Creating Specific Policy Enforcement options using DSCP (Rules/Selectors) and Field Software Upgrade Instructions

Mark Panas

GDMS

Date: October 7, 2020

Table of Contents

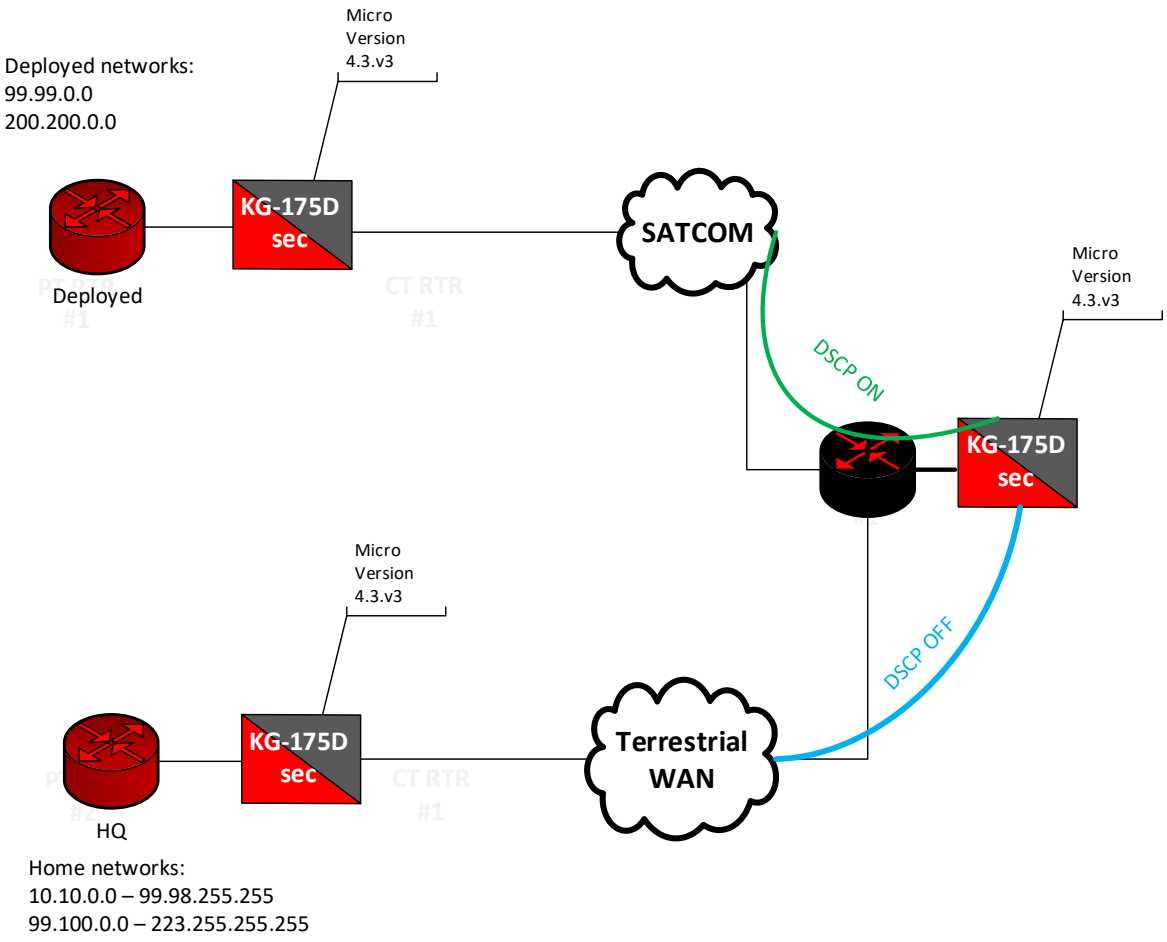


Figure shows need to Only allow DSCP traffic to be routed to Satellite networks and disable DSCP for all other traffic.

Creating Security Attributes for Specific Traffic

Task: Create Security attributes to secure specific traffic streams to forwarded DSCP options verse traffic streams without the DSCP options.

Steps:

1. Change HMI to Full Configuration Mode.
2. Fill FFVS Key.
3. Configure IPv4 Comms with valid IP addresses and Prefixes.
4. Create Peer Enclave routes to all remote PT networks.

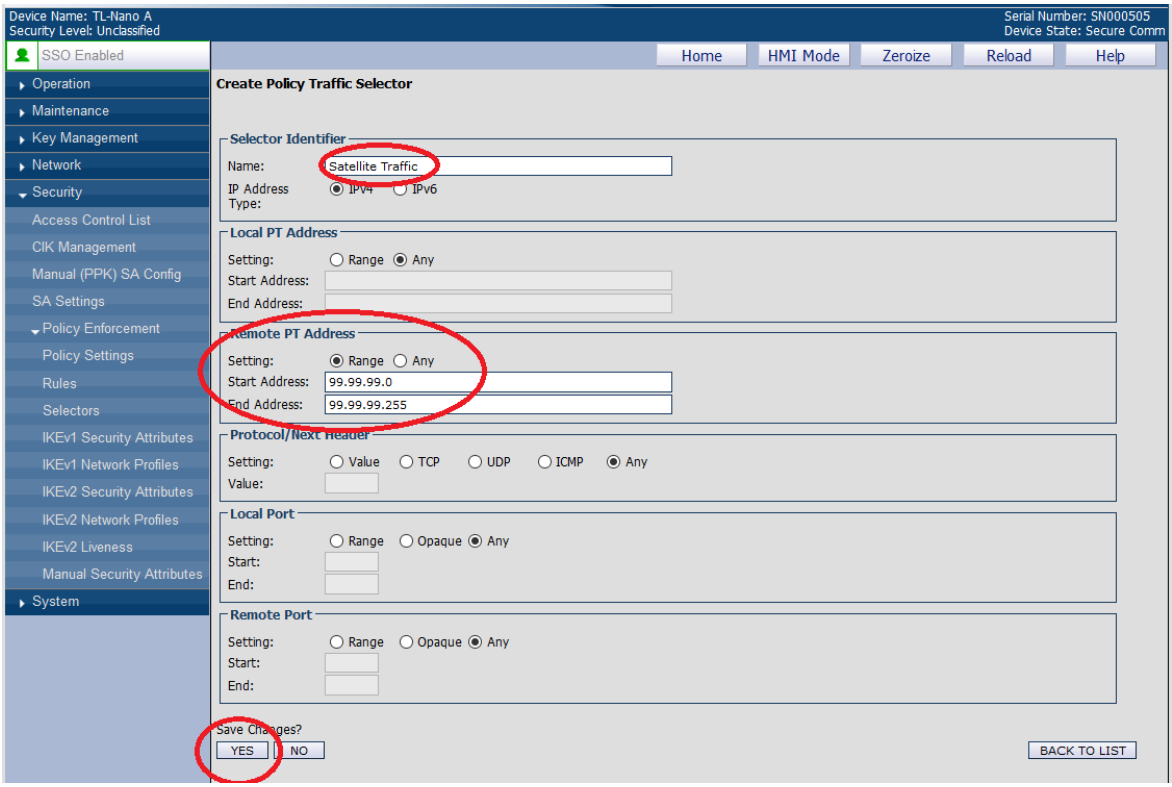
Additional Configuration: Modification to Security attributes and Policy settings to force the device to use transforms that support the DSCP (TOS bits).

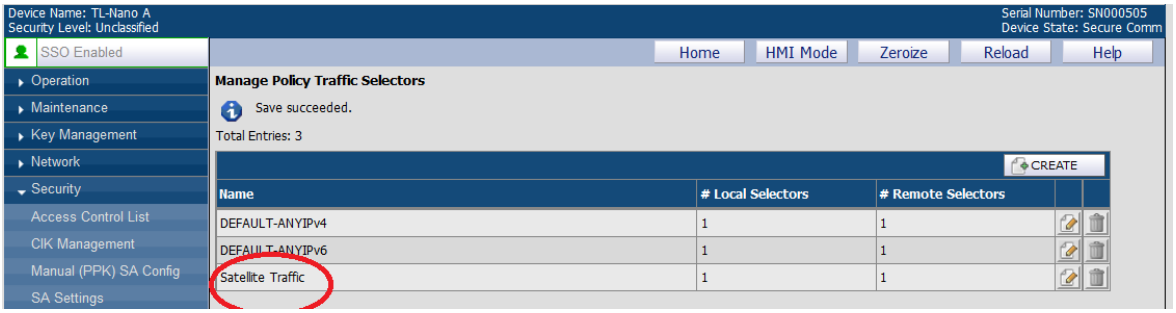
Steps to Solution:

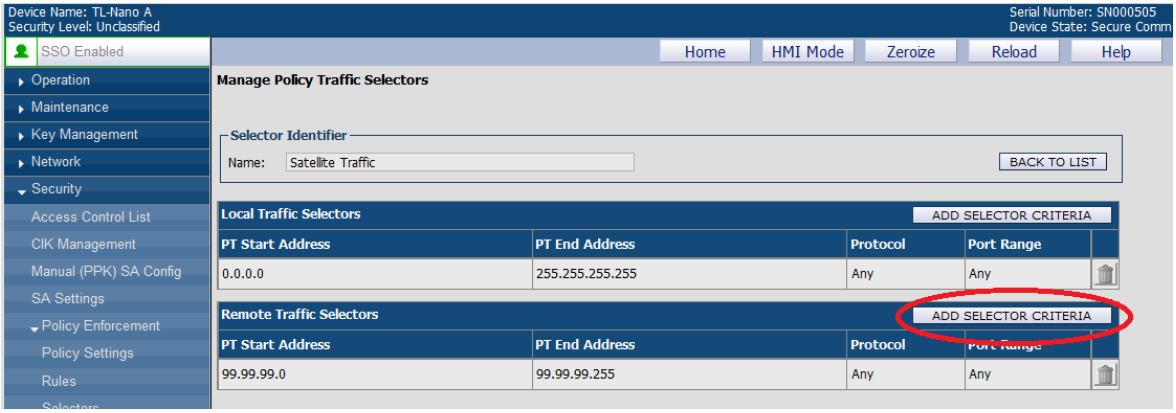
Create Selector to separate Satellite IP networks from Terrestrial IP networks.

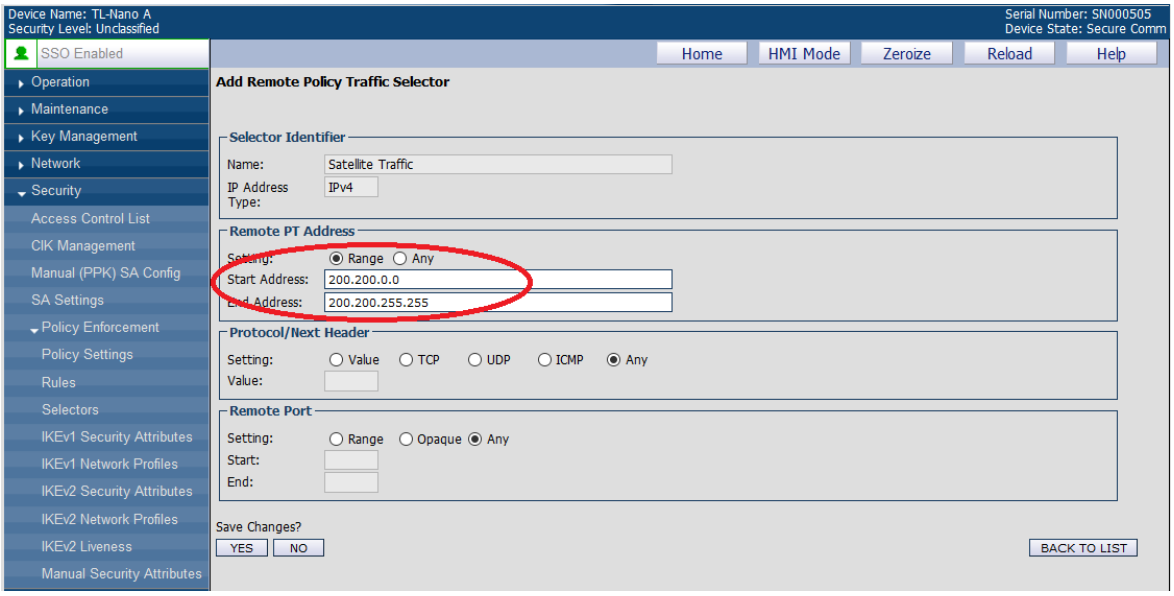
A. Create Traffic Selector (Security → Policy Enforcement → Selectors)

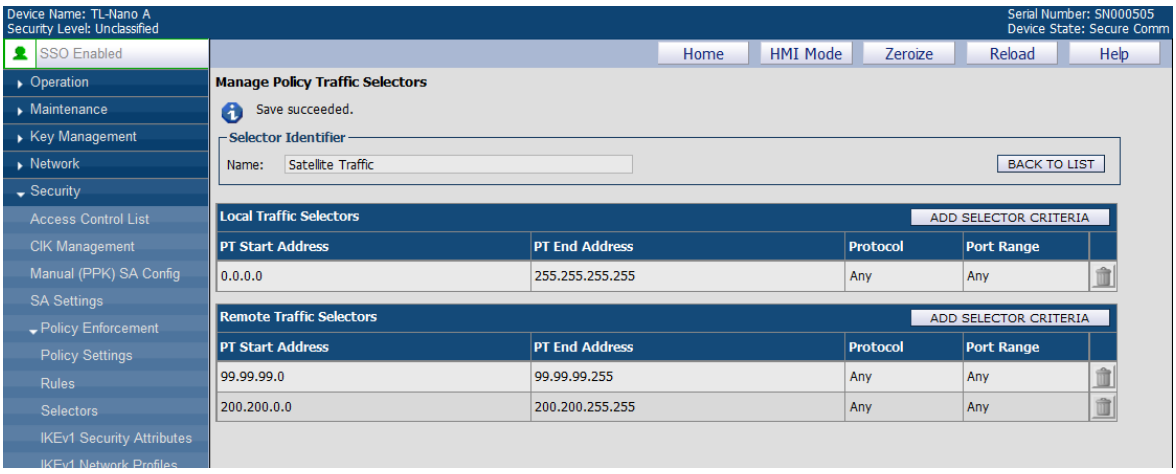
1. Go to Security → Policy Enforcement → Selectors
2. Select Create
3. Set Name to “Satellite Traffic”
4. Define Remote PT Address Range (*adding your Specific IP ranges*)
   a) 99.99.0.0 to 99.99.255.255
   b) 200.200.0.0 to 200.200.255.255
5. Save Changes







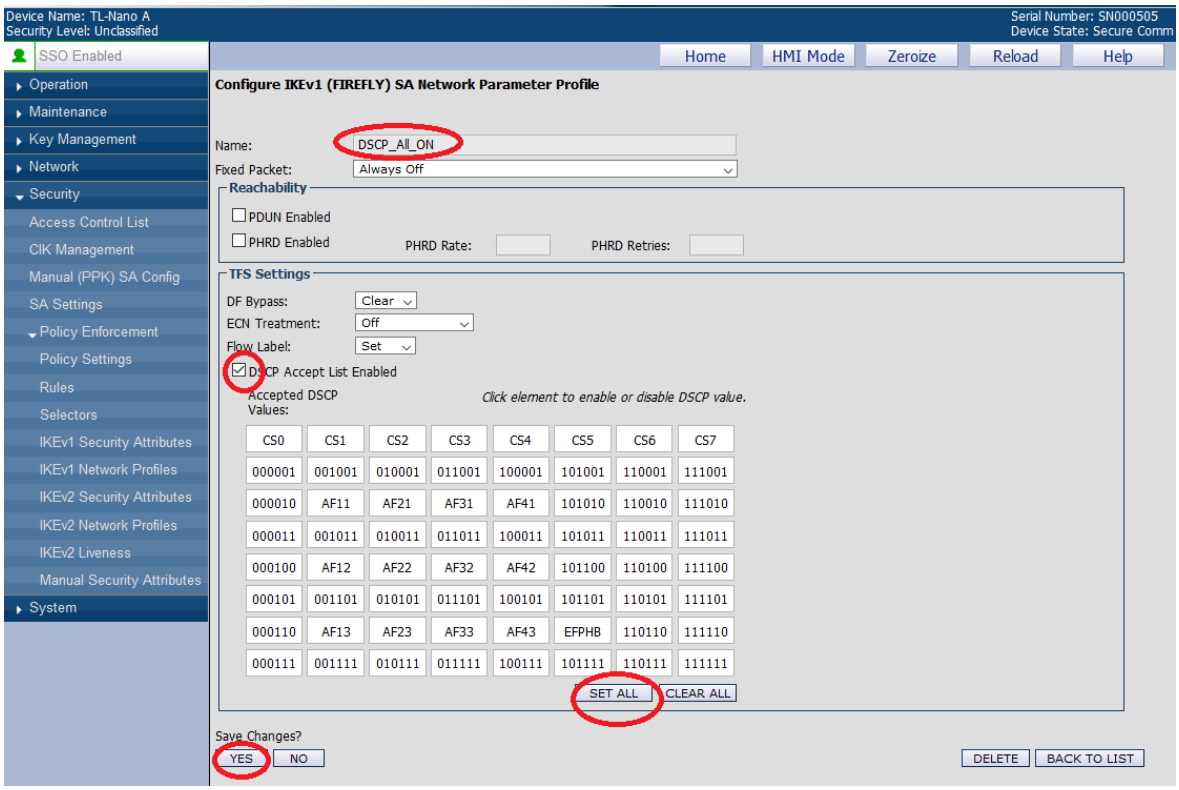




B. Create IKEv1 Network Parameters Profile (NPP)

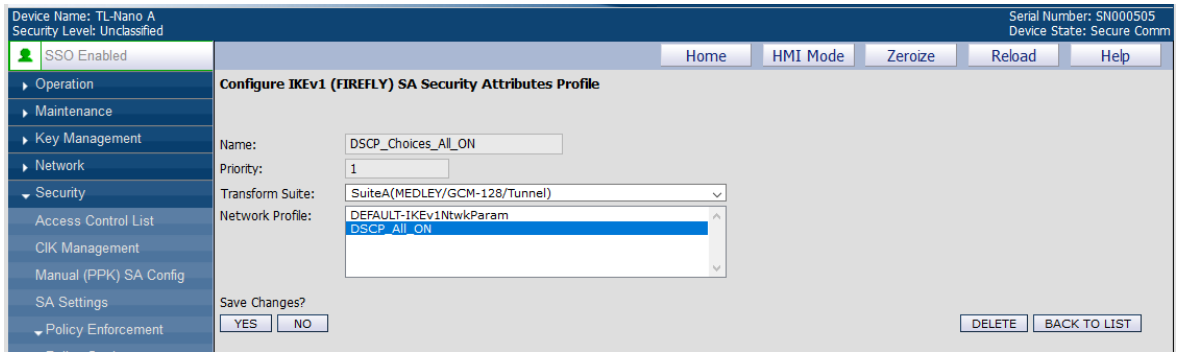
1. Go to Security → Policy Enforcement → IKEv1 Network Parameters Profile
2. Select Create
3. Set Name to “DSCP_ALL_ON”
4. Select DSCP Accept List Enabled Check box and **SET ALL** DSCP Values

5. Save Changes



C. Create IKEv1 Security Attributes Profile

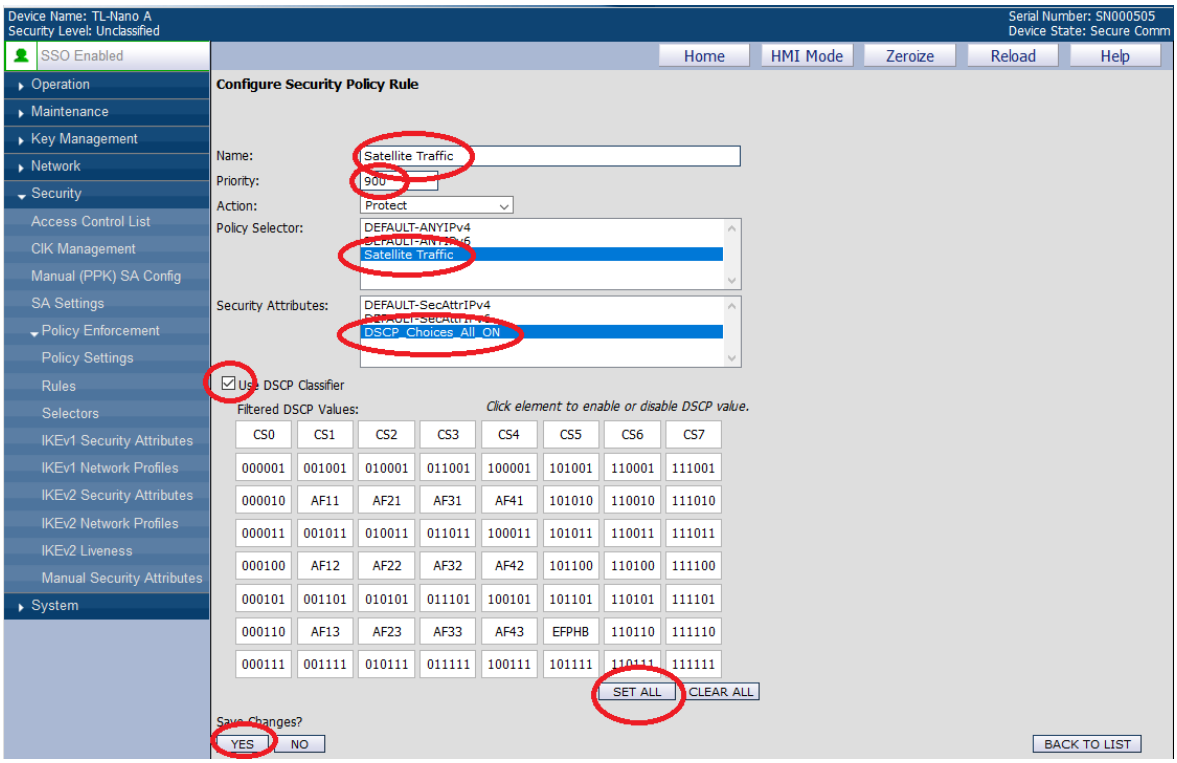
1. Go to Security → Policy Enforcement → IKEv1 Security Attributes
2. Select Create
3. Set Name to “DSCP_Choices_All_ON”
4. Set Priority to ”1”
5. Select “Suite A (MEDLEY/GCM-128/Tunnel) in Transform Suite dropdown
6. Select Network Profile “DSCP_ALL_ON”
7. Save Changes



Create one Rule with higher priority than the default Rules (*Lower the number higher the priority*), using the "Satellite Traffic and DSCP_Choices_All_ON" were previously created.

D. Create one new rule

1. Go to Security> Policy Enforcement> Rules
2. Select Create
3. Name Rule "Satellite Traffic"
4. Set Priority to 900
5. Action will be "Protect"
6. Policy Selector will be "Satellite Traffic"
7. Change Security Attribute to "DSCP_Choices_All_ON"
8. Check "Use DSCP Classifier"
9. Save Changes



Field Software Upgrade

Task: In this lab the student will upgrade the TACLANE to a newer software release.

Materials Provided:

Windows XP, Vista, or Win 7 PC (with port 69 open and assessable for use)

Field Software upgrade file

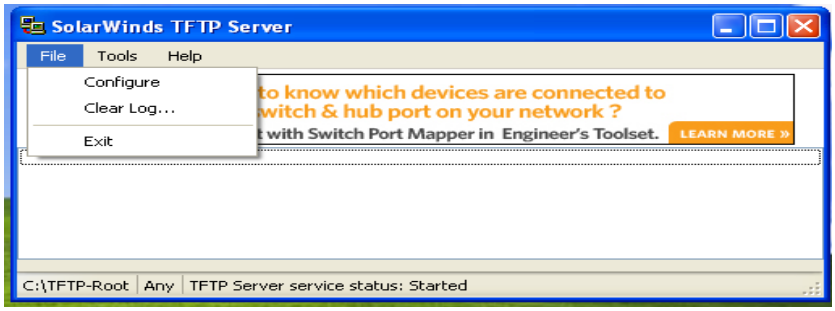
Third party TFTP Server software

Operator's manual, section titled **Maintaining TACLANE** - Configuring/Modifying the Download Server, Downloading an FSU File, and Installing an FSU File.

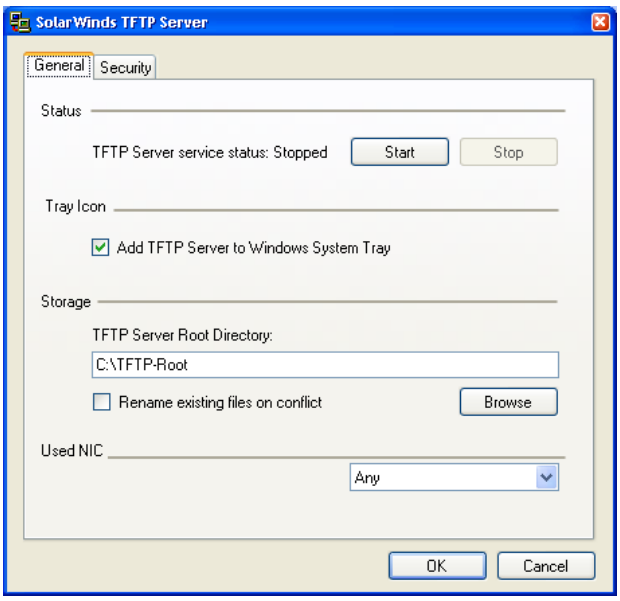
Note: A file named TL-Micro_R4.1v2-v6_to_R4.1v7_swdl.out was copied to C:\TFTP-root and renamed **fsu_4_1.out**. At the appropriate time you will download file **4_1.out** to your TACLANE (Instructor will verify file name).

1. Your taskbar contains an icon called "TFTP Server" click on this icon twice to open the SolarWinds TFTP Server application.

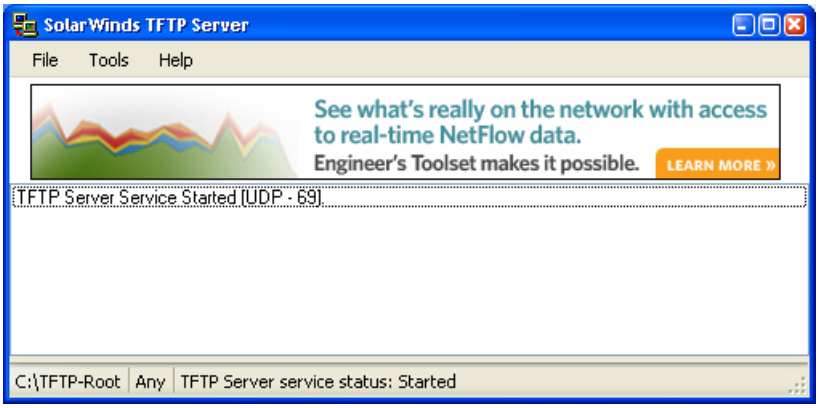
2. Select the "File" menu option, and then select “Configure”.



3. Start the TFTP Server if not already started.



Note: The TFTP Server should now be running.

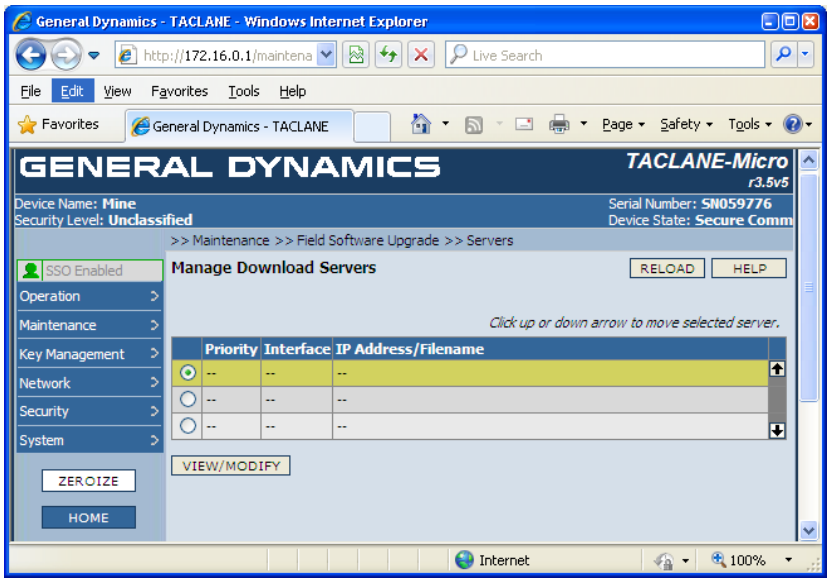


4. On the **TACLANE**, Configure Download Server.

a. Enter the SSO Pin.

b. From Main Menu, select **Maintenance → Field Software Upgrade → Servers.**

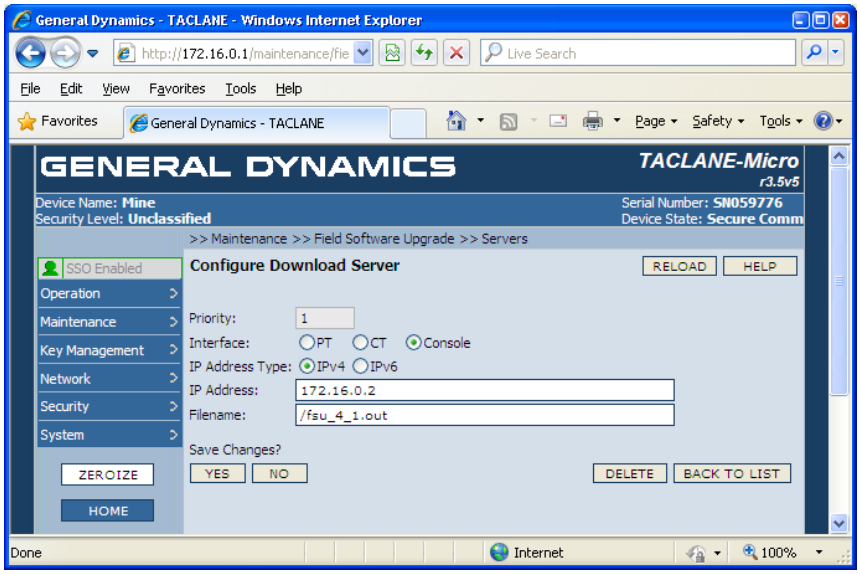
c. Select the first row radio button, and then select **View/Modify.**



Note: Selection of the first row defines the priority as 1.

d. Configure TACLANE to retrieve fsu_4_1.out via the console port (172.16.0.2)

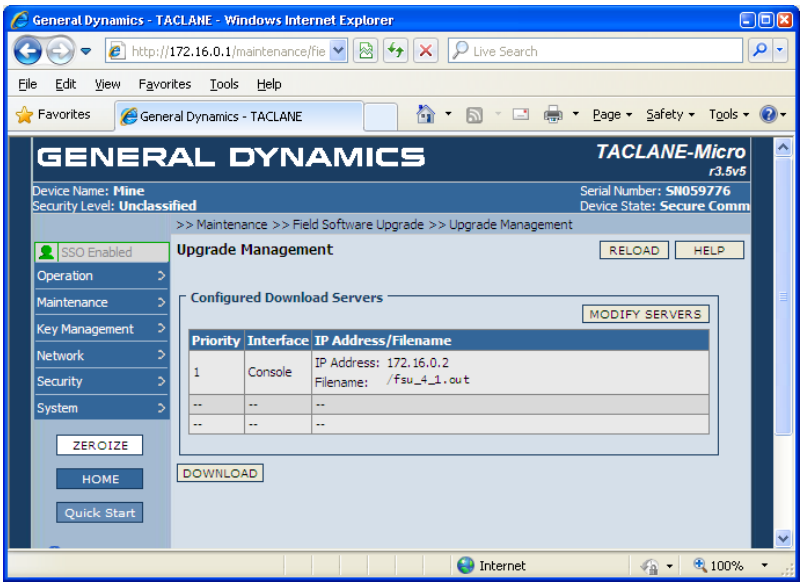
Interface: Console
IP address Type: IPv4
IP address <172.16.0.2>
Filename: /fsu_4_1.out (be sure to include the forward slash "/")
Save Changes? Yes



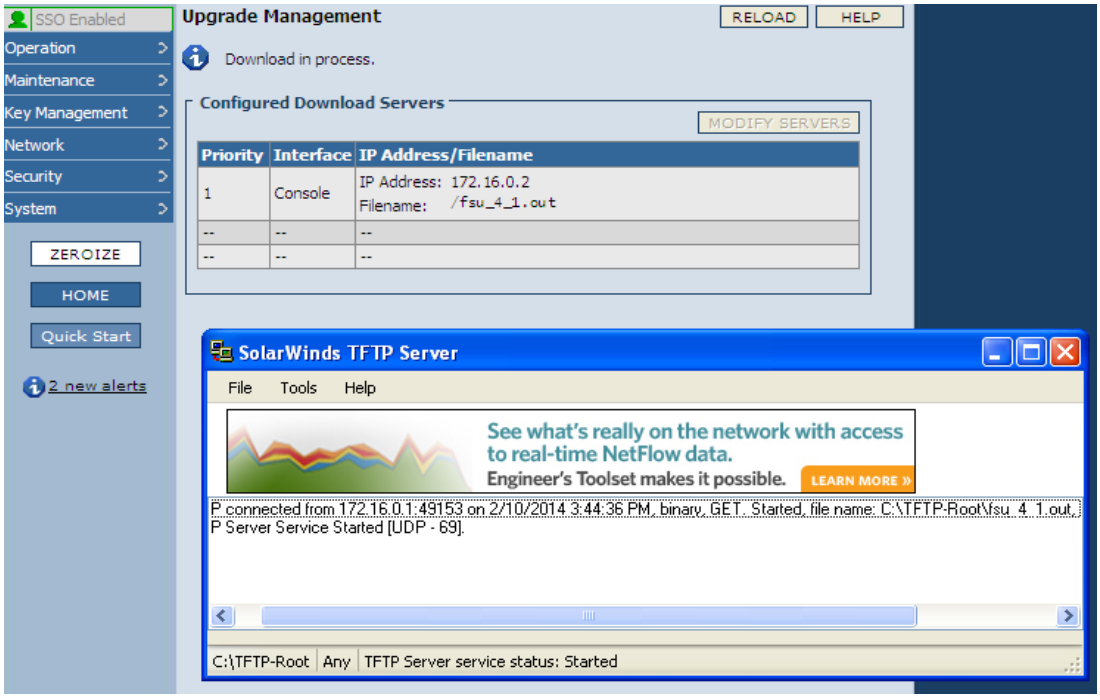
5. Download the FSU file

a. Select Maintenance → **Field Software Upgrade → Upgrade Management.**

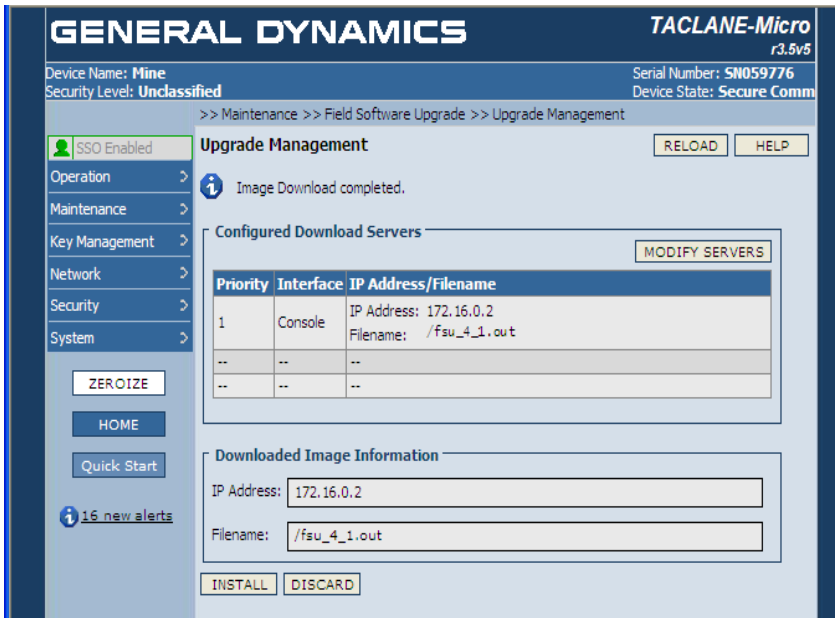
b. Select **Download.**



Note: TACLANE Browser and SolarWinds TFTP Server will indicate download is in progress.

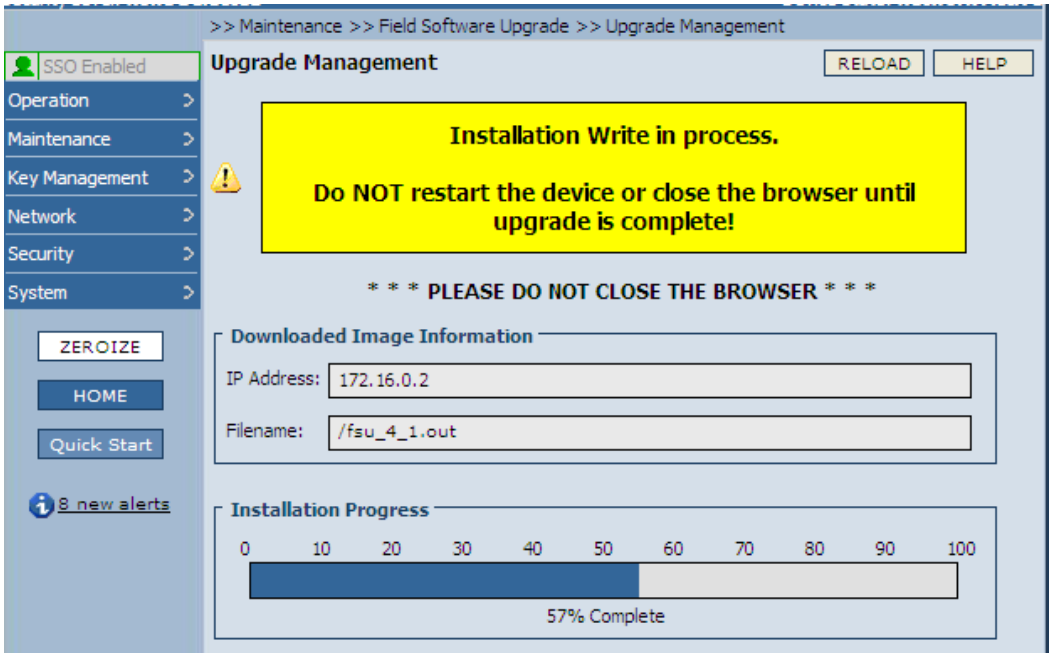


Note. At completion the TACLANE browser will indicate download is complete.



6. To install the 4.1 software upgrade, click **Install.**

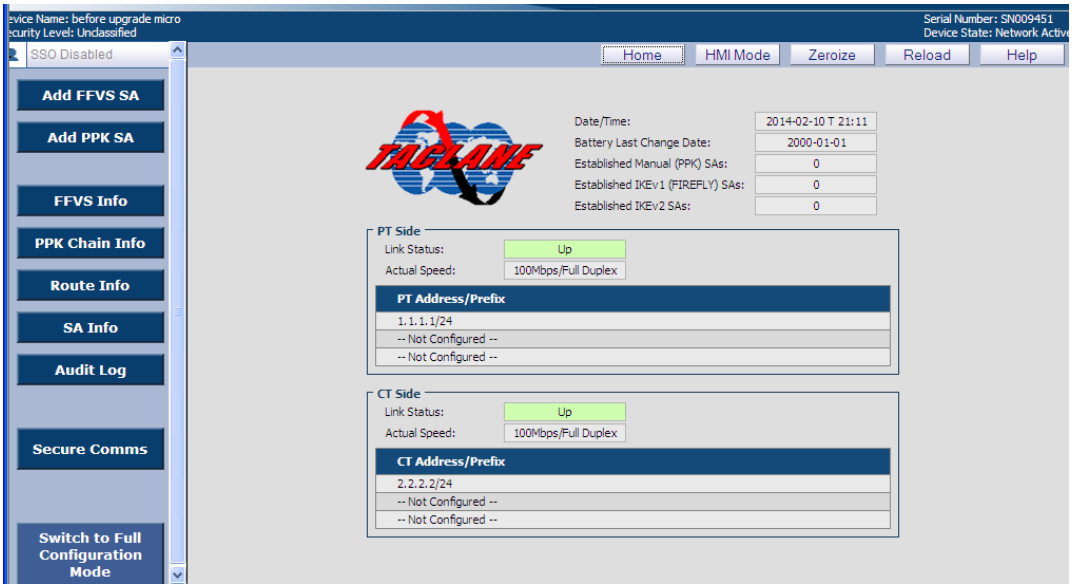
Note: Do not restart the device or close the browser until the install is complete!



7. Upon completion of the install, restart the TACLANE.

8. Select the SolarWinds File Menu → **Clear log** option and click on Yes.

10. Clear browser cookies, close the browser and then restart the browser. (*After the TACLANE reboot is complete, the new software release is listed in the upper right hand corner of the screen).*



11. Notice that the screen displays the PT and CT status.

12. Select FFVS Info.

13. Select Route Info.

Lab 14: Enabling VLAN Feature

Task:

In this lab the student will enable the VLAN feature.

Materials Provided:

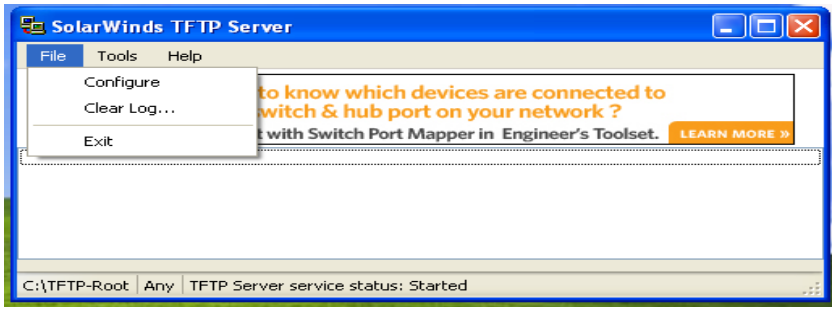
License File

Steps:

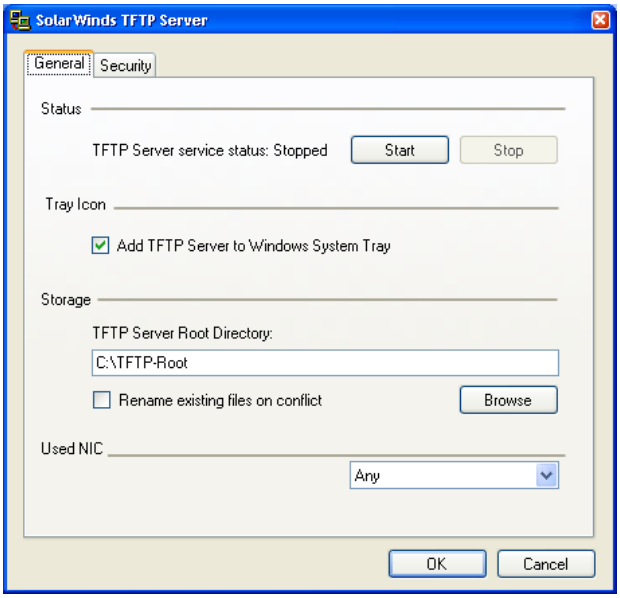
Note: License file must be under the TFTP root folder to allow the program to find it for transfer to the Taclane. User must have a working knowledge of a FTP program and the Ethernet settings.

1. Your taskbar contains an icon called "TFTP Server" click on this icon twice to open the SolarWinds TFTP Server application.

2. Select the "File" menu option, and then select “Configure”.



3. Start the TFTP Server if not already started.



Note: The TFTP Server should now be running.

Connect the RJ-45 network cable to the Console port of the unit and connect power.

4. Power on the unit.

5. Once the unit has booted to the main menu, connect the IE window to 172.16.0.1 which is the default console port IP address.

6. The Internet Explorer window should connect to the Taclane menu and show it is zeroized.

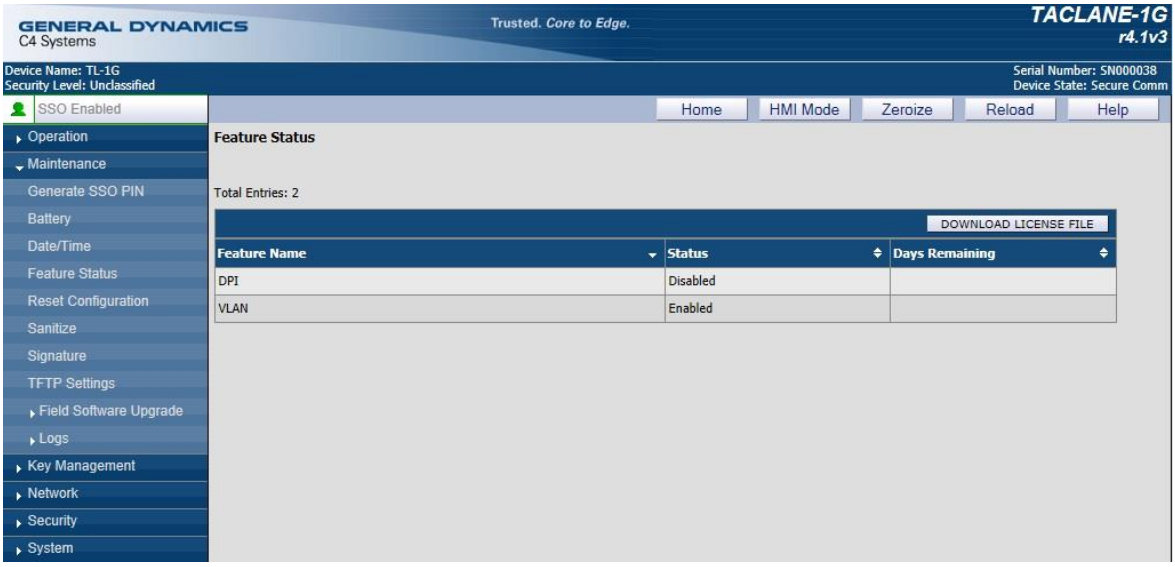
7. Click “OK”.

8. On the next screen, click on the left side of screen that says “SSO Disabled”.

9. It should prompt for an SSO PIN, type 123456789.

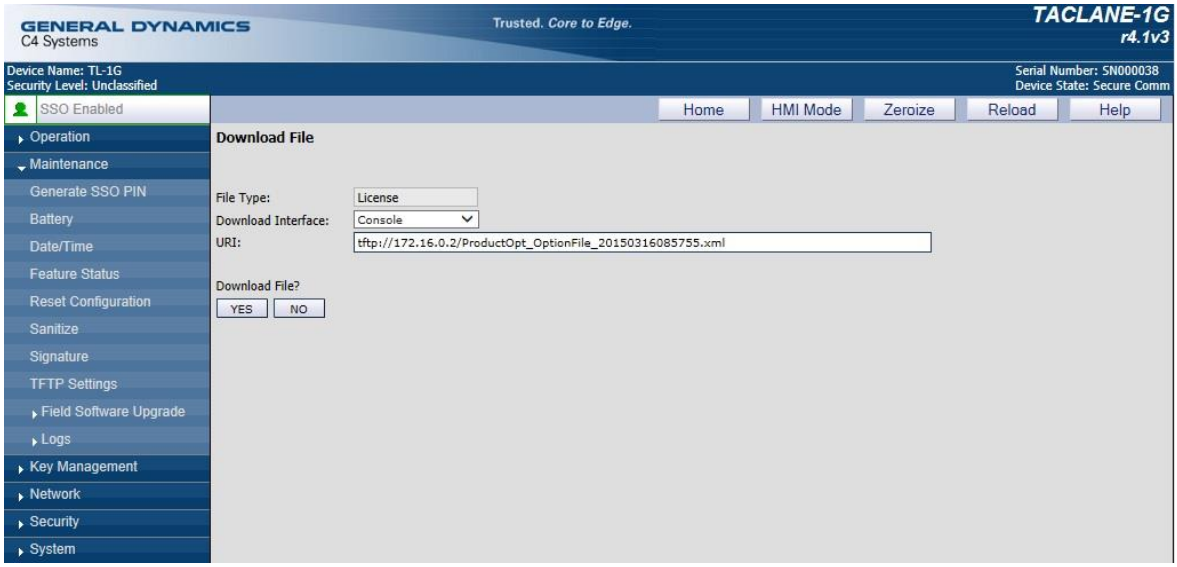
10. Click “OK”.

11. Once the screen shows the SSO is enabled, go to “Maintenance” and select “Feature Status”.



12. The screen should show the VLAN Feature and that it is disabled.

13. Click on the button “Download License File”.



14. Click on the “Interface” drop down box and select “**Console**”.

15. Enter a URI script into the box provided. Format is: location of file://IP Address/filename which will be provided by the instructor.
    Example: **(tftp://172.16.0.2/kg175d_vlan_enable.xml)**

16. Click “Yes” to download file.
    Note: There should be activity in the events viewer window

17. The Taclane window should now show the VLAN Feature enabled.