3: ifAlias.1000003 (octet string) Port-3 [50.6F.72.74.2D.33 (hex)]
4: ifAlias.1000004 (octet string) Port-4 [50.6F.72.74.2D.34 (hex)]
5: ifAlias.1000005 (octet string) Port-5 [50.6F.72.74.2D.35 (hex)]
6: ifAlias.1000006 (octet string) Port-6 [50.6F.72.74.2D.36 (hex)]
7: ifAlias.1000007 (octet string) Port-7 [50.6F.72.74.2D.37 (hex)]
8: ifAlias.1000008 (octet string) Port-8 [50.6F.72.74.2D.38 (hex)]

==

TSS 5188: SSH authentication method follows telnet configuration, rather than SSH

Mantis 5436: Gigabit Ethernet port in auto-negotiation mode can't link up while using 100Mb cable

Mantis 5591: If oid inside LLDP TLV which is too long and received by ISW, ISW would have chance to reboot when user enter "show lldp neighbors" command.

Mantis 5693: ALM LED abnormal, Alarm Current/History table doesn't show correct alarm status.

~ END of Release Note