

Network Management System Routing and Switching Service and Infrastructure Management

Lab351, Revision H

Network Management System 8.1

NMS Controller Suite

Hands-on Training Lab Guide



Contents

Lab 1: Log Into NMS	3
Lab 2: Network Element Enrollment.....	5
Lab 3: Network Management System Fundamentals	12
Lab 4: Network Element and Equipment Management.....	18
Lab 5: Network Element Backup	24
Lab 6: Provisioning a Static Unprotected MPLS-TP Tunnel.....	29
Lab 7: Provisioning an Ethernet Virtual Private Line (EVPL) Service	37
Lab 8: Provisioning an Ethernet Virtual Private LAN (EVP-LAN) Service	42
Lab 9: Viewing and Troubleshooting Provisioned Services and Infrastructure	46
Appendix A: 802.1ag Operations, Administration and Maintenance (OAM)	55
Appendix B: Provisioning a Link Aggregation Group (LAG).....	57
Appendix C: Provisioning a Dynamic Unprotected MPLS-TP Tunnel.....	62
Appendix D: Configuring Custom Network Map Groups	68
Appendix E: Add Unmanaged NEs and Links.....	72
Appendix F: Provisioning a TDM Metro Ethernet Forum 8 (MEF-8) Service	74
Appendix G: Provisioning a TDM Circuit Emulation (CEM) Service.....	78

Documentation Resources

Refer to the following manual as needed as you perform lab exercises:

- Network Management System Documentation can be accessed via Network Management System UI



Lab 1: Log Into Network Management System

Objectives

- Login to the Network Management System server.
- Access Network Management System Documentation.

Task 1: Gather Information

1. Gather information from your instructor:

IP address or hostname of Network Management System server:

Network Management System username:

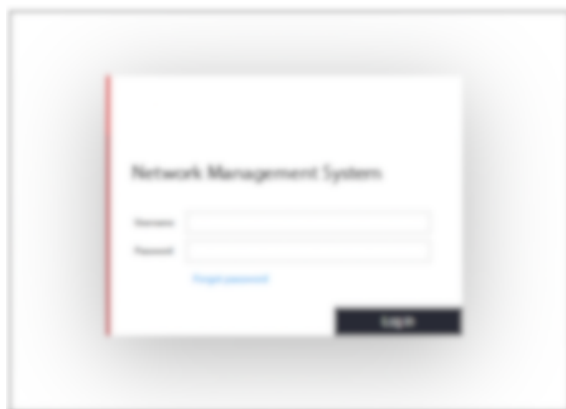
Network Management System password:

Task 2: Login to Network Management System

1. Use your Chrome or FireFox web browser to connect to the Network Management System server.

Note: When you attempt to connect to a Network Management System server, your web browser may give you a connection warning. The text of the warning varies somewhat, depending on the type of browser you are using. Contact your administrator to determine if it is safe to proceed to the Network Management System server. The error may be harmless and caused by a certificate configuration problem on the server but contact your administrator anyway to make sure that it is safe to proceed.

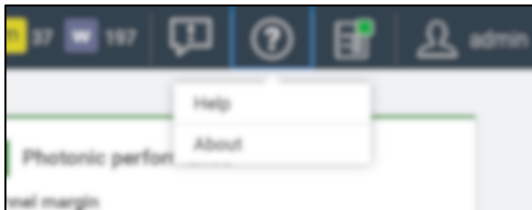
2. At the Network Management System Login screen, enter your Network Management System username and password.



Task 3: Access Network Management System Documentation

In this task you will access the Network Management System documentation from the UI. The documents are in a html format. This will require some modifications to enable search capabilities within the document. Directions to do this can be found within the documentation. The second method is to access the documentation from Network Management System UI. That is what you will do here.

1. Select the question mark icon in the upper right of the screen.
2. Select Help from the dropdown.



3. The Network Management System documentation will appear in a new tab. The upper right text entry box allows you to search for a specific topic.

End of Lab

Lab 2: Network Element Enrollment

Objectives

After completing this activity, you will be able to:

- Enroll a single NE
- Do a bulk enrolment
- Place NEs on the network map
- Add an unmanaged NE
- Add a manual link
- Add searchable tags
- De-enroll a single NE

Task 1: Gather Information

If necessary, divide into teams for this lab. Write down the NE(s) and profile(s) information provided by your instructor:

I am on Team: _____

NE IP	Profile

Task 2: View NE Connection Profiles

Before an NE can be enrolled a connection profile must be created for the NE type. A connection profile defines the protocols that are necessary for Network Management System to communicate with the NE. You will not be creating a profile here. Instead, you will view the profiles to gain a better understanding of what they contain and why they are important.

1. Navigate to the NE connection profiles page (**System > NE connection profiles**).



2. This page is used to create and edit connection profiles. The list shows all of the connection profiles that have been created. Select the OS 6 profile.



3. Select **Edit** on the bottom right of the screen. A popup box appears. Here you see the protocols that are required and have been defined for this profile. The necessary protocols differ for each NE type.

Edit connection profile

Identification

Name:

Profile description:

Profile type:

SMI

☒ Enable SMI protocol

Host:

Username:

Password:

Community:

SNMP

☒ Enable SNMP protocol

Host:

Username:

Password:

Community:

Task 3: Enroll a Single NE

You'll enroll NEs, one at a time. Repeat this procedure for each NE to be enrolled:

1. Navigate to the Enrollment page (**Network > Enrollment**).
2. Select Pre-enroll.



3. Specify the IP address of the NE and the appropriate NE connection profile. We won't be using partitions so select none. We also will not be defining a Backup schedule so select No schedule.

Pre-enroll network elements

Pre-enroll by: IP address

IP address: Enter IP address

Profile: Required

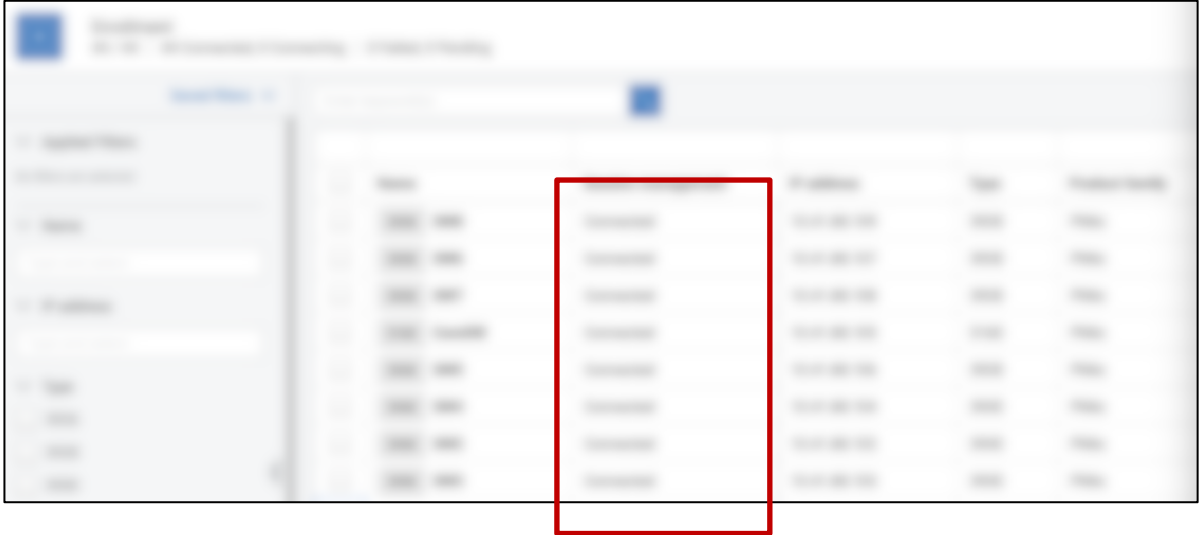
Partition: Required

Backup schedule: Required

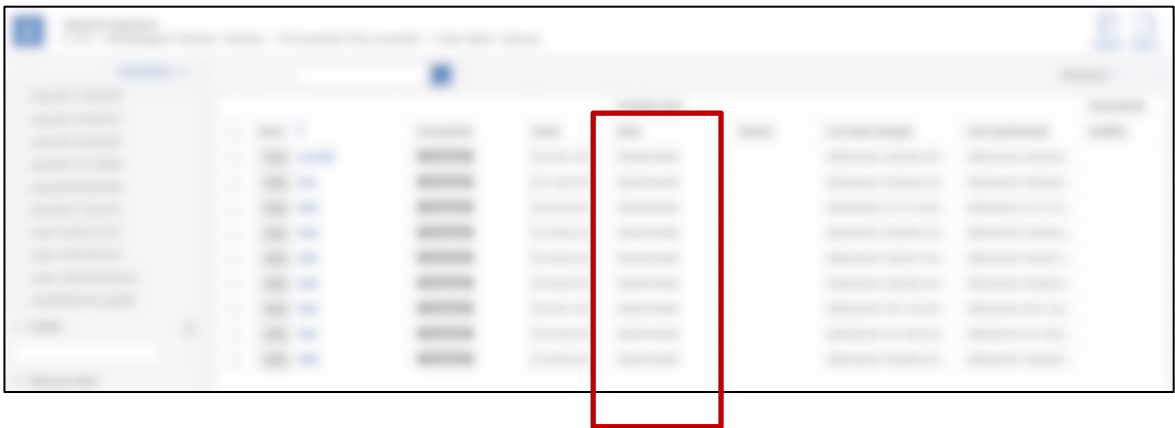
Cancel Pre-enroll

4. What is the status of the NE that you just pre-enrolled? _____
5. On the Enrollment page, select the NE to be enrolled and click the Enroll button.

6. Monitor the NE status. The NE status under **Session management** will transitions from connecting to connected if successful.



7. After the NE is Connected, navigate to the Network Elements page (**Network > Network Elements**). Scroll to the right until you find the Inventory Sync columns. The NE will take a moment to synchronize with Network Management System Its status will move from synchronizing to synchronized. Network Management System is discovering services that have been provisioned with the NE. These services are added to the Network Management System inventory and identified as discovered.



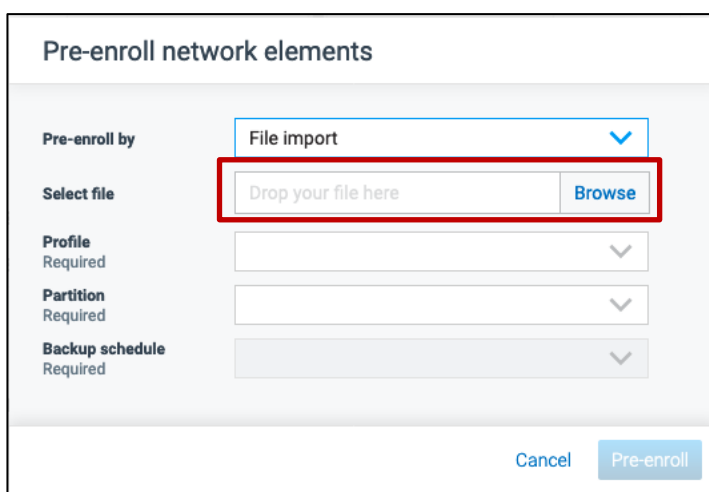
8. Is the NE synchronizing with Network Management System (check one)? ☐ Yes ☐ No

Bulk Enrollment

You will not be enrolling NEs via bulk enrollment in this lab, but it is a valuable feature when you have many NEs to enroll. You perform a bulk enrollment as follows:

1. Use Notepad to create a text file containing a list of the NE IP addresses, one per line. For example:

10.41.88.51
10.41.88.52
10.41.88.53
2. Pre-enroll by File import, drag and drop the text file to the Select file field and select the PN6x NE connection profile.



Pre-enroll network elements

Pre-enroll by: File import

Select file: Drop your file here [Browse](#)

Profile Required

Partition Required

Backup schedule Required

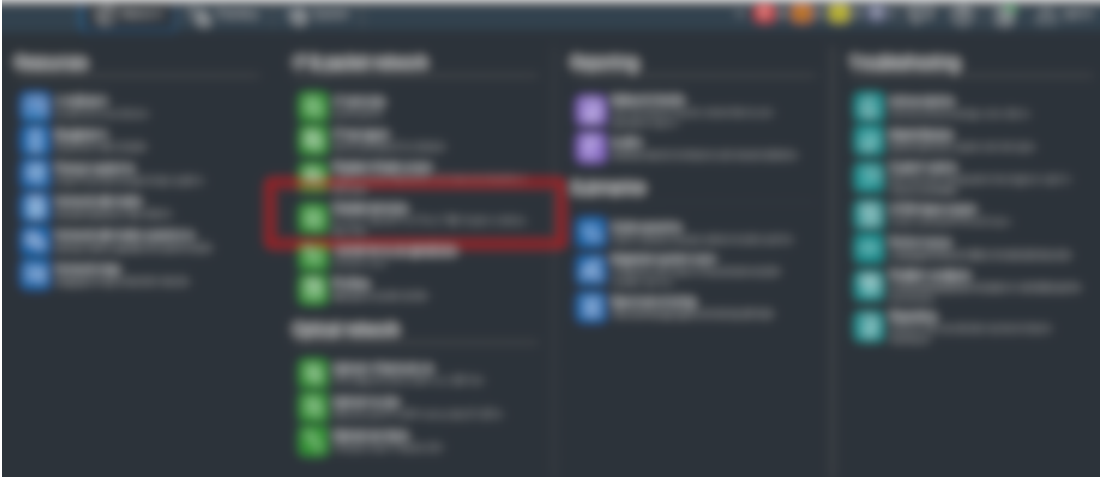
[Cancel](#) [Pre-enroll](#)

3. Click Pre-enroll. If the addresses are valid, they will all show on this list with a pending status.
4. On the Enrollment page, select all the NEs and click the Enroll button.

Task 4: Identify Discovered Services

As mentioned, Network Management System discovers services that utilize an NE when it is enrolled. Look at the current services to determine if any have been discovered.

1. Navigate to the Packet Services page (**Network > Packet**).



2. Notice the status of each service in the Deployment column. The value here will be either Discovered or Deployed. Do you see any services that have a value of Deployed? At this point you probably won't. Deployed services are those that have been provisioned via Network Management System.

Packet services 25 / 25		Report Export Create							
Saved filters		Enter keyword(s)							
Applied Filters No filters are selected.		1 to 25 of 25							
Type ☐ ETransit ☐ EVC ☐ VLAN		☐	Name	Type	Connectivity status	Layer rate	Note	Endpoints	Deployment
		☐	Mgmt	VLAN		ETHERNET		SW4 9-127 (pt-vlan) SW4 10-127 (pt-vlan)	Discovered
		☐	Mgmt	VLAN		ETHERNET		SW3 9-127 (pt-vlan) SW3 10-127 (pt-vlan)	Discovered
		☐	Mgmt	VLAN		ETHERNET		SW1 9-127 (pt-vlan) SW1 10-127 (pt-vlan)	Discovered
									Resilience
									Domains

End of Lab

Lab 3: Network Management System Fundamentals

Objectives

- View Dashboard.
- Add NEs to the Network Map.
- View Alarms

Task 1: View the Dashboard

The Dashboard appears when you first log into Network Management System. If you are not on the Dashboard screen, click on the logo on the top left of the screen and you will be taken to the Dashboard. The Dashboard may reflect a server with little data but will become populated with more information as the class continues.



On the Dashboard verify the following:

1. Can you navigate directly to the Packet services page directly from the Dashboard (check one)?
☐ Yes ☐ No
2. Can you navigate directly to the Packet infrastructure page directly from the Dashboard (check one)?
☐ Yes ☐ No

Task 2: View the Network Map

The network map is the primary means of visualizing the connectivity of the entire network, and provides a variety of tools for network inspection, context-specific workflows, and troubleshooting.



Task 3: Add NEs to the Network Map

If an NEs longitude and latitude are not defined, they will not appear on the map. In this task, the NEs will be added to the map. **If the NEs had already been placed on the map, will display even if they have been de-enrolled and then re-enrolled.** Follow these steps if you see NEs that do not display on the map.

1. Put the map in Edit mode by selecting Edit Topology from the Mode selector | the toolbar.
2. From the Add to map popup on the right, drag one or more enrolled NEs to the map (sample screenshot below).



The following example shows some NEs on the map (sample screenshot is shown).



3. Identify the NEs and on the map.

How many x440 NEs? _____

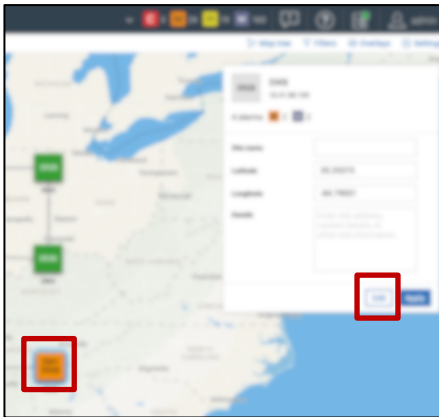
How many x78 NEs? _____

Are any of the NEs colored to reflect alarm states (check one)? ☐ Yes ☐ No

4. Display shelf-level details for one or more NEs.
5. Display details on any links between NEs.
6. Optionally, organize the NEs into network map groups. Refer to Appendix B for more information.

Task 4: Add Searchable Tags

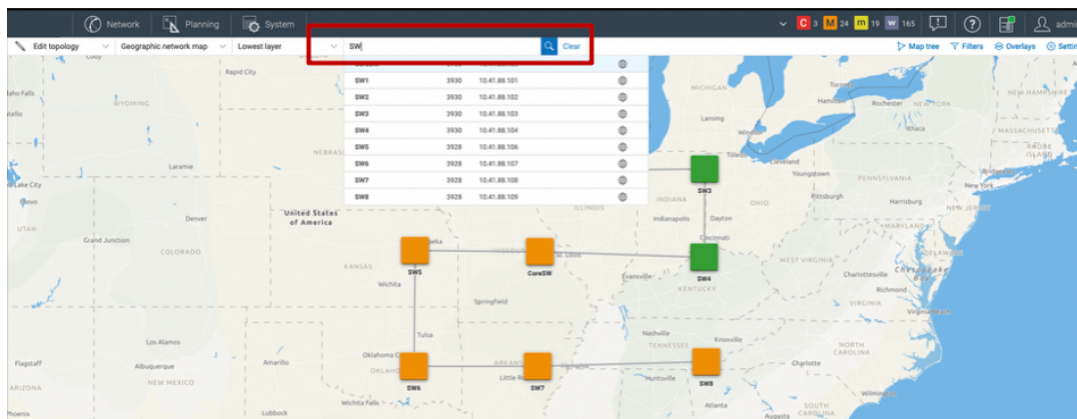
1. Select an NE on the map and click the select Edit Topology from the map modes options (sample screen follows).



2. Enter one or more tags for the NE.



- On the map, enter the tags in the search field to search for the NE.



Task 5: De-enroll an NE

- Navigate to the Network Elements page (**Network > Network elements**).
- Select one of the enrolled NEs.
- Click More > De-enroll. Did the NE disappear from the Network Elements page?
- Navigate to the map (Network > Network map). Does the NE still appear on the map?

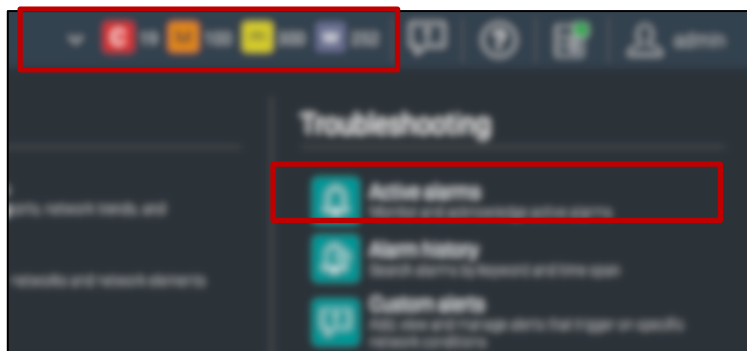
Yes ☐ No ☐

- Re-enroll the NE if necessary.

Task 6: View Alarms

The NMS UI provides Active Alarms View and Historical Alarms View. There are several ways to navigate to the Alarm screens. You can do so from the Network Map, NE details or the Dashboard.

- Notice the Alarm symbols in the upper right corner. Identify the number of Critical, Major, Minor or Warning. Clicking on one of these will take you to the Alarms and events screen filtered by the alarm severity you clicked on



2. In the Network menu, navigate to the Alarms and events page by selecting **Active alarms**.

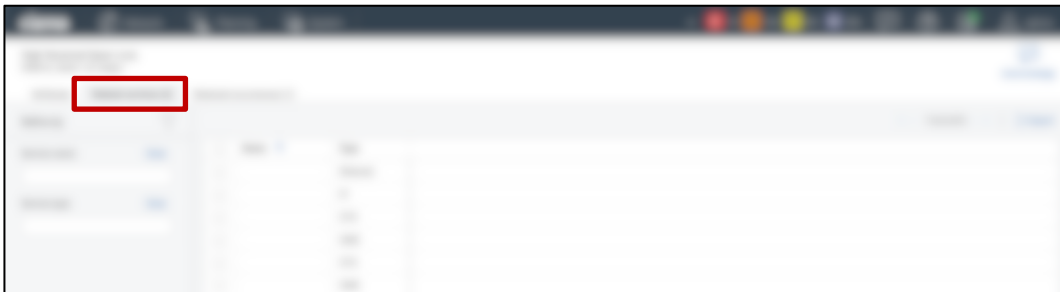
3. Select an alarm instance and identify the following:

a. Device Type and Name that raised the alarm: _____

4. Select Details or click on the description to see further details.



5. Are there related services to this alarm? _____



End of Lab

Lab 4: Network Element and Equipment Management

Objectives

After completing this activity, you will be able to:

- View Network Element Details
- View Network Element Equipment
- View All Equipment and Associated Attributes
- Place Equipment In and Out of Maintenance

Task 1: Gather Information

If necessary, divide into teams for this lab. Write down information provided by your instructor:

Network Element	Card type

Task 2: Access Network Element Details

1. Navigate to the Network Elements screen by selecting **Network > Network Elements**.
2. Select a Network Element.
3. Select **Details**. The details screen will open in a new browser window.

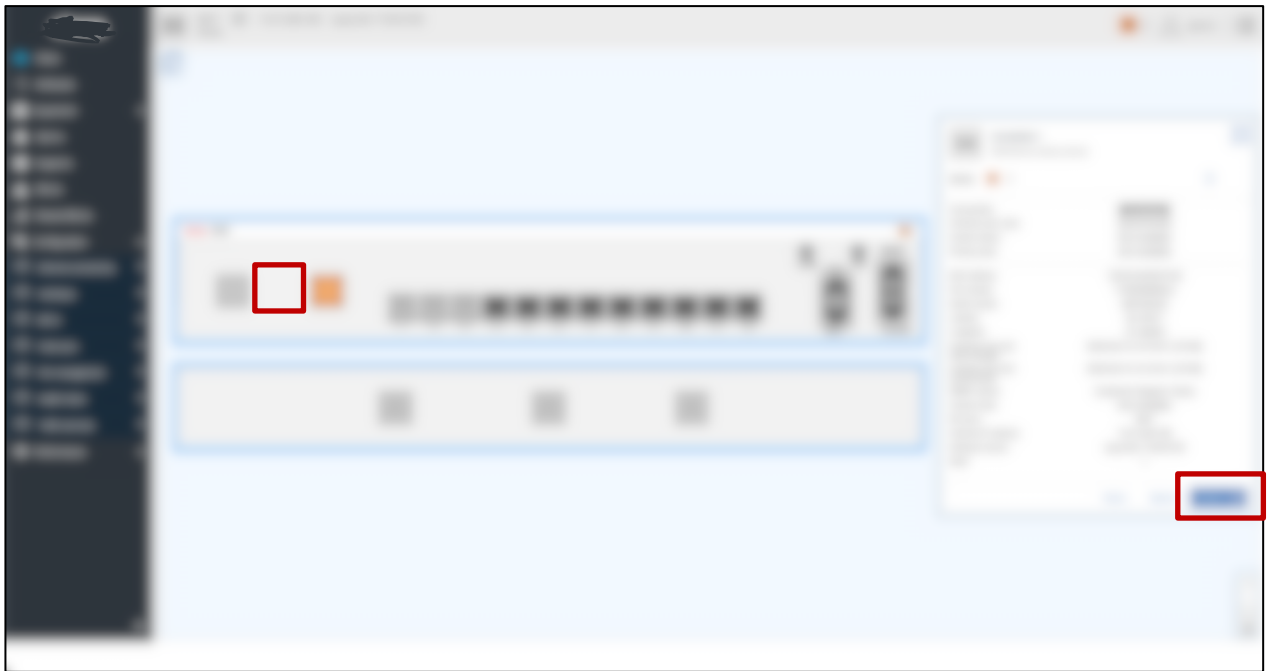
Note: You can click on the device name and the details screen will open in the same window.



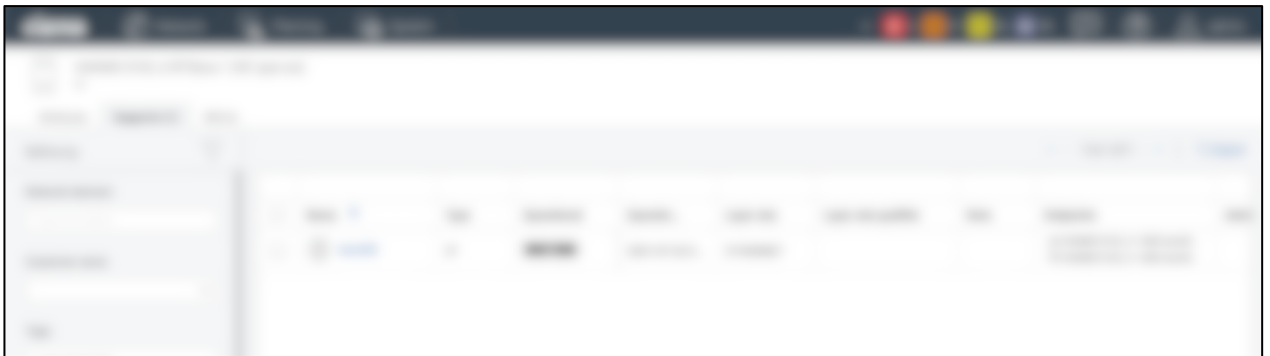
Task 3: View Port Details via Shelf Level View

1. In the NE details screen select Views on the details menu to display the shelf level view.

Note: This is the default landing page when navigating to the details page.

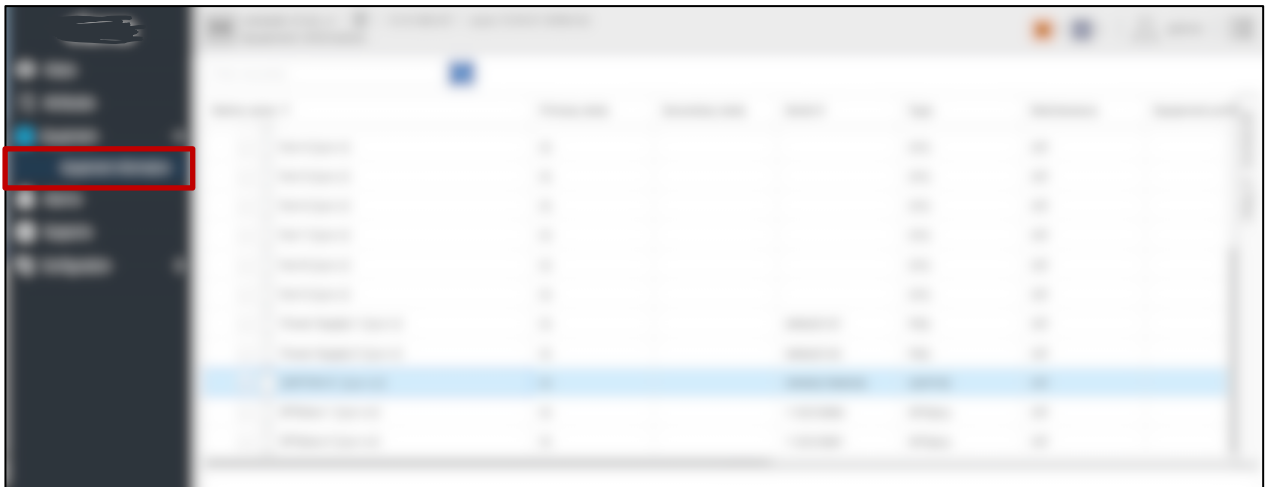


2. Select a port on the shelf level view. Information regarding the will display in the information box. What is the operational state of the port?
3. Select the Details button. Note that the operational state must be in the “Up” for the button to be active.
4. On the port details screen, select Supports. Does the device support any service?



Task 4: View the NE Equipment

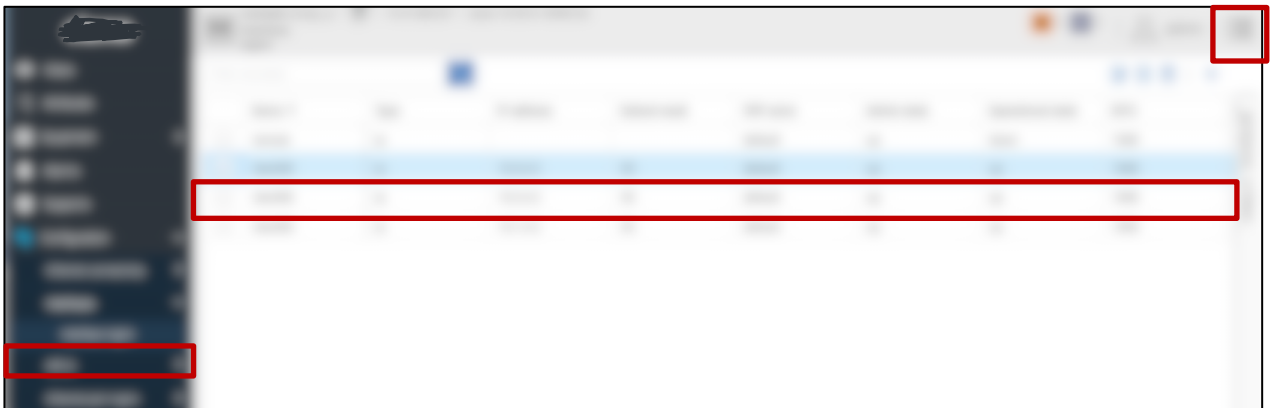
1. In the NE details screen select Equipment then Equipment Information.



2. Select a port from the equipment list. What facilities display in the lower half of the screen?

Task 5: Modify an IP Interface

1. In the NE details screen select **Configuration > Interfaces > Interface mgmt.**
2. Select an IP Interface from the list.
3. Select the edit icon.



4. Decrease the maximum transmission unit (MTU) by 10 and click **Confirm**. When complete, verify the change was made by checking MTU value in selected interface's row.

Edit interface: vlan200

Interface attributes

General attributes

Name

vlan200

IP address

10.3.4.2

Subnet mask

30

MTU

1500

Description

L2 forwarding domain

VLAN type

tagged

VLAN id

200

Port

41

Forwarding domain

vlan200

Admin state

up

LDP

Associate LDP

false

ISIS

Associate ISIS

true

Instance

1

Level

level-1-2

Interface type

broadcast

LSP interval (msec)

33

LSP re-transmit interval (sec)

5

IPv4 unicast default disable

false

LDP/IGP sync level

Padded-hello

true

BFD enable

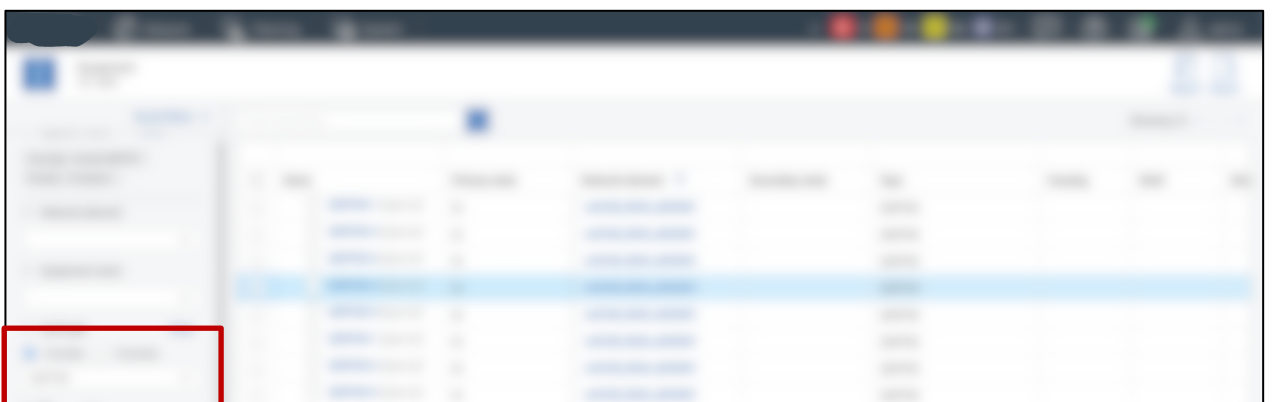
true

Cancel

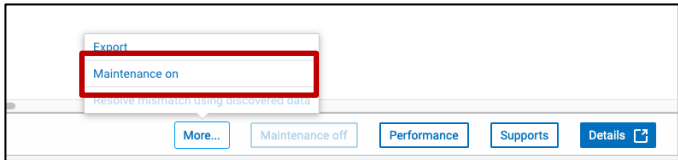
Confirm

Task 6: Maintenance Mode

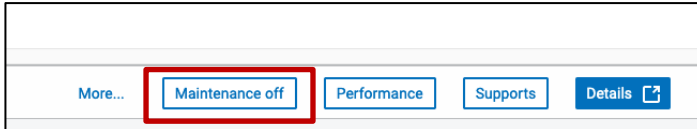
1. Navigate to the Equipment screen by selecting **Network > Equipment**.
2. Filter the list by selecting the card type provided by your instructor from the dropdown list on the left side of the screen.



3. Select the card provided type your instructor.
4. Select **More > Maintenance on**.



5. Click on **Confirm**. No provisioning can be performed while equipment is in Maintenance Mode. The Maintenance Mode button will now be active (you may need to refresh your browser).



6. Place the card out of maintenance by clicking on **Maintenance off** and then **Confirm**.

End of Lab

Lab 5: Network Element Backup

Objectives

After completing this activity, you will be able to:

- Backup a Network Element (NE) immediately
- Schedule a Backup for Network Elements (NEs)

Task 1: Gather Information

Fill in the table below with information from the Engineering Design Plan (EDP) or information provided to you by your instructor.

NE/Shelf Name	IP Address	FTP Server IP	Username	Password

Task 2: Backup a Network Element Immediately

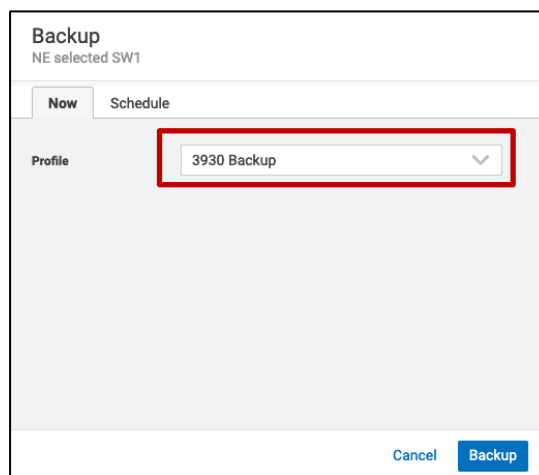
1. Login to the NAVIGATOR MC server.
2. In the Network tab, select NE operations (**Network > Network elements operations**). A sample screenshot is shown.



3. Select one or multiple network elements for which you want the data to be backed up. Click on the Backup button (sample screenshot is shown).



4. From the maintenance profile list, select the maintenance profile you want to use (sample screenshot is shown).

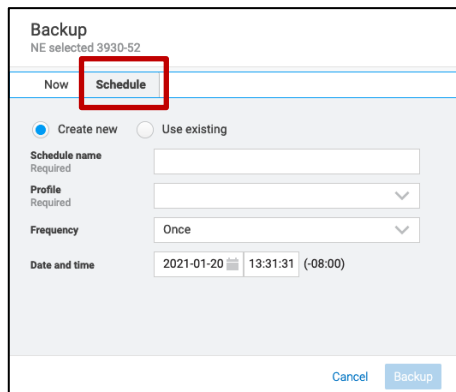


Note: If no profiles are available you need to create a maintenance profile using the Profiles tab on the NE operations screen. For the profile, specify the IP address, username, and password you get from your instructor.

5. With the profile selected, click on the Backup button. NAVIGATOR MC starts the backup.
6. When the backup status displays as Completed, then NAVIGATOR MC has created the network element backup file(s) (sample screenshot is shown).

Task 3: Schedule a Network Element Backup

1. Login to the Network Management System server.
2. In the Network tab, select NE operations (**Network > Network element operations**).
3. Just as you did in the previous task, select one or multiple network elements for which you want the data to be backed up. Click on the Backup button.
4. When the Backup screen appears, click on the Schedule tab (sample screenshot is shown).

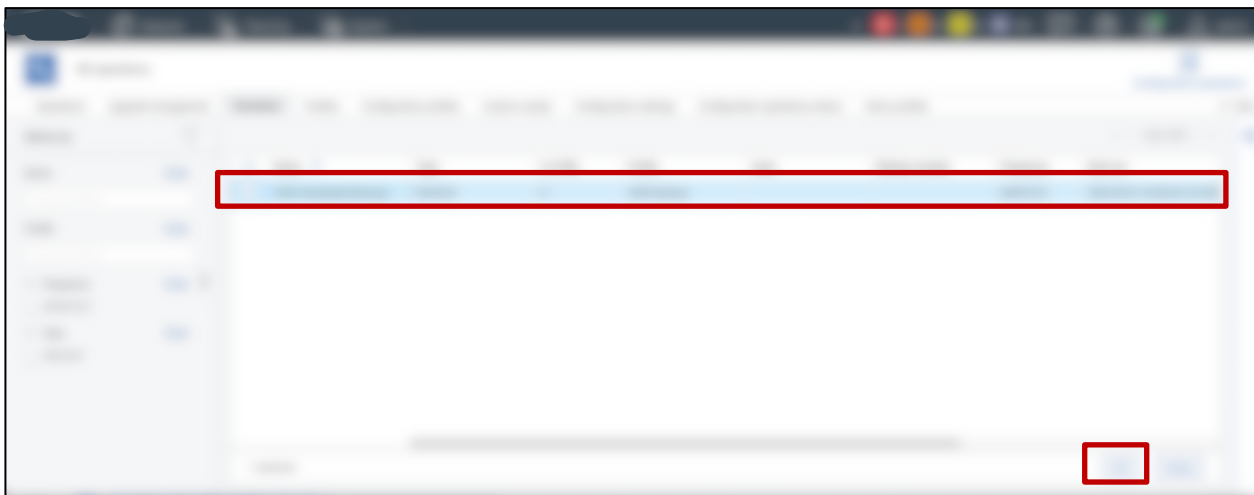
A screenshot of the 'Backup' configuration window in a network management system. The window title is 'Backup' with a subtitle 'NE selected 3930-52'. There are two tabs: 'Now' and 'Schedule'. The 'Schedule' tab is selected and highlighted with a red rectangle. Below the tabs, there are two radio buttons: 'Create new' (selected) and 'Use existing'. Below these are four required fields: 'Schedule name' (text input), 'Profile' (dropdown menu), 'Frequency' (dropdown menu set to 'Once'), and 'Date and time' (calendar and time picker set to '2021-01-20 13:31:31 (-08:00)'). At the bottom right are 'Cancel' and 'Backup' buttons.

5. Fill out the form:
 - Specify Create new (default) to create a new schedule.
 - Select a Backup profile (use the same profile from the previous task).
 - Specify the default Frequency (Once).
 - Specify a Start date in the near future.
 - Specify a start time in the Run at field.

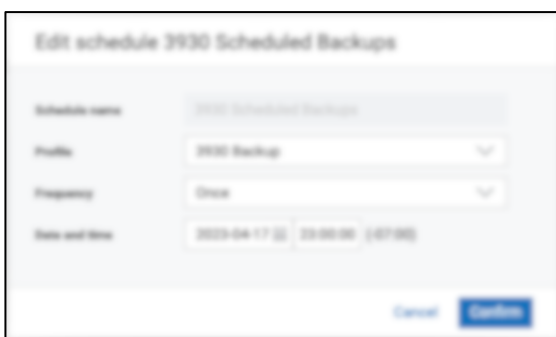
NOTE:

The time is in HH:MM (24 hours) format and considers the user's machine's local time zone.

6. Click Schedule. The scheduled backup appears on the Schedule tab of the NE operations screen (sample screenshot is shown).



7. Select the scheduled backup and click Edit. The Edit schedule screen appears (sample screenshot is shown).



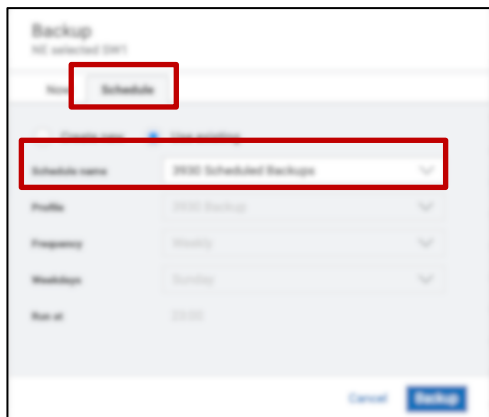
8. Change the schedule frequency from Once to Weekly, specify one or more days of the week. Enter a and click Confirm.

NOTE:

The time is in HH:MM (24 hours) format and considers the user's machine's local time zone.

Now, we'll apply the edited schedule to a different NE.

9. From the NE operations screen, select an NE. Don't select the same NE you selected before – use a different one.
10. Click the Backup button.
11. Click the Schedule tab.
12. On the Schedule tab, select Use existing (sample screenshot is shown).



13. In the Schedule name drop down list, select the schedule you just edited.

14. Click Backup.

End of Lab

Lab 6: Provisioning a Static Unprotected MPLS-TP Tunnel

Check list

- Lab drawing (review)
- Supported equipment
- Endpoint and intermediate NEs have been commissioned with the necessary loopback interfaces required at each MPLS node, and the IP interfaces associated with a VLAN and associated port on each node, as well as Bidirectional Forwarding Detection (BFD) profiles and/or Alarm Indication Signal (AIS) profiles.
 - BFD profiles are used for establishing sessions between tunnel endpoints for detecting failures along the path.
 - AIS profiles are used for fault detection and protection switching at the endpoints and transit nodes along the path.
- Endpoint and intermediate NEs are enrolled in Network Management System

Objectives

After completing this lab, you will be able to:

- Launch the Network Management System GUI
- Connect to appropriate Network Elements via the Network Management System GUI
- Provision a static unprotected MPLS-TP tunnel

Task 1: Gather Information

Your instructor will provide you with the names of the two endpoint NEs on the unprotected MPLS-TP tunnel, as well as the slot and port numbers on the NEs.

Your hardware and network configuration will determine what types of modules you have on NEs and their positions in the NEs.

Fill in the table below with information from your instructor.

NE Tunnel Endpoint 1	Slot/Port on endpoint 1	NE Tunnel Endpoint 2	Slot/Port on endpoint 2	Assigned Bandwidth	Booking Factor

Lab Diagram (may not match the lab you are using)



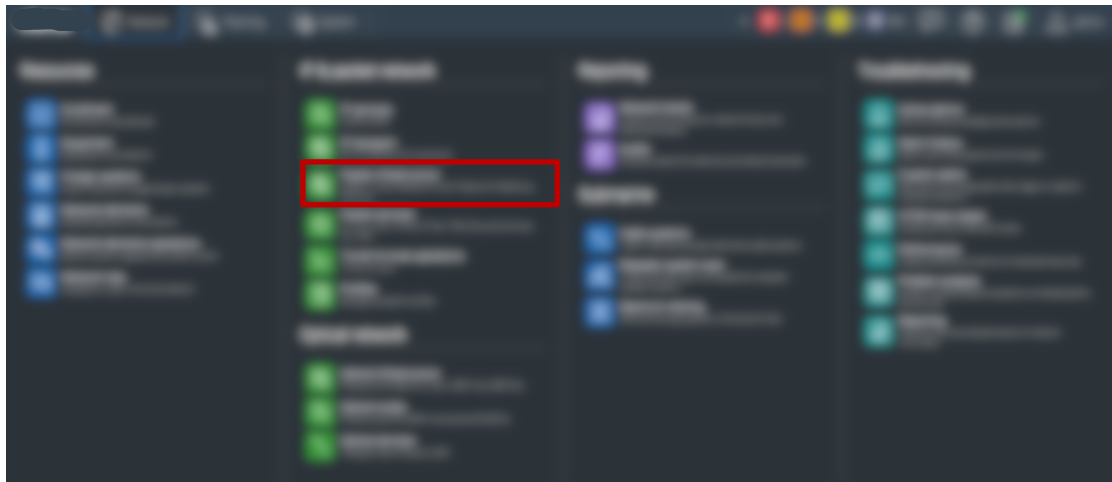
Task 2: Locate Endpoints

1. From the Network Management System menu bar, select **Network > Network elements**.
2. Select one of the NEs that will provide an endpoint for the tunnel, display Details, and locate the circuit pack and port that will act as one of the endpoints on the shelf-level view.
3. Repeat the procedure for the other endpoint.

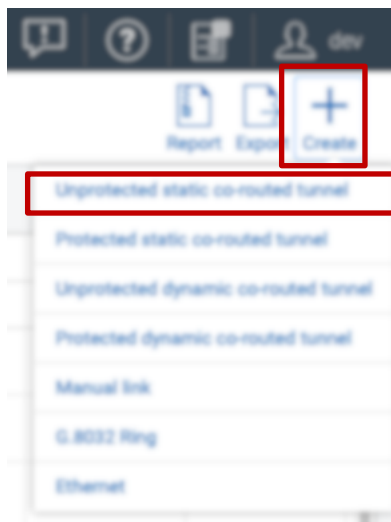
Task 3: Provision the Static Unprotected MPLS-TP Tunnel

We are going to provision an unprotected static MPLS-TP tunnel between two endpoints. Use the information you gathered above to complete the following procedure.

1. In the Network menu, select **Packet infrastructure**.



2. Select Create (+) and Unprotected static co-routed tunnel.



3. Enter the following information (refer to the screenshot below):

- Enter a name (leave the Label field blank).
- Enter a Customer name in the Customer field.
- Select Provision time “Now”.

NOTE:

When selecting a provision time, the time is in HH:MM (24 hours) format and considers the user’s machine’s local time zone.

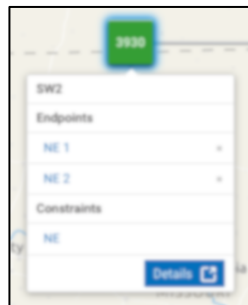
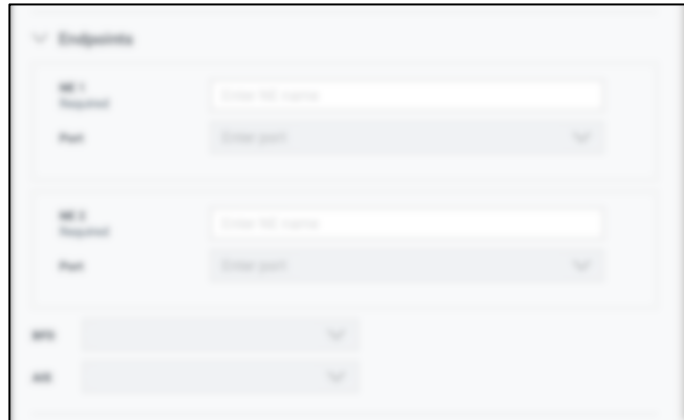
- Select Deletion time “Never”.
- You have an option to add a note. Simply click on the check box next to “Add Note”, a popup window appears, and the end user can then add a note



4. Identify the end points, fill in the information required for the “Endpoints” field, and select a BFD profile. Ignore AIS unless your instructor tells you otherwise.

NOTE:

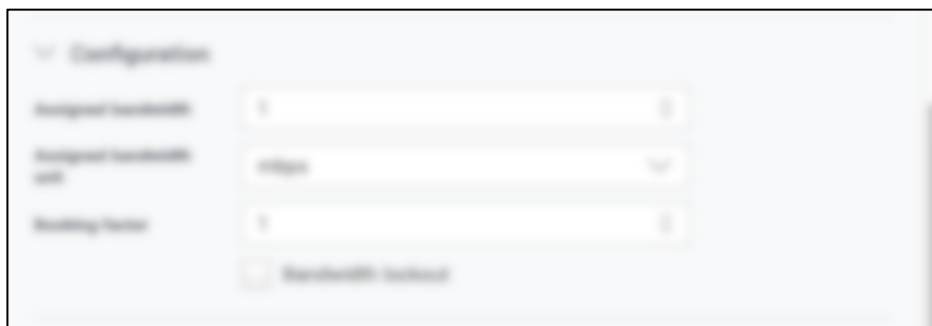
Bidirectional Forwarding Detection (BFD) is used to detect faults between connected switches and can only be used for static tunnels. It is required for tunnel failover.



You can enter the endpoint NEs by either typing the name of the NE in the text area or selecting an NE on the map and assigning it an endpoint.

5. Fill in the information required for the “Configuration” fields:

- Assigned bandwidth
- Assigned bandwidth unit
- Booking factor



NOTE:

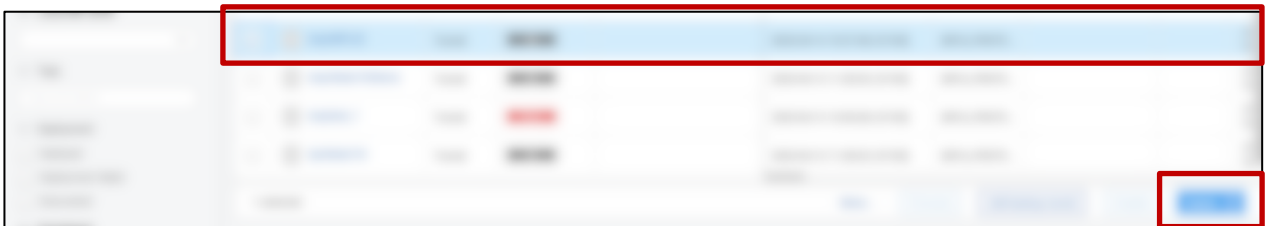
The booking factor is an integer multiplier of the assigned bandwidth that can be assigned to provide Excess Information Rate (EIR). This result is the maximum reservable bandwidth for the tunnel. A

booking factor of one means the maximum bandwidth is equal to the assigned bandwidth. The assigned bandwidth is the Committed Information Rate (CIR). A booking factor of 2 means the amount of EIR is equal to the amount of CIR, so the maximum reservable bandwidth for that tunnel is twice the assigned bandwidth value. If we set the booking factor to a value of two the maximum reservable bandwidth would be 2 gigabits per second.

- Under “Constraints”, set up the route by selecting one or more intermediate NEs between the endpoints. You can select the NE directly on the map or by entering the NEs name. Once you have completed filling in these parameters, click on “Calculate routes.” Network Management System will select up to five route options, select a route then click on “Submit”.



- Return to the “Packet infrastructure” window and identify the new static MPLS-TP tunnel just provisioned. Notice that the Deployment value is “Deployed” as opposed to Discovered.
- Select the tunnel and click Details to view tunnel details. Navigate from one “details” tab to another to view all the details. Is the tunnel operational?



Task 4: Add Backup Tunnel

Now we will add a backup tunnel to our unprotected MPLS tunnel.

Note: This is available to static tunnels created via Network Management System. If the unprotected tunnel was discovered, it must first be promoted before attempting this operation.

- On the Packet Infrastructure screen select the unprotected tunnel.

2. Select **Add backup tunnel**.



3. Provide a name for the backup tunnel.
4. For our purposes we will let Network Management System configure the endpoints so leave those blank. Additionally, we don't need to add any constraints.
5. Select **Calculate Routes**.
6. Select **Submit**.

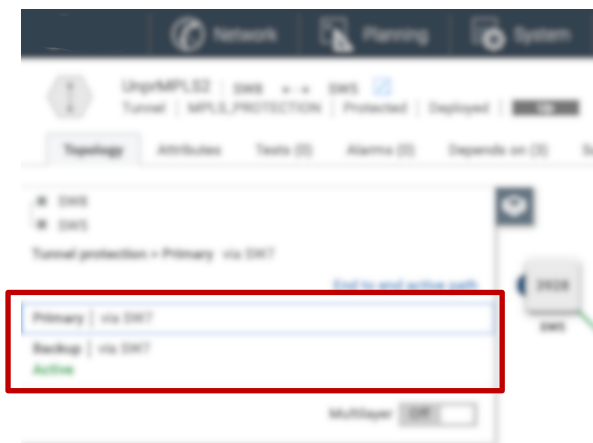
Task 5: Switch to Backup Tunnel

In this task you will switch over to the backup tunnel.

1. On the Packet Infrastructure screen select the unprotected tunnel.
2. Select **Details**.
3. Select **Switch Tunnel**.



4. On the confirmation box, select **Confirm**. If successful, the backup path will now show as active.

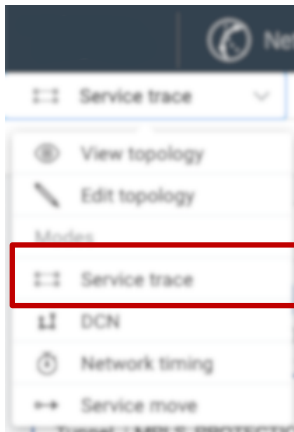


5. Select **Switch tunnel** to return to the primary path.

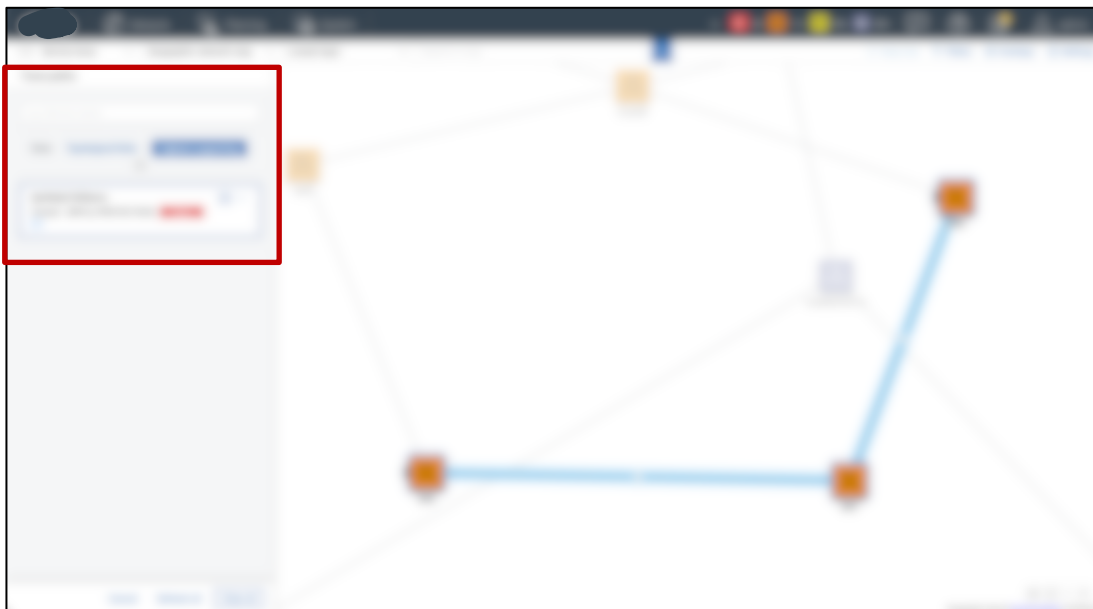
Task 5: View Service on Map

In this task you will switch over to the backup tunnel.

1. Navigate to the Network Map.
2. On the menu bar select Service Trace from the drop down.



3. Search for the service on the Trace paths overlay.
4. The map will highlight and center on the service.



End of Lab

Lab 7: Provisioning an Ethernet Virtual Private Line (EVPL) Service

Check list

- Lab drawing (review)
- Supported equipment
- EPL endpoints are enrolled in Network Management System
- MPLS-TP tunnel available for use by the EPL service (can be the same tunnel provisioned in one of the previous exercises or another tunnel available in the lab)

Objectives

After completing this lab, you will be able to:

- Launch the Network Management System GUI
- Connect to appropriate Network Elements via the Network Management System GUI
- Provision an EPL service

Task 1: Gather Information

Your instructor will provide you with the names of the two endpoint NEs for the EPL service, and slot/port information.

Fill in the table below with information from your instructor.

NE EPL Endpoint 1	Slot/Port on Endpoint 1	NE EPL Endpoint 2	Slot/Port on Endpoint 2

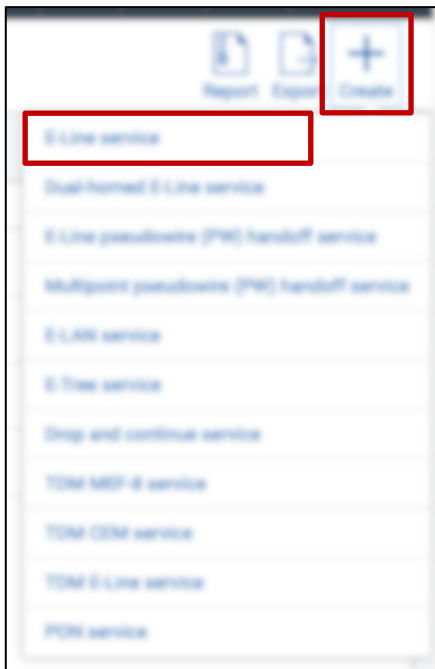
Task 2: Locate Endpoints

1. From the Network Management System menu bar, select **Network > Network elements**.
2. Select one of the NEs that will provide an endpoint for the EPL service, display Details, and locate the circuit pack and port that will act as one of the endpoints.
3. Repeat the procedure for the other endpoint.

Task 3: Provision an EVPL Service

We are going to provision a simple EVPL service on top of the MPLS-TP tunnel provisioned in one of the previous lab exercises (or another MPLS-TP tunnel available in the lab).

1. Select Network and, under Services, select Packet services.
2. Select “+ Create” and select “E-Line service”.



3. Provide the service name; select the “Provision time” to “Now” and the Deletion time to “Never”. Ignore the Label, Customer, and Add note fields.



4. Select EVPL for the service type. Ask your instructor if you should leave the 802.1ag box checked or unchecked. If 802.1ag is checked, then a CFM service instance will be created between the endpoints. Specify CCM and MA Name values in consultation with your instructor. Ignore the Profile and Protected pseudowire fields. Core SVID can be explicitly provided instead of using auto calculated core SVID by system.

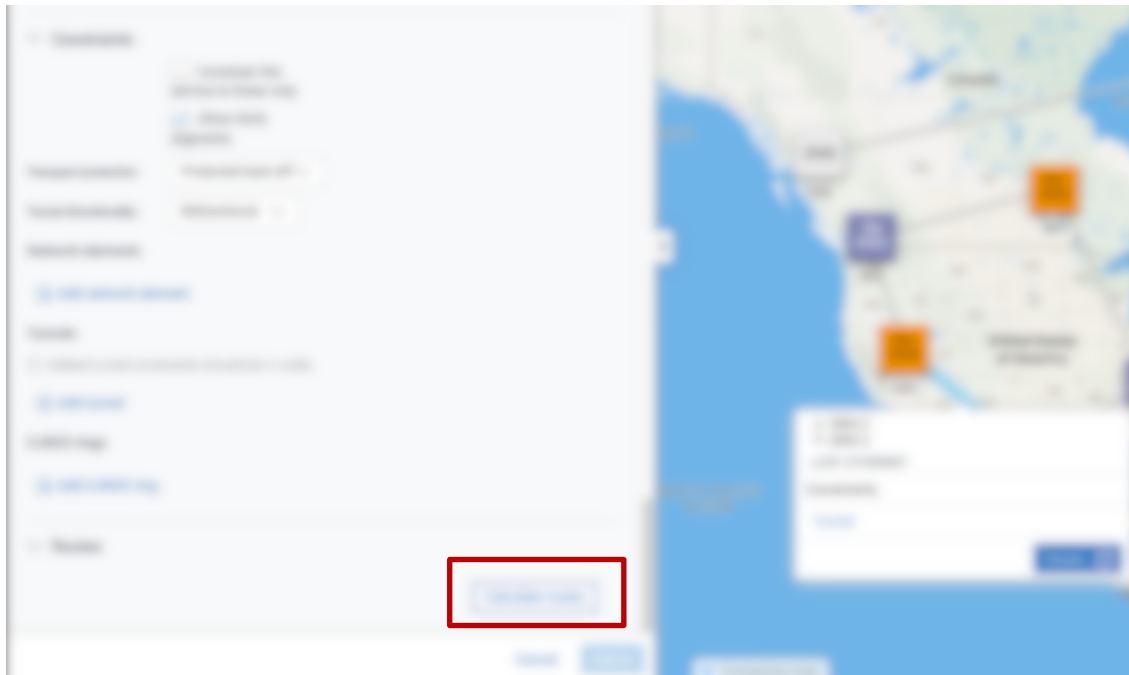
Note: Refer to **Appendix A** for more information on configuring 802.1ag.

5. Identify the endpoints, and specify the following information (see image on next page):
 - Endpoint type – Accept the default (UNI) for the endpoint types for both endpoints.
 - NE – Specify the EVPL endpoint NEs you wrote down prior to this procedure.
 - Port - Specify the EPL endpoint ports you wrote down prior to this procedure.
 - Profile – Leave blank.
 - VID - Sets the configuration of the endpoint Customer Edge VLAN ID (CVID). Select CVID.
 - CVID – Select a VLAN ID for the service endpoint as appropriate for the configured service / endpoint. The tag can a specific value or range (that is, 1, 3-5).
 - Skip over the Ingress CoS policy fields.
 - If you enabled 802.1ag previously, enter information in the 802.1ag fields in consultation with your instructor.

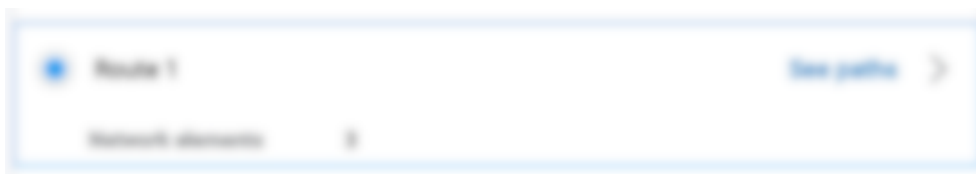


6. Under Constraints:
 - a. Skip over the following fields:
 - Constrain the service to linear only
 - Allow QinQ segments
 - Transport protection
 - Tunnel directionality
 - Network elements

Select Add tunnel and then select the MPLS-TP tunnel you provisioned in one of the previous exercises (or another available tunnel). Specify Include for the tunnel. The EVPL service will use the MPLS-TP tunnel as the network transport.



7. Click Calculate routes. Select the route associated with the MPLS-TP tunnel.
8. NAVIGATOR MC provides up to 5 route options. Click [see paths] to view the details of a route. Select a route and click on "Submit". NAVIGATOR MC sends the necessary commands to the end nodes and all transit nodes in the calculated path to configure the service.



9. Click close to return to the packet services screen where our new service is now listed.
10. Select the new service and click Details. Navigate from one detail tab to another to view all the service details. Is the service operational?

End of Lab

Lab 8: Provisioning an Ethernet Virtual Private LAN (EVP-LAN) Service

Check List

- Lab drawing (review)
- Supported equipment
- MPLS tunnel(s) for the infrastructure (suggest you use tunnels created earlier in the class)

Objectives

After completing this lab, you will be able to:

- Launch the NAVIGATOR MC GUI
- Connect to appropriate Network Elements via the NAVIGATOR MC GUI
- Provision an EVP-LAN service between three endpoints

Task 1: Gather Information

Your instructor will provide you with the names of three endpoint NEs for the EP-LAN service, and slot/port information.

Fill in the blanks below with information from your instructor.

NE EVP-LAN endpoint 1	Slot/Port on endpoint	NE Tunnel Endpoint
Endpoint 1		
Endpoint 2		
Endpoint 3		

Task 2: Locate Endpoints

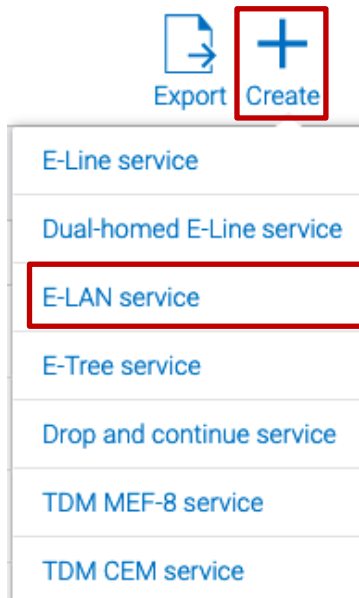
1. From the NAVIGATOR MC menu bar, select **Network > Network elements**.
2. Select one of the NEs that will provide an endpoint for the EVP-LAN service, display Details, and locate the circuit pack and port that will act as one of the endpoints.
3. Repeat the procedure for the other endpoints.

Task 3: Provision an EVP-LAN Service between Two of the Endpoints

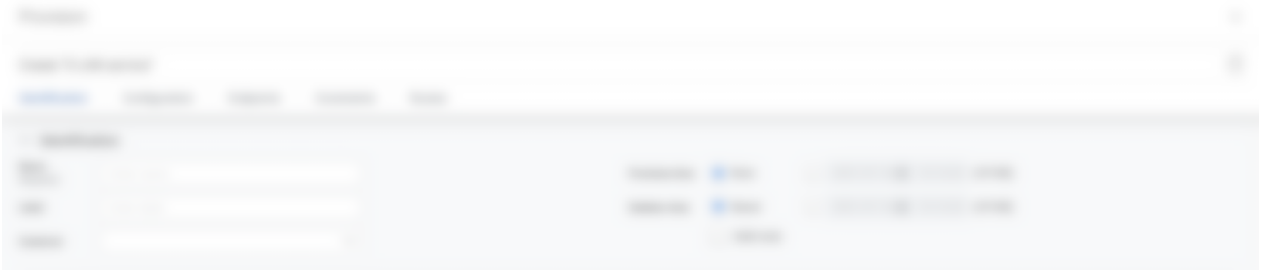
We are going to provision a simple EVP-LAN service on top of MPLS tunnel(s) (either provisioned during this lab or other available tunnels). We'll start by provisioning the first two endpoints. Then, we'll add the third endpoint.

1. From the NAVIGATOR MC menu bar, select **Network > Packet services**.

2. Select “+ Create” and select E-LAN service.

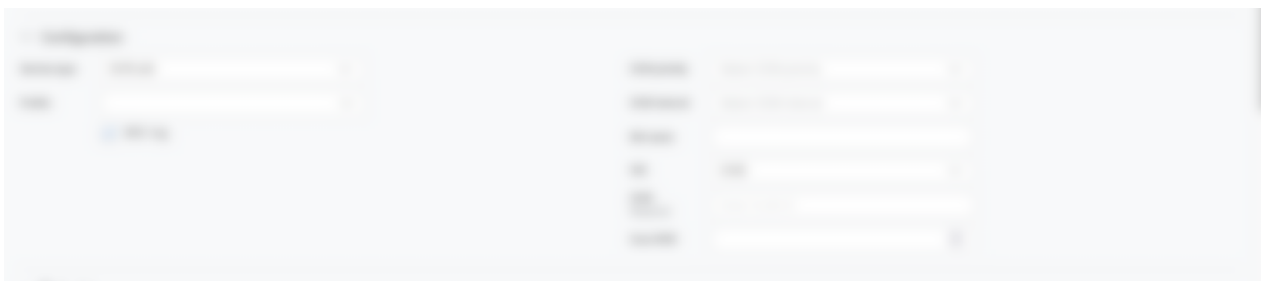


3. Provide the service name; select the “Provision time” to “Now” and the Deletion time to “Never”. Ignore the Label, Customer, and Add note fields Provide the service name.



4. Select EP-LAN for the service type. Ask your instructor if you should leave the 802.1ag box checked or unchecked. If 802.1ag is checked, then a CFM service instance will be created between the endpoints. Specify CCM and MA Name values in consultation with your instructor. Ignore the Profile field. If 802.1ag is checked, then a CFM service instance will be created between the endpoints. .

Note: Refer to **Appendix A** for more information on configuring 802.1ag.



5. Identify two of the EVP-LAN endpoints, and specify the following information:
 - Endpoint type – Accept the default (UNI) for the two endpoints.
 - NE – Specify two of the endpoint NEs you wrote down prior to this procedure.
 - Port - Specify the two endpoint ports you wrote down prior to this procedure.
 - Profile and L2 control frame tunneling – Leave blank.
 - Skip over the Ingress CoS and Bandwidth management fields.
 - If you enabled 802.1ag previously, enter information in the 802.1ag fields in consultation with your instructor.



6. Skip Constraints.
7. Select “Calculate routes”.



8. Select a route and click on “Submit”.
9. Wait for verification from your Instructor.

Task 4: Add the Third Endpoint to the EVP-LAN Service

We’re now going to add the third endpoint to the EVP-LAN service.

1. In the NAVIGATOR MC UI select **Network > Packet services**.

2. From the list of Packet services, select the EVP-LAN service to which you are adding an endpoint. The EVP-LAN service must be in a Deployed state before you can successfully add a new endpoint.
3. Click the Add endpoint button at the bottom of the page.



4. Enter information that will identify this endpoint:
 - Specify Endpoint type.
 - Enter an NE name.
 - Select a port.
 - If your instructor asks you to do so, enable 802.1ag and enter information in the 802.1ag fields.
 - Skip all other fields.
5. Click Submit. The endpoint is added to the EVP-LAN service.
6. To view all three EVP-LAN endpoints you added, select the EVP-LAN service that you modified on the Packet services page and click Details. All three endpoints will appear in the Topology view.

End of Lab

Lab 9: Viewing and Troubleshooting Provisioned Services and Infrastructure

Check List

- Lab drawing (review)
- Tunnels and packet services provisioned on enrolled NEs

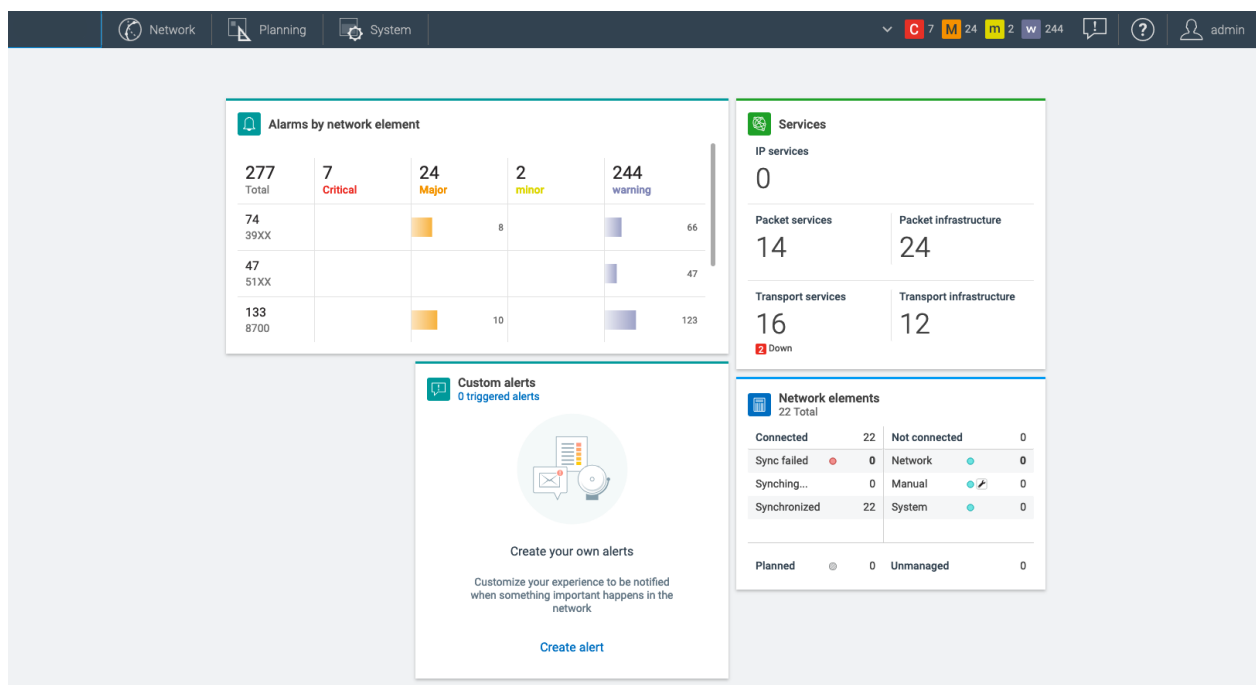
Objectives

After completing this lab, you will be able to:

- Identify problems with services and infrastructure on the Dashboard
- View service and infrastructure topology, attributes, alarms, and dependencies
- Perform an LSP ping and LSP traceroute
- Perform a pseudowire ping and pseudowire traceroute

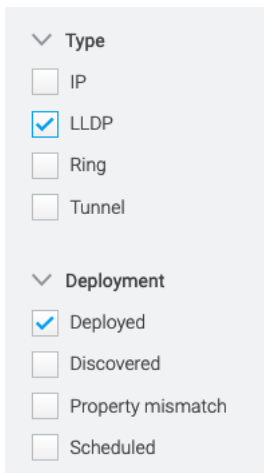
Task 1: Identify Problems on the Dashboard

1. Login to the Network Management System Server.
2. Does the Dashboard indicate problems with packet services and/or infrastructure, similar to the sample Dashboard that follows?



Task 2: View Tunnel Topology, Attributes, Alarms, and Dependencies

1. Login to the Network Management System server.
2. At the Dashboard, click on the Packet infrastructure link.
3. On the Packet infrastructure page, filter on Tunnel and also filter on Deployed. Do you see any of the tunnels provisioned during the lab?



A filter panel with two sections: 'Type' and 'Deployment'. The 'Type' section has four options: IP, LLDP (checked), Ring, and Tunnel. The 'Deployment' section has four options: Deployed (checked), Discovered, Property mismatch, and Scheduled.

Type
☐ IP
☒ LLDP
☐ Ring
☐ Tunnel

Deployment
☒ Deployed
☐ Discovered
☐ Property mismatch
☐ Scheduled

4. Select a tunnel.
5. Click the Details button. The Topology view appears by default. You'll see two graphical topology diagrams: the top view and the bottom or subway view.



- 6. On the top view, click on the various elements of the diagram from left to right. Where do you see the Sync status?
- 7. On the subway view, can you get component (module) details? Yes ☐ No ☐
- 8. Click the Attributes tab.
- 9. Can you identify the endpoints?
- 10. Click the Alarms tab. Do you see any alarms? If you don't see any alarms, try finding a tunnel that has alarms, such as one that is Down or Degraded.
- 11. If you can see alarms, select an alarm and click the Export button to export alarm data. Then, get details for the alarm.
- 12. Click on the Depends on tab. Do you see the IP/Ethernet link(s) that the tunnel depends on (see the example below)?

Alarms (0) Depends on (1) Supports (6)			
<< < 1 to 1 of 1 > >>			
☐	Name ↑	Type	Operational
☐	 if20_217,if8_217	IP	Up

Task 3: View G.8032 Ring Topology, Attributes, Alarms, and Dependencies

1. Login to the NAVIGATOR MC server.
2. At the Dashboard, click on the Packet infrastructure link.
3. On the Packet infrastructure page, filter on Ring. Optionally, filter on Ring type (Major and/or Sub ring).

Type

☐ IP
 ☐ LLDP
 ☐ Ring
 ☐ Tunnel

Deployment

☐ Discovered

Ring type

☐ Major
 ☐ Sub ring

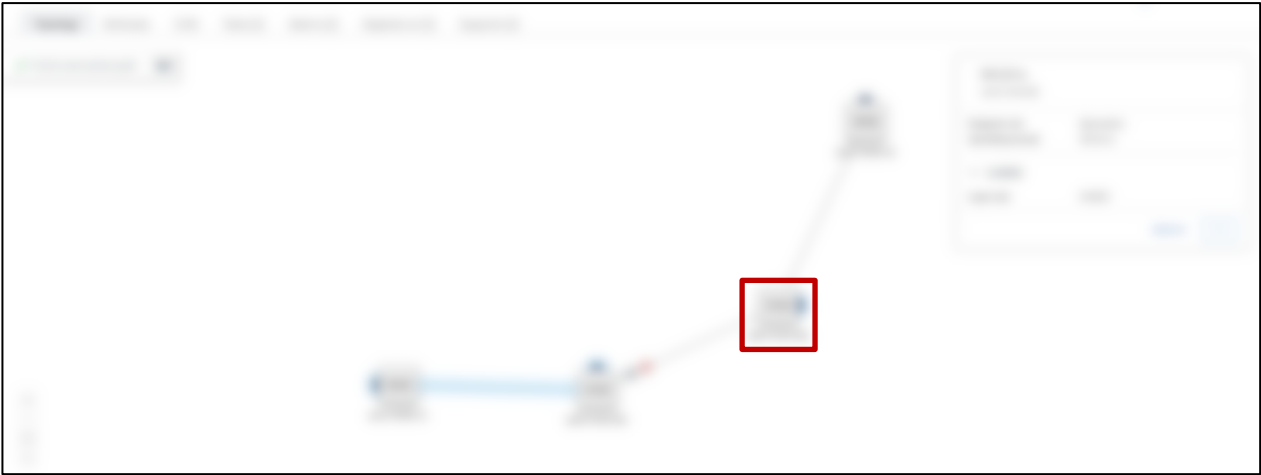
4. Select a G.8032 ring and click the Details button.
5. In the Topology view, look at both the Configured working view and the Configured RPL view. Do you see a subway view for both Configured working and Configured RPL?



6. In both the Configured working and Configured RPL views, click on each link in the ring and review the attributes (example for the Configured working view follows).



7. Click on each ring endpoint and review the attributes (sample endpoint shown).



8. Review the other tabs for the ring.



VR-221s | 4 endpoints 

Ring | G.8032 | Protected | Discovered | Sub ring | Complete

Topology

Attributes

CCM

Tests (0)

Alarms (0)

Depends on (3)

Supports (0)

Task 4: View Service Topology, Attributes, Alarms, and Dependencies

1. Login to the Network Management System server.
2. Navigate to the Packet services page (**Network > Packet services**).
3. Filter on EVC and also filter on Deployed. Do you see any of the services provisioned during the lab?.
4. Select a Packet service and click Details.
5. Is the first view the topology view of the service? Yes ☐ No ☐
6. Do you get a top view and a subway view? Yes ☐ No ☐
7. Click the Attributes tab.
8. Can you identify the endpoints?
9. Click the Alarms tab. Do you see any alarms? If you don't see any alarms, try finding a service that has alarms, such as one that is Down or Degraded.
10. If you can see alarms, select an alarm and export alarm data. Then, get details for the alarm.
11. Click on the Depends on tab. Do you see the tunnel the packet service depends on (see the example below)?

Pseudowires Performance Tests (0) Alarms (1) Depends on (6)					
☐	Name 	Type	Operational	Operatio...	Layer ra
☐		LLDP		2020-12-17T0...	ETHER
☐		LLDP		2020-12-17T0...	ETHER

3.

Task 5: Test a Tunnel with LSP Ping and LSP Traceroute

1. Login to the NAVIGATGOR MC server.
2. Navigate to the Packet infrastructure page (**Network > Packet infrastructure**).
3. Filter on Tunnel, select a tunnel, and click Details.

- Click the Test button (example of the screen that appears follows).

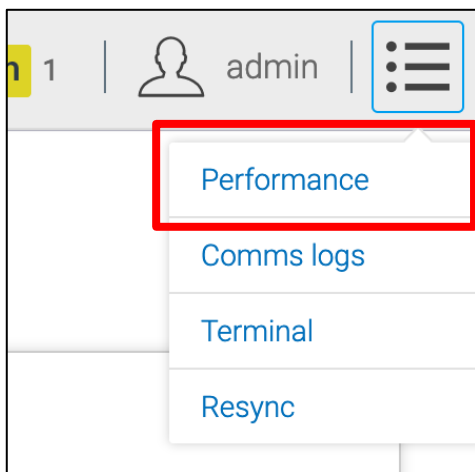


- Select LSP ping.
- In the Local point drop-down, select one of the tunnel endpoints. The Remote point field auto-populates with the other endpoint.
- Click Test. Did the ping succeed or fail?
- Scroll down and examine the raw data.
- Click Close until you return to the tunnel details.
- Click the Test button.
- Select LSP traceroute.
- In the Local point drop-down, select one of the tunnel endpoints. The Remote point field auto-populates with the other endpoint.
- Click Test. Did the traceroute succeed or fail?
- Scroll down and examine the raw data.



Task 6: Use the Performance Monitoring Browser

1. Login to the Network Management System server.
2. Navigate to the Network elements page (**Network > Network elements**).
3. Select an NE and click Details.
4. Click the hamburger icon in the upper right-hand corner of the screen.
5. Select Performance from the dropdown list.



6. Browse 15-minute and 24-hour measurements.
7. Can you create custom time ranges?

Task 7: Test a Service with Pseudowire Ping and Pseudowire Traceroute

8. Login to the NAVIGATOR MC server.
9. Navigate to the Packet services page (**Network > Packet services**).
10. Filter on EVC, select a packet service, and click Details.
11. Click the Depends on button to verify that the service depends on an MPLS tunnel.

12. Click the Test button (example of the screen that appears follows).



13. Select Pseudowire ping. Can you also select LSP ping for the underlying tunnel?
14. In the Local NE drop-down, select one of the NE endpoints to be the Local NE.
15. Select the pseudowire.
16. Select the segment (one segment for single-segment pseudowire; multiple segments for multi-segment pseudowire). Ignore the Encapsulation type.
17. Click Test. Did the ping succeed or fail?
18. Scroll down and examine the raw data.
19. Click Close until you return to the service details.
20. Click the Test button.
21. Select Pseudowire traceroute. Can you also select LSP traceroute for the underlying tunnel?
22. In the Local NE drop-down, select one of the NE endpoints to be the local NE.
23. Click Test. Did the traceroute succeed or fail?
24. Scroll down and examine the raw data.

End of Lab

Appendix A: 802.1ag Operations, Administration and Maintenance (OAM)

NAVIGATGOR MC supports 802.1ag for E-Line, E-LAN, and E-Tree packet services. This appendix shows some sample 802.1ag parameters and tests.

The sample Configuration screenshot shows the configuration for an Ethernet Private Line (EPL) service.

Configuration

Service type

EPL

Profile

☐ Protected pseudowire

☒ 802.1ag

CCM priority

4

CCM interval

100ms

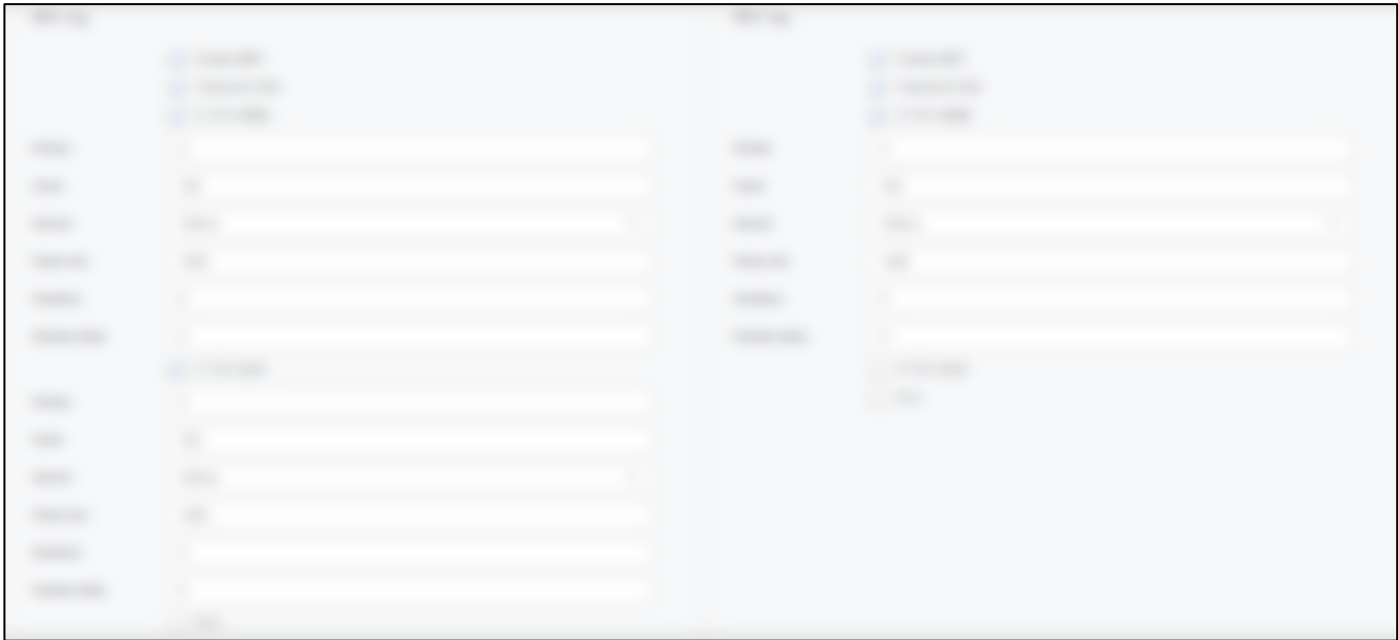
MA name

eline_svc

In this example:

- 802.1ag is enabled
- Continuity Check Message (CCM) priority is set to 4 (values are to 7 with 7 being the highest priority).
- CCM messages will be transmitted at intervals of 100 milliseconds.
- Maintenance Association (MA) name is eline_svc. This name associates the Maintenance End Points (MEPs) and any optional Maintenance Intermediate Points (MIPs) configured on intermediate ports between the endpoints.

The following example shows the 802.1ag configuration for two service endpoints.



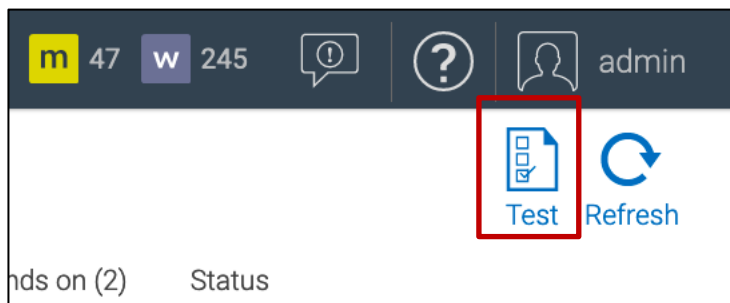
In this example:

- MEP creation is enabled on both endpoints.
- Both endpoints transmit CCMs.
- Y.1731 Delay Measurement Messages (DMMs) are enabled for both endpoints, along with associated DMM parameters (priority, loss, frame count and so on). DMMs are used to measure delay, jitter and frame loss for the service.
- Y.1731 Synthetic Loss Measurement (SLM) is enabled for one of the endpoints, and associated parameters are specified (priority, loss, frame count, etc.). SLM measures frame loss without affecting customer traffic.

When the service is deployed, you can check the 802.1ag status for the endpoints on the CCM tab. A sample CCM tab is shown here.



You run 802.1ag loopback or 802.1ag linktrace tests by clicking the Test button on the service details screen.



After you click the Test button, select 802.1ag loopback or 802.1ag linktrace.

Appendix B: Provisioning a Link Aggregation Group (LAG)

Check list

- Lab drawing (review)
- Supported equipment.
- Endpoint NEs are enrolled in NAVIGATOR MC

Objectives

After completing this lab, you will be able to:

- Launch the NAVIGATOR MC GUI
- Connect to appropriate Network Elements via the NAVIGATOR MC GUI
- Provision a LAG

Task 1: Gather Information

Your instructor will provide you with the names of the two endpoint NEs on the LAG, as well as the primary and backup slot and port numbers on the NEs.

Your hardware and network configuration will determine what types of modules you have on NEs and their positions in the NEs.

Fill in the table below with information from your instructor.

NE Endpoint 1	Primary Slots/Ports on Endpoint 1	Backup Slots/Ports on Endpoint 1	NE Endpoint 2	Primary Slots/Ports on Endpoint 2	Backup Slots/Ports on Endpoint 2

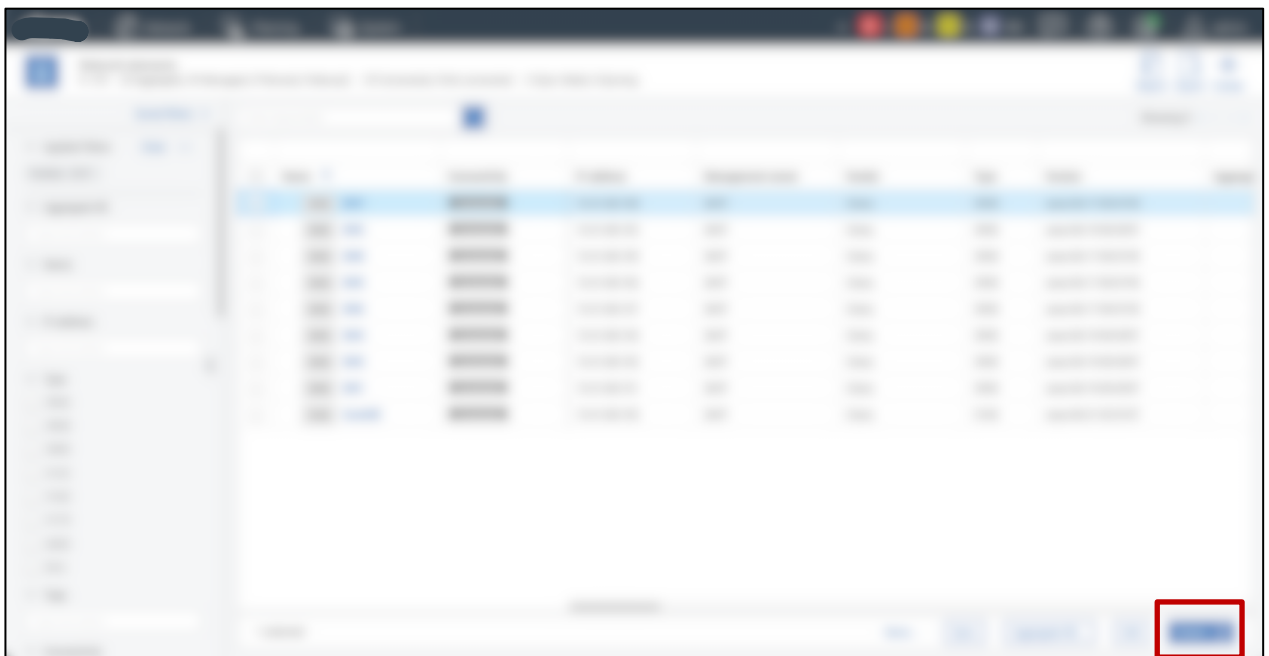
Task 2: Provisioning a LAG

We are going to provision a LAG between two NEs. Use the information you gathered above to complete the following procedure.

1. From the Network Management System menu bar, select **Network > Network elements** (sample screenshot is shown).



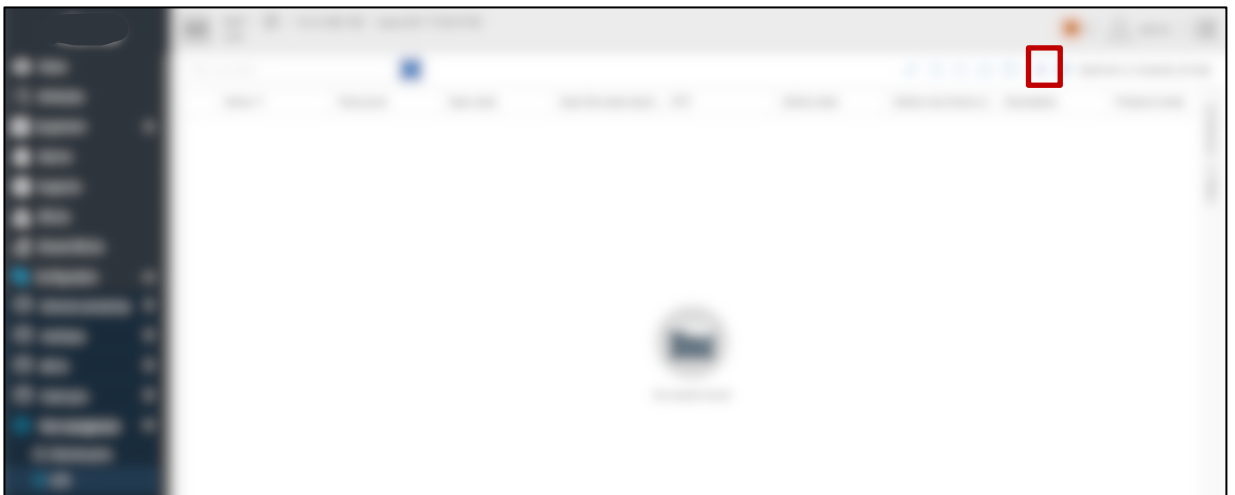
2. Select one of the NEs that will provide an endpoint for the LAG (sample screenshot is shown).



3. Click the Details button.
4. When the Details screen displays, click Configuration > Ethernet port mgmt. > LAG from the left side menu. (sample screenshot is shown).



5. The LAG screen displays. In the example below, no LAGs have been added (sample screenshot is shown).



6. Click on the + button. The + button is the create button. Provide a name for the LAG and select Confirm.
7. Select the new lag and then the edit button. The screen shown is an example. Consult your instructor for the values you should provide.

8. Enter the attributes (consult your instructor):
 - Type in a name for the LAG (e.g., LAG1).
 - Set the minimum link aggregation (e.g., on).
 - Set the minimum link threshold (e.g., 2).
 - Set the protocol mode (e.g. LACP).
 - Set the protection mode (e.g., proprietary).
 - Set the reversion delay in milliseconds (e.g., 5000).
 - Set reversion to on.
 - Set system priority (e.g., 32768).

NOTE:

System priority for the LAG applies to LAG protection and is used to determine which NE controls the Active ports on the LAG. The NE endpoint that is assigned the lower system priority value controls which LAG ports are Active. For example, if the LAG instance on one NE endpoint is set to 32768 and the LAG instance on the other NE endpoint is set to 10, then the NE endpoint assigned the system priority of 10 controls which LAG ports are Active.

9. Select the primary ports. We'll add a backup port later.
10. Click Confirm. Make sure the LAG instance appears.
11. Repeat the procedure for the other NE. Make sure that:
 - The attributes match what you entered for the other NE on the link.
 - The primary ports face the primary ports for the first NE you configured on the link.

Now, we'll add backup (protection) ports for both NE endpoints:

1. For one of the NE endpoints, navigate to the NE's shelf-level view, click on Ethernet port mgmt and then click on LAG.
2. Select the LAG you created earlier in this exercise.
3. Click the Add Ports button.

The screenshot shows a web-based configuration interface for adding ports to a LAG. The title is 'Add port: Demo LAG'. There are two main sections: 'Primary ports' and 'Backup ports'. The 'Primary ports' section has a dropdown menu. The 'Backup ports' section has a list of ports from 1 to 18, with port 12 selected. A 'Clear all' button is next to the list. A warning icon and text 'Editing may affect network' are visible. A 'Confirm' button is at the bottom right.

4. Add a backup port and click Confirm.
5. Select the LAG and click on Details and view the attributes. Make sure you see the primary and backup ports.
6. Repeat the procedure for the other NE endpoint. Make sure that the backup port you add faces the backup port on the first NE for which you added a backup port.

End of Lab

Appendix C: Provisioning a Dynamic Unprotected MPLS-TP Tunnel

Check list

- Lab drawing (review)
- Supported equipment
- Endpoint and intermediate NEs have been commissioned with:
 - The necessary loopback interfaces required at each MPLS NE, and the IP interfaces associated with a VLAN and associated port on each node
 - Bidirectional Forwarding Detection (BFD) profiles (Alarm Indication Signal (AIS) profiles not applicable for dynamic MPLS-TP)
 - An Interior Gateway Protocol (IGP) - Intermediate System to Intermediate System (ISIS) or Open Shortest Path First (OSPF) - on all NEs along the dynamic MPLS tunnel path
 - Resource Reservation Protocol with Traffic Engineering (RSVP-TE) enabled on all NEs along the dynamic MPLS-TP tunnel path
 - Label Distribution Protocol (LDP) enabled on pseudowire endpoints for dynamic pseudowires
 - NAVIGATOR MC server configured as SNMP trap destination on Label Edge Routers (LERs), so that the LERs can update NAVIGATOR MC on the status of the current dynamic tunnel path
 - Resource color groups on NEs along the tunnel paths, but this is optional (only if resource color groups are needed to constrain routes) and will not be used in this lab
- Endpoint and intermediate NEs are enrolled in NAVIGATOR MC

Objectives

After completing this lab, you will be able to:

- Launch the NAVIGATOR MC GUI
- Connect to appropriate Network Elements via the NAVIGATOR MC GUI
- Provision an unprotected dynamic MPLS-TP tunnel

Task 1: Gather Information

Your instructor will provide you with the names of the two endpoint NEs on the unprotected dynamic MPLS-TP tunnel, as well as the slot and port numbers on the NEs.

Your hardware and network configuration will determine what types of modules you have on NEs and their positions in the NEs.

Fill in the table below with information from your instructor.

NE Tunnel Endpoint 1	Slot/Port on endpoint 1	NE Tunnel Endpoint 2	Slot/Port on endpoint 2	Maximum Bandwidth	Minimum Bandwidth

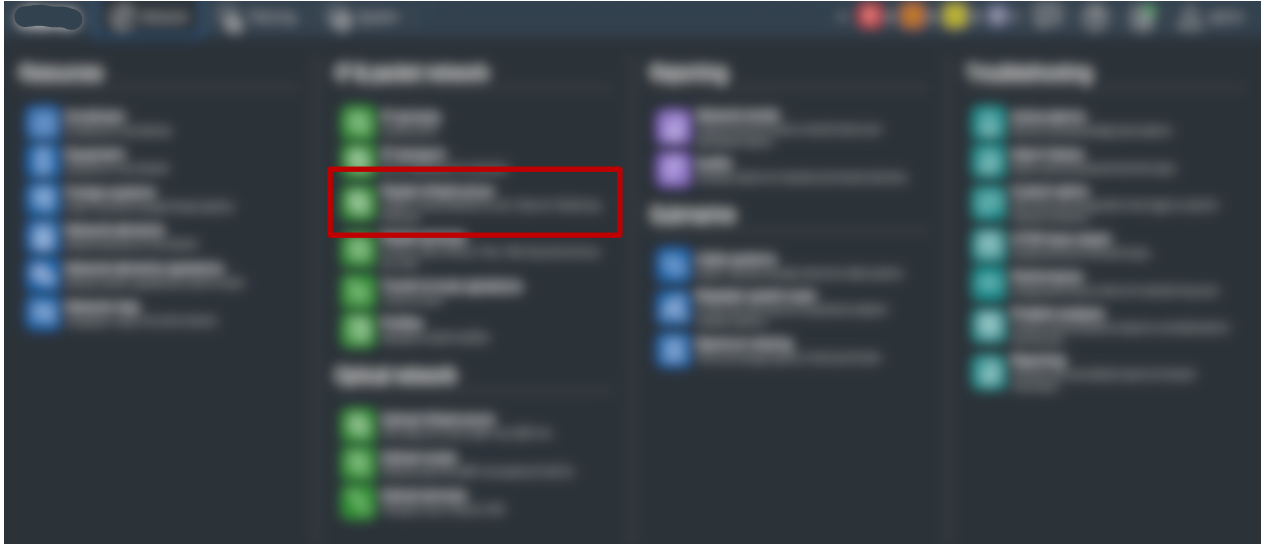
Task 2: Locate Endpoints

1. From the NAVIGATOR MC menu bar, select **Network > Network elements**.
2. Select one of the NEs that will provide an endpoint for the tunnel and display Details. Locate the circuit pack and port that will act as one of the endpoints on the shelf-level view. Unlike static tunnels, you do not need to supply the port when you provision the tunnel, but it is helpful to know how the endpoints are connected to the network.
3. Repeat the procedure for the other endpoint.

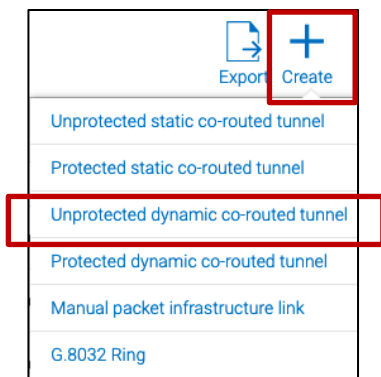
Task 3: Provision an Unprotected Dynamic MPLS-TP Tunnel

We are going to provision an unprotected dynamic MPLS-TP tunnel between two endpoints. Use the information you gathered above to complete the following procedure.

1. In the Network menu, select **Packet infrastructure**.



2. Select Create (+) and Unprotected dynamic co-routed tunnel.



3. Enter the following information (refer to the screenshot that follows):
 - a. Enter a name (leave the Label field blank).
 - b. Enter a Customer name in the Customer field.
 - c. Select Provision time "Now".
 - d. Select Deletion time "Never".
 - e. You have an option to add a note. Simply click on the check box next to "Add Note", a popup window appears, and the end user can then add a note.

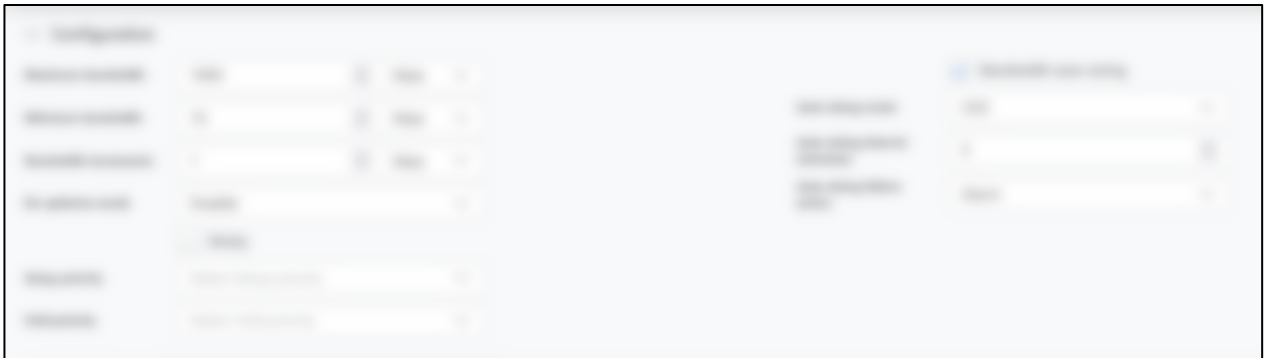
The screenshot shows the 'Identification' tab of a configuration window. At the top, there is a title bar with 'Identification' and a close button. Below the title bar, there is a breadcrumb navigation path: 'Identification' > 'Endpoints' > 'Configuration' > 'Endpoints'. The main content area is titled 'Identification' and contains several input fields: 'Name' (text input), 'Label' (text input), 'Customer' (dropdown menu), 'Provider Role' (radio buttons for 'None' and 'Provider'), and 'Subscriber Role' (radio buttons for 'None' and 'Subscriber'). There is also an 'Add roles' button at the bottom.

•

4. Identify the end points, fill in the information required for the “Endpoints” field, and select the BFD profile.

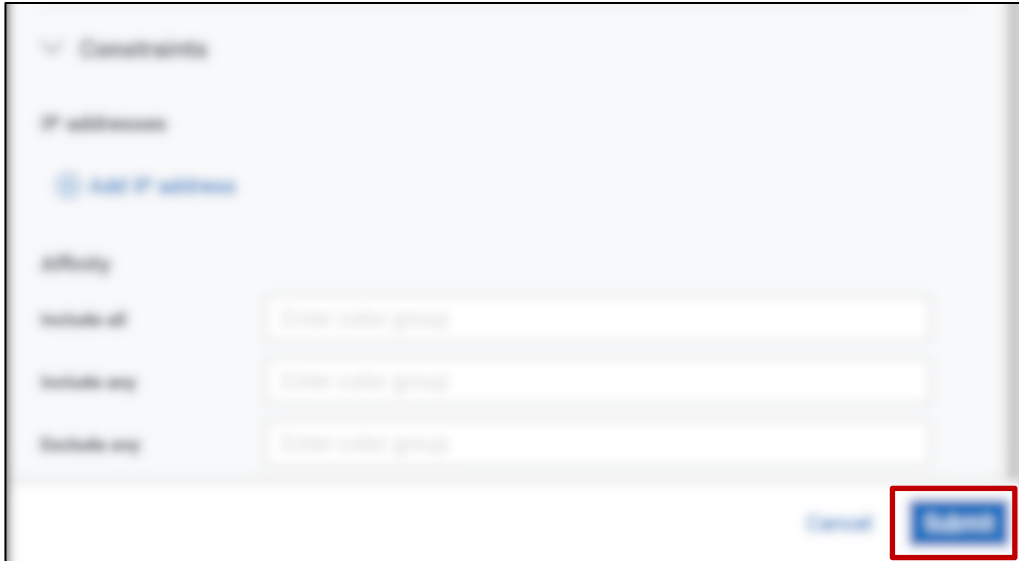
The screenshot shows the 'Endpoints' tab of a configuration window. It contains three rows of input fields for 'Endpoint 1', 'Endpoint 2', and 'Endpoint 3'. Each row has a 'Name' field, a 'Label' field, and a 'Customer' dropdown menu. There is also a 'BFD Profile' dropdown menu at the bottom right.

5. Consulting with your instructor, fill in the information required for the “Configuration” fields (refer to the sample screenshot below):
 - Maximum bandwidth
 - Minimum bandwidth
6. Select a **Re-optimize mode**: Disable (no optimization), Manual (only upon user request), or Periodic (timed and upon user request).
7. For Periodic optimization, also provide a **Re-optimize interval** (in minutes, between 5 and 60)
8. Select a **Sticky**: Enable (If LSP goes down then tunnel will not come back up until the original path is available)
9. Select a **Setup Priority**: Available range is 0-7, 0 signifies highest priority and 7 signifies least priority.
10. Select a **Hold Priority**: Available range is 0-7, 0 signifies highest priority and 7 signifies least priority.



Keep the default values for all other fields (refer to the *NAVIGATOR MC Documentation* and the *OS Routing and MPLS Configuration* manual for more information on these fields).

11. This step is optional. Perform it only if your instructor asks you to do it and provides you with the necessary IP addresses of intermediate NEs to enter. Under “Constraints”, add the IP address of one or more intermediate NEs between the endpoints. This will override the path that will otherwise be set up automatically. Ignore the Affinity (color group) fields unless your instructor tells you to do otherwise and provides the necessary color groups to include/exclude.



12. Click on “Submit”.

A dialog displays the provisioning information. The devices go into Syncing state. (See the Enrollment window **[Network > Enrollment]**).

After the devices finished syncing, the Done status displays in the Enrollment window.

When the provisioning process is completed, a success message displays, indicating what entities were created.

After the provisioning or reservation is complete, the new entities display on the Packet Infrastructure page.

13. Refresh the Packet Infrastructure page.

The new MPLS tunnel displays in the list as Planned. The status changes to Deployed immediately, since you specified a Provision time of Now.

Note: If the tunnel state does not change to "Deployed" even after a few minutes, manually resynchronize the tunnel by viewing the tunnel details on the Packet infrastructure page and clicking the Resync button. If the tunnel state still does not change after few more minutes, it likely means the NE could not signal the tunnel properly and the tunnel creation is partial or failed.

End of Lab

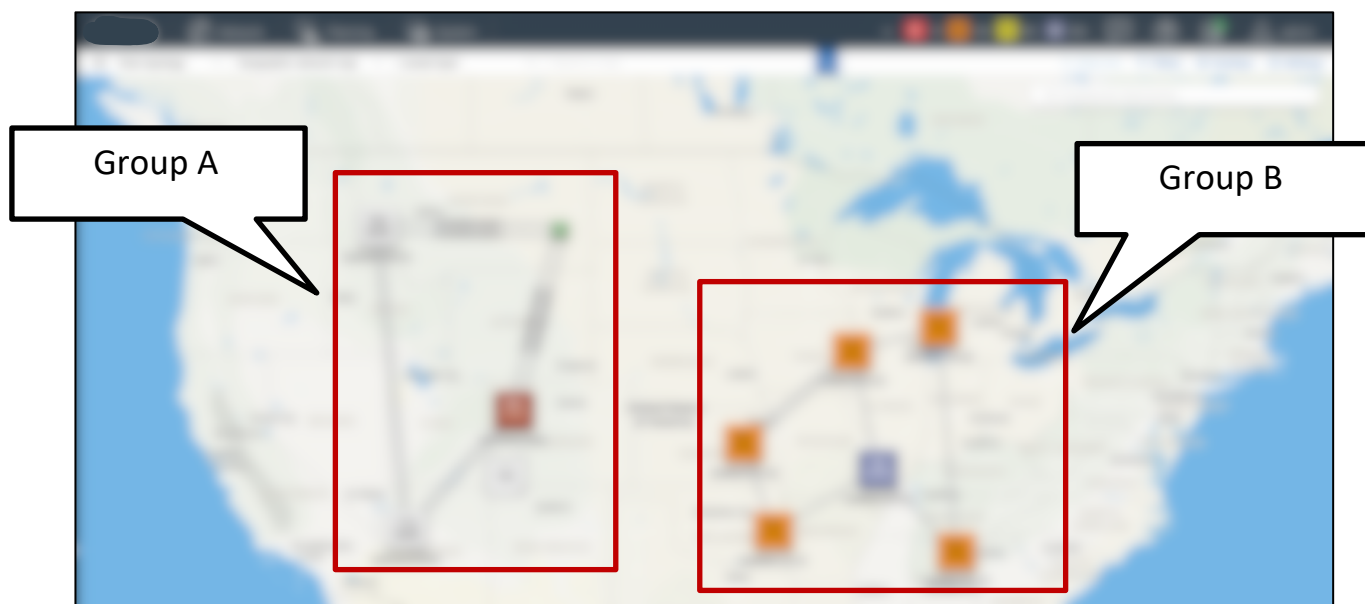
Appendix D: Configuring Custom Network Map Groups

NEs on the network map can be organized into custom map groups. Users can then navigate from one group of NEs to another. Groups can be organized hierarchically, with groups within groups.

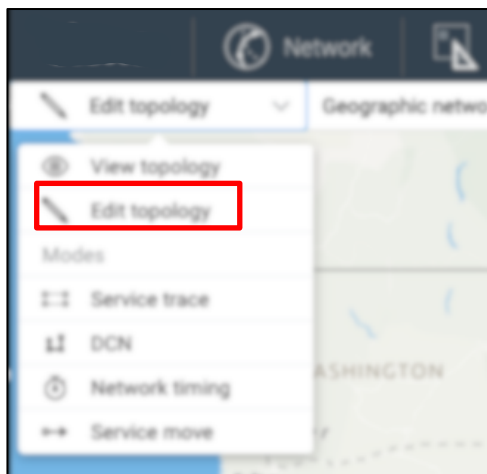
Note: Map groups are not the same as partitions. Partitions restrict user access to NEs and services. Map groups simply organize NEs on the map.

We'll look at an example of creating map groups: We'll organize the highlighted NEs into 2 map groups: Group A and Group B.

We'll create the map groups using searchable tags that match the name of the map group, starting on the next page:



1. Put the map in Edit mode by selecting **View topology** and selecting **Edit topology**.



2. Select one of the NEs in Group A and click the **Edit** button to enter the tag A then click **Save**.

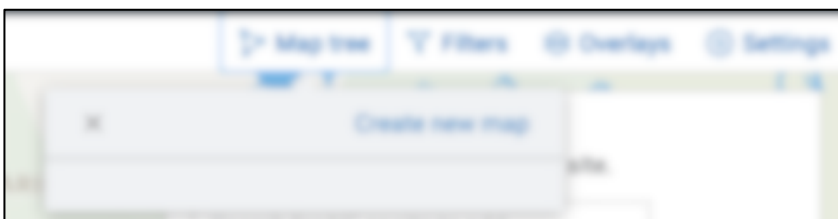
NOTE: You can hold down the Shift key and select multiple NEs.



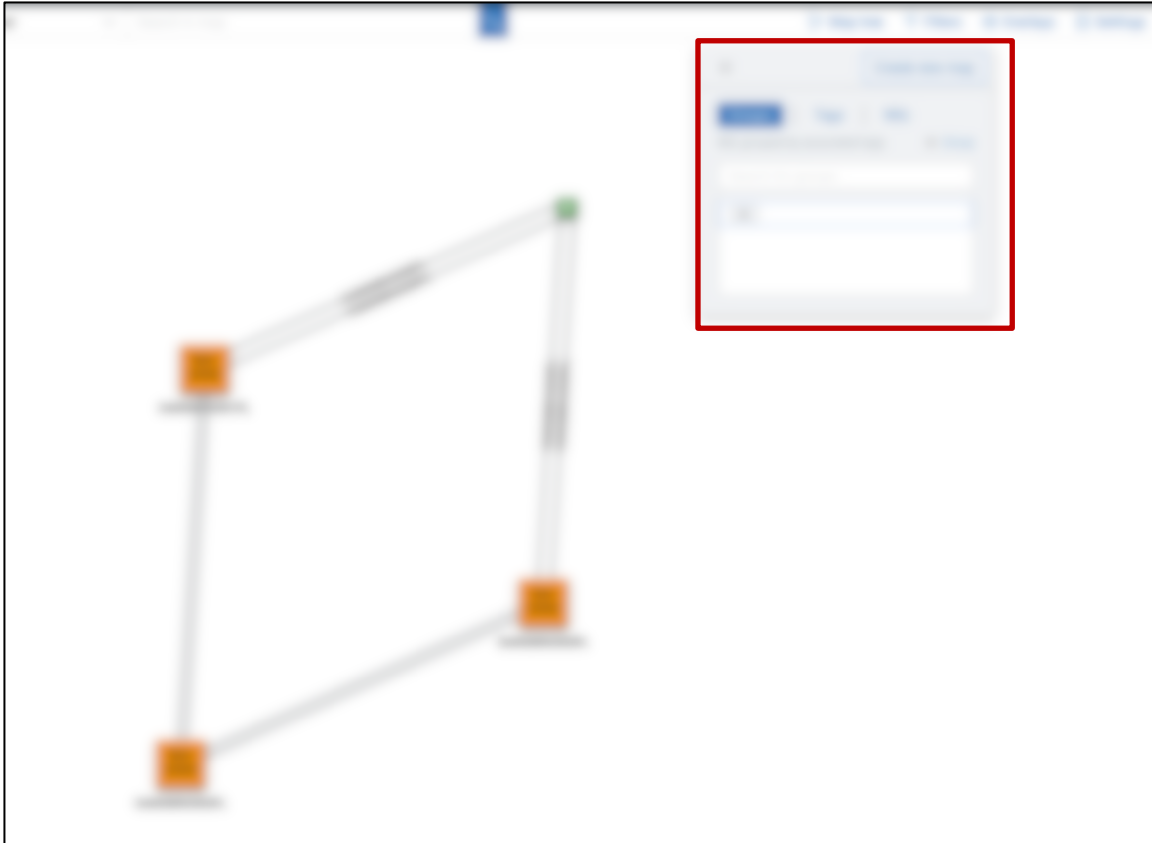
Edit network element

Tags

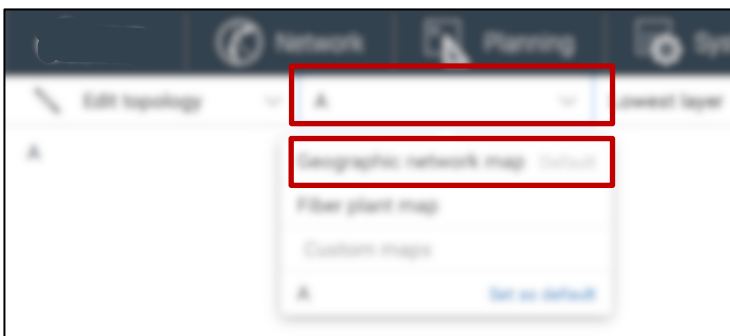
3. Select the NEs in Group A and enter the same tag.
4. Select **Map tree**.
5. Select **Create new map**.



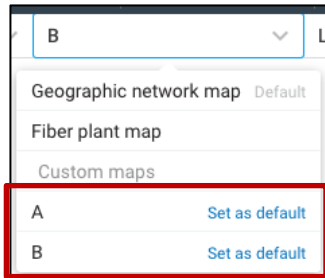
6. Enter A as the name for the map. The custom map group A is created, and the group is automatically populated with NEs assigned the A tag. Additional NEs or Tag groups can be added via the map tree box.



7. The Menu item Geographic network map will have changed to the name of the new map. Select the new name, then select **Geographic network map**. This will return you to the full network map. You now have an option within the menu to return to map A.



8. Create Map B following the same procedure that you followed for A. When you are finished, you have two custom map groups to which you can navigate.



End of Lab

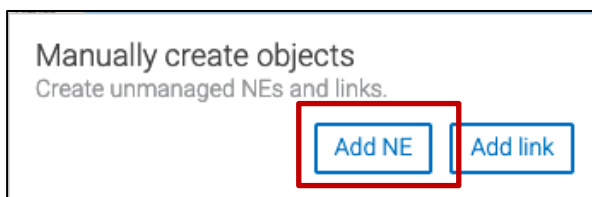
Appendix E: Add Unmanaged NEs and Links

NEs on the network map can be organized into custom map groups. Users can then navigate from one group of NEs to another. Groups can be organized hierarchically, with groups within groups.

Note: Map groups are not the same as partitions. Partitions restrict user access to NEs and services. Map groups simply organize NEs on the map.

Task 1: Add an Unmanaged NE

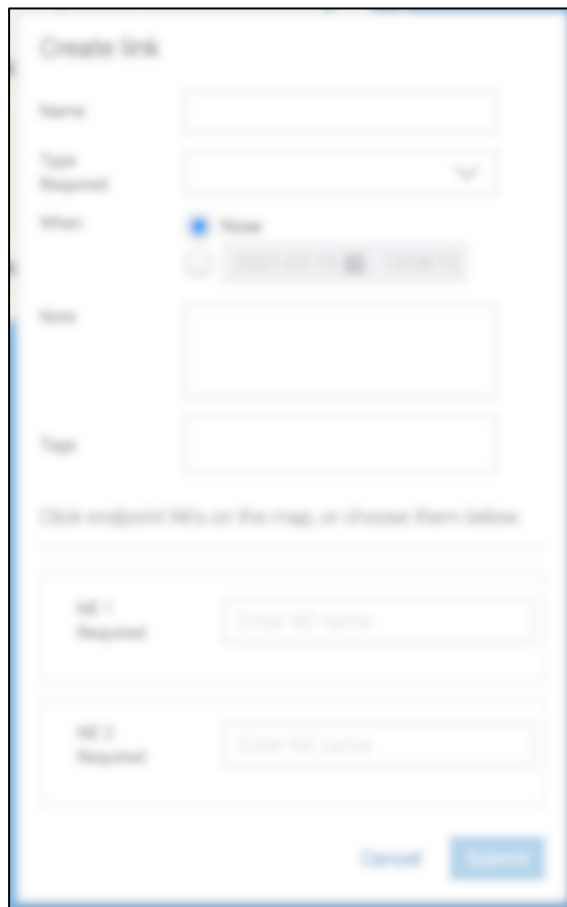
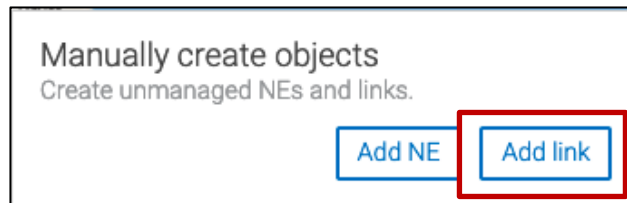
1. Add an unmanaged NE (a non-enrolled NE) to the map (sample screenshot is shown). Hint: You don't have to type in Latitude/Longitude map coordinates.



Task 2: Add a Manual Link

In certain cases, NAVIGATOR MC cannot discover a packet infrastructure link. In these cases, you can manually add a packet infrastructure link between two NEs.

1. Add a link between the unmanaged NE and one of the managed (enrolled) NEs on the map (sample screenshot is shown).



2. Turn Edit mode off. Do you see the link you created?

End Lab

Appendix F: Provisioning a TDM Metro Ethernet Forum 8 (MEF-8) Service

Check list

- Lab drawing (review)
- Supported equipment
- TDM MEF-8 service endpoints are enrolled in NAVIGATOR MC
- MPLS-TP tunnel available for use by the TDM service (can be the same tunnel provisioned in one of the previous exercises or another tunnel available in the lab). This tunnel connects the two endpoint NEs.

Objectives

After completing this lab, you will be able to:

- Launch the NAVIGATOR MC GUI
- Connect to appropriate Network Elements via the NAVIGATOR MC GUI
- Provision a TDM MEF-8 service

Task 1: Gather Information

Your instructor will provide you with the names of the two endpoint NEs for the TDM service, and slot/port information. For TDM MEF-8 services, the instructor will also provide you with a VLAN, which must be configured on both NE endpoints.

Fill in the table below with information from your instructor.

NE TDM Endpoint 1	Slot/Port/Channel on endpoint 1	NE TDM Endpoint 2	Slot/Port/Channel on endpoint 2	VLAN

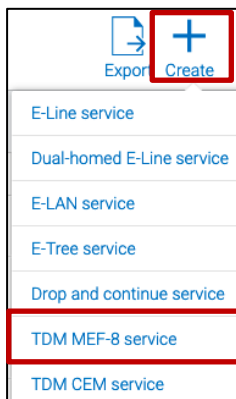
Task 2: Locate Endpoints

1. From the NAVIGATOR MC menu bar, select **Network > Network elements**.
2. Select one of the NEs that will provide an endpoint for the TDM MEF-8 service, display Details, and locate the circuit pack and port that will act as one of the endpoints. Is the port a channelized port or a native port (no channels)?
3. Repeat the procedure for the other endpoint.

Task 3: Provision a TDM MEF-8 Service

We are going to provision a simple TDM MEF-8 service on top of an MPLS-TP tunnel provisioned previously in this lab.

1. Select Network and, under Services, select Packet services.
2. Select “+ Create” and select “TDM MEF-8 service.”



3. Provide the service name; select the “Provision time” to “Now” and the Deletion time to “Never”. Ignore the Customer and Add note fields.



4. Under Configuration, enter the VLAN provided by your instructor. Ignore the Re-use existing pseudowire and Protected pseudowire check boxes.



Configuration

☐ Re-use existing pseudowire

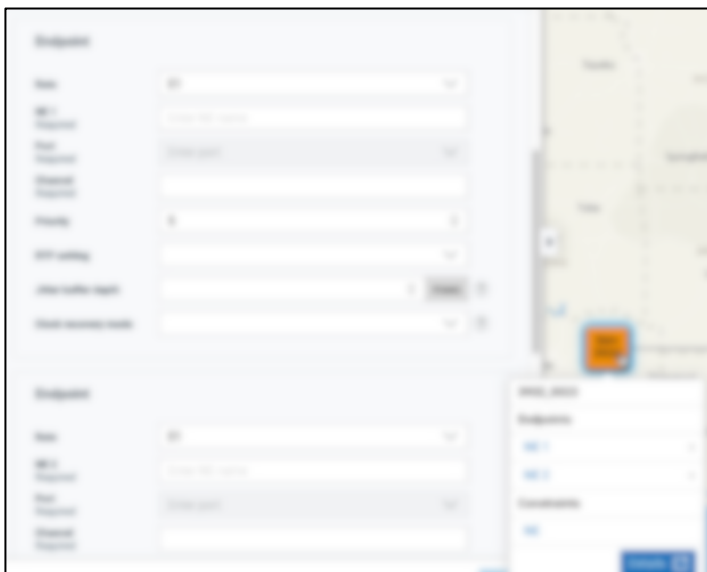
☐ Protected pseudowire

VLAN Required

Enter VLAN

5. Identify the end points, and specify the following information:
 - NE – Specify the two TDM MEF-8 endpoint NEs you wrote down prior to this procedure.
 - Port - Specify the two TDM MEF-8 endpoint ports you wrote down prior to this procedure.
 - Channel – Specify the channel number (for channelized ports only).
 - Priority – Accept the default (5).
 - Skip the RTP, Jitter buffer depth, and Clock recovery mode fields unless your instructor tells you otherwise.

Note: Refer to the TDM Services over PSN Configuration chapter in the OS 6.x *Advanced Ethernet Configuration Guide* for more information on RTP, Jitter buffer, and clock recovery mode. These parameters are designed mainly for delay-sensitive applications like audio and video conferencing.



6. Under Constraints:

- Accept the Transport protection default (Any).
- Select Add tunnel and then select the MPLS-TP tunnel you provisioned in one of the previous exercises (or another available tunnel). This tunnel connects the two endpoint NEs. Specify Include for the tunnel.



7. Click Calculate routes. Then, select the route associated with the MPLS-TP tunnel.
8. Select a route and click on "Submit". NAVIGATOR MC sends the necessary commands to the end nodes and all transit nodes in the calculated path to configure the service.
9. Click close to return to the packet services screen where our new service is now listed.
10. Select the new service and click Details. Navigate from one details tab to view the topology and attributes of the service.

End of Lab

Appendix G: Provisioning a TDM Circuit Emulation (CEM) Service

Check list

- Lab drawing (review)
- Supported equipment
- TDM CEM service endpoints on OS-Based NEs that are enrolled in NAVIGATOR MC
- MPLS-TP tunnel available for use by the TDM service (can be the same tunnel provisioned in one of the previous exercises or another tunnel available in the lab). This tunnel connects the two endpoint NEs.

Objectives

After completing this lab, you will be able to:

- Launch the NAVIGATOR MC GUI
- Connect to appropriate Network Elements via the NAVIGATOR MC GUI
- Provision a TDM CEM service

Task 1: Gather Information

Your instructor will provide you with the names of the two endpoint NEs for the TDM service, and slot/port information.

Fill in the table below with information from your instructor.

NE TDM Endpoint 1	Slot/Port/Channel on Endpoint 1	NE TDM Endpoint 2	Slot/Port/Channel on Endpoint 2

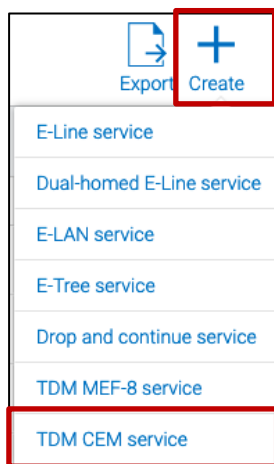
Task 2: Locate Endpoints

1. From the NAVIGATOR MC menu bar, select **Network > Network elements**.
2. Select one of the 6500 PTS NEs that will provide an endpoint for the TDM CEM service, display Details, and locate the circuit pack and port that will act as one of the endpoints.
3. Repeat the procedure for the other endpoint.

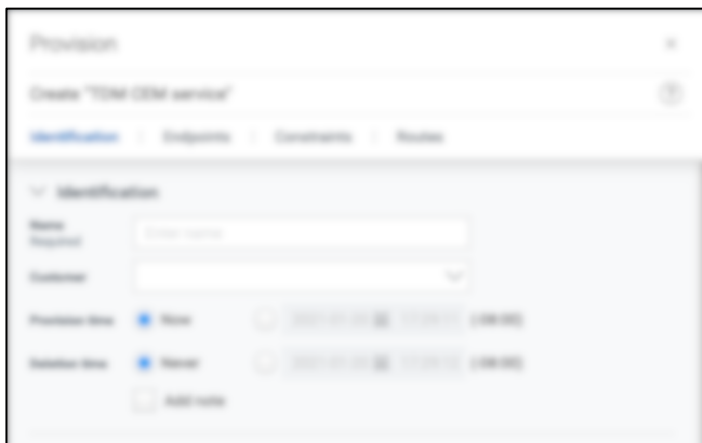
Task 3: Provision a TDM CEM Service

We are going to provision a simple TDM CEM service on top of an MPLS-TP tunnel provisioned previously in this lab.

1. Select Network and, under Services, select Packet services.
2. Select “+ Create” and select “TDM CEM service.”



3. Provide the service name; select the “Provision time” to “Now” and the Deletion time to “Never”. Ignore the Customer and Add note fields.

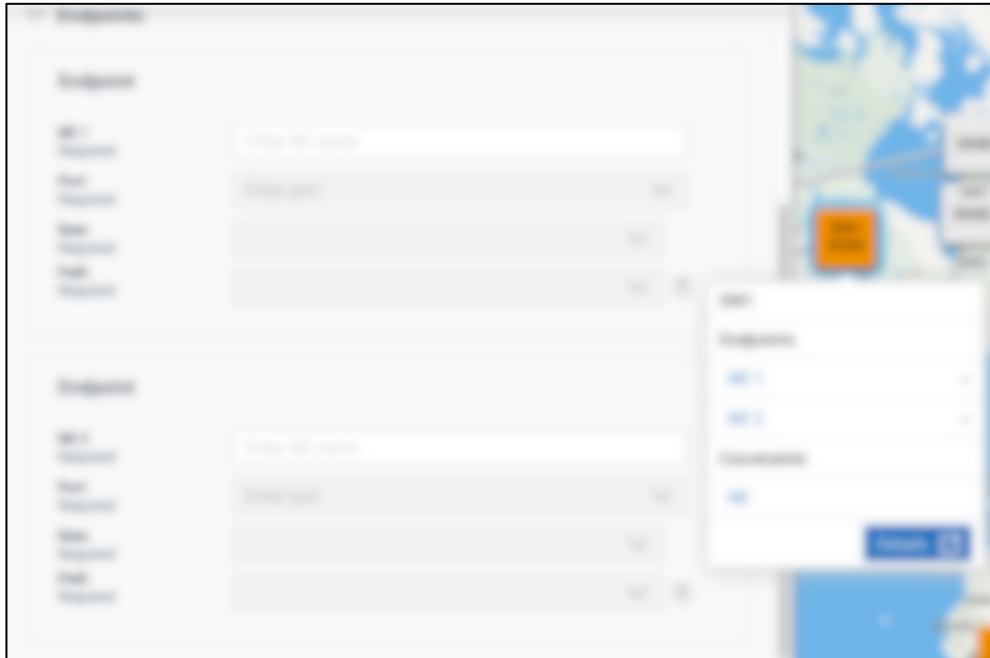


4. Identify the end points, and specify the following information:

- NE – Specify the two TDM CEM endpoint NEs you wrote down prior to this procedure.
- Port - Specify the two TDM CEM endpoint ports you wrote down prior to this procedure.
- The Rate and Path should auto populate once the port is selected.

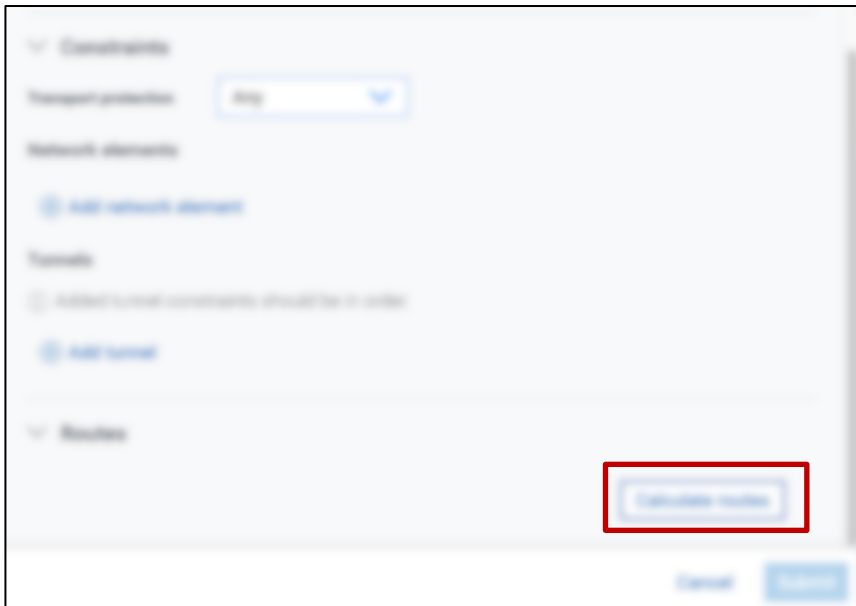
NOTE:

Rate and Path selections are only applicable to 6500 PTS devices.



5. Under Constraints:

- Accept the Transport protection default (Any).
- Select Add tunnel and then select the MPLS-TP tunnel you provisioned in one of the previous exercises (or another available tunnel). This tunnel connects the two endpoint NEs. Specify Include for the tunnel.



6. Click Calculate routes. Then, select the route associated with the MPLS-TP tunnel.
7. Select a route and click on "Submit". NAVIGATOR MC sends the necessary commands to the end nodes and all transit nodes in the calculated path to configure the service.
8. Click close to return to the packet services screen where our new service is now listed.
9. Select the new service and click Details. Navigate from one detail tab to another to view all the service details. Is the service operational?

End of Lab