



Network Visibility. Optimized.

**VSS Distributed Traffic Capture System
Comprehensive Test Plan for <Company>**

Revision CS3

6/24/2011

Table of Contents

1	Revision History	4
2	Executive Summary	5
2.1	Objective	5
2.2	Scope	5
2.3	Duration.....	5
3	Test Case Selection and Results	6
4	Management and System Settings	7
4.1	Management Console	7
4.1.1	Using the Serial Cable	7
4.1.2	Using Web Browser for Initial Configuration	10
4.1.3	Connecting Through Web Management Console	12
4.2	System Settings.....	14
4.2.1	Basic System Settings	14
4.2.2	System Clock / Timestamping Clock Source	16
4.3	User Access Control	18
5	Port Configuration and Testing	28
5.1	Port Configuration.....	28
5.1.1	Span Ports	28
5.1.2	Monitor Ports	29
5.1.3	Tap Ports	30
5.1.4	vStack Ports.....	30
5.2	vAssure	30
5.2.1	Enabling vAssure	31
5.2.2	Initiate and Activate vAssure:	31
5.2.3	Verify vAssure	32
5.3	LinkSafe	36
5.3.1	Fail Link on One Port of Tap Pair	36
5.3.2	Restore Link.....	37
6	Standard Feature and Configuration Testing	38

6.1	Selective Aggregation.....	38
6.1.1	Selective Aggregation Configuration	38
6.1.2	Configure and Verify Selective Aggregation	39
6.2	Filtering.....	39
6.2.1	Quick Filters	40
6.2.2	Detailed Filters	43
6.2.3	Advanced Filters	46
6.3	Load Balancing.....	50
6.3.1	Load Balancing Groups	51
6.3.2	Load Balancing In a Failover Scenario	52
6.4	VLAN Tagging.....	54
7	Advanced Feature Configuration and Testing	57
7.1	Port Stamping	57
7.2	Time Stamping	60
7.3	MPLS Label Stripping.....	63
7.4	VLAN Tag Stripping.....	65
7.5	GTP De-encapsulation	67
7.6	vSlice	69
8	vStack+	75
8.1	vStack+ Configuration	75
8.2	Verify vStack+ Web Console Redirection	76
8.3	Verify vStack+ System	77
8.4	Features Configuration including Mesh vStack+ and Testing.....	79
9	SNMP and syslog Capabilities.....	80
9.1	SNMP Configuration and MIB Structure	80
9.2	SNMP Traps	81
9.3	Syslog.....	82
10	Appendix A: Factory Default Values	84
11	Appendix B: Images of v.24 and v2x16 Distributed Taps.....	85
12	Appendix C: VSS Monitoring Latency Measurements.	86

1 Revision History

Revision	Author	Date	Notes
CS1	Chetan Shah	5/03/2010	New test plan created
CS2	Chetan Shah	5/04/2010	Added test cases for VLAN filtering and custom filtering
CS3	Sharon Chang	6/23/2011	General updates of test plan to reflect the current product capabilities

2 Executive Summary

2.1 Objective

The purpose of this document is to provide an evaluation framework for VSS Distributed Traffic Capture System (DTCS) at a client site.

2.2 Scope

This document provides test procedures to demonstrate key features offered in the DTCS system. While the test plan serves well as a quick “getting started” guide, it does not cover all the options and functionalities available in the DTCS.

If additional details on the DTCS are required, please contact the VSS Representative.

2.3 Duration

The project evaluation is expected to be <NumberOfDays> days

- Start Date: <StartDate>
- End Date: <EndDate>

Commented [SC1]: Provide number of days

Commented [SC2]: Provide start date

Commented [SC3]: Provide end date

3 Test Case Selection and Results

Test Case to Validate	Test Case		Result	
			Accepted	Not Accepted
✓	4.1.1	Using the Serial Cable		
✓	4.1.2	Using Web Browser for Initial Configuration		
✓	4.1.3	Connecting Through Web Management Console		
✓	4.2.1	Basic System Settings		
✓	4.2.2	System Clock / Timestamping Clock Source		
	4.3	User Access Control		
✓	5.1.1	Span Ports		
✓	5.1.2	Monitor Ports		
✓	5.2	vAssure		
✓	5.3	LinkSafe		
✓	6.1.1	Selective Aggregation Configuration		
✓	6.2.1	Quick Filters		
✓	6.2.2	Detailed Filters		
✓	6.2.3	Advanced Filters		
✓	6.3.1	Load Balancing Groups		
✓	6.3.2	Load Balancing In a Failover Scenario		
	6.4	VLAN Tagging		
	7.1	Port Stamping		
	7.2	Time Stamping		
	7.3	MPLS Label Stripping		
	7.4	VLAN Tag Stripping		
	7.5	GTP De-encapsulation		
✓	7.6	vSlice		
✓	8	vStack+		
	9	SNMP and syslog Capabilities		

4 Management and System Settings

The hardware configuration requirements of the VSS Products devices used are as follows:

Quantity	VSS Product	Requirements		
		Space	Power Outlets	IP Address for Management
1	v24	1U ¹	1-2	1
0	v24 Expert	2U	1-2	1
1	v4x24	1U	1-2	1
0	v2x16	1U	1-2	1
Total	2		2-4	2

4.1 Management Console

VSS Monitoring solutions provide management options via a simple-to-use graphical user interface (GUI) using web access, and command line interface (CLI). The following test procedures demonstrate both access methods with all the VSS DTCS products.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- A PC/laptop with Ethernet (GbE) and serial connectivity is available.
- A serial cable is available (section 4.1.1 only).
- An Ethernet cable (CAT5) is available (section 4.1.2, 4.1.3 only).
- Designated IP address(es) for the DTCS units is provided.
- Network access is available such that the DTCS management port can be accessed remotely once configuration is complete.
- The DTCS units are racked securely and powered.

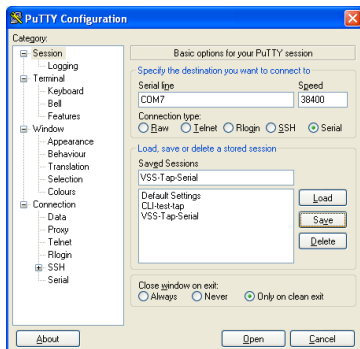
4.1.1 Using the Serial Cable

The following test procedure describes the method for accessing DTCS management console through a serial connection. The test procedure is valid for all VSS DTCS units that preserve the default admin login information. In general, the VSS DTCS units provided are delivered with factory default configuration.

1. Connect a standard straight DB9 male-to- female cable between the DTCS unit and a PC with a terminal emulator (eg. HyperTerminal or PuTTY.exe).
2. Launch the terminal emulator on the PC and apply the following the configurations parameters:
 - Bits per second: 38400
 - Data Bits: 8 bits

¹ Each 1U device is 17.3"(w) x 22.5"(d) x 1.75" (h); 1RU high, fits standard 19" rack 21" deep.

- Parity: No Parity
- Stop Bits: 1 Bit
- Flow control: No Flow Control



3. Click **Open**. The following screen with a login prompt should appear; If you do not see the screen below, notify the VSS that the serial connection to the CLI is not functioning as expected.



4. Enter the default login information and click **Enter**:

Login: **admin**

Password: <no password>

After successfully logging into the unit, the following menu of options should appear:


```
login--> admin
password-->

*****
*      VSS Monitoring      *
*      Command Line Shell  *
*
* Enter '?' to see list of available command *
* groups. The 'spacebar' or 'tab key' will *
* display available command options or can *
* be used for command completion. Enter '??' *
* following a command for extended help. *
*****

Welcome admin it is Tue May  3 21:33:59 UTC 2011
>
```

5. Enter “?” to see the list of available commands.

```
COM3 - PuTTY
filter      show/add/delete a filter
filtermap   Add/remove/change the mapping of a filter to one-or-more ports
.
help        Enter a command group
history     Display the current session's command line history
logout      Logout of the current CLI session
mpls-strip  Show/add/delete an MPLS Stripping map
ping        Ping a target IP node
port        Get/Set port attributes
ports       Display known port IDs/port names
reboot      Reboot this TAP (**WARNING: all connections will be closed!)
snmp        Get/Set a TAP SNMP configuration parameter
status      View a (read-only) summary of current TAP system status
system      Get/Set a TAP system configuration value
trigger-policy Show/add/delete a trigger
vslice-filter show/add/delete a filter
vslice-filtermap Show/add/delete a VSlice mapping
vstack-ports Display known VStack remote monitor port IDs/port names

> system
contact      dns      gateway      gettime      ip      location
name         netmask  ntpserver  product      settime  syslogserver
timestring   version
> system
```

6. Enter command “**system ip**” to view the current management IP configuration.
7. Enter command “**system ip <assigned_ip>**” to modify the DTCS to use the assigned IP address for the management port. The system will return “**+OK**” when the change is successfully applied.
8. Repeat Step 6 to verify that the IP address change is in effect.
9. In a similar manner, modify the subnet mask and router settings to the designed values by using the following commands:

```
system gateway <gateway>
system netmask <mask_value>
```

10. Enter “**exit**” to logout of the current terminal session.
11. Repeat Steps 1 to 10 to configure all the DTCS units supplied.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Configure DTCS system properties via CLI	DTCS management port IP address, subnet mask, and routing settings are applied			

Overall Result

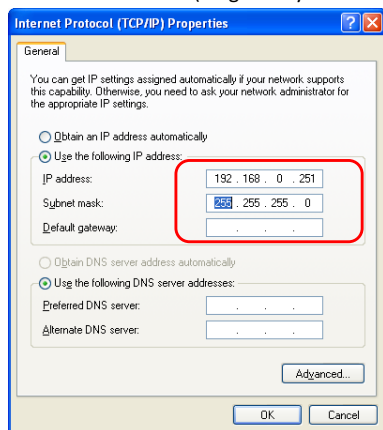
Test case accepted: ☐, not accepted ☐

4.1.2 Using Web Browser for Initial Configuration

The following test procedure describes the method the method for accessing DTCS management console through an Ethernet connection. The test procedure is valid for all VSS DTCS units that preserve the default admin login information. In general, the VSS DTCS units provided are delivered with factory default configuration.

This test procedure is not an continuation of section 4.1.1 Using the Serial Cable as the parameters used assumes that the DTCS unit still has all the factory default settings.

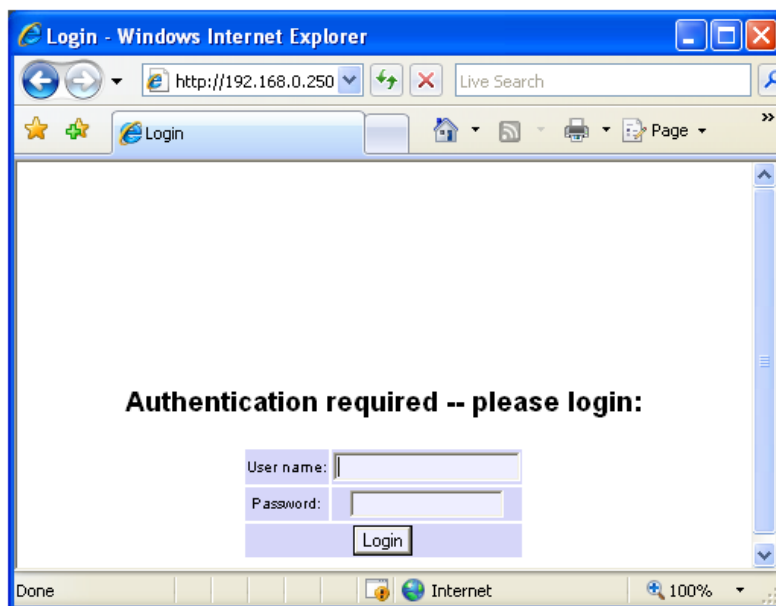
1. Connect the DTCS management port to a PC with an Ethernet cable.
2. From Windows Control Panel, change the network adaptor’s IPv4 settings to:
 - IP Address 192.168.0.251
 - Mask 255.255.255.0 (no gateway is necessary)



3. Click **OK** to apply the changes.
4. Power on the DCTS .
5. From Windows **Start** menu, go to **Run** and enter “**cmd**” to open an command prompt.
6. In the command prompt, enter the command below to verify connectivity between the PC and the DTCS unit:

ping 192.168.0.250

7. If the connection is successful, launch a web browser and go to URL <http://192.168.0.250> as shown below:



8. Enter the default login information below and click **Login**.
Login: **admin**
Password: <no password>
9. In the Web UI, go to the **System Settings** link on the left frame.

- Under **Network Settings** section, enter the assigned IP address, subnet mask and gateway/router. The following is a sample screenshot of the Network Settings information:

The screenshot shows a web management console for a DTCS unit. On the left is a navigation menu with links for Status (System Status, Network Activity), Settings (System Settings, Port Settings, SNMP Settings, Access Control), Filter Library (Filter Settings), Save Settings, Load Settings, and Support (System Software, Contact Us). The main area displays the 'System Settings' and 'Network Settings' sections. The 'System Settings' section has input fields for 'System Name', 'System Location', and 'System Contact'. The 'Network Settings' section has input fields for 'IP Address' (192.168.11.24), 'Subnet Mask' (255.255.254.0), 'Gateway/Router' (192.168.10.1), 'DNS Server', and 'Syslog Server'.

- Click the **Submit** button to save the configuration.
- After the change is successfully applied, the current login session will no longer be connected. Enter the assigned IP address in the web browser again to verify that the change has taken effect. If the assigned IP address is not on the 192.168.0.0/24 subnet, the PC network adaptor IPv4 setting needs to be updated in order for connectivity to the DTCS unit to resume.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Configure DTCS system settings via web UI	DTCS management port IP address, subnet mask, and routing settings are applied			

Overall Result

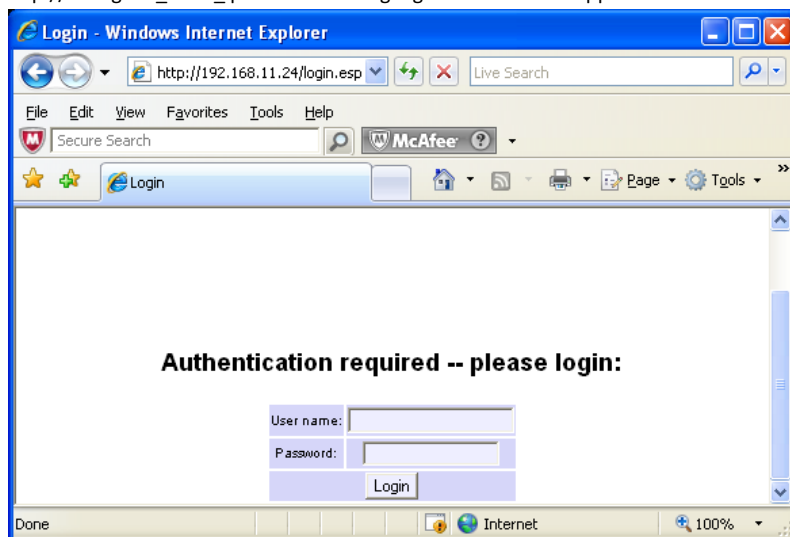
Test case accepted: ☐, not accepted ☐

4.1.3 Connecting Through Web Management Console

The following test procedure provides final verification for DTCS unit connectivity in a network. The procedure should be executed upon successful reconfiguration of the DTCS IP address described in 4.1.1 and 4.1.2.

- Connect the DTCS unit to the network it is assigned to.

- From a PC on the same network as the DTCS unit, launch a web browser and enter URL `http://<assigned_DTCS_ip>`. The following login screen should appear:



- Enter the default login information below and click **Login**.
Login: **admin**
Password: <no password>
- Repeat Steps 1-3 for all the DTCS units provided.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Connect DTCS system from a remote PC on the same network	DTCS unit can be reached via a web browser with URL being its assigned IP			

Overall Result

Test case accepted: ☐, not accepted ☐

4.2 System Settings

4.2.1 Basic System Settings

The following test procedure describes how additional DTCS system settings parameter can be modified via the web UI remotely. The system settings covered in this section includes System Name, Location, and Contact Information.

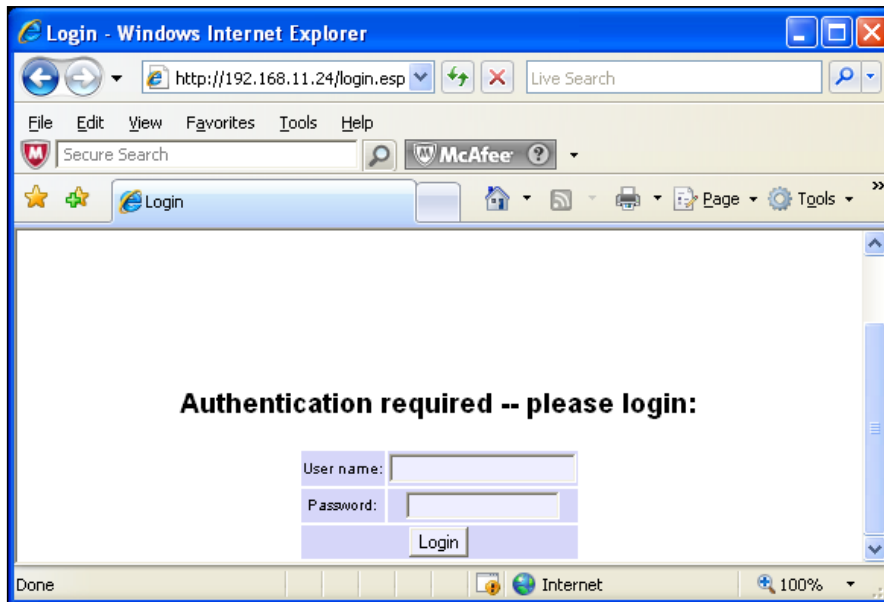
Refer to the DTCS User Manual for details on system settings not covered in this test plan.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.

1. Launch the web browser and access the URL **http://<assigned_DTCS_ip>** as shown below:



2. Enter the default login information below and click **Login**.
Login: **admin**
Password: <no password>

Upon successful login, the System Status page similar to below should appear:

Status
[System Status](#)
[Network Activity](#)

Settings
[System Settings](#)
[Port Settings](#)
[SNMP Settings](#)
[Access Control](#)

[Filter Library](#)
[Filter Settings](#)
[Slicing Library](#)

V2.16X.C-NF-AF-PM

Friday, May 14, 2010 3:46:55 PM (14 May 2010 22:46:55 UTC) Booted Friday, May 14, 2010 3:28:07 PM (14 May 2010 22:28:07 UTC)

System Name: Running 0 days, 0 hours, 18 minutes, 48 seconds

System Location: Last configuration change Friday, May 14, 2010 3:28:05 PM

System Contact: The Monitor Buffer is OK

Internal Temperature: 93 °F, 34 °C

Main Power Supply #1: Normal voltage Main Power Supply #2: **Zero or low voltage**

Power Supply / Voltage Alert

- In the Web UI, go to the **System Settings** link on the left frame.
- Under **System Settings**, Type the following information in the System Settings dialog boxes:
 - System Name: **<any_name>**
 - System Location: **<lab_location>**
 - System Contact: **<contact_name_email>**

System Settings

System Name: v24S.P-SPAN

System Location: Lab1, Rack3

System Contact: VSS SE

- Click the **Submit** button at the bottom of the page to save the System Settings. Verify in the System Status page that the name, location and contact information changes are applied.

V24S.P-SPAN

Fri Jun 24 2011 15:47:34 GMT-0700 (Pacific Daylight Time) (24 Jun 2011 22:47:34 GMT) Booted Thu Jun 23 2011 10:38:18 GMT-0700 (Pacific Daylight Time) (23 Jun 2011 17:38:18 GMT)

System Name: v24S.P-SPAN Running 1 days, 5 hours, 9 minutes, 16 seconds

System Location: Lab1, Rack3 Last configuration change Fri Jun 24 2011 15:47:29 GMT-0700 (Pacific Daylight Time)

System Contact: VSS SE The Monitor Buffer is OK

Internal Temperature: Normal (127 °F, 53 °C)

Main Power Supply #1: Normal voltage Main Power Supply #2: **Zero or low voltage**

Power Supply / Voltage Alert

- Repeat Steps 1-5 for all the DTCS units supplied.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Configure and save the DTCS system name, location, and contact information	Assigned system name, location, and contact information are correctly applied and displayed in the System Status page			

Overall Result

Test case accepted: ☐, not accepted ☐

4.2.2 System Clock / Timestamping Clock Source

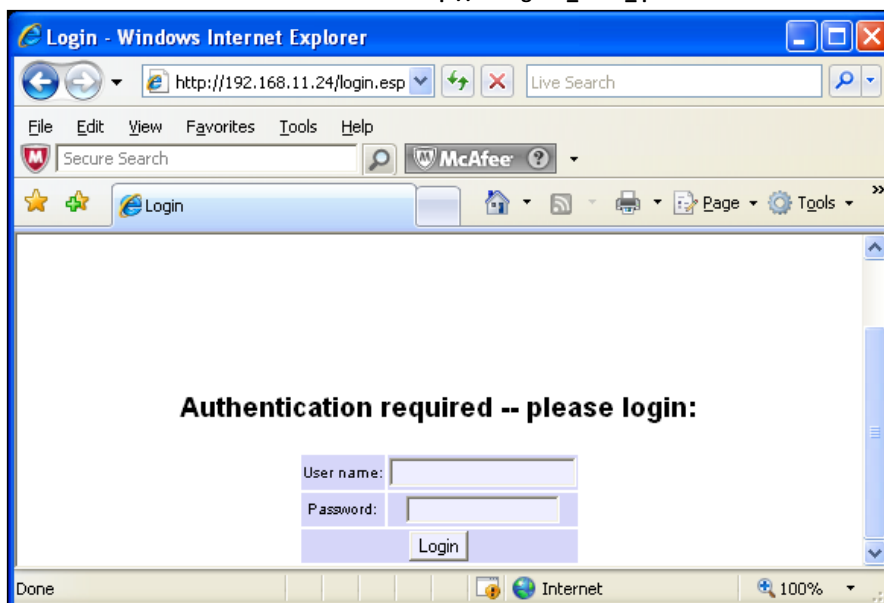
The following test procedure describes how DTCS system clock source is defaulted to the local clock, but can be modified to a NTP clock source if correctly configured. GPS clock source is not described in this section but is also supported for selected DTCS version with firmware 2.3 or above.

Refer to the DTCS User Manual for details not covered in this test plan.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.
 - The DTCS units have connectivity to an external NTP server (eg. us.pool.ntp.org)
1. Launch the web browser and access the URL http://<assigned_DTCS_ip> as shown below:



2. Enter the default login information below and click **Login**.
Login: **admin**
Password: <no password>

Upon successful login, the System Status page similar to below should appear:

Status System Status Network Activity Settings System Settings Port Settings SNMP Settings Access Control Filter Library Filter Settings Slicing Library	<table border="1"> <tr> <th colspan="2">V2.16X.C-NF-AF-PM</th> </tr> <tr> <td>Friday, May 14, 2010 3:46:55 PM (14 May 2010 22:46:55 UTC)</td> <td>Booted Friday, May 14, 2010 3:28:07 PM (14 May 2010 22:28:07 UTC)</td> </tr> <tr> <td>System Name:</td> <td>Running 0 days, 0 hours, 18 minutes, 48 seconds</td> </tr> <tr> <td>System Location:</td> <td>Last configuration change Friday, May 14, 2010 3:28:05 PM</td> </tr> <tr> <td>System Contact:</td> <td>The Monitor Buffer is OK</td> </tr> <tr> <td>Internal Temperature: 93 °F, 34 °C</td> <td></td> </tr> <tr> <td>Main Power Supply #1: Normal voltage</td> <td>Main Power Supply #2: Zero or low voltage</td> </tr> <tr> <td colspan="2">Power Supply / Voltage Alert</td> </tr> </table>	V2.16X.C-NF-AF-PM		Friday, May 14, 2010 3:46:55 PM (14 May 2010 22:46:55 UTC)	Booted Friday, May 14, 2010 3:28:07 PM (14 May 2010 22:28:07 UTC)	System Name:	Running 0 days, 0 hours, 18 minutes, 48 seconds	System Location:	Last configuration change Friday, May 14, 2010 3:28:05 PM	System Contact:	The Monitor Buffer is OK	Internal Temperature: 93 °F, 34 °C		Main Power Supply #1: Normal voltage	Main Power Supply #2: Zero or low voltage	Power Supply / Voltage Alert	
V2.16X.C-NF-AF-PM																	
Friday, May 14, 2010 3:46:55 PM (14 May 2010 22:46:55 UTC)	Booted Friday, May 14, 2010 3:28:07 PM (14 May 2010 22:28:07 UTC)																
System Name:	Running 0 days, 0 hours, 18 minutes, 48 seconds																
System Location:	Last configuration change Friday, May 14, 2010 3:28:05 PM																
System Contact:	The Monitor Buffer is OK																
Internal Temperature: 93 °F, 34 °C																	
Main Power Supply #1: Normal voltage	Main Power Supply #2: Zero or low voltage																
Power Supply / Voltage Alert																	

3. In the Web UI, go to the **System Settings** link on the left frame.
4. Under **System Clock**, **NTP Configuration**, enter the NTP servers. Refer to <http://www.pool.ntp.org/en/> for the full listing of NTP servers.

System Clock	
<div>Local Clock Settings</div> <div> <input checked="" type="checkbox"/> Set clock from browser's (PC's) clock </div> <div> Date: 06 / 24 / 2011 Time: 16 : 15 : 56 </div>	<div>NTP Configuration</div> <div> <input type="checkbox"/> = Timestamping clock source </div> <div> NTP Server 1: us.pool.ntp.org NTP Server 2: ca.pool.ntp.org NTP Status: Never Synchronized State Deviation: 0 </div>

Note: If the DTCS is connected to a private lab network, the correct **DNS server** for the DTCS unit may need to be specified under **System Settings**, **Network Settings** for the NTP configuration to work

5. Click the **Submit** button at the bottom of the page to save the System Settings. Verify in the System Status page that the name, location and contact information changes are applied.

V24S.P-SPAN	
Fri Jun 24 2011 15:47:34 GMT-0700 (Pacific Daylight Time) (24 Jun 2011 22:47:34 GMT)	Booted Thu Jun 23 2011 10:38:18 GMT-0700 (Pacific Daylight Time) (23 Jun 2011 17:38:18 GMT)
System Name: V24S.P-SPAN	Running 1 days, 5 hours, 9 minutes, 16 seconds
System Location: Lab1, Rad3	Last configuration change Fri Jun 24 2011 15:47:29 GMT-0700 (Pacific Daylight Time)
System Contact: VSS SE	The Monitor Buffer is OK
Internal Temperature: Normal (127 °F, 53 °C)	
Main Power Supply #1: Normal voltage	Main Power Supply #2: Zero or low voltage
Power Supply / Voltage Alert	

6. Wait for a few minutes and go to **System Settings**, verify that the timestamping clock source has been updated to NTP and the status is in "Normal Synchronized State".²³

² In the scenario where NTP configuration is not correctly applied, or if synchronization failed, the local clock will be used as the timestamping source.

³ In DTCS Firmware Release 2.3 and above, selected hardware will also support GPS as the timestamping source. Contact the VSS Representative for more details.

7. Remove the NTP Server settings and click **Submit**. Verify that the NTP Status is now blank and the timestamping clock source switched back to Local Clock.

8. Repeat Steps 1-**Error! Reference source not found.** for all the DTCS units supplied.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Configure and save the NTP servers as the timestamping source	NTP status is in "Normal Synchronized State"; NTP is used as the primary timestamping clock source			
2	Remove NTP server setting and submit change	NTP status is immediately updated to <blank> and the timestamping clock source switches back to local clock			

Overall Result

Test case accepted: ☐, not accepted ☐

4.3 User Access Control

Use VSS Distributed Tap Web UI to manage and control user access to System Settings, Network Port Settings, Monitor Port Settings and Filter settings on the DTCS units.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.
- Internet browser allows users to clear cache; if using IE8, IE8 mode is ON and Compatibility mode is OFF. This is only required to work around a known issue in DTCS firmware v2.1: Access control content may look incorrect in GUI when the same browser is used by different users.

Configuring User Access Control:

1. In the VSS web UI, click on the [Access Control](#) link to view the list of Authorized Users.

Authorized Users					
User	Password	Confirm	Access Permissions	Accessible Ports	+Add User
admin			<input checked="" type="checkbox"/> System Settings <input checked="" type="checkbox"/> Network Port Settings <input checked="" type="checkbox"/> Filter Library	<input checked="" type="checkbox"/> Monitor Port Settings <input checked="" type="checkbox"/> Filter Settings/Maps 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	

2. Click on [+ Add User](#) and fill in the login information and access permissions for the following users:

User	Password	Confirm	Access Permissions	Accessible Ports
TestUser1	<password>	<matching password>	System Settings	<None>
TestUser2	<password>	<matching password>	Network Port Settings Monitor Port Settings Filter Settings/Maps	1, 2, 13, 14, 15, 16
TestUser3	<password>	<matching password>	Filter Library	<None>
TestUser4	<password>	<matching password>	Network Port Settings Monitor Port Settings Filter Library Filter Settings/Maps	3, 4, 5, 6, 7, 8

- Click **Submit** at the bottom of the page to apply the user access and other security settings. The resulting user access configuration below is now saved:

Authorized Users						
User	Password	Confirm	Access Permissions	Accessible Ports	+Add User	
admin			<input checked="" type="checkbox"/> System Settings <input checked="" type="checkbox"/> Network Port Settings <input checked="" type="checkbox"/> Filter Library	<input checked="" type="checkbox"/> Monitor Port Settings <input checked="" type="checkbox"/> Filter Settings/Maps 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 <input checked="" type="checkbox"/> 17 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 19 <input checked="" type="checkbox"/> 20 <input checked="" type="checkbox"/> 21 <input checked="" type="checkbox"/> 22 <input checked="" type="checkbox"/> 23 <input checked="" type="checkbox"/> 24		
TestUser1	****	****	<input checked="" type="checkbox"/> System Settings <input type="checkbox"/> Network Port Settings <input type="checkbox"/> Filter Library	<input type="checkbox"/> Monitor Port Settings <input type="checkbox"/> Filter Settings/Maps 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24	-Delete	
TestUser2	****	****	<input type="checkbox"/> System Settings <input checked="" type="checkbox"/> Network Port Settings <input type="checkbox"/> Filter Library	<input checked="" type="checkbox"/> Monitor Port Settings <input checked="" type="checkbox"/> Filter Settings/Maps 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 <input checked="" type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24	-Delete	
TestUser3	****	****	<input type="checkbox"/> System Settings <input type="checkbox"/> Network Port Settings <input checked="" type="checkbox"/> Filter Library	<input type="checkbox"/> Monitor Port Settings <input type="checkbox"/> Filter Settings/Maps 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24	-Delete	
TestUser4	****	****	<input type="checkbox"/> System Settings <input checked="" type="checkbox"/> Network Port Settings <input checked="" type="checkbox"/> Filter Library	<input checked="" type="checkbox"/> Monitor Port Settings <input checked="" type="checkbox"/> Filter Settings/Maps 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24	-Delete	

- Logout from the current session and clear browser cache. (This is required to work around a known issue in DTCS firmware v2.1: Access control content may look incorrect in GUI when the same browser is used by different users.)

5. Login as **TestUser1**. Verify that on the left, TestUser1 only has access to system configuration privilege: System Settings, SNMP Settings, Access Control.

The screenshot displays the VSS monitoring web interface. On the left sidebar, the 'VSS monitoring' logo is at the top. Below it, the 'Status' section includes links for 'System Status' and 'Network Activity'. The 'Settings' section includes links for 'System Settings' (highlighted in orange), 'SNMP Settings', and 'Access Control'. Below these are links for 'Save Settings' and 'Load Settings'. The 'Support' section includes links for 'System Software' and 'Contact Us'. At the bottom of the sidebar, it shows 'User: TestUser1' and a 'Logout' link.

The main content area contains three configuration sections:

- System Settings:** A form with three input fields: 'System Name:', 'System Location:', and 'System Contact:'.
- Network Settings:** A form with several input fields: 'IP Address:' (192, 168, 0, 250), 'Subnet Mask:' (255, 255, 255, 0), 'Gateway/Router:' (192, 168, 0, 1), 'DNS Server:' (192, 168, 0, 1), 'Syslog Server 1:', and 'Syslog Server 2:'.
- Date/Time (in this local/PC timezone):** A form with a dropdown menu set to 'Set clock from browser's (PC's) clock', a 'Date:' field (06 / 17 / 2011), a 'Time:' field (09 : 25 : 20), and two 'NTP Server' fields.

6. Repeat Step 4 to logout and clear cache. Login as **TestUser2**. Verify that on the left, TestUser2 only has access to Port Settings and Monitor Settings.

7. Verify that in Port Settings, TestUser2 can only access ports 1, 2, 13, 14, 15, 16.

VSS monitoring

Status
[System Status](#)
[Network Activity](#)

Settings
[Port Settings](#)
[Monitor Settings](#)
[vSlice Settings](#)
[MPLS Stripping](#)
[Save Settings](#)
[Load Settings](#)

Support
[Contact Us](#)

User: **TestUser2**
[Logout](#)

Port 1 Settings

Port Name:

Speed: ☐ 1G ☒ 10G

Type:

SFP+ Module Identification:

Class: ☒ Span ☐ Monitor ☐ vStack+

8. Verify that in Monitor Settings, TestUser2 can only create port mappings for ports 1, 2, 13, 14, 15, 16; but can still access the filters already in the Filter Library.

Filtering and Monitor Output Settings

Each row below represents a mapping of Network Port input to Monitor Port output.
 To add a new mapping row, click the "+Add" button below.
 To remove a mapping row, click the "Delete" button on the desired row.

Filter Expression	Network Port Input	Monitor Port Output	Rank
<input type="button" value="(Unfiltered)"/> <input type="button" value="(Nonmatch)"/> <input type="button" value="(Unfiltered)"/> <input type="button" value="HTTP"/> <input type="button" value="ICMP"/>	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 Load Balancing: <input type="text" value="None (output to all selected ports)"/>	<input checked="" type="checkbox"/>

- Repeat Step 4 to logout and clear cache. Login as **TestUser3**. Verify that on the left, TestUser3 only has access to the Filter Library and can save/delete/copy filters in the Filter Library.

The screenshot shows the VSS monitoring interface. On the left sidebar, the user is logged in as **TestUser3**. The main content area is titled "Monitor Filtering". It includes a "Filter:" dropdown with a "+ Add new filter" button, a "Filter Name:" text input, and buttons for "Save Filter", "Delete Filter", and "Copy Filter". Below this is a "Condition:" text area. At the bottom, there are tabs for "Quick", "Detailed", and "Advanced". The "Quick" tab is selected, showing "Monitor packets to or from:" with fields for "MAC/Ethernet Address" and "or IP Address", and "Using protocol(s):" with a list of protocols including Any/Ignore, ICMP, IGMP, OSPF, RSVP, ARP, RARP, TCP, HTTP, HTTPS, Telnet, SSH, RSH, FTP, SMTP, POP3, NNTP, NNTPS, IRC, LDAP, UDP, SNMP, NTP, DNS, NetBIOS, TFTP, and BOOTP/DHCP.

- Repeat Step 4 to logout and clear cache. Login as **TestUser4**. Verify that on the left, TestUser4 has access to Port Settings, Monitor Settings, Filter Library, and Filter Settings/Maps.
- Verify that in Port Settings, TestUser4 can only access ports 3, 4, 5, 6, 7, 8.

The screenshot shows the VSS monitoring interface. On the left sidebar, the user is logged in as **TestUser4**. The main content area is titled "Port 3 Settings". It includes a "Port Name:" text input, a "Speed:" dropdown with options for "1G" and "10G", a "Type:" dropdown with "SFP+" selected, and a "SFP+ Module Identification:" text input with "FINISAR CORP. FTLX8571D3BCV (1G/10G)" entered. Below this is a "Class:" dropdown with options for "Span", "Monitor", and "vStack+", and a "Save Changes" button.

12. Verify that in Filter Library, TestUser4 is able to save/delete/copy filters.

13. Verify that in Monitoring Settings, TestUser4 can only create port mappings for ports 3, 4, 5, 6, 7, 8; and can access all the filters in the Filter Library

Filter Expression	Network Port Input	Monitor Port Output	Rank
(Unfiltered)	[3] [4]	[5] [6] [7] [8] Load Balancing: None (output to all selected ports)	

Note for users with “Filter Settings/Maps” access privilege can view *all* the existing monitor mappings, including mappings for ports they are not permitted to access. This means they are able to delete mappings created by other users for other ports, or modify these mappings to use the ports they have access to.

The following example shows how users with “Filter Settings/Map” access may affect other users’ configuration:

- Both TestUser2 and TestUser4 have access to Filter Settings/Map access
- TestUser2 is only allowed to access ports 1, 2, 13, 14, 15, 16.
- TestUser4 is only allowed to access ports 3, 4, 5, 6, 7, 8.

As seen from the admin view, TestUser2 and TestUser4 have created their own mappings as follows:

Filter Expression	Network Port Input	Monitor Port Output	Rank
HTTP	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4	<input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	
(Nonmatch)	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4	<input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	
ICMP	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4	<input checked="" type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	
HTTP	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4	<input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	
(Nonmatch)	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4	<input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	

When TestUser2 logs in, the Monitor Setting view shows all 5 mappings, including the mappings created by TestUser4.

Status

[System Status](#)
[Network Activity](#)

Settings

[Port Settings](#)
[Monitor Settings](#)
[vSlice Settings](#)
[MPLS Stripping](#)
[Save Settings](#)
[Load Settings](#)

Support

[Contact Us](#)

 User: **TestUser2**
[Logout](#)

Model:
 V245-P-SPAN
 Software:
 2.1.19

Filter Expression	Network Port Input	Monitor Port Output	Rank
HTTP	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2	<input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	
(Nonmatch)	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2	<input type="checkbox"/> 13 <input type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	
ICMP	<input type="checkbox"/> 1 <input type="checkbox"/> 2	<input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	
HTTP	<input type="checkbox"/> 1 <input type="checkbox"/> 2	<input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	
(Nonmatch)	<input type="checkbox"/> 1 <input type="checkbox"/> 2	<input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	

Save Settings

Add new mapping

Delete

If TestUser2 deletes the last mapping (“Nonmatch” filter, from ports 3, 4 to port 8), the settings can be saved without any errors or warning.

** Settings have been saved **

Filter Expression	Network Port Input	Monitor Port Output	Rank
HTTP	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2	<input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	<input type="button" value="X"/> <input type="button" value="+"/>
(Nonmatch)	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2	<input type="checkbox"/> 13 <input type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	<input type="button" value="X"/> <input type="button" value="+"/>
ICMP	<input type="checkbox"/> 1 <input type="checkbox"/> 2	<input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	<input type="button" value="X"/> <input type="button" value="+"/>
HTTP	<input type="checkbox"/> 1 <input type="checkbox"/> 2	<input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	<input type="button" value="X"/> <input type="button" value="+"/>

Add new mapping

Save Settings

As the result, in the admin view, the last mapping created by TestUser4 is permanently removed by TestUser2, despite the fact that TestUser2 does not have access to ports 3, 4, and 8.

Filter Expression	Network Port Input	Monitor Port Output	Rank
HTTP	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4	<input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	<input type="button" value="X"/> <input type="button" value="+"/>
(Nonmatch)	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4	<input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	<input type="button" value="X"/> <input type="button" value="+"/>
ICMP	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4	<input checked="" type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	<input type="button" value="X"/> <input type="button" value="+"/>
HTTP	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4	<input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 Load Balancing: IP Dest+Source, & TCP/UDP Dest+Source	<input type="button" value="X"/> <input type="button" value="+"/>

Add new mapping

Because of this current behavior, the recommend practice for modifying monitor mappings in a multi-user environment is to modify/delete only the mappings of ports the users have access to, and recognize that mappings shown with “no ports selected” may belong to other users and should not be modified or deleted.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Login as “admin” and configure user access control	Users with “System Settings” access (admin) can add/delete users, set password, grant specific access privilege to ports and specific configuration areas)			
2	Login as user with limited Network Port and Monitor Port access	Users can only access the assigned ports in Port Setting and Monitor Setting views; Users			

		cannot view/modify filters, but can apply pre-existing filters for Monitor Settings			
3	Login as users with only Filter Setting access	Users only add/delete/copy filters and cannot access any port or monitor settings			

Overall Result

Test case accepted: ☐, not accepted ☐

5 Port Configuration and Testing

5.1 Port Configuration

The DTCS product family supports a range of physical media and port link speed, including fiber at 10G and 1G, and copper at 1G and 10/100. Depending on the hardware configuration, each port can be configured in different classes: Tap, Span, Monitor, and vStack. The following sections will demonstrate the configuration of each port class and the special features VSS supports to allow these devices to be the most reliable capturing system when installed inline with the live network.

5.1.1 Span Ports

Different from what common industry term for “span” ports, a “Span” port in the DTCS means the port is in a simple input port. When configured as “Span”, the port runs in a unidirectional receive mode.

All DTCS ports can be configured to “Span” mode.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.

1. Click on the **Port Settings** on the left and select the port number that will be a input port
2. Select **SPAN** as Class, and type an appropriate name in **Port Name** dialog box as shown below:

Port 5 Settings	
Port Name: pswdma201-Te11/4	Type: SFP+
Speed: <input type="radio"/> 1G <input checked="" type="radio"/> 10G	SFP+ Module Identification: FINISAR CORP. FTLX8571D3BCV (1G/10G)
	Class: <input checked="" type="radio"/> Span <input type="radio"/> Monitor <input type="radio"/> vStack+
<button>Save Changes</button>	

3. If there are other ports to be configured as SPAN ports, click on the number of the next port to be configured to apply the configuration to the current port, and to access the configuration page for the next port. Repeat Steps 2-3 to configure additional SPAN ports.
4. Click **Save Changes** to apply port configuration to the current port. This action will redirect the browser to the **System Status** page, which reflects all the port class configuration:

5	pswdma201-Te11/4	Up	10G	Span	OK	-2.56 dBm,-2.75 dBm	Setup
6	pswdma202-Te11/4	Up	10G	Span	OK	-2.59 dBm,-2.56 dBm	Setup

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Configure and save the port in SPAN mode	System status shows that the port is running SPAN mode			

Overall Result

Test case accepted: ☐, not accepted ☐

5.1.2 Monitor Ports

As the name suggests, a “Monitor” port in the DTCS runs in the unidirectional transmitting mode, which is generally used to connect to a monitor or analysis tool that processes the data.

All DTCS ports can be configured to “Monitor” mode.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.

1. Click on the **Port Settings** on the left and select the port number that will be a input port
2. Select **Monitor** as Class, and type an appropriate name in **Port Name** dialog box as shown

Port 2 Settings

Port Name: port 2

Speed: ☐ 1G ☒ 10G

Type: SFP+

SFP+ Module Identification: FINISAR CORP. FTLX1471D3BCV (1G/10G)

Class: ☐ Span ☒ Monitor ☐ vStack+

Monitor Port Tagging:
☐ Insert Network Port number VLAN tags in Monitor Port output

Save Changes

below:

3. If there are other ports to be configured as Monitor ports, click on the number of the next port to be configured to apply the configuration to the current port, and to access the configuration page for the next port. Repeat Steps 2-3 to configure additional Monitor ports.

- Click **Save Changes** to apply port configuration to the current port. This action will redirect the browser to the **System Status** page, which reflects all the port class configuration:

2	port 2	Up	10G	Monitor	OK	-1.56 dBm,-1.73 dBm	Setup
3	port 3	Up	10G	Monitor	OK	-1.34 dBm,-2.01 dBm	Setup

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Configure and save the port in Monitor mode	System status shows that the port is running Monitor mode			

Overall Result

Test case accepted: ☐, not accepted ☐

5.1.3 Tap Ports

Please refer to sections 5.2 vAssure and 5.3 LinkSafe for more details in tap port configuration.

5.1.4 vStack Ports

Please refer to section 8 vStack+ for more details on vStack configuration.

5.2 vAssure

The vAssure link recovery technology, exclusive to VSS Monitoring, minimizes tap switchover times to within 30-150ms. vAssure applies to GbE copper links and allows tap power up/down without loss of link and without requiring link re-negotiation on the physical connection. Switchover times less than 200ms prevent Spanning Tree and secondary routes to be initiated in complex networking environments which minimizes the effects known to be issues in tapping GbE copper environments.

This test procedure provided in the sections below will verify tap switchover time for power off or power up is less than 150 ms using the fping utility with set testing parameters easy to determine the switchover time.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS unit supplied is equipped with built-in GbE UTP port pairs
- The DTCS units can be reached remotely via web browser.

- Successful login into the DTCS management console via a web browser.
- Fping.exe (on a Windows system) program is available.
This is generally in the ./system32/ directory or can be downloaded from <http://fping.sourceforge.net/>.
- Network elements connected directly to the DTCS tap ports are enterprise grade late model devices. If equipment older than five years or low grade network gear such as D-link, Netgear, Linksys, etc. is used for testing, results may not be consistent. Low grade equipment is commonly overwhelmed by high ping count testing. Rebooting the low grade equipment while the DT is powered on and vAssure is enable may be necessary to increase success rate of the test.

5.2.1 Enabling vAssure

1. Launch your browser and go to the URL **http://<IPaddr>**
2. On the VSS Web UI, click the **Port Settings** link and select a port that is a member of a tapping UTP port pair.
3. Verify the radio button in the **Class** section is set to **Tap**.
4. To enable vAssure, go to the **vAssure Fast Failover** configuration box, click the radio button next to **Enable**.

Port 1 Settings	
Port Name:	
Auto Negotiate:	<input checked="" type="checkbox"/> On
Auto Negotiation Advertisements	
<input checked="" type="checkbox"/> 10H	<input checked="" type="checkbox"/> 100H
<input checked="" type="checkbox"/> 1000H	<input checked="" type="checkbox"/> Symmetric Pause
<input checked="" type="checkbox"/> 10F	<input checked="" type="checkbox"/> 100F
<input checked="" type="checkbox"/> 1000F	<input checked="" type="checkbox"/> Asymmetric Pause
Link state:	<input checked="" type="radio"/> Auto (normal) <input type="radio"/> Force down
Type:	10Base-T/100Base-TX/1000Base-T
Class:	<input checked="" type="radio"/> Tap <input type="radio"/> Span <input type="radio"/> Monitor
Linksafe:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Monitor output timestamping:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Monitor output portstamping:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
vAssure Fast Failover:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

5. Click **Save Changes**. This will automatically take you to the **System Status** page. **Port 2** will automatically have vAssure enabled as the tap port partner of **Port 1**.

5.2.2 Initiate and Activate vAssure:

6. To initiate vAssure, logout of the Distributed Tap Web UI and **power off the tap**.
7. Connect the Ethernet cables from the two network elements between which the link will be tapped. (See Figure 1 Connection diagram for verifying vAssure).
8. Wait until you have link light on for both network elements.

9. Check each network element to verify speed/duplex of 1 gigabit/full was negotiated through the unpowered tap.
10. Test your network connection through the unpowered tap by launching your browser from a system connected on the switch side of the tapped link and connecting to www.vssmonitoring.com.
11. For the tap to “learn” the proper link values of the end devices, power on your tap and wait until you hear the magnetic relay click open.
12. Connect to the tap **Web UI** and go to the **System Status** page.
13. Verify that your two ports have negotiated **1G/Full** for **speed/duplex** and link state is “**Up**”.

Note: If the speed is any other than 1G then vAssure will not give consistent expected results. This feature was designed to enhance only 1G copper environments.

Port Status																				
Port	Name	Link	Speed	Duplex	Negotiate	MDI	Class	Monitor											Status	
A		Down	---	--	--	--	Monitor												--	
B		Down	---	--	--	--	Monitor												--	
C		Down	---	--	--	--	Monitor												--	
D		Down	---	--	--	--	Monitor												--	
1		Up	1G	Full	Auto	Auto	Tap	A	B	C	D	17	18	19	20	21	22	23	24	LinkSafe
2		Up	1G	Full	Auto	Auto	Tap	A	B	C	D	17	18	19	20	21	22	23	24	LinkSafe
3		Down	---	--	Auto	Auto	Tap	A	B	C	D	17	18	19	20	21	22	23	24	LinkSafe En
4		Down	---	--	Auto	Auto	Tap	A	B	C	D	17	18	19	20	21	22	23	24	LinkSafe En
5		Down	---	--	Auto	Auto	Tap	A	B	C	D	17	18	19	20	21	22	23	24	LinkSafe En

5.2.3 Verify vAssure

1. To activate vAssure, power off your tap and back on again.
2. Verify once again the negotiated **speed/duplex** is **1G/Full** on the System Status page.
3. While the DT is powered on go to a command, from a system on one side of the tap use the fping utility to ping a system on the other side of the tap with the following parameters set to run a test of 3000 pings at a 1 ms interval with a timeout of 10 ms.

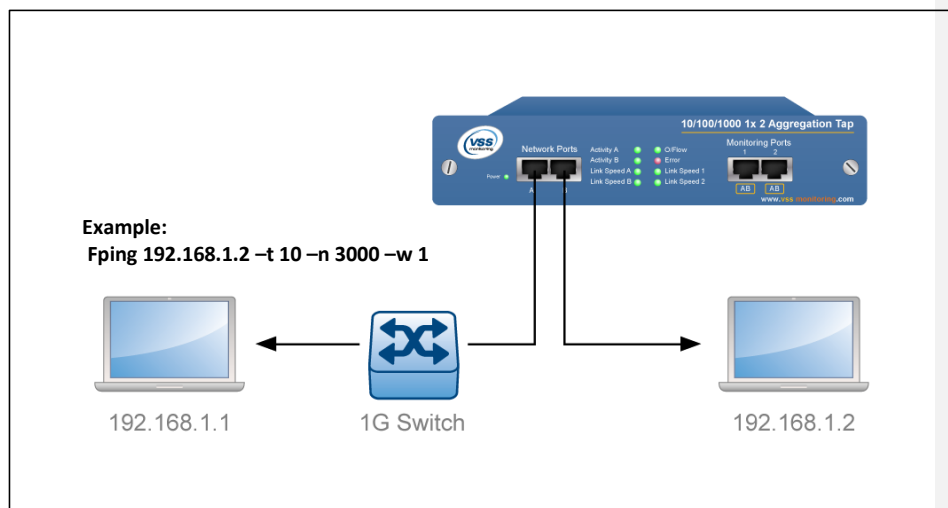


Figure 1 Connection diagram for verifying vAssure

At a command prompt type:

Fping <IP_addr> -t 10 -n 3000 -w 1

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>fping 192.168.11.1 -t 10 -n 3000 -w 1
```

4. You should receive results similar to the following screenshot:

```
Reply[2996] from 192.168.11.1: bytes=32 time=1.8 ms TTL=64
Reply[2997] from 192.168.11.1: bytes=32 time=1.8 ms TTL=64
Reply[2998] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64
Reply[2999] from 192.168.11.1: bytes=32 time=1.5 ms TTL=64
Reply[3000] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64

Ping statistics for 192.168.11.1:
    Packets: Sent = 3000, Received = 2996, Lost = 4 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 1.5 ms, Maximum = 18.8 ms, Average = 1.6 ms

C:\>
```

Explanation: Each ping lost (4 in this case) represents 10 ms because that is the setting for the timeout for a response. Therefore 4x 10 ms = 40 ms when vAssure is enabled and the DT is powered on.

5. Record the loss in ms for baseline fping test : _____

6. Next launch the test again then immediately pull the power cord from the rear of the DT.

```
Reply[2996] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64
Reply[2997] from 192.168.11.1: bytes=32 time=2.0 ms TTL=64
Reply[2998] from 192.168.11.1: bytes=32 time=1.5 ms TTL=64
Reply[2999] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64
Reply[3000] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64

Ping statistics for 192.168.11.1:
    Packets: Sent = 3000, Received = 2993, Lost = 7 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 1.5 ms, Maximum = 51.8 ms, Average = 1.7 ms

C:\>
```

Explanation: Each ping lost (7 in this case) therefore $7 \times 10 \text{ ms} = 70 \text{ ms}$ when vAssure is enabled and the DT is powered off.

7. Record the loss in ms for test during power down of the DT: _____
8. While the power is still off, launch the test again then immediately restore power the DT.

```
Reply[2996] from 192.168.11.1: bytes=32 time=1.5 ms TTL=64
Reply[2997] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64
Reply[2998] from 192.168.11.1: bytes=32 time=1.5 ms TTL=64
Reply[2999] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64
Reply[3000] from 192.168.11.1: bytes=32 time=1.5 ms TTL=64

Ping statistics for 192.168.11.1:
    Packets: Sent = 3000, Received = 2996, Lost = 4 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 1.4 ms, Maximum = 18.0 ms, Average = 1.6 ms

C:\>
```

9. Record the loss in ms for the test during power restoration: _____
10. Through the **Web UI** click on the [System Status](#) link, select the [Setup](#) button at the end of the **Port 1** row.
11. Next to [vAssure Fast Failover](#), select the radio button next to [Disable](#).

Port 1 Settings

Port Name: <input type="text"/> Auto Negotiate: <input checked="" type="checkbox"/> On Auto Negotiation Advertisements <input checked="" type="checkbox"/> 10H <input checked="" type="checkbox"/> 100H <input checked="" type="checkbox"/> 1000H <input checked="" type="checkbox"/> Symmetric Pause <input checked="" type="checkbox"/> 10F <input checked="" type="checkbox"/> 100F <input checked="" type="checkbox"/> 1000F <input checked="" type="checkbox"/> Asymmetric Pause Link state: <input checked="" type="radio"/> Auto (normal) <input type="radio"/> Force down	Type: 10Base-T/100Base-TX/1000Base-T RJ45 Class: <input checked="" type="radio"/> Tap <input type="radio"/> Span <input type="radio"/> Monitor <input type="radio"/> vStack+ Linksafe: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Monitor output timestamping: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Monitor output portstamping: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <div style="border: 2px solid red; padding: 2px;"> vAssure Fast Failover: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled </div>
--	--

[Save Changes](#)

12. Next launch the test again then immediately pull the power cord from the rear of the DT now that vAssure is disabled.

```

Reply[2996] from 192.168.11.1: bytes=32 time=3.5 ms TTL=64
Reply[2997] from 192.168.11.1: bytes=32 time=3.5 ms TTL=64
Reply[2998] from 192.168.11.1: bytes=32 time=2.9 ms TTL=64
Reply[2999] from 192.168.11.1: bytes=32 time=3.3 ms TTL=64
Reply[3000] from 192.168.11.1: bytes=32 time=3.2 ms TTL=64

Ping statistics for 192.168.11.1:
    Packets: Sent = 3000, Received = 2986, Lost = 14 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 1.5 ms, Maximum = 128.1 ms, Average = 2.8 ms

C:\>

```

13. Record the loss during power down in ms for the test when vAssure is not enabled: _____

```

Reply[2996] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64
Reply[2997] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64
Reply[2998] from 192.168.11.1: bytes=32 time=1.6 ms TTL=64
Reply[2999] from 192.168.11.1: bytes=32 time=1.9 ms TTL=64
Reply[3000] from 192.168.11.1: bytes=32 time=1.5 ms TTL=64

Ping statistics for 192.168.11.1:
    Packets: Sent = 3000, Received = 2985, Lost = 15 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 1.4 ms, Maximum = 18.0 ms, Average = 1.6 ms

C:\>

```

14. Lastly, restore power to the DT and launch the final test with vAssure disabled during power restoration.
15. Record the lost during power restoration with vAssure disabled: _____

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Launch a browser on a system connected to the switch side of tapped link while DTCS is in "power off" state	There should be link on and 1G/full for both network elements connected to the DTCS tap port pair. The connection to the website should be successful through the unpowered tap			
2	vAssure test using fping during power down and restoration	Packet loss represents <150ms			

Overall Result

Test case accepted: ☐, not accepted ☐

5.3 LinkSafe

VSS removes ‘point of failure’ concerns associated with copper gigabit taps placed inline. The LinkSafe feature monitors both sides of a tap for link status. If one link fails, the tap causes the other link to drop immediately, thereby enabling the router to realize the failure and reroute packets through a redundant path. The tap then continues to monitor both links until they become available again, at which time the tap re-establishes the primary link between the router and switch. This is bi-directional, and no user intervention is required when the link fails or is re-established.

To simplify installation, the LinkSafe feature is not enabled until both links are up. Immediately after power up, the tap will leave both links enabled. This allows for easy link verification during the installation process. Once both network links are up, the LinkSafe feature will begin to watch each link’s status and propagate any error conditions.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS unit supplied is equipped with built-in GbE UTP port pairs
- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.

5.3.1 Fail Link on One Port of Tap Pair

1. Go to the [System Status](#) page and verify “LinkSafe OK” is in the **Status** column for **Port 1** and **Port 2**. This means LinkSafe is enabled and active for that tap port pair.

Port Status										
Port	Name	Link	Speed	Duplex	Negotiate	MDI	Class	Monitor	Status	Setup
A		Down	---	--	--	--	Monitor		--	Setup
B		Down	---	--	--	--	Monitor		--	Setup
1	IMS-HSS (S6a)-SR1	Up	1G	Full	Auto	Auto	Tap	A B	LinkSafe OK	Setup
2	IMS-HSS (S6a)	Up	1G	Full	Auto	Auto	Tap	A B	LinkSafe OK	Setup

2. Unplug the copper Ethernet cable connected to **Port 2**.
3. Go to the [System Status](#) page and verify link down has been detected on **Port 2** and that **Port 1** has also been forced to a “disabled” state.

Port Status										
Port	Name	Link	Speed	Duplex	Negotiate	MDI	Class	Monitor	Status	Setup
A		Down	---	--	--	--	Monitor		--	Setup
B		Down	---	--	--	--	Monitor		--	Setup
1	IMS-HSS (S6a)-SR1	Down	---	--	Auto	Auto	Tap	A B	Link Disabled	Setup
2	IMS-HSS (S6a)	Down	---	--	Auto	Auto	Tap	A B	Link Failure	Setup

5.3.2 Restore Link

1. Reconnect the copper Ethernet cable to **Port 2**.
2. Go to the **System Status** page and verify restoration was detected on **Port 2** and that **Port 1** has also been returned to “**LinkSafe OK**” state.

6 Standard Feature and Configuration Testing

6.1 Selective Aggregation

Not all aggregation is alike. Static aggregation, like that used in traditional network taps, does not allow users to configure what network traffic is aggregated to each monitor port. With selective aggregation, available in all VSS Monitoring Distributed Traffic Capture devices, users can define how network input ports are directed to each monitor output port, allowing each monitor port an independent, completely selectable view of network inputs.

6.1.1 Selective Aggregation Configuration



The objective for this portion of the test procedure is to demonstrate the flexible nature of selective aggregation.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- The following port configurations are successfully applied:
 - SPAN Ports: Ports 1, 4 (or any other Span ports)
 - Monitor Ports: Port 2, 3, 6, 8 (or any other 4 Monitor ports)
- Traffic generator with 2x GbE port connection to the DTCS SPAN ports (eg. Laptop with any type of packet player)
- Traffic capture tool with 2x GbE port connection to the DTCS monitor ports (eg. Laptop with Wireshark installation)

1. In the VSS web GUI, go to **Monitor Settings**.
2. Check the boxes next to **Ports 1 and 4** in the **Network Port Input** column.
3. Check the box next to **Port 2 and 3** in the **Monitor Port Output** column, with **Load Balancing** selected as **None**:

Filter Expression	Network Port Input	Monitor Port Output	Rank
(Unfiltered)	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 23	<input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 24 Load Balancing: None (output to all selected ports)	 

4. Click **Save Settings**.
5. Connect ports 1 and 4 to the traffic generator.

6. Connect ports 2 and 3 to the traffic capture tool.
7. In the VSS web GUI, go to **Network Activity, All Counters**. Scroll down to the bottom and click on **Clear Counters** to reset the aggregated statistics on all the ports.
8. Start traffic generation.
9. Wait for 10 seconds and stop traffic generation.
10. Verify that the Tx for Port 2 and 3 is the same as the Rx from both Ports 1 and 4.
11. Use Wireshark or other traffic capture tools and repeat Steps 8-9 to verify that the packets received on the monitor ports are not altered.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Transmit traffic into SPAN Ports 1 and 4	Network Activity counters show the correct Rx packet count on ports 1 and 4			
2	Map SPAN Ports 1 and 4 traffic into Monitor Ports 2 and 3	Network Activity counters show the correct Tx packet counts on ports 2 and 3, which is the combined Rx counts from ports 1 and 4			
3	Capture packets transmitted by the Ports 2 and 3	The captured packets from Monitor ports 2 and 3 are not altered			

Overall Result

Test case accepted: ☐, not accepted ☐

6.1.2 Configure and Verify Selective Aggregation

Note: Selective Aggregation testing will be combined with using filters. Please continue to the section 6.2 Filtering.

6.2 Filtering

When aggregating multiple network input ports together it is possible to oversubscribe either the monitor output interface or the processing capacity of the monitor device connected to the interface. Filtering the traffic to a smaller portion of traffic is one way to mitigate this tendency.

The following test procedure will demonstrate how filters of different complexity can be configured and applied.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- The following port configurations are successfully applied:
 - SPAN Ports: Ports 1, 4 (or any other Span ports)
 - Monitor Ports: Port 2, 3, 6, 8 (or any other 4 Monitor ports)
- Traffic generator with 2x GbE port connection to the DTCS SPAN ports (eg. Laptop with any type of packet player).
- Traffic capture tool with 2x GbE port connection to the DTCS monitor ports (eg. Laptop with Wireshark installation)

6.2.1 Quick Filters

In this section a simple filter called HTTP will be created and used to send only HTTP traffic to certain monitor output port while all other packets will be sent to the other monitor output port. Selective aggregation in combination with filtering will be shown to demonstrate a technique for preventing the oversubscription of monitor output ports.

1. In the VSS Web UI, click on the [Filter Library](#) link.
2. Click on **Add new filter** and select the [Quick](#) tab.

The screenshot shows the 'Monitor Filtering' web interface. At the top, there's a header 'Monitor Filtering'. Below it, there's a 'Filter:' section with a '+ Add new filter' button and a 'Filter Name:' text input. To the right are 'Save Filter', 'Delete Filter', and 'Copy Filter' buttons. Below this is a 'Condition:' section. A red box highlights the 'Quick' tab, with 'Detailed' and 'Advanced' tabs also visible. Under the 'Quick' tab, there's a 'Monitor packets to or from:' section with 'MAC/Ethernet Address' and 'or IP Address' input fields, each with a '-or-' separator. Below that is a 'Using protocol(s):' section with radio buttons for 'Any/Igmp', 'ICMP', 'IGMP', 'OSPF', 'RSVP', 'ARP', 'RARP', 'TCP:', 'HTTP', 'HTTPS', 'Telnet', 'SSH', 'RSH', and 'FTP'. The 'Any/Igmp' radio button is selected.

3. Type **HTTP** into the [Filter Name](#): dialog box.
4. Click the **TCP** radio button and [check](#) the box next to **HTTP**.

- Click the **Save Filter** button.

Monitor Filtering

Filter: [+ Add new filter](#)

Filter Name:

[Save Filter](#) [Delete Filter](#) [Copy Filter](#)

Condition:

[Quick](#) [Detailed](#) [Advanced](#)

Monitor packets to or from:

MAC/Ethernet Address -or-

or IP Address -or-

Using protocol(s):

☐ Any/Ignore ☐ ICMP ☐ IGMP ☐ OSPF ☐ RSVP ☐ ARP ☐ RARP

☒ TCP: ☒ HTTP ☐ HTTPS ☐ Telnet ☐ SSH ☐ RSH ☐ FTP

☐ SMTP ☐ POP3 ☐ NNTP ☐ NNTPS ☐ IRC ☐ LDAP

☐ UDP: ☐ SNMP ☐ NTP ☐ DNS ☐ NetBIOS ☐ TFTP ☐ BOOTP/DHCP

- In the VSS Web UI, click on the **Monitor Settings** (Filter Settings depending on model) link.
- Click on the **Delete** button at the end of the default network ports to monitor ports mapping row. A pop-up warning message will appear to confirm deleting the mapping for the filter “(Unfiltered)”.
- Click **OK** and the following screen should appear:

Filtering and Monitor Output Settings

Each row below represents a mapping of Network Port input to Monitor Port output.
To add a new mapping row, click the "+Add" button below.
To remove a mapping row, click the "Delete" button on the desired row.

Filter Expression	Network Port Input	Monitor Port Output
<input type="text"/>	<input type="checkbox"/> Ports 1 and 4	<input type="text"/>

[+Add](#)

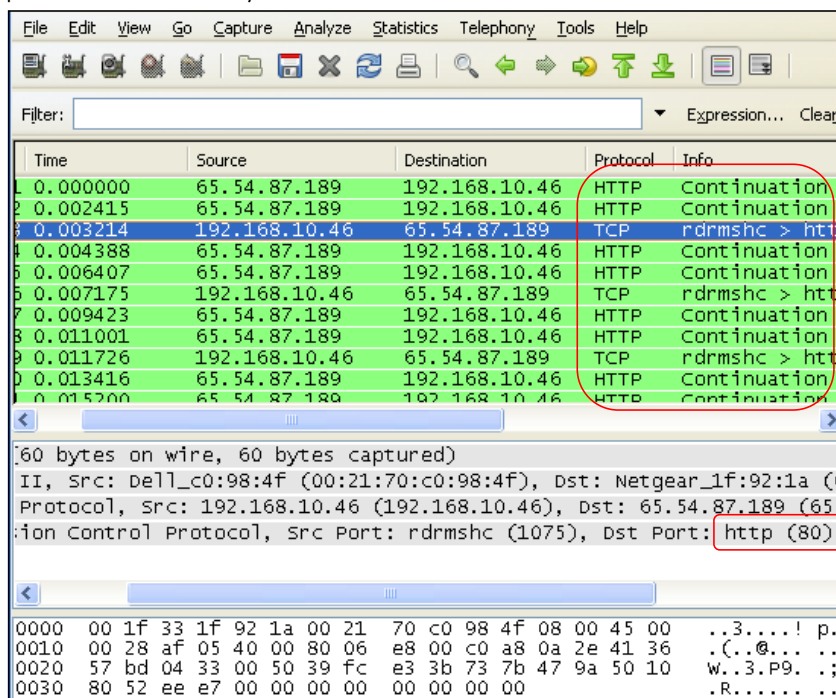
[Save Settings](#)

- Click the **+Add** button.
- Select **HTTP** from the **Filter Expression** pull-down menu.
- Check the boxes next to **Ports 1 and 4** in the **Network Port Input** column.

- Check the box next to **Port 2 and 3** in the **Monitor Port Output** column. You should have something similar to the screenshot below:

Filter Expression	Network Port Input	Monitor Port Output	Rank
http	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 23	<input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 24 Load Balancing: None (output to all selected ports)	<input type="button" value="X"/> <input type="button" value="D"/>

- Click **Save Settings**.
- Connect a network cable from your laptop to Monitor **Port 2**.
- Launch **Wireshark (or analyzer of your choice)** and start a capture in **promiscuous mode**.
- Generate a mix of HTTP and other traffic to ports 1 and 4. Verify that the packets captured on ports 2 and 3 are HTTP only.



Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail

1	Attach Wireshark or probe of your choice to verify only HTTP packets are delivered to monitor output port	Receive only HTTP packets on device connected to the monitor output port on the DT			
---	---	--	--	--	--

Overall Result

Test case accepted: ☐, not accepted ☐

6.2.2 Detailed Filters

In addition to the Quick Filters, the DTCS also supports **Detailed Filters** with the following filtering methods:

- MAC Source Address
- MAC Destination Address
- Ethernet Type
- 802.1q VLAN Tag (ID)
- 802.1p/q VLAN Tag (Priority)
- IP Source Address
- IP Destination Address
- IP Type of Service (TOS) [IPv4] / IP Traffic Class [IPv6]
- IP Protocol
- IP Flow [IPv6 only]
- TCP/UDP Source/Destination
- Byte offset

The following test procedure will demonstrate how a filter can be created to match on only a specific VLAN ID. In the screenshot below, the filter is matching on packets with VLAN ID 32 (0x20)

Monitor Filtering

Filter: SGSN3/4-PGW1/2
SGSN3/4-PGW3/4
VLAN 32
+ Add new filter

Filter Name: VLAN 32

Save Filter
Delete Filter
Copy Filter

Condition: ~~VLAN~~ 32

Quick Detailed Advanced

MAC Destination -or- -and-
MAC Source -or- -and-
EType Shortcuts -and-
802.1q Tag VLAN ID 32 -and-
802.1p/q Tag Priority -and-
IP Destination -or- -and-
IP Source -or- -and-
IP Type of Service (TOS) [IPv4] / Traffic Class [IPv6] -and-

The test procedure is similar to 6.2.1 Quick Filters, with the difference in the filter configuration described below:

1. In the VSS web UI, click on **Filter library**.
2. Click **Add New Filter** from the filter scroll list and select **Detailed** tab.

Monitor Filtering

Filter: HTTP
+ Add new filter

Filter Name:

Save Filter
Delete Filter
Copy Filter

Condition:

Quick Detailed Advanced

Warning: If your existing filter expression contains OR relationals, or complex parenthetical expressions, then this fill-in-the-blanks tab should not be used.

3. In the 802.1q Tag VLAN ID field, enter 32 to configure the VLAN ID value to filter on.

Detailed Advanced

If your existing filter expression contains OR relationals, or complex par

MAC Destination

MAC Source

EType

802.1q Tag VLAN ID 32

802.1p/q Tag Priority

- Click on the **Condition** text box, the filter string **VLAN 32** should be automatically generated.
- Click **Save Filter** to save the filter. This filter can now be used in **Monitor Settings** as shown below:

VLAN 32

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Load Balancing: None (output to all selected ports)

Add new mapping

In the setup depicted in the screenshot, all traffic coming into ports 1 and 2 (Tap or SPAN) with VLAN tag 32 traffic will be send to ports 16 and 17 (Monitor).

- To verify that the packets are filtered correctly, connect ports 1 and 2 (or the selected Tap or SPAN ports) to a traffic generator sending traffic containing packets with VLAN ID 32 and other packets without VLAN ID 32; Connect ports 16 and 17 (or the selected Monitor ports) to a traffic capture tool and verify that the captured packets are only packets with VLAN ID 32.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Attach Wireshark or probe of your choice to verify that only packets that match the VLAN ID in the filter are delivered to monitor output port.	Receive only filtered VLAN ID packets on device connected to the monitor output port			

Overall Result

Test case accepted: ☐, not accepted

6.2.3 Advanced Filters

This section describes the custom offset filtering capabilities of the VSS devices. Offset filters are used when you need to filter by looking into the packet for specific sequence of bytes at specific offsets.

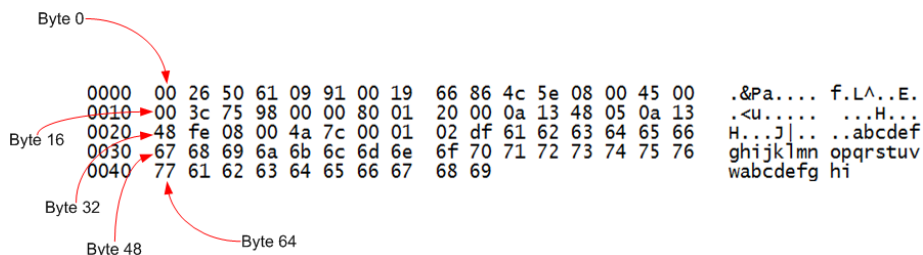
To aid creation of a custom offset filter, Wireshark is often used as a reference tool to locate the exact byte (or bytes) offset to be filtered on. As an example, consider the following ICMP Echo Request Packet:

0000	00	26	50	61	09	91	00	19	66	86	4c	5e	08	00	45	00	.&Pa.... f.L^..E.
0010	00	3c	75	98	00	00	80	01	20	00	0a	13	48	05	0a	13	.<u..... ..H...
0020	48	fe	08	00	4a	7c	00	01	02	df	61	62	63	64	65	66	H...Jabcdef
0030	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	ghijklmn opqrstuv
0040	77	61	62	63	64	65	66	67	68	69							wabcdefg hi

The values in the first column denote the byte numbers of the first bytes on that line:

- On the first line, '0000' represents the 1st byte in the packet, 0x00.
- On the second line, '0010' represents the 16th byte in the packet, 0x00.
- On the third line, '0020' represents the 32nd byte in the packet, 0x48.
- On the fourth line, '0030' represents the 48th byte in the packet, 0x67.
- On the fifth line, '0040' represents the 64th byte in the packet, 0x77.

The following diagram shows the byte number and the actual values corresponding to that number:



A useful tip when calculating the location of a byte value that you wish to filter using Offset Filters is to count from the start of line in question to the location of the byte you wish to filter on. Locating this byte can be accelerated by also using Wireshark to highlight the element of the protocol in question. For example, let's say that we wanted to filter packets which are ICMP Echo Requests. We would first expand the ICMP layer of the packet and then highlight the line 'Type: 8 (Echo (ping) request)' like so:

```

Frame 349 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Asiarock_86:4c:5e (00:19:66:86:4c:5e), Dst: 2wire_61:09:91 (00:26:50:61:09:91)
Internet Protocol, Src: 10.19.72.5 (10.19.72.5), Dst: 10.19.72.254 (10.19.72.254)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x4a7c [correct]
Identifier: 0x0001
Sequence number: 735 (0x02df)
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
[Length: 32]
0000  00 26 50 61 09 91 00 19 66 86 4c 5e 08 00 45 00  .&Pa.... f.L^..E.
0010  00 3c 75 98 00 00 80 01 20 00 0a 13 48 05 0a 13  .<u..... ..H...
0020  48 fe 08 00 4a 7c 00 01 02 df 61 62 63 64 65 66  H.].]... ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69  wabcdefg hi

```

Byte 34

Byte 32

From the above example, we can see the Wireshark conveniently highlights the byte value in question. We then see that this is on the 3rd line, and know that the 1st byte on this line ('48') is the 32nd byte in the packet. We can count along the line to the byte we wish to filter (in this case '08') and can see that this is at offset 34.

Now we have located our byte value, we can then use the following syntax in our filter:

```
offset 34 08
```

Whilst this is useful, it is important to remember that the flexibility of the VSS Filtering technology allow us to create logical expressions to define precisely the packets we want to filter. As I am sure you can appreciate, there may be other packets that contain the byte value '08' at offset 34. In this way will not receive ICMP Echo Request packets if we use the Offset Filter on its own. To get exactly what we want, we can then use the Offset Filter expression in a larger more complex expression. In our example, it would make more sense to say 'if the packet has a pattern of 08 at offset 34 **and** the IP Protocol is ICMP' we could use the below expression:

```
IP Protocol 1 and offset 34 08
```

The power of VSS' Filter technology doesn't end here, we can also be even more specific and use the source or destination IP's, the MAC Addresses and even add in additional Offset Filters. The easiest way to achieve this is to build the filter with the pre-sets within the GUI if you don't want to write the expression out directly. So, using the above example, we can firstly select the ICMP protocol from within the GUI like so:

Monitor Filtering		
Filter:	<div>+ Add new filter</div>	<div>Filter Name:</div> <div>ICMP_Echo</div> <div>Save Filter</div> <div>Delete Filter</div> <div>Copy Filter</div>
Condition:	IP Protocol 1	
<div>Quick Detailed Advanced</div> <div>Monitor packets to or from:</div> <div>MAC/Ethernet Address -or- </div> <div>or IP Address -or- </div> <div>Using protocol(s):</div> <div> <input type="radio"/> Any/Ignore <input checked="" type="radio"/> ICMP <input type="radio"/> IGMP <input type="radio"/> OSPF <input type="radio"/> RSVP <input type="radio"/> ARP <input type="radio"/> RARP </div> <div> <input type="radio"/> TCP: <input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> Telnet <input type="checkbox"/> SSH <input type="checkbox"/> RSH <input type="checkbox"/> FTP </div> <div> <input type="checkbox"/> SMTP <input type="checkbox"/> POP3 <input type="checkbox"/> NNTP <input type="checkbox"/> NNTPS <input type="checkbox"/> IRC <input type="checkbox"/> LDAP </div> <div> <input type="radio"/> UDP: <input type="checkbox"/> SNMP <input type="checkbox"/> NTP <input type="checkbox"/> DNS <input type="checkbox"/> NetBIOS <input type="checkbox"/> TFTP <input type="checkbox"/> BOOTP/DHCP </div>		

You will see from the above that I have given the filter a name: 'ICMP_Echo'. I have also clicked the radio button 'ICMP' and by doing so this has automatically entered the syntax for the *Condition* (i.e. the expression). I can then expand upon this by manually entering my Offset Filter using the 'and' keyword:

Monitor Filtering		
Filter:	<div>ICMP_Echo</div> <div>+ Add new filter</div>	<div>Filter Name:</div> <div>ICMP_Echo</div> <div>Save Filter</div> <div>Delete Filter</div> <div>Copy Filter</div>
Condition:	IP Protocol 1 and offset 34 08	
<div>Quick Detailed Advanced</div> <div>Monitor packets to or from:</div> <div>MAC/Ethernet Address -or- </div> <div>or IP Address -or- </div> <div>Using protocol(s):</div> <div> <input type="radio"/> Any/Ignore <input checked="" type="radio"/> ICMP <input type="radio"/> IGMP <input type="radio"/> OSPF <input type="radio"/> RSVP <input type="radio"/> ARP <input type="radio"/> RARP </div> <div> <input type="radio"/> TCP: <input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> Telnet <input type="checkbox"/> SSH <input type="checkbox"/> RSH <input type="checkbox"/> FTP </div> <div> <input type="checkbox"/> SMTP <input type="checkbox"/> POP3 <input type="checkbox"/> NNTP <input type="checkbox"/> NNTPS <input type="checkbox"/> IRC <input type="checkbox"/> LDAP </div> <div> <input type="radio"/> UDP: <input type="checkbox"/> SNMP <input type="checkbox"/> NTP <input type="checkbox"/> DNS <input type="checkbox"/> NetBIOS <input type="checkbox"/> TFTP <input type="checkbox"/> BOOTP/DHCP </div>		

This is now ready for me to apply to the Monitor Settings within the GUI to filter out 'Ping Echo Request' packets.

If however we wanted to filter the 'Ping Echo Response' packets as well we could use a filter expression which contains an Offset Filter for the response code. In this instance, we would use the **or** keyword along with our Offset Filter. Firstly, we calculate the Offset Filter expression to use for the 'Echo Ping Reply':

```

Frame 350 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 2wire_61:09:91 (00:26:50:61:09:91), Dst: Asiarock_86:4c:5e (00:19:66:86:4c:5e)
Internet Protocol, Src: 10.19.72.254 (10.19.72.254), Dst: 10.19.72.5 (10.19.72.5)
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0 ()
  Checksum: 0x527c [correct]
  Identifier: 0x0001
  Sequence number: 735 (0x02df)
Data (32 bytes)
  Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
  [Length: 32]
0000  00 19 66 86 4c 5e 00 26 50 61 09 91 08 00 45 00  ..f.L^.& Pa...E.
0010  00 3c 67 17 40 00 ff 01 6f 80 0a 13 48 fe 0a 13  .<g.@... o...H...
0020  48 05 00 00 52 7c 00 01 02 df 61 62 63 64 65 66  H.R|... .abcdef
0030  68 63 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi

```

Byte 34

Byte 32

Again, we can see that the byte value we want (after highlighting the line 'Type: 0 (Echo (ping) reply)' in the ICMP Layer of the packet) is actually at the same position: offset 34. This time however, the value for this byte is '00'. So the Offset Filter that we would use would be:

```
offset 34 00
```

Now we can combine this into our Condition in the GUI like so:

The image shows the 'Monitor Filtering' window in Wireshark. The 'Filter' field contains 'ICMP_Echo-Reply' with a '+ Add new filter' button. The 'Filter Name' field also contains 'ICMP_Echo-Reply'. There are buttons for 'Save Filter', 'Delete Filter', and 'Copy Filter'. The 'Condition' field contains the expression 'IP Protocol 1 and (offset 34 08 or offset 34 00)'.

You'll notice that in this expression I have used the **or** keyword and that I have wrapped the two Offset Filters in parenthesis; this is because expressions are evaluated from left to right, so we really want the result of the Offset Filters to be calculated first and then for the IP Protocol filter to be evaluated separately.

This filter can now be applied to our Monitor Settings so we can now filter exactly the information we wish to collect.

This is of course a very simple example but should be enough to get you started on creating more complex (and useful!) filters.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Understanding and creating custom offset filters	Successfully created a custom offset filter based on the information in this section			

Overall Result

Test case accepted: ☐, not accepted

6.3 Load Balancing

The load balancing feature, available on all DTCS models, distributes traffic across multiple monitor ports, effectively summing the bandwidth of the load balanced ports; output from the load balanced group is designed to maintain packet order within any given conversation, as well as guarantee a consistent output port for any single conversation. This ensures that the monitoring tool will see every packet of a given conversation. To obtain as close to even distribution of traffic as possible, the number of ports in a monitor group must be 2, 4, or 8.

Prior to the DTCS firmware v2.2M, load balancing is achieved by selecting multiple monitor ports in a given port map. In release v2.2M, the concept of a "Load Balancing Group" is introduced. A load balancing group includes one or multiple monitor ports, just like before, but also supports the failover mitigation in events where one or more monitor tools participating in the same load balancing group becomes unavailable.

The test procedure described below will demonstrate the configuration and the capabilities of the load balancing group.

Assumptions:

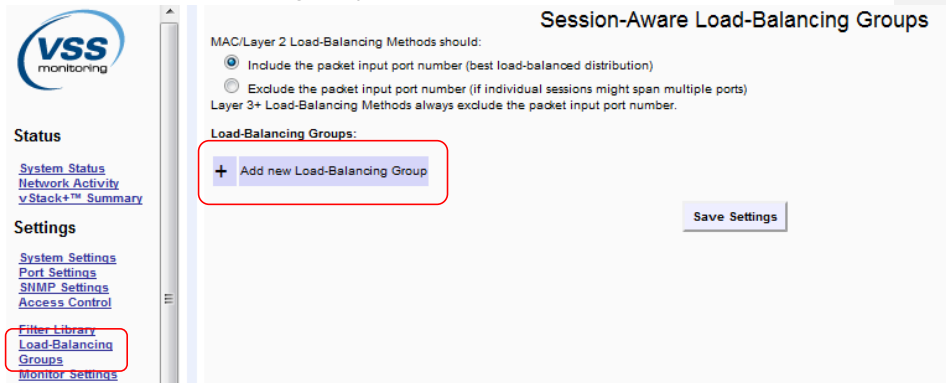
Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- The following port configurations are successfully applied:
 - SPAN Ports: Ports 1, 4 (or any other Span ports)
 - Monitor Ports: Port 2, 3, 6, 8 (or any other 4 Monitor ports)
- Traffic generator with 2x GbE port connection to the DTCS SPAN ports (eg. Laptop with any type of packet player).

- Traffic capture tool with 2x GbE port connection to the DTCS monitor ports (eg. Laptop with Wireshark installation)

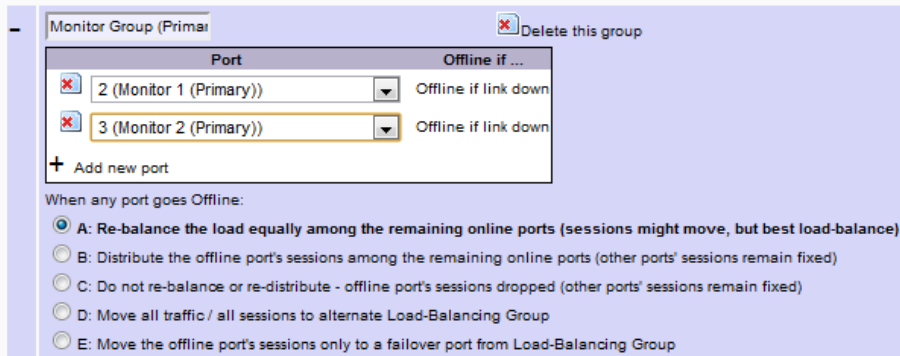
6.3.1 Load Balancing Groups

1. In the VSS web UI, go to **Load-Balancing Groups**.
2. Click on **Add new Load-Balancing Group**.



3. Enter the load balancing group name **Monitor Group (Primary)**.
4. Click on **Add new port** and select ports 2 and 3

Load-Balancing Groups:



5. Click **Save Settings** to save this load balancing group.
6. Go to **Monitor Settings**. Delete all the previously saved port mappings and click **Save Settings**.
7. Click **Add a new mapping** and select ports 1 and 4 as Network Port Input.
8. From the **Load Balancing Type** drop-down menu, select **IP Dest+Source, & TCP/UDP Dest+Source**.
9. From the **Load-Balancing Group** drop-down menu, select the load balancing group **Monitor Group (Primary)**.
10. Click **Save Settings** to save the port mapping.

11. From ports 1 and 4, generate traffic with varying IP source/destination addresses, as well as a varying TCP/UDP source/destination ports if possible.
12. From the VSS web GUI, go to **Network Activity, All Counters**, and click **Clear Counters** at the bottom of the page.
13. Start transmitting traffic to ports 1 and 4. Verify that the traffic coming into ports 1 and 4 are distributed between ports 2 and 3 in the load balancing group **Monitor Group (Primary)**.

Note: The distribution of traffic to the monitor ports depends heavily on the type of traffic injected. The more variation on the selected load balancing criteria, the more even the distribution will be. For example, if the injected traffic is always from the same source, going to the same destination, and the load balancing criteria depends on the source and destination, all the traffic will go to only 1 monitor port as they are considered to be in the same “session”. If in the same scenario, there are traffic from 10 different sources to 10 different destinations, then the distribution of traffic between monitor ports will be more even, because there are 10 unique “sessions” being distributed.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Add new load balancing group with multiple monitoring ports	Load balancing group is saved and can be selected when the Load Balancing Type is not “None”			
2	Send traffic from the SPAN ports to the load balancing group	Traffic from the SPAN ports are distributed between the monitor ports in the load balancing group, based on the Load Balancing Type selected			

Overall Result

Test case accepted: ☐, not accepted

6.3.2 Load Balancing In a Failover Scenario

14. Continue from section 6.3.1 Load Balancing Groups, go to **Load-Balancing Groups** and click on **Add new Load-Balancing Group**.
15. Enter group name as **Monitor Group (Secondary)**.

16. Add secondary monitor ports 6 and 8.

Monitor Group (Secondary) ✖ Delete this group

Port	Offline if ...
6 (Monitor 1 (Secondary))	Offline if link down
8 (Monitor 2 (Secondary))	Offline if link down

+ Add new port

When any port goes Offline:

- ☒ A: Re-balance the load equally among the remaining online ports (sessions might move, but best load-balance)
- ☐ B: Distribute the offline port's sessions among the remaining online ports (other ports' sessions remain fixed)
- ☐ C: Do not re-balance or re-distribute - offline port's sessions dropped (other ports' sessions remain fixed)
- ☐ D: Move all traffic / all sessions to alternate Load-Balancing Group
- ☐ E: Move the offline port's sessions only to a failover port from Load-Balancing Group

17. For **Monitor Group (Primary)**, change the **When any ports goes Offline:** selection from the default option A: Re-balance the load equally among the remaining ports to **D: Move all traffic / all session to alternate Load-Balancing Group**, and select **Monitor Group (Secondary)**.

Monitor Group (Primary) ✖ Delete this group

Port	Offline if ...
2 (Monitor 1 (Primary))	Offline if link down
3 (Monitor 2 (Primary))	Offline if link down

+ Add new port

When any port goes Offline:

- ☐ A: Re-balance the load equally among the remaining online ports (sessions might move, but best load-balance)
- ☐ B: Distribute the offline port's sessions among the remaining online ports (other ports' sessions remain fixed)
- ☐ C: Do not re-balance or re-distribute - offline port's sessions dropped (other ports' sessions remain fixed)
- ☒ D: Move all traffic / all sessions to alternate Load-Balancing Group: Monitor Group (Secondary)
- ☐ E: Move the offline port's sessions only to a failover port from Load-Balancing Group

Monitor Group (Secondary) ✖ Delete this group

18. Click **Save Settings** at the bottom of the page to apply the change.
19. Go to **Network Activity, All Counters** and click on **Clear Counters**.
20. Start traffic on ports 1 and 4. The traffic from ports 1 and 4 should be distributed between ports 2 and 3 from **Monitor Group (Primary)** as observed in section 6.3.1 Load Balancing Groups.
21. Remove the cable between port 2 and the traffic capture/monitoring tool connected to it. This will result in an offline port in **Monitor Group (Primary)** and trigger the DTCS to take action **D: Move all traffic / all session to alternate Load-Balancing Group: Monitor Group (Secondary)**.
22. From **Network Activity**, verify that the traffic originally going to ports 2 and 3 are distributed between ports 6 and 8.

Note: The same procedure can be used for additional network tap/SPAN ports and monitor ports as necessary in the test environment.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Add a second load balancing group with multiple monitoring ports	Second load balancing group is saved and can be selected when the Load Balancing Type is not "None"			
2	Send traffic from the SPAN ports to the primary load balancing group	Traffic from the SPAN ports are distributed between the monitor ports in the primary load balancing group, based on the Load Balancing Type selected			
3	Trigger an offline port condition in the primary load balancing group while traffic is running	Traffic from the primary load balancing group is redistributed to the secondary load balancing group			

Overall Result

Test case accepted: ☐, not accepted

6.4 VLAN Tagging

The VLAN tagging feature adds a VLAN tag to each packet, prior to forwarding out the monitor ports. This feature also doubles as a port stamping mechanism. In the default configuration, the VLAN tag value corresponds to the port number. For example, traffic coming from network input port 6 will have VLAN tag 6 inserted. User can also optionally define the starting VLAN tag value for the monitor ports when vStack is not in use.

The following test procedure is not a continuation of the previous test cases.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS unit can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- The following port configurations are successfully applied:
 - SPAN Ports: Ports 1, 4 (or any other Span ports)
 - Monitor Ports: Port 2 (or any other Monitor ports)
- vStack is not in use for the DTCS unit.
- Traffic generator with 2x GbE port connections to the DTCS SPAN ports (eg. Laptop with any type of packet player).
- Traffic capture tool with a GbE port connection to the DTCS monitor ports (eg. Laptop with Wireshark installation)

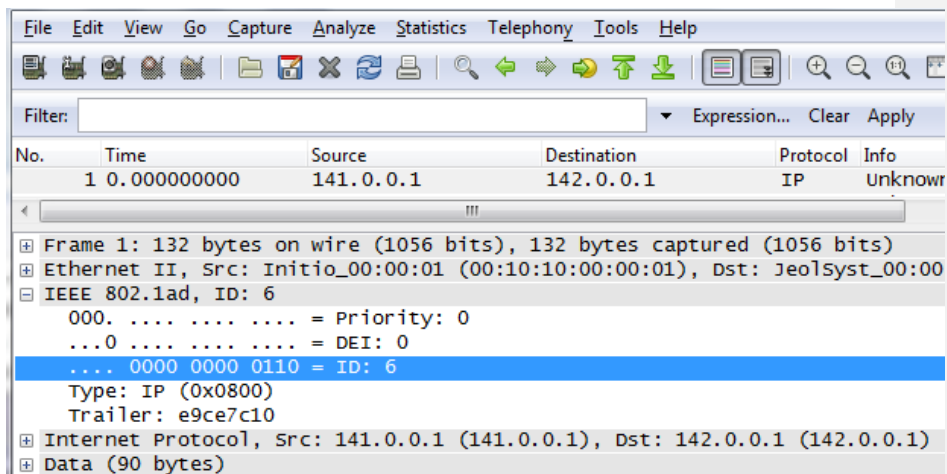
1. In the VSS web UI, go to **Port Settings**.
2. Click on port 2 and select **Insert Network Port Number VLAN tags in Monitor Port output**.

Port 2 Settings	
Port Name:	Monitor 2
Auto Negotiate:	<input checked="" type="checkbox"/> On
Auto Negotiation Advertisements	
<input checked="" type="checkbox"/> 10H	<input checked="" type="checkbox"/> 100H
<input checked="" type="checkbox"/> 10F	<input checked="" type="checkbox"/> 100F
<input checked="" type="checkbox"/> 1000H	<input checked="" type="checkbox"/> 1000F
<input checked="" type="checkbox"/> Symmetric Pause	<input checked="" type="checkbox"/> Asymmetric Pause
Link state:	<input checked="" type="radio"/> Auto (normal) <input type="radio"/> Force down
Type:	10Base-T/100Base-TX/1000Base-T RJ45
Class:	<input type="radio"/> Tap <input type="radio"/> Span <input checked="" type="radio"/> Monitor <input type="radio"/> vStack+
Monitor Port VLAN Tagging:	
<input checked="" type="checkbox"/> Insert Network Port number VLAN tags in Monitor Port output	
Save Changes	

3. Click on **Save Changes** to apply the changes.
4. [Optional] Go to **System Settings** and change **Starting VID** to **6**. Click **Submit** to apply the change. This means that instead of inserting VLAN tag 1 for network input port 1, VLAN tag 6 will be used for port 1, and VLAN tag 9 for port 4.

Monitor Port VLAN Tagging	
TPID (E-type):	88A8
Starting VID:	5
VLAN ID = Starting VLAN ID + network port number	

5. Generate traffic for ports 1 and 4.
6. Launch Wireshark on the system connected to port 2 and start a packet capture in promiscuous mode.
7. Wait for packets to arrive and stop capture. Check that the VLAN tags are inserted correctly for the traffic from ports 1 and 4. If Step 4 was skipped, the VLAN tag for traffic from port 1 is 1, and from port 4 is 4. If Step 4 was executed, the VLAN tag for traffic from port 1 is 6, from port 4 is 9.



Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Add a second load balancing group with multiple monitoring ports	Second load balancing group is saved and can be selected when the Load Balancing Type is not "None"			
2	Send traffic from the SPAN ports to the primary load balancing group	Traffic from the SPAN ports are distributed between the monitor ports in the primary load balancing group, based on the Load Balancing Type selected			
3	Trigger an offline port condition in the primary load balancing group while traffic is running	Traffic from the primary load balancing group is redistributed to the secondary load balancing group			

Overall Result

Test case accepted: ☐, not accepted

7 Advanced Feature Configuration and Testing

7.1 Port Stamping

The port stamping feature on an input port adds a single byte at the end of the data payload of each packet (immediately before the CRC) to indicate the input port of the device from which the packet originated. Once the port stamp is added to the packet, it is passed on to the destination port or ports as a standard Ethernet packet. Only monitor ports on the device will see port stamped packets. Port stamping is very useful in differentiating what would otherwise be duplicate packets giving visibility back to where a particular packet was captured within the DTCS.

The test procedure below demonstrates how the additional port stamp information is inserted to the packets sent to the monitor ports, and how this information can be located in the captured packets.

This test is not a continuation of any previous test cases.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- A DTCS Advanced or Expert model with tap ports is used.
- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- The following port configurations are successfully applied:
 - a. Tap Port Pairs: Ports 1/2, 3/4 (or any other tap ports)
 - b. Monitor Ports: Ports 10, 12 (or any other monitor ports)
- Ports 1 and 3 are connected to a traffic generator (eg. A laptop).
- Ports 10 and 12 are connected to traffic capture tools (eg. Wireshark).
- The selected tap port has Port Stamping option activated.

8. In the VSS web UI, click on the [Port Settings](#) link and select [Port 1](#).

9. Select the **Enable** radio button next to **Monitor output port stamping**.

The screenshot shows the 'Port 1 Settings' window. The 'Monitor output port stamping' option is highlighted with a red rectangle, indicating it is the setting to be modified. The 'Enabled' radio button is selected for this option.

Port 1 Settings	
Port Name:	IMS-HSS (S6a)-SR1
Auto Negotiate:	<input checked="" type="checkbox"/> On
Auto Negotiation Advertisements	
<input checked="" type="checkbox"/> 10H	<input checked="" type="checkbox"/> 100H
<input checked="" type="checkbox"/> 10F	<input checked="" type="checkbox"/> 100F
<input checked="" type="checkbox"/> 1000H	<input checked="" type="checkbox"/> 1000F
<input checked="" type="checkbox"/> Symmetric Pause	<input checked="" type="checkbox"/> Asymmetric Pause
Link state:	<input checked="" type="radio"/> Auto (normal) <input type="radio"/> Force down
Type:	10Base-T/100Base-TX/1000Base-T RJ45
Class:	<input checked="" type="radio"/> Tap <input type="radio"/> Span <input type="radio"/> Monitor <input type="radio"/> vStack
Linksafe:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Monitor output timestamping:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Monitor output port stamping:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
vAssure Fast Failover:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input type="button" value="Save Changes"/>	

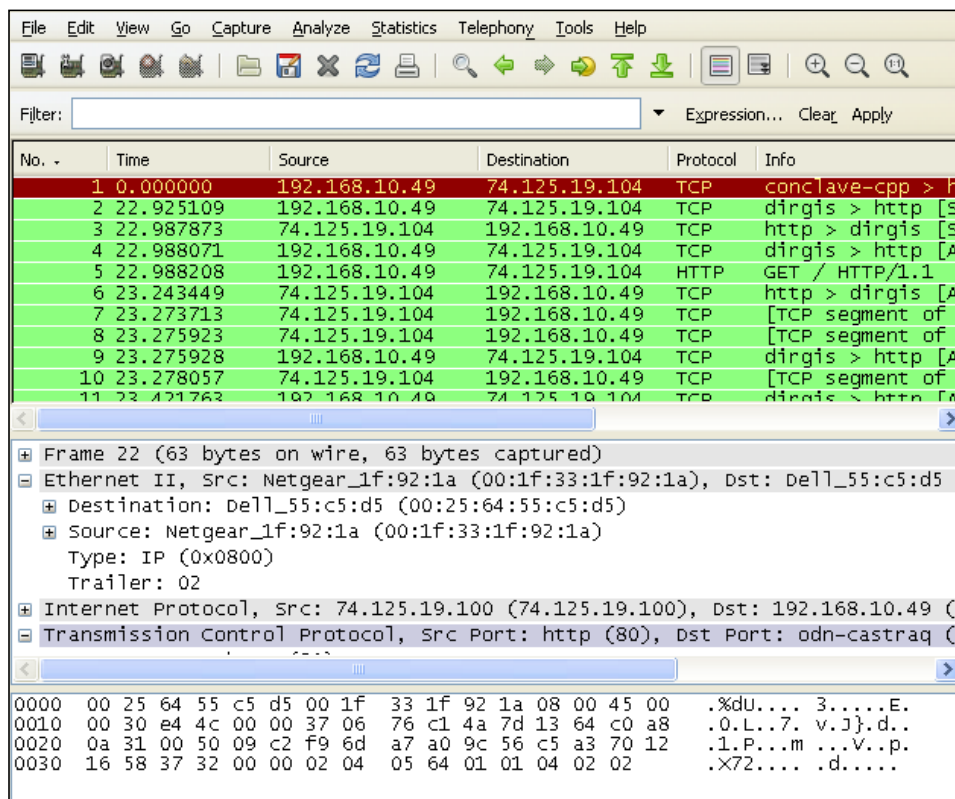
10. Click on the next port, port **2** to apply the configuration on port 1.
11. Repeat the Steps 9 to apply port stamping setting for all the tap ports 2, 3 and 4.
12. Click the **Save Changes** to apply the changes.
13. Go to **Monitor Settings** and add 2 port maps to have traffic from tap port pairs 1/2 and 3/4 going to monitor ports 10 and 12, respectively.
14. To verify that the port stamps are correctly inserted, generate traffic on the link tapped by **Port 1 and 2**.
15. Launch **Wireshark** on the system connected to **Port 10** and start a packet capture in promiscuous mode.
16. Wait for packets to arrive and stop capture. Check that the last byte before the CRC (Ethernet FCS) corresponds to the port number of the tap port.
17. Repeat Steps 14-16 for tap port pair 3/4 to monitor port 12 to verify that a different port stamp is applied when the traffic is tapped from a different physical port.

Note: Port numbering starts with "0" on the first physical port on the tap and counts up from there. Therefore the first UTP port on a v2x16 will be stamped with "2".

For v2x16, Port A has port number 0x00, and will insert port stamp 0x00 if Port Stamping is enabled on this port. Similarly, Port B will insert port stamp 0x01, while Port 1 will insert port stamp 0x02, and so on.

For v4x24, Ports A through D have port numbers 0x00 through 0x03. Port 1 will insert port stamp 0x04.

For v24, Port 1 has port number 0x00, Port 2 0x01, and so on.



Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Enable and save port stamping on the port	Port stamping configuration is saved			
2	Send traffic from the tap ports with port stamping enabled	Traffic received on the monitor port contains the port number in the last byte before CRC			

Overall Result

Test case accepted: ☐, not accepted

7.2 Time Stamping

The Time stamping feature on an input network port basis, adds an 8 byte time stamp to the end of the data payload of each packet. The CRC is recalculated, preserving packet integrity. Once the time stamp is added to the packet, it is passed on to the destination port or ports as a standard Ethernet packet. Time Stamping provides, on an input network port basis, the addition of an 8-byte time stamp to the end of the data payload of each packet. The first four bytes provides a seconds count, reference to Unix Epoch time (1st January 1970), while the second four bytes consists of 30-bits for the sub-second value that is a count of 20ns increments, and a 2-bit value that identifies the clock source. These two groups of bytes are effectively separated by a decimal point. The time stamp is created as the first bit enters the input network port. Time Stamping never alters loop-through traffic on the tap. If port stamping and time stamping are used on the same port at the same time, the 8 byte time stamp will precede the single byte port stamp, followed by the packet's 4 byte CRC.

This test is a continuation of 7.1 Port Stamping.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- A DTCS Advanced or Expert model with tap ports is used.
- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- The following port configurations are successfully applied:
 - a. Tap Port Pairs: Ports 1/2 (or any other tap ports)
 - b. Monitor Ports: Ports 10 (or any other monitor ports)
- 18. Port 1 is connected to a traffic generator (eg. A laptop).
- 19. Ports 10 is connected to traffic capture tools (eg. Wireshark).
- The selected tap ports have Time Stamping option activated.

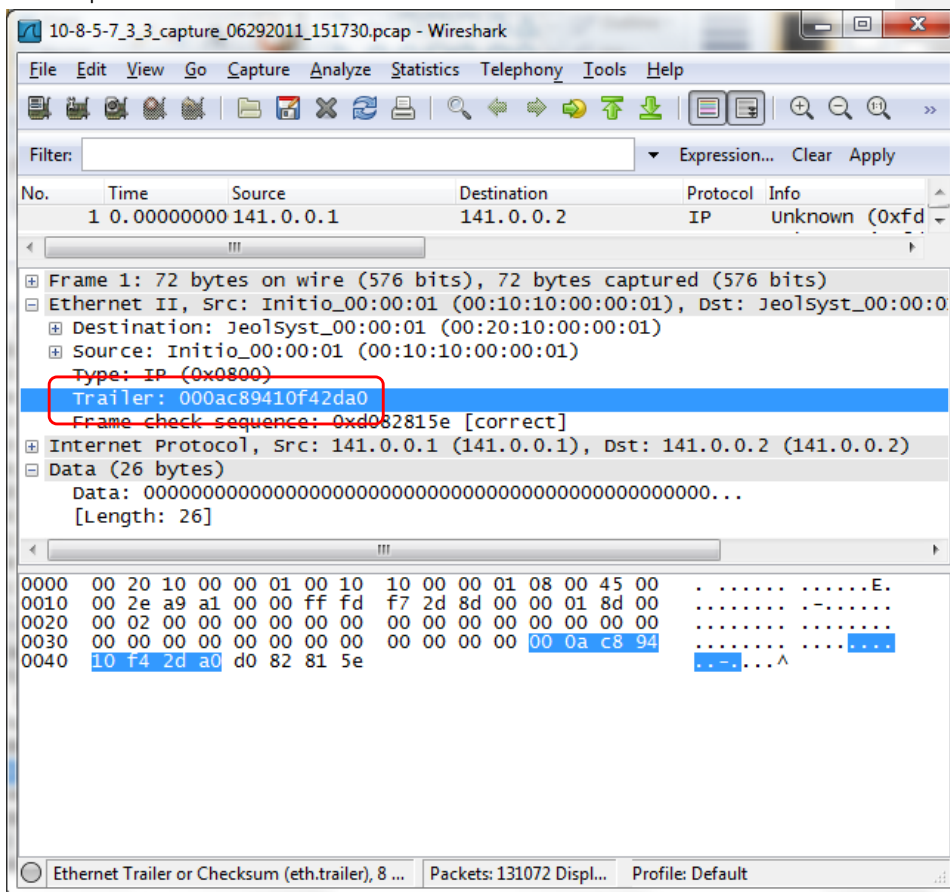
1. In the VSS web UI, click on the [Port Settings](#) link and select **Port 1**.
2. Select the **Enable** radio button next to **Monitor output time stamping**.

3. Select the **Disable** radio button next to **Monitor output port stamping**.

Port 1 Settings	
Port Name:	IMS-HSS (S6a)-SR1
Type:	10Base-T/100Base-TX/1000Base-T RJ45
Auto Negotiate:	<input checked="" type="checkbox"/> On
Class:	<input checked="" type="radio"/> Tap <input type="radio"/> Span <input type="radio"/> Monitor <input type="radio"/> vStack+
Auto Negotiation Advertisements	<input checked="" type="checkbox"/> 10H <input checked="" type="checkbox"/> 100H <input checked="" type="checkbox"/> 1000H <input checked="" type="checkbox"/> Symmetric Pause <input checked="" type="checkbox"/> 10F <input checked="" type="checkbox"/> 100F <input checked="" type="checkbox"/> 1000F <input checked="" type="checkbox"/> Asymmetric Pause
Link state:	<input checked="" type="radio"/> Auto (normal) <input type="radio"/> Force down
Linksafe:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Monitor output timestamping:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Monitor output portstamping:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
vAssure Fast Failover:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input type="button" value="Save Changes"/>	

4. Click on the next port, port **2** to apply the configuration on port 1.
5. Click the **Save Changes** to apply the changes.
6. To verify that the time stamps are correctly inserted, generate traffic on the link tapped by **Port 1 and 2**.
7. Launch **Wireshark** on the system connected to **Port 10** and start a packet capture in promiscuous mode.

8. Wait for packets to arrive and stop capture. Check that the last 8 bytes correspond to the timestamp.



9. To interpret the timestamp, note the last 8 bytes. In the screenshot above, “00 0a c8 94 10 f4 2d a0” is the timestamp; 0x000ac894 = 706708 seconds since Epoch time; in the second 4 bytes, 0x10f42da0, the upper 2 bit 0b00 indicates that the clock source is internal (0b01 = NTP, 0b10 = GPS, 0b11 = PTP), and the lower 30 bits indicates $284437920 * 20\text{ns} = 5688758400\text{ns} \approx 5.689\text{ seconds}$. The resultant value is approximately 706713.689 seconds.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Enable and save time stamping on the port	Time stamping configuration is saved			

2	Send traffic from the tap ports with time stamping enabled	Traffic received on the monitor port contains the time number in the last byte before CRC			
---	--	---	--	--	--

Overall Result

Test case accepted: ☐, not accepted

7.3 MPLS Label Stripping

MPLS tag stripping removes MPLS labels from the traffic being sent to the monitoring ports. When enabled, all the MPLS packets coming through the enabled port will have their MPLS headers removed, and by default, the E-Type of these packets will be substituted by IPv4 type 0x0800. User can also specify MPLS label that can be searched for and optionally define what E-Type is used in the stripped packet (IPv4 is the default) and what MAC address to be substituted in the stripped packet (the actual MPLS source MAC address is the default).

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- A DTCS Advanced or Expert model with tap ports is used.
- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- The following port configurations are successfully applied:
 - a. Tap Port Pairs: Ports 5A/5B (or any other tap ports)
 - b. Monitor Ports: Ports 2A (or any other monitor ports)
- 20. The following monitor mapping is successfully applied:
 - a. Unfiltered, Network Port Input 5A → Monitor Port Output 2A
- 21. Port 5A is connected to a traffic generator (eg. A laptop).
- 22. Ports 2A is connected to traffic capture tools (eg. Wireshark).
- The selected tap ports have MPLS Stripping option activated

1. In VSS web UI, go to **MPLS Stripping**.

- | Network Ports | | MPLS Label Action | | |
|----------------------|---|-------------------------------------|----------------------|--|
| Label | E-Type | MAC Source (click checkbox to edit) | | |
| <input type="text"/> | 0000 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | <input type="text"/> | |
| <input type="text"/> | 0000 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | <input type="text"/> | |
| <input type="text"/> | 0000 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | <input type="text"/> | |
| <input type="text"/> | 0000 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | <input type="text"/> | |
| <input type="text"/> | 0000 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | <input type="text"/> | |
| <input type="text"/> | 0000 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | <input type="text"/> | |
| <input type="text"/> | 0000 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | <input type="text"/> | |
| <input type="text"/> | 0000 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | <input type="text"/> | |
| Non-specific | 0000 <input type="text" value="IPv4"/> | <input type="checkbox"/> | <input type="text"/> | |

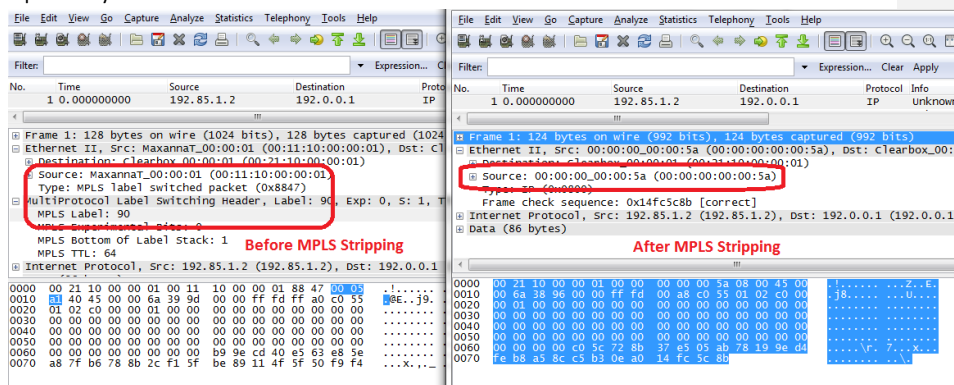
☒ 5A
 ☐ 5B
 ☐ 6A
 ☐ 6B

MPLS Network Link 1 (A)

-
- The image displays two side-by-side Wireshark packet capture windows. The left window, titled 'Before MPLS Stripping', shows a packet list with 11 packets. The selected packet (No. 1) is expanded, showing the 'MPLS Label Stack' with 1 label (Router Alert). The packet details pane shows the 'MPLS Label Stack' with 1 label (Router Alert) and 'MPLS TTL: 64'. The packet bytes pane shows the 'Data (86 bytes)'. The right window, titled 'After MPLS Stripping', shows the same packet list. The selected packet (No. 1) is expanded, showing the 'Ethernet II' and 'Internet Protocol' layers. The packet details pane shows the 'Ethernet II' layer with 'Type: Clearbox (0x00)' and the 'Internet Protocol' layer with 'Source: 192.85.1.2 (192.85.1.2), Destination: 192.0.0.1 (192.0.0.1)'. The packet bytes pane shows the 'Data (86 bytes)'. Red circles highlight the 'MPLS Label Stack' in the left window and the 'Ethernet II' and 'Internet Protocol' layers in the right window.

- | Network Ports | | MPLS Label Action | | |
|--|--------------|---|-------------------------------------|--------------|
| Label | | E-Type | MAC Source (click checkbox to edit) | |
| <input checked="" type="checkbox"/> 5A | 0005A | 0800 <input type="text" value="IPv4"/> | <input checked="" type="checkbox"/> | 00000000005A |
| <input type="checkbox"/> 7A | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> 5B | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> 6A | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> 7B | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> 8B | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| | | 0800 <input type="text" value="shortcuts"/> | <input type="checkbox"/> | |
| | Non-specific | 0800 <input type="text" value="IPv4"/> | <input type="checkbox"/> | |

- Repeat Step 5 to verify that all MPLS frames with label 90 (0x0005a) have their source MAC replaced by 00:00:00:00:00:5A:



Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Create mapping for MPLS stripping	MPLS stripping configuration is saved			
2	Send traffic from the tap ports with MPLS stripping enabled	Traffic received on the monitor port has the MPLS headers removed			
3	Configure mapping to substitute source MAC based on specific MPLS label value	Traffic received on the monitor port with specific MPLS label has source MAC substituted by the user-defined MAC address			

Overall Result

Test case accepted: ☐, not accepted

7.4 VLAN Tag Stripping

Many monitoring and analysis tools are unable to support more than a small number of VLANs, if any at all, and some network switches are also unable to handle more than a couple of hundred unique VLAN's

VLAN stripping removes VLAN tag information from the packets that is forwarded out the monitor ports. This can be one, two or all VLAN tags that may be nested in a packet, including Q-in-Q VLAN tags.

This test procedure is not a continuation from the previous test cases.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

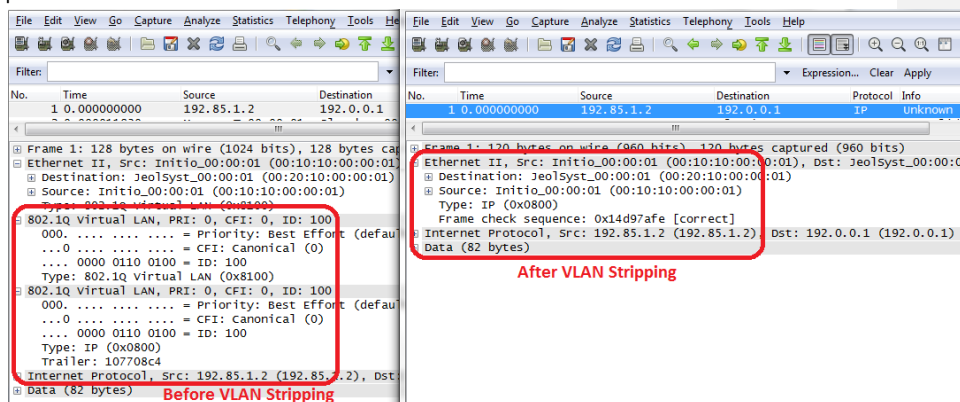
- A DTCS Advanced or Expert model with tap ports is used.
 - The DTCS units can be reached remotely via web browser.
 - Successful login into the DTCS management console via a web browser.
 - The following port configurations are successfully applied:
 - a. Tap Port Pairs: Ports 5A/5B (or any other tap ports)
 - b. Monitor Ports: Ports 2A (or any other monitor ports)
23. The following monitor mapping is successfully applied:
- a. Unfiltered, Network Port Input 5A → Monitor Port Output 2A
24. Port 5A is connected to a traffic generator (eg. A laptop).
25. Ports 2A is connected to traffic capture tools (eg. Wireshark).
- The selected tap ports have VLAN Stripping option activated

1. In VSS web UI, go to **Port Settings**.
2. Select Port **5A** (or another designated tap ports with VLAN Stripping activated).
3. From the **VLAN Tag Stripping** drop-down menu, select **All Tags**.

The screenshot displays the 'Port 5A Settings' configuration page. On the left, there are fields for 'Port Name' (VLAN Network Link 1 (A)), 'Auto Negotiate' (checked On), 'Auto Negotiation Advertisements' (checked for 10H, 100H, 1000H, Symmetric Pause, 10F, 100F, 1000F, Asymmetric Pause), and 'Link state' (Auto (normal)). On the right, there are fields for 'Type' (10Base-T/100Base-TX/1000Base-T RJ45), 'Class' (Tap selected), 'Linksafe' (Enabled), 'Monitor output timestamping' (Disabled), 'Monitor output portstamping' (Disabled), 'vAssure Fast Failover' (Disabled), and 'VLAN Tag Stripping' (All tags selected). Below these, the 'TPID(s)' field shows '8100' and '88A8' with a 'Reset' button. A 'Save Changes' button is at the bottom.

4. Click **Save Changes** to apply the change. In this configuration, all frames with VLAN headers going through this port will have their VLAN headers removed. If VLAN header is only to be removed for specific TPIDs, specify the TPIDs. By default, VLAN headers with TPIDs 0x8100 or 0x88A8 or 0x9100 will be removed.
5. Start sending VLAN traffic to port 5A.

- Start capture on port 2A. Wait for packets to arrive and stop capture. Verify that the received packets now have their VLAN headers removed:



Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	In Port Settings, enable VLAN stripping	VLAN stripping configuration is saved			
2	Send traffic from the tap ports with VLAN stripping enabled	Traffic received on the monitor port has the VLAN headers removed			

Overall Result

Test case accepted: ☐, not accepted

7.5 GTP De-encapsulation

Many monitoring and analysis tools are unable to handle data flows that are encapsulated using the GPRS Tunneling Protocol (GTP). GTP De-encapsulation strips the GTP header information from each packet, thereby restoring the GTP payload and hence the packet to what it was before the encapsulation. The packet is then forwarded to the monitor ports configured.

This test procedure is not a continuation from the previous test cases.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- A DTCS Advanced or Expert model with tap ports is used.

- The DTCS units can be reached remotely via web browser.
 - Successful login into the DTCS management console via a web browser.
 - The following port configurations are successfully applied:
 - a. Tap Port Pairs: Ports 5A/5B (or any other tap ports)
 - b. Monitor Ports: Ports 2A (or any other monitor ports)
26. The following monitor mapping is successfully applied:
- a. Unfiltered, Network Port Input 5A → Monitor Port Output 2A
27. Port 5A is connected to a traffic generator (eg. A laptop).
28. Ports 2A is connected to traffic capture tools (eg. Wireshark).
- The selected tap ports have GTP De-encapsulation option activated

1. In VSS web UI, go to **Port Settings**.
2. Select Port **5A** (or another designated tap ports with VLAN Stripping activated).
3. For **GTP Decapsulation**, select **Enabled**.

The screenshot shows the VSS web UI for Port 1A Settings. The 'GTP Decapsulation' option is highlighted with a red box and is set to 'Enabled'. The 'Class' is set to 'Tap'. The 'Link state' is set to 'Auto (normal)'. The 'Auto Negotiate' option is checked 'On'. The 'Auto Negotiation Advertisements' section shows various options checked, including 10H, 100H, 1000H, Symmetric Pause, 10F, 100F, 1000F, and Asymmetric Pause. The 'Link speed' is set to 'Auto (normal)'. The 'Monitor output timestamping' and 'Monitor output port timestamping' options are both set to 'Disabled'. The 'vAssure Fast Failover' option is set to 'Disabled'. The 'GTP Decapsulation' option is set to 'Enabled'.

4. Click **Save Changes** to apply the change
5. Start sending GTP traffic to port 5A.
6. Start capture on port 2A. Wait for packets to arrive and stop capture. Verify that the received packets are now de-encapsulated.

Test Result

#	Test Action	Expected Behavior	Result
---	-------------	-------------------	--------

			Accept	Deviation	Fail
1	In Port Settings, enable GTP Decapsulation	GTP de-encapsulation configuration is saved			
2	Send traffic from the tap ports with GTP de-encapsulation enabled	GTP traffic received on the monitor port is de-encapsulated			

Overall Result

Test case accepted: ☐, not accepted

7.6 vSlice

Packet slicing is a traffic grooming technique that allows users to define & discard part of a packet from copied traffic destined for monitoring tools, thereby, increasing capture rates, processing & write speeds on monitoring tools. vSlice extends this capability by allowing users to set slicing points at different offsets for each packet as well as to specify the types of traffic to be sliced, capabilities previously only available on monitor ports. The CRC is recalculated for each packet.

vSlice also enables packet slicing closer to the point of capture, rather than at a limited & specialized number of monitoring tools. As a result, vSlice can decrease all traffic sent to network monitoring devices, thus increasing their efficiency. vSlice also increases the throughput of the distributed traffic capture process itself by reducing load on the filters in distributed traffic capture devices and network taps. In addition, by providing more granular control over each packet, vSlice allows organizations to remove user identifying information earlier, thus reducing the risk & severity of a privacy breach.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- v24 Expert with vSlice-enabled ports (Refer to the sticker on the v24 Expert front plate for information on which ports are vSlice-enabled). vSlice-enabled ports must be running in 10G mode.
- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- Traffic generator and traffic capturing/monitoring tool via 1G or 10G interface.

Note: As of DTCS firmware v2.2M, vSlice does not work with MPLS or VLAN tagged traffic. Refer to the release notes for other limitations

1. Go to **vSlice Library**.

2. Click on **+Add new filter**, and enter filter name as **vSlice-HTTP**
3. Select **TCP** radio dial button, and check **HTTP and HTTPS** check box.
4. Click on **Save Filter**. The new slicing filter should appear in the available filters list, and selecting it should show the selected components.

5. Go to **vSlicing Settings**

- Click on **+Add new mapping**. Note that on the Network Port Input column, only vSlice-enabled ports configured in SPAN mode will appear.
- Select **vSlice-HTTP** as the filter expression. This means that vSlice will apply only to HTTP or HTTPS packets. All non-HTTP/HTTPS packets will not be sliced regardless of their lengths.

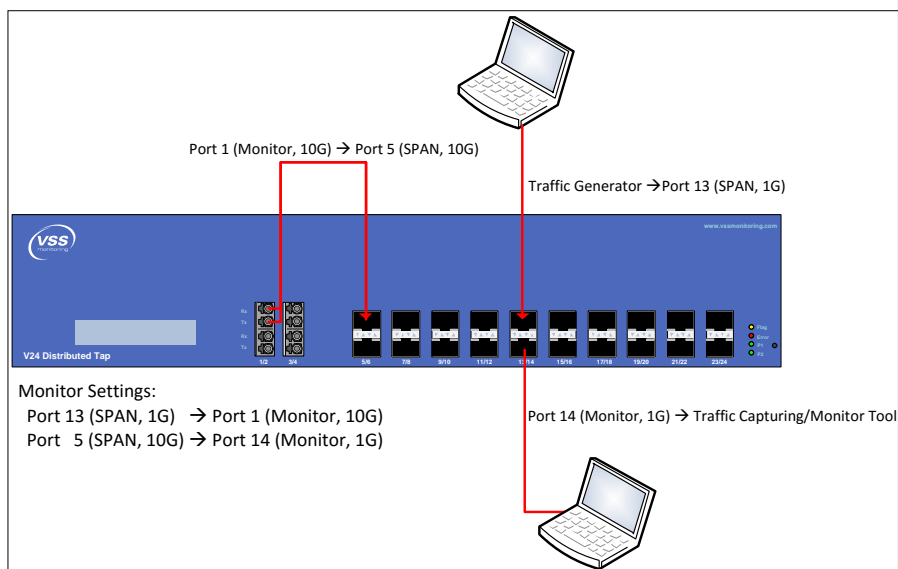
Filter Expression	Network Port Input	Slice point and offset
vSlice-HTTP (Nonmatch) vSlice-HTTP	<input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 7	Start of packet + offset: 64

Add new mapping

- For the **Slice Point and offset**, choose **Start of packet** and enter **64** for the offset value. This means that packet lengths > 64 will be sliced off after the 64th byte.
- Click on **Save Settings** to apply the change.
- Generate varied traffic including HTTP traffic with packet lengths > 64 bytes on the port that has vSlice configured.

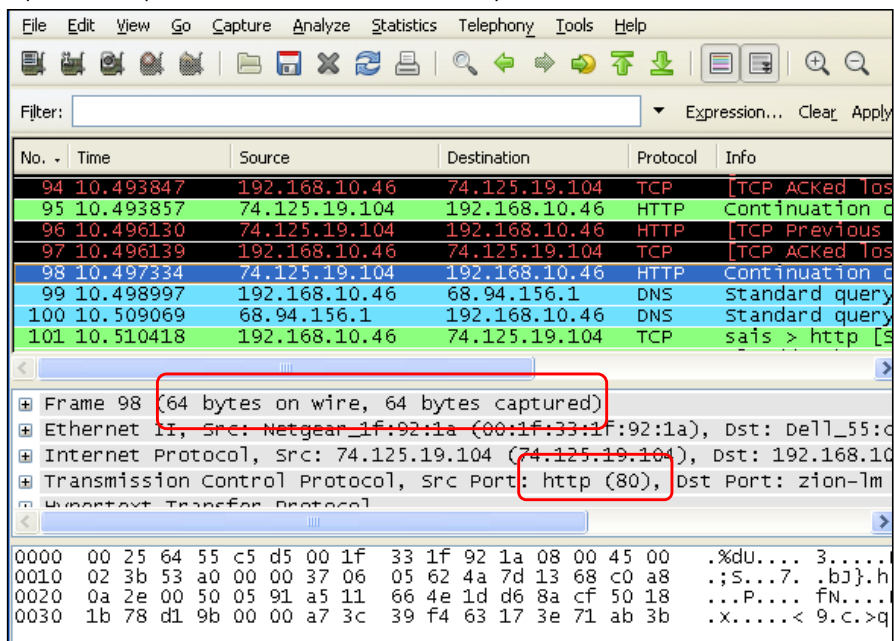
In absence of 10G interfaces for the traffic generator and traffic capturing tool, this can be achieved by the following v24 Expert configuration:

- Connect 1G traffic generator port to a **1G SPAN port** on v24 that does not have vSlice or High Data Burst Buffer (eg. Port 13).
- In v24 web UI, create a **monitor port mapping** to map the 1G SPAN port to a 10G Monitor port (eg. Port 13 (1G) to Port 1 (10G)).
- Physically connect the 10G Monitor port to a 10G SPAN port (eg. Port 1 (10G) to Port 5 (10G)).
- In v24 web UI, create a **monitor port mapping** to map the 10G SPAN port to a 1G monitor port (eg. Port 5 (10G) to Port 14 (1G)).

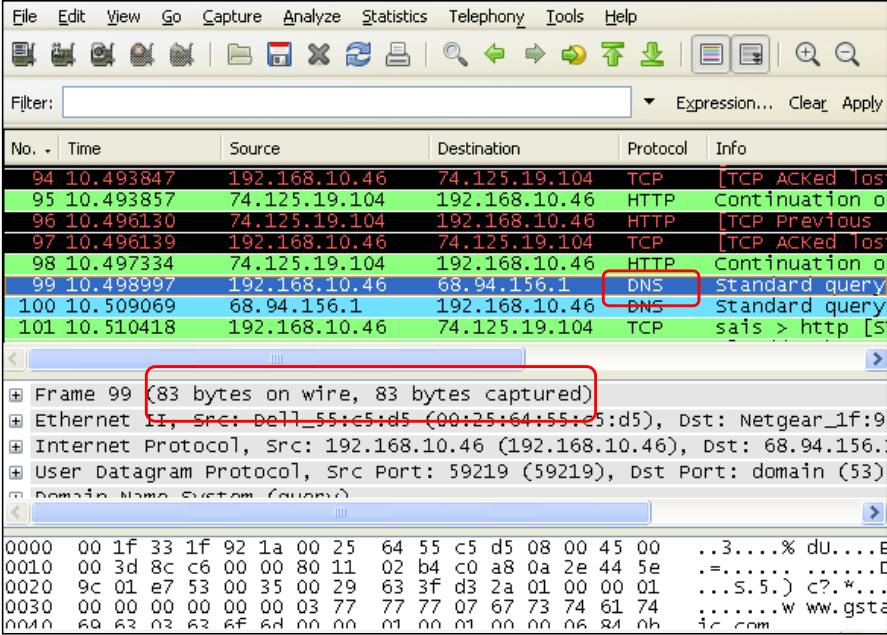


11. From the 1G Monitor port, use Wireshark or other capturing to start a packet capture in promiscuous mode.
12. Stop capturing when a good sample of packets have been received.

13. If Wireshark is used, apply HTTP filter to view all the HTTP packets captured. Verify that the captured HTTP packets have been sliced down to 64 bytes.



14. If Wireshark is used, clear the HTTP filter to verify that the lengths of these packets are preserved and the contents are unaltered.



Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Add a new filter to the vSlice library	A new filter is saved and available to use in vSlice Setting			
2	Apply filter to vSlice Settings with offset 64 bytes from the beginning of the packet	Only filtered packets are sliced down to 64 bytes; all other packets remain intact			

Overall Result

Test case accepted: ☐, not accepted

8 vStack+

vStack+ is a cutting edge stacking technology that allows the DTCS to grow in an organic manner as the network and monitoring needs grow. With vStack+, network input traffic can be directed to any desired monitor port, regardless of where the target monitor port is located. Meaning it allows for capturing traffic on one tap and sending the captured traffic to and out of a monitoring port on a second DTCS directly or indirectly connected to the first DTCS. This results in leveraging the full investment in network analysis equipment, where monitored traffic may be directed to centrally-located analyzers.

The test procedure below demonstrates how traffic captured from one DTCS unit can be sent to monitor tools connected to another DTCS unit, where the 2 DTCS units are interconnected via vStack ports.

This test procedure is not a continuation of the previous test cases.

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- 2 DTCS units with the same firmware version.
- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.

8.1 vStack+ Configuration

1. Connect 1x 10G port from DTCS Unit 1 to 1x 10G port from DTCS Unit 2. The connection can be done either as a direct physical link, or through a L2 tunnel.

For DTCS Unit 1:

2. In VSS web UI, go to **Port Settings**.
3. Select the 10G port connected to DTCS Unit 2 and enter port name **vStack Link to DTCS-2**.
4. Select port class as **vStack+**. Click **Save Changes** to apply the port setting.


Port 1 Settings	
Port Name:	vStack Link to DTCS-2
Speed:	<input type="radio"/> 1G <input checked="" type="radio"/> 10G
Type:	SFP+
SFP+ Module Identification:	FINISAR CORP. FTLX8571D3BCV (1G/10G)
Class:	<input type="radio"/> Span <input type="radio"/> Monitor <input checked="" type="radio"/> vStack+
<div>Save Changes</div>	

- Go to **System Settings** and verify that the vStack class configuration is applied and the link status is **OK**.

Port Status								
Port	Name	Link	Speed	Class	Monitor	Status	Optical Pwr. (Tx/Rx)	Setup
1	vStack Link to DTCS-2	Up	10G	vStack+		OK	-3.22 dBm,-2.28 dBm	Setup
2								

For DTCS Unit 2:

- Repeat Steps 2-5 for the vStack link on DTCS Unit 2 that is connected to DTCS Unit 1.
- In VSS web UI, go to **vStack+ Summary** and verify that the vStack links do not have any errors.



Status

[System Status](#)
[Network Activity](#)
[vStack+™ Summary](#)
[Settings](#)

vStack+™ Connections

10.8.6.6

Port 23 (vStack Link1) Connected to v4x24 (port 23:vStack Link1) 1G
Port 24 (vStack Link2) Connected to v4x24 (port 24:vStack Link2) 1G

v4x24

Setup

Port 23 (vStack Link1) Connected to 10.8.6.6 (port 23:vStack Link1) 1G
Port 24 (vStack Link2) Connected to 10.8.6.6 (port 24:vStack Link2) 1G

Note: If the physical link connected between the vStack+ configured ports is good but the vStack+ process is not communicating between the units, you will see the beginning of the status line red but link speed at the end of the status line black.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Configure and connect ports on the two DTCS units to be vStack ports	vStack+ connections for selected ports are set properly and displayed correctly in vStack+ Summary.			

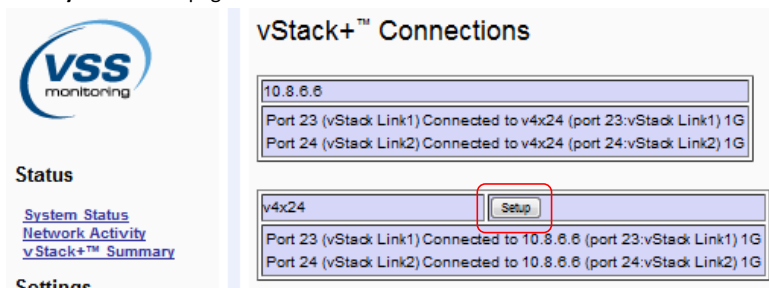
Overall Result

Test case accepted: ☐, not accepted

8.2 Verify vStack+ Web Console Redirection

For DTCS Unit 1:

8. In VSS web UI, go to **vStack+ Summary** and click on **Setup** for DTCS Unit 2. Verify that the page is now redirected to the web UI for DTCS Unit 2 by checking the IP address and the information on in **System Status** page.



Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	From the vStack Summary page, select Setup for another vStacked DTCS unit	Page redirected to the web UI for the other DTCS unit			

Overall Result

Test case accepted: ☐, not accepted

8.3 Verify vStack+ System

For DTCS Unit 1:

9. Go to **Monitor Settings** on DTCS Unit 1 and delete all existing monitor mappings.
10. Click on **Add a new mapping** and select local ports for network port input.

11. Click to expand **Remote Monitor Ports** and select the remote monitor ports from DTCS Unit 2.

Filter Expression	Network Port Input	Monitor Port Output	Rank
(Unfiltered)	<input type="checkbox"/> 1 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 7 <input checked="" type="checkbox"/> 10 <input type="checkbox"/> 12	Load Balancing Type: None (output to all selected ports) Ports: <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 6 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 11 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 Remote Monitor Ports: <input type="checkbox"/> v4x24 : 1 <input type="checkbox"/> v4x24 : 15 <input type="checkbox"/> v4x24 : 2 <input type="checkbox"/> v4x24 : 21 <input checked="" type="checkbox"/> v4x24 : 5 <input checked="" type="checkbox"/> v4x24 : 6 <input checked="" type="checkbox"/> v4x24 : 7 <input checked="" type="checkbox"/> v4x24 : 8 <input type="checkbox"/> Monitor Other (Primary) <input type="checkbox"/> v4x24 : C <input type="checkbox"/> v4x24 : D	

12. [Optional] Under **Filter Expressions**, select a predefined filter to send only filtered traffic to the remote monitor ports.
13. Click **Save Settings** to apply the configuration.
14. Connect the local network port input to a traffic generator.
15. Start Traffic.
16. In VSS web UI, go to **Network Activity, All Counters**. Verify that the network port input is showing Rx statistics corresponding to the traffic generated.
17. Verify that the vStack port is showing Tx statistics corresponding to the traffic generated.
Note that the vStack statistics includes both traffic transported through the vStack links and communication between the 2 vStack ports.

For DTCS Unit 2:

18. In VSS web UI, go to **Network Activity, All Counters**. Verify that the monitor port is showing Tx statistics corresponding to the traffic generated.
19. Connect the monitor ports selected in Step 11 to a traffic capturing/monitoring tool. Verify that the only packets matching the filter expression are received, and the packets from the monitor ports remain intact.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Send various types of traffic to the network port input on DTCS Unit 1, capture and filter packets and send them to monitor port on DTCS Unit 2	If filter is applied, Only packets matching the filter expression will be observed on the traffic capturing/monitoring tool connected to the monitor output port on DTCS Unit 2			

Overall Result

Test case accepted: ☐, not accepted

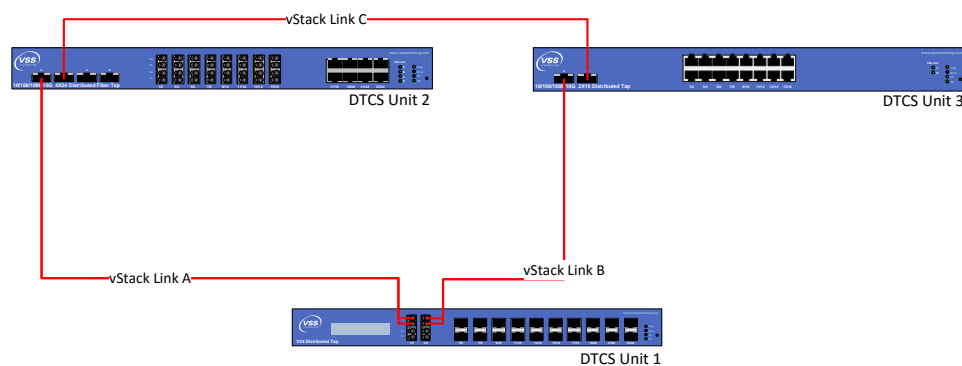
8.4 Features Configuration including Mesh vStack+ and Testing

After 2 DTCS units are successfully installed and configured, additional DTCS units can be incrementally added to test the features of a fully mesh distributed traffic capture system.

This portion of the test plan is open to customization to the user environment now that the basics have been laid out for installation, network input to monitor output port mapping, filtering, vSlice and vStack.

A sample test setup may be to combine 3 DTCS units in a full mesh and have multiple units mapping network input ports to the same remote monitoring port. Redundancy test may also be applied to this setup by removing 1 vStack link to validate that mapped traffic continues to arrive at the monitor port through another vStack path.

The diagram below demonstrates a setup where 3 DTCS units are connected via vStack. Both DTCS Unit 2 and 3 have maps their respective inputs to monitor ports on DTCS Unit 1 (bottom). During normal operations where vStack Links A, B, and C are all up, network traffic from DTCS Unit 2 to DTCS Unit 1 will be passed through vStack Link A, and DTCS Unit 3 to DTCS Unit 1 through vStack Link B. In events where vStack Link A becomes unavailable, traffic from DTCS Unit 2 will continue to arrive at DTCS Unit 1 using redundant path vStack Link C and B.



Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- 2 or more DTCS units with the same firmware version.
- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- Successful completion of 8.3 Verify vStack+ System.

9 SNMP and syslog Capabilities

Assumptions:

Before proceeding to the test procedures below, the following conditions must be satisfied:

- The DTCS units can be reached remotely via web browser.
- Successful login into the DTCS management console via a web browser.
- 4 MIB files from VSS. Please contact the VSS Sales Engineer if these files were not provided
- A SNMP MIB Browser (eg. iReasoning MIB Browser) or a SNMP manager application (eg. HP OpenView or IBM NetCool)
- A Syslog server is available to receive event notifications from the DTCS units (eg. [Kiwi Syslog server](#))
- DTCS user manual. Details on the SNMP and syslog features are on pages 10 and then 52-56

9.1 SNMP Configuration and MIB Structure

1. In VSS web UI, go to **SNMP Settings**.
2. Select the appropriate **SNMP Version V1, V2 or V3**.
3. Enter the IP address of the **SNMP Trap Manager**.
4. Enter the **Community Strings** for V1 and V2 or the **Passphrase** for V3.
5. Load the 4 VSS MIB files in the MIB Browser.
6. Walk the MIB to get the values of the parameters via SNMP. The following screenshot shows a sample view from the iReasoning MIB browser:

Name/OID	Value	Type	IP:Port
sysDescr.0	V16.8C-C-FAS-PM	OctetString	10.8.6.5:161
sysObjectID.0	vssMonitoringProductsId	OID	10.8.6.5:161
sysUpTime.0	95 hours 48 minutes 50 seconds (34493005)	TimeTicks	10.8.6.5:161
sysContact.0		OctetString	10.8.6.5:161
sysName.0		OctetString	10.8.6.5:161
sysLocation.0		OctetString	10.8.6.5:161
sysServices.0	1	Integer	10.8.6.5:161
1.3.6.1.2.1.1.8.0	10 seconds (1093)	TimeTicks	10.8.6.5:161
1.3.6.1.2.1.1.9.1.2.1	1.3.6.1.6.3.1	OID	10.8.6.5:161
1.3.6.1.2.1.1.9.1.2.2	vacmBasicGroup	OID	10.8.6.5:161
1.3.6.1.2.1.1.9.1.2.3	1.3.6.1.6.3.10.3.1.1	OID	10.8.6.5:161
1.3.6.1.2.1.1.9.1.3.1	The MIB module for SNMPv2 entities	OctetString	10.8.6.5:161
1.3.6.1.2.1.1.9.1.3.2	View-based Access Control Model for SNMP.	OctetString	10.8.6.5:161
1.3.6.1.2.1.1.9.1.3.3	The SNMP Management Architecture MIB.	OctetString	10.8.6.5:161
1.3.6.1.2.1.1.9.1.4.1	10 seconds (1092)	TimeTicks	10.8.6.5:161
1.3.6.1.2.1.1.9.1.4.2	10 seconds (1092)	TimeTicks	10.8.6.5:161
1.3.6.1.2.1.1.9.1.4.3	10 seconds (1093)	TimeTicks	10.8.6.5:161
snmpInPkts.0	1694	Counter32	10.8.6.5:161
snmpOutPkts.0	1685	Counter32	10.8.6.5:161
snmpInBadVersions.0	0	Counter32	10.8.6.5:161
snmpInBadCommunityNames.0	0	Counter32	10.8.6.5:161
snmpInBadCommunityUses.0	0	Counter32	10.8.6.5:161
snmpInParseErrs.0	0	Counter32	10.8.6.5:161
snmpInTooBigs.0	0	Counter32	10.8.6.5:161
snmpInNoSuchNames.0	0	Counter32	10.8.6.5:161
snmpInBadValues.0	0	Counter32	10.8.6.5:161
snmpInReadOnly.0	0	Counter32	10.8.6.5:161
snmpInGenErrs.0	0	Counter32	10.8.6.5:161
snmpInTotalReqs.0	1692	Counter32	10.8.6.5:161
snmpInTotalErrs.0	0	Counter32	10.8.6.5:161
snmpInGetRequests.0	0	Counter32	10.8.6.5:161
snmpInGetNexts.0	1698	Counter32	10.8.6.5:161
snmpInGetRequests.0	0	Counter32	10.8.6.5:161
snmpInGetResponses.0	0	Counter32	10.8.6.5:161
snmpInTraps.0	0	Counter32	10.8.6.5:161
snmpOutTooBigs.0	0	Counter32	10.8.6.5:161
snmpOutNoSuchNames.0	2	Counter32	10.8.6.5:161
snmpOutBadValues.0	0	Counter32	10.8.6.5:161
snmpOutGenErrs.0	0	Counter32	10.8.6.5:161

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Load the SNMP MIB files into a MIB browser and walk the VSS MIB structure	The various VSS parameter values are visible as the MIB is walked.			

Overall Result

Test case accepted: ☐, not accepted

9.2 SNMP Traps

The VSS devices also send SNMP traps under the following conditions

- Cold start (power on/ boot)
- Warm start (reboot after a reset console command)
- Any change to configuration setting
- Login to the console interface
- Logout from the console interface
- Console authentication failure (unsuccessful login)
- Any port changing state from link-down to link-up after boot-up
- Any port changing state from link-up to link-down after boot-up
- Power supply #1 low or zero voltage
- Power supply #1 returned to normal
- Power supply #2 low or zero voltage
- Power supply #2 returned to normal
- Internal temperature high
- Internal temperature returned to normal

Description	Source	Time
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.consoleLogout	10.8.6.5	2011-05-03 13:02:59
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.portLinkUp	10.8.6.5	2011-05-03 12:33:02
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.systemConfigCh...	10.8.6.5	2011-05-03 12:32:59
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.portLinkDown	10.8.6.5	2011-05-03 12:30:10
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.systemConfigCh...	10.8.6.5	2011-05-03 12:30:09
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.portLinkUp	10.8.6.5	2011-05-03 12:27:58
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.systemConfigCh...	10.8.6.5	2011-05-03 12:27:56
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.portLinkDown	10.8.6.5	2011-05-03 12:27:23
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.systemConfigCh...	10.8.6.5	2011-05-03 12:27:22
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.consoleLogin	10.8.6.5	2011-05-03 12:27:05
trapOID: .iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.consoleLogout	10.8.6.5	2011-05-03 12:27:01

Source:	10.8.6.5	Timestamp:	58 minutes 6 seconds	SNMP Version:	2
Trap OID:	.iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotification.vssNotifications.systemConfigChange				

Variable Bindings:

Name:	.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0
Value:	[TimeTicks] 58 minutes 6 seconds (348603)

Name:	snmpTrapOID
Value:	[OID] systemConfigChange

Name:	.iso.org.dod.internet.private.enterprises.vssMonitoring.vssMonitoringNotificationInfo.configChangeType
Value:	[Integer] portConfig (3)

Description: "One or more system configuration settings have been changed."

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Start the SNMP trap listener on port 162 on the SNMP manager. Change the configuration on a port or a monitor setting	The configuration change triggers a trap that shows in the trap receiver window			

Overall Result

Test case accepted: ☐, not accepted

9.3 Syslog

Syslog is an industry-standard method for event reporting. If a syslog server is configured, then all of the events that can generate a SNMP traps will also cause an event message to be sent to the configured Syslog server.

The Syslog messages described below are sent to the Syslog server when configured.

- System is rebooted
- A port that was online is now offline
- A port that was offline is now online
- Cold start (power-up)
- Voltage out-of-range: Main power supply #1
- Voltage out-of-range: Main power supply #2

1. In VSS web UI, go to **System Settings**.
2. Under **Network Settings**, enter the IP address(es) of the Syslog server(s).
3. While the syslog server is available, manually connect/disconnect the port to trigger port online/offline activities. Verify that the events are being reported to the syslog server.

Test Result

#	Test Action	Expected Behavior	Result		
			Accept	Deviation	Fail
1	Configure the kiwi syslog server on a laptop, enter that configuration on the VSS device, configure and connect a port to make it online	The event generated by the port being online will be reported to the syslog server			

Overall Result

Test case accepted: ☐, not accepted

10 Appendix A: Factory Default Values

The following are the **factory default settings** in each VSS traffic capture device.

TCP / IP SETTINGS

Default IP Address:	<input type="text" value="192.168.0.250"/>
Net/Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway/Router:	<input type="text" value="192.168.0.1"/>
SNMP Manager:	<input type="text" value="0.0.0.0"/>

SERIAL CONNECTION SETUP

Bits Per Second:	<input type="text" value="38400 BPS"/>
Data Bits:	<input type="text" value="8 bits"/>
Parity:	<input type="text" value="No Parity"/>
Stop Bits:	<input type="text" value="1 Stop Bit"/>
Flow Control:	<input type="text" value="No Flow Control"/>

DEFAULT SETTINGS

	<i>User Name</i>	<i>Password</i>
Serial:	<input type="text" value="admin"/>	<input type="text"/>
Telnet:	<input type="text" value="admin"/>	<input type="text"/>
Web:	<input type="text" value="admin"/>	<input type="text"/>

SNMP:

Get Community String	<input type="text" value="public"/>
Set Community String	<input type="text" value="private"/>
Trap Community String	<input type="text" value="trap"/>
SNMP Version:	SNMP V 3.0
Supported SNMP Mibs:	mit2.system

11 Appendix B: Images of v.24 and v2x16 Distributed Taps

V24



V2x16



12 Appendix C: VSS Monitoring Latency Measurements.

Network-to-Network Port Delay – VSS Results			
# Bytes Tx	Speed		Packet Delay
" +4-bit CRC"	Network A	Network B	Start-Start
60	10	10	4.4 - 5.4 μ s
1514	10	10	4.4 - 5.4 μ s
60	100	100	576 - 616 ns
1514	100	100	576 - 616 ns
60	1000	1000	314 - 340 ns
1514	1000	1000	314 - 340 ns

Network-to-Monitor Port Delay – VSS Results					
# Bytes Tx	Speed		Packet Delay		
" +4-bit CRC"	Network	Monitor	Start-Start	End-End	End-Start
60	10	10	76 μ s	76 μ s	20 μ s
1514	10	10	1.24 ms	1.24 ms	20 μ s
60	10	100	68 μ s	19.2 μ s	14 μ s
1514	10	100	1.24 ms	136 μ s	14 μ s
60	100	100	8.2 μ s	8.2 μ s	2.5 μ s
1514	100	100	124 μ s	124 μ s	2.5 μ s
60	100	1000	7.92 μ s	2.7 μ s	2.1 μ s
1514	100	1000	124 μ s	3.2 μ s	2.1 μ s
60	1000	1000	1.52 μ s	1.52 μ s	1 μ s
1514	1000	1000	13.2 μ s	13.2 μ s	1 μ s