Configure Circuits

The OTN circuits allow you to setup end to end circuits from the origin to a destination network element. The Optical Channel Trail circuits allow you to create circuits in a network where the NCS 4000 series node is connected to ONS 15454, ONS 15454 M2, or ONS 15454 M6 nodes. This chapter provides the CTC procedures to configure the circuits.

Understand OTN Circuits

An OTN circuit provides the ability to aggregate different types of traffic such as Ethernet, SONET or SDH, and packet over OTN at different data rates such as 1.25, 2.5, 10, 40, or 100 GBit per second. This aggregated traffic is transported by network elements that acts as OTN cross connections.

ODUk controllers can be cross connected with controllers of the same rate in an OTN circuit by a fabric card. The following network applications are associated with OTN network elements:

- End-to-end circuits from any rate or any payload client service
- End-to-end circuit from a client service versus the OTN (OTUk) network
- Aggregation of OTN traffic (OTUk)

Understand Circuit Diversity

This feature enables the user to create a circuit that is diverse from an existing circuit in the network. This is to increase survivability and availability in case of link failures.

During the computation of a diverse circuit, the GMPLS algorithm attempts to find a shared resource link group (SRLG) diverse path. If the path is not available, node and link diversity is used to compute the new path. Enabling circuit diversity on an existing circuit causes re-signaling of the circuit.

The following restrictions are applicable to ODU TUNNEL circuits:

- The diverse circuit must have the same head node.
- Supported only for 1+0 circuits.
- If a diverse path is not found, the circuit is not created.

This feature is supported on the NCS4K-4H-OPW-QC2 card.

Understand OSPF

Open Shortest Path First (OSPF) is a routing protocol designed to run an autonomous system. It maintains an identical database describing the topology of an autonomous system. From the identical database, a shortest path-tree calculates the routing table. OSPF-TE allows controlling the data packet's path.

OSPF provides following features:

- Routing of area.
- Routing of protection.
- Minimizing the routing protocol traffic.

Understand MPLS TE

MPLS TE learns the topology and resources available in a network and then maps traffic flows to respective paths based on resource requirements and network resources, for example, bandwidth. MPLS TE builds a unidirectional tunnel from a source to a destination in the form of a label switched path (LSP), which is then used to forward traffic. Tunnel head end or tunnel source is the point where the tunnel begins, the tunnel tail end or tunnel destination is the node where the tunnel ends .

Understand Tandem Connection Monitoring

Tandem Connection Monitoring (TCM) layer is used for protection applications, for example, APS. The path layer can be used for protection, however, it can be influenced by errors that occur outside a given operators network and cause undesired protection switch events to occur within their network. Since TCM can isolate a service to a given domain, it can be used to trigger protection applications and avoid such issues.

Six levels of TCM, each with various modes of operation, are provided to allow for simultaneous use for different monitoring applications along any each and every individual ODU trail. These applications include: segment protection, administrative domain monitoring, service monitoring, fault localization, verification of delivered quality of service, delay/latency measurements and adjacency discovery.

Understand Automatic Protection Switching

Automatic Protection Switching (APS) is a protection mechanism for OTN networks that enables OTN connections to switch to another circuit when a circuit failure occurs. A protect circuit serves as the backup circuit for the working circuit. When the working circuit fails, the protect circuit quickly assumes its traffic load.

In a linear protection architecture, protection switching occurs at the two distinct endpoints of a protected circuit. For a given direction of transmission, the head-end or the tail-end of the protected signal performs a bridge function, and places a copy of a normal traffic signal onto a protection entity when required. The tail-end or the head-end performs a selector function, where it is capable of selecting a normal traffic signal either from its usual working entity, or from a protection entity.

The widely used protection mechanism is the 1+1 architecture. Here, a single normal traffic signal is protected by a single protection entity. The bridge at the head-end is permanent. Switching occurs entirely at the tail-end.

In the case of bidirectional transmission, it is possible to choose either unidirectional or bidirectional switching. With unidirectional switching, the selectors at each end are fully independent. With bidirectional switching, an attempt is made to coordinate the two ends so that both have the same bridge and selector settings, even for a unidirectional failure. Bidirectional switching always requires an APS and/or protection communication channel (PCC) to coordinate the two endpoints. Unidirectional switching can protect two unidirectional failures in opposite directions on different entities.

Hierarchy in APS

There are different levels of priority that can be set for the path to switch from a working circuit to the protect circuit (or vice-versa). The hierarchy levels are (listed priority-wise, with lockout having the highest priority):

- Lockout - the path continues to be in the working circuit, even if a failure is detected in the working circuit, switch to the protect circuit is not permitted. If the path is currently using the protect circuit, then it automatically switches back to the working circuit.
- Forced switch - forces a switch from the protect circuit to the working circuit (even when the protect circuit is down, this scenario can happen during a maintenance activity).
- Manual switch - manually switches from the working circuit to the protect circuit or from the protect circuit to the working circuit.
- Exercise - enables the APS protocol.

  m

Understand Subnetwork Connection

Subnetwork Connection Protection (SNCP) configurations provide duplicate fiber paths for a circuit. Working traffic flows in one direction and protection traffic flows in the opposite direction. If a problem occurs with the working traffic path, the receiving node switches to the path coming from the opposite direction. The node at the end of the path and the intermediate nodes in the path select the best traffic signal. The virtual container is not terminated at the intermediate node, instead, it compares the quality of the signal on the two incoming ports and selects the better signal.

SNC can be classified into three types:

- SNC/I (inherent) - Protection switching is triggered by defects detected at the ODUk link connection.
- SNC/N (non-intrusive) - Protection switching is triggered by a non-intrusive monitor of the ODUkP trail.
- SNC/S (sublayer) - Protection switching is triggered by defects detected at the ODUkT sublayer trail (TCM). An ODUkT sublayer trail is established for each working and protection entity.

Understand 1+R Protection

1+R protection mechanism is SNC-based. In case of work path failure, the circuit uses the restore path. Here, the protect path is not defined by the user (as in case of other protection mechanisms). The restore path is defined by the GMPLS protocol. To enable GMPLS, see Enabling GMPLS Using CTC, on page 8

1+1+R

In 1+1+R protection mechanism, a circuit is protected by two redundant paths, one is the protect path and the other one is the restore path. When a failure occurs on the working and the protect paths, then the restore path takes over. Wait to Restore (WTR) timers are available on both the working and protect paths. Restoration path signalling is triggered as soon as a defect is detected on either of the paths (working or protect). So, when the working path fails, the traffic shifts to the protect path. In this period of time, the restore path is ready to take over as soon as the protect path fails too; the switchover time is less than 50ms.

These are the limitations for 1+1+R protection mechanism:

- Unidirectional protection type is not supported.
- Manual switch to restore is not supported.

Understand ISSU Upgrade

In-Service Software Upgrade (ISSU) is a technique that updates the software packages on a network element without affecting the traffic. By using ISSU, you can deploy new Cisco IOS XR Software images that supports new software features and services. The Cisco IOS XR ISSU capability extends Cisco high availability innovations for minimizing planned downtime for service provider networks.

Understand GCC Management

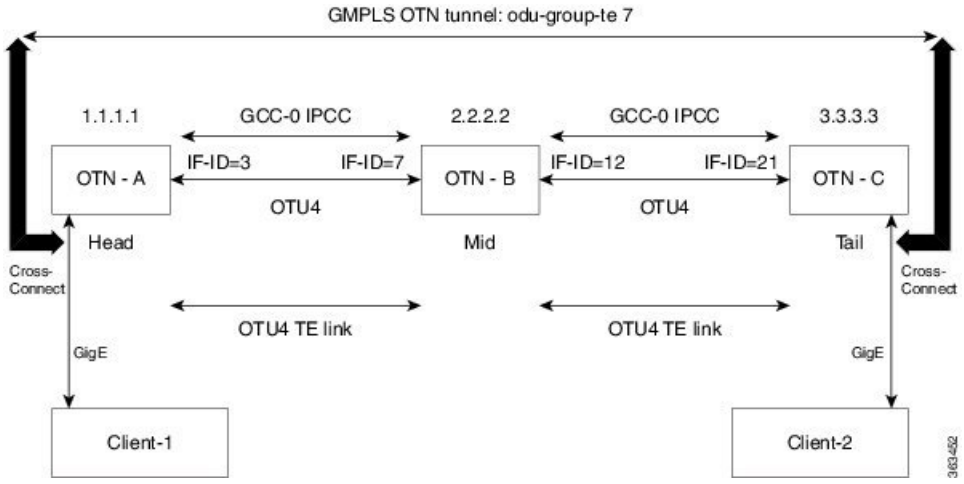
General Communication Channel (GCC) is an in-band side channel that carries transmission management and signaling information within optical transport network elements.

There are two types of GCC links:

- GCC0 - two bytes within OTUk overhead.
- GCC1 - two bytes within ODUk overhead.

Understand GMPLS

Generalized Multi-Protocol Label Switching (GMPLS) extends the packet based MPLS protocol to allow creation and maintenance of tunnels across the networks that consist of non-packet switching devices. GMPLS tunnels can traverse the Time-Division Multiplex (TDM) interface and switching types.



The following protocols are associated with GMPLS:

- **OSPF**
- **OSPF-TE**
- **RSVP-TE**
- **MPLS-TE**
- **LMP**

Understand Explicit Path

Explicit path refers to a user defined path taken by a circuit. GMPLS dynamically determines the path to be taken by a circuit but user can override this path by configuring an explicit path.

Interoperability between NCS 4000 and MSTP Nodes using NCS4K-4H-OPW-QC2 Card

Interoperability between NCS 4000 and MSTP nodes is achieved by creating a Link Management Protocol (LMP) numbered or unnumbered UNI link between NCS4K-4H-OPW-QC2 interface on the NCS 4000 node and the optical channel Add/Drop interface on the MSTP nodes.

To create OTN circuits between the NCS 4000 nodes via the MSTP network, a GMPLS OCH Trail circuit must be created between the two NCS 4000 nodes that are connected to MSTP nodes. The traffic transmitted by the OCH Trail circuit is used as a OTU4 or OTUC2 link by the OTN layer.

To configure interoperability, complete the Configure Interoperability Between NCS 4000 and MSTP Nodes, on page 35 procedure.

Provision Management IP Address

Purpose	This procedure provisions the manageme
Tools/Equipment	None
Prerequisite Procedures	" Login to CTC" in *System Setup and Sof*
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, click the **Provisioning** > **Network** > **General** tabs.

Active RP—Displays the details of the active route processor.

Step 2 In the **Mgmt IP** area, complete the following information:

- Virtual IP Address - Enter an IP address drawn from the management IP address pool that supersedes the IP addresses of RP0 and RP1.
- Mask - Enter the subnet mask of the IP address.

Step 3 In the **RP0-EMS IP** and **RP1-EMS IP** areas, complete the following information:

- IPv4—Enter the IPv4 address assigned to RP0/RP1 EMS.
- IPv4 Mask—Enter the IPv4 subnet mask.
- Service State—Select the state from the drop-down menu. The available options are - IS (in-service) and OOS (out-of-service).

Step 4 In the **RP0-Craft IP** and **RP1-Craft IP** areas, complete the following information:

- IPv4—Enter the IPv4 address assigned to RP0/RP1 Craft panel.
- IPv4 Mask—Enter the IPv4 subnet mask.
- Service State—Select the state from the drop-down menu. The available options are - IS (in-service) and OOS (out-of-service).

Step 5 In the **RP0-Mgmt IP** and **RP1-Mgmt IP** area, complete the following information:

- IPv4—Enter an IP address drawn from the management IP address pool.
- IPv4 Mask—Enter the subnet mask for the IP address.
- Mac Address—Displays the MAC address of RP0/RP1.
- IPv6—Enter an IP address drawn from the management IP address pool.
- IPv6 Prefix Length—Enter the prefix length for the IP address.
- Service State—Select the state from the drop-down menu. The available options are - IS (in-service) and OOS (out-of-service).

Step 6 In the **Gateway** area, enter IPv4 or IPv6 address and enter the prefix length if you use IPv6 address. The prefix length must be between 0 and128.

Step 7 Click **Apply**.

Stop. You have completed this procedure.

Configure the Loopback on an Interface Using CTC

Purpose	This procedure provides instructions to configure the loopback on an interface using CTC. It also helps in management logging and authentication of a user on an interface for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS or NCS4K-4H-OPW-QC2 Line cards.
Tools/Equipment	None
Prerequisite Procedures	Login to CTC in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View**, double-click the line card.

Step 2 Click the **Maintenance** > **Loopback** tab.

Step 3 To configure loopback on OTN controllers, perform the following steps in the screen that appears:

a) Click the **Controller** column and select a name of the controller.
b) Click the **Admin State** Column.
c) Choose **Service State** for the controller. For more information, see Administrative and Service States.
d) From the **Loopback Type** drop-down list, choose **Internal**, **Line** or **None**.
e) Click **Apply**.
f) Click **Refresh** to refresh all the controllers.

Stop. You have completed this procedure.

Enabling GMPLS Using CTC

Purpose	This procedure helps in enabling the Traffic Engineering (TE) links.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	Required.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 To configure a GCC on a controller, complete Configuring GCC Using CTC, on page 8.

Step 2 To configure OSPF on an interface, complete Add OSPF on an Interface Using CTC, on page 9.

Step 3 To configure OSPF-TE, complete Configure OSPF-TE on an Interface Using CTC, on page 10.

Step 4 To configure MPLS-TE, complete Configure an MPLS-TE Instance Using CTC, on page 11.

Step 5 To configure RSVP-TE, complete Configure a RSVP-TE Instance Using CTC, on page 12.

Stop. You have completed this procedure.

Configuring GCC Using CTC

Purpose	This procedure enables you to configure General Communication Channel (GCC) on a controller for NCS4K-20T-O-S, NCS4K-2H-O-K, NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC
Required/As Needed	Required.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, double-click the line card.

Step 2 Click the **Provisioning** > **Controllers** > **OTU or ODU** tabs.

Step 3 To enable GCC on the controller, perform one of the following steps:

a) For OTU controller, check the **GCC0** check box.

b) For ODU controller, check the **GCC1** check box.

Step 4 Click **Apply**.

Step 5 In the Node View, click the **Provisioning** > **Comm Channels** tabs.

Step 6 To assign IP address to the GCC, add IP address in the **IP address** field and network mask in the **NetMask** field.

Note
To assign loop back IP address to the GCC, select a **Loopback** from the drop down list.

Same loop back IP address can be assigned to multiple GCC's .

Step 7 Click **Apply**.

Step 8 Return to your originating procedure.

Add OSPF on an Interface Using CTC

Purpose	This procedure enables you to configure the OSPF on an interface using CTC. Adding OSPF allows to setup a link between two different routers and maintain the connectivity interface.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure the Loopback on an Interface Using CTC, on page 7
Required/As Needed	Required
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **Network** > **OSPF** tabs.

Step 2 Perform following steps to create an OSPF instance:

a) From **OSPF Instance Name** drop down list, select OTN.

b) From **Router Id** drop down list, select the router id.

Note
Recommended configuration is Virtual IP.

c) Click **Apply**.

Step 3 Select the NSR check-box to enable redundant route processors to maintain its Open Shortest Path First (OSPF) state and adjacencies across planned and unplanned IP switchovers.

NSR stands for Non -Stop Routing.

Step 4 Select the NSF (IETF) check-box to continue forwarding IP packets following a supervisor engine switchover.

NSF stands for Non-Stop Forwarding.

Step 5 Perform following steps to add GCC interface to OSPF:

a) In **OSPF Interfaces** section, click **Add**. The Create OSPF Entry dialog box appears.

b) In the **Interface** drop down list, select the interface.

Note
Add Loopback interface and GCC interface both, if loopback IP is assigned to GCC .

Repeat step3 to add multiple interfaces.

c) In the Area ID field, a default value of 0 is populated.(non-editable).

d) (Optional) In the Cost field, enter the cost.

e) (Optional) Check the **Passive** check box to ensure the updates are not sent beyond an OSPF interface.

f) Click **OK**.

Step 6 Click **Apply**.

Step 7 Return to your originating procedure.

Configure OSPF-TE on an Interface Using CTC

Purpose	This procedure enables you to configure the OSPF-TE using CTC. OSPF-TE allows controlling the path of data packets and advertise the capabilities of TE links to remote nodes.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC Add OSPF on an Interface Using CTC, on page 9
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **Network** > **OSPF-TE** tabs.

Step 2 From the **OSPF-TE Router Id** drop down list, select router id.

Note
Recommended configuration is Virtual IP.

Step 3 To configure the OSPF-TE on an Interface, complete the following:

a) In the Area ID field, a default value of 0 is populated (non-editable).
b) Check the **Autoconfig** check box to enable all the interfaces of the OSPF-TE.
c) Click **Apply**.

Step 4 Return to your originating procedure.

Configure an MPLS-TE Instance Using CTC

Purpose	This enables you to configure an MPLS-TE instance that helps to route network traffic using CTC. Traffic engineering enables to reduce the cost of the network and offer the best service to the users.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* Configure an OTN Controller Using CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **Network** > **MPLS-TE** tabs.

Step 2 Click **Create**. The Create MPLS Topology Instance Entry dialog box appears.

Step 3 Click **OK** to create a MPLS-TE instance.

Step 4 In the **Controllers** section expand the row for the line card on which you want to configure MPLS-TE and perform the following steps to update the default values of the parameters:

a) To enable TE link, set **Enable** field as true.

b) From the **TTI mode** drop down list, select the TTI mode. Available options are PM, SM, TCM1,TCM2, TCM3, TCM4, TCM5, and TCM6.

c) (Optional) Set the **Admin Weight** field with value ranging from 0 to 65535.

Step 5 Click **Apply**.

Step 6 Return to your originating procedure.

Configure a RSVP-TE Instance Using CTC

Purpose	This procedure enables you to configure a RSVP-TE instance.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As Needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node View, click the **Provisioning** > **Network** > **RSVP-TE** tabs.

Step 2 In the **Interface List** area, for an **Interface Name**, select the **RSVP State** from the drop-down menu. The available options are - Enable and Disable.

Step 3 In the **Card** section, expand the row for required LC to view the list of configured controllers.

Step 4 Select a controller and perform the following sub steps:

a) Set the **Enable** field of the controller to **true**.

b) (Optional) Input value for **Refresh Optical Interval**. Valid range is 180 to 86400 seconds.

c) (Optional) Input value for **Missed Messages**. Valid range is 1 to 110000.

Step 5 Click **Apply** to save the changes.

Stop. You have completed this procedure.

Configure OTN Circuits Using CTC

Purpose	This procedure configures an OTN Circuit Using CTC.
Tools/Equipment	None
Prerequisite Procedures	Configure an OTN Controller Using CTC Enabling GMPLS Using CTC, on page 8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Perform any of the following procedures as needed to create, load, and store the path protection profile:

- Add a Path Protection Profile Using CTC, on page 14
- Load a Path Protection Profile Using CTC, on page 16
- Store a Path Protection Profile Using CTC, on page 16

Step 2 Perform any of the following procedures as needed to configure an OTN circuit:

- #unique_97
- Discover a Circuit Using CTC, on page 21
- Edit General Parameters of a Circuit Using CTC, on page 22
- Edit ODU Configuration of a Circuit Using CTC, on page 23

Step 3 Perform any of the following procedures as needed to create, load, and store the explicit path:

- Add an Explicit Path Using CTC, on page 26
- Store an Explicit Path Using CTC, on page 26
- Load an Explicit Path Using CTC, on page 27
- Create an Local UNI LMP Using CTC, on page 28

Stop. You have completed this procedure.

Add a Path Protection Profile Using CTC

Purpose	This procedure provides instructions to add a path protection profile using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Path Protection Profiles**.

Step 2 Click **Add**. Perform the following steps in the editable row:

a) In the **Name** column, enter the Path Protection Profile name.

b) In the **Wait to Restore** (WTR) field (in seconds), enter the duration of time (in seconds).

Note
It defines the time the system must wait to restore a circuit. To edit the **WTR** value, **Revertive** should be set to **Yes**. The valid range is 0 or from 300 to 720 seconds. WTR value is in multiple of 60. Default value for WTR is 300.

WTR is not supported on a non-revertive circuit.

c) From the **Sub Network Connection Mode** drop-down list, choose any from the following: SNC_N (default), SNC_I and SNC_S.

Note
A new entry will be created with Sub Network Connection Mode value as **SNC_N** and TCM-ID value as **NONE.**

d) In the **Hold Off (milli sec)** field, enter the duration of time (in seconds) .

Note
It defines the time the system waits before switching to the alternate path. The valid range is 0 or from 100 to 10000 seconds. Hold off value is in multiple of 100. Default value is 0.

e) From the **Protection Type** drop-down list, choose a protection type from the available options 1+1-BIDIR-APS (Default) or 1+1-UNIDIR-APS or 1+1-UNIDIR-NO-APS.

f) From the **Revertive** drop-down list, choose **Yes** or **No**. Default is **No**.

g) From the **TCM-ID** drop-down list, choose **None**.

Step 3 From the Sub Network Connection mode drop-down list, choose **SNC_S**.

Step 4 From the TCM drop-down list, choose an option.

Note

By default, **TCM-4** is selected once you select **SNC-S** as Sub Network Connection mode. You can change the TCM-ID column value from **TCM4** to TCM1-TCM6 for SNC-S.

Note
For SNC-I and SNC-N, You are not allowed to change the TCM-ID value. It should be set to **None**.

Step 5 Click **Store** to store the profile for the particular node.

Step 6 The Store Profile(s) window is displayed.

Step 7 By default, the **To Node(s)** radio button is selected. Select the required nodes from the **Node Names** area, to set the profile. Click **Select All** to set the profile for all the selected nodes. Click **Select None** to undo your earlier selection.

Step 8 Click **OK**.

Step 9 Select the **To File** radio button, and click **Browse** to save the profile in your local machine.

Step 10 Return to your originating procedure.

Provision Loopback Interface

Purpose	This procedure provisions the loopback interf
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in System Setup and Softwa
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 In the node view, click the **Provisioning** > **Network** > **Loopback IF** tabs.

Step 2 If you want to create a loopback interface, complete the following:

- Click **Create**. The Create Loopback Interface dialog box appears.
- Enter the Interface ID, IP address, and network mask in the respective fields and click **OK**.

Step 3 If you want to edit a loopback interface, complete the following:

- Click **Edit**. The Edit Loopback Interface dialog box appears.
- Modify the values of the IP Address and network mask as required and click **OK**.

Step 4 Return to your originating procedure.

Load a Path Protection Profile Using CTC

Purpose	This procedure provides instructions to load a path protection profile using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning, higher or retriever

Procedure

Step 1 In the **Network View**, click the **OTN** > **Path Protection Profiles** tab.

Step 2 Click **Load**. Perform one of the following in the Load Profile (s) dialog box that appears.

a) From the **From Node (s)** pane, select a name of the node to load the path protection profiles.

b) Click **OK**.

c) In the **From File** field enter the path of the file or browse to the file, to load the path protection profile.

Note
You can load the profiles from a file that has OTN extension.

d) Click **OK**.

Step 3 Return to your originating procedure.

Store a Path Protection Profile Using CTC

Purpose	Storing a Path Protection Profile allows to store cross connection on the same chassis. This procedure provides instructions to store a path protection profile using CTC.
Tools/Equipment	None
Prerequisite Procedures	• "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* • Add a Path Protection Profile Using CTC, on page 14 • Load a Path Protection Profile Using CTC, on page 16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Path Protection Profiles**tab.

Step 2 Click **Store**. Perform one of the following in the Store Profile (s) dialog box that appears.

a) From the **To Node (s)** pane, select a name of the node to store the path protection profiles.
b) Click **Select All** to select all the node names.
c) Click **Select None** to deselect the selected node names.
d) To store the profile to a file, select the **To File** option and click**Browse** to select the required file, to store the path protection profile.

Step 3 Click **OK**

Step 4 Return to your originating procedure.

Configure an Open End OTN Circuit Using CTC

Purpose	OTN circuit allows the end user to setup end to end circuits from an origin to a destination Network Element. This procedure provides instructions to configure an open end OTN circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Circuits** tab.

Step 2 Click **Create**. The Circuit Creation wizard appears.

Step 3 In the **Circuit Type** screen of the wizard, choose a circuit type **ODU UNI** from the list.

Step 4 Enter a value between 1 to 80 for the number of circuits to be created.

Step 5 Click **Next**.

Step 6 In the Circuit Attributes screen of the wizard:

a) From the **Source Node** drop-down list, choose a source node for the circuit.
b) From the **Destination Node** drop-down list, choose a destination node for the circuit.
c) In the **Name**field, enter the circuit name.

Note
The length must not exceed 64 characters.

d) From the **Bandwidth** drop-down list, choose a bandwidth.
e) Click the **Bandwidth Configuration** hyperlink.

Note
This hyperlink is enabled when you select the bandwidth type as **ODUFLEX**.

Perform the following steps in the Bandwidth Configuration dialog box that appears.

- In the **Bit Rate** field enter the bit rate. The bit rate per time slot is 1249177. Example for ODU2 we have 8 timeslots, so bit rate will be 1249177 * 8 = 9993416.
- From the **Framing Type** drop-down list, choose **CBR** or **GFP-F-Fixed** (for 10 Gigabit Ethernet).
- Click **OK**.

f) From the **Protection Type** drop-down list, choose an option **1+0**, **1+1** or **1+R**.
g) Click the **Path Option Configuration** hyperlink. The Path Option Configuration screen appears.

Note
It is optional to configure the working path option. When you configure the path option using **Path Option Configuration** hyperlink, the selection made in the **Protection Type** drop-down list will be overridden.

Click **Add**. Perform the following steps in the Create/ Edit Path Option dialog box:

- In the **Index** field enter a unique index. The valid range is from 1 to 1000.
- In the **Path Option** drop-down list, choose **Working** or **Protect**.
- From the **Path Option Type** drop-down list, choose **Dynamic** or **Explicit**.
- From the **Path Name** drop-down list, choose an explicit path name.

  Note
  The **Path Name** field is disabled, if the path option type is dynamic.

- From the **Protected By** drop-down list, choose a protected path option.

  Note
  The **Protected By** drop-down list is disabled if the **Path Option** is set to Protect.

- From the **Restored By** drop-down list, select a restored path option. If any of the working or protected path fails, restored path replaces the failed path.

  Note
  The **Restored By** drop-down list is disabled if you have selected path option as Restored.

- Click **OK**.

h) From the **Path Protection Profile** drop-down list, choose an option. The option available is **None**. This drop-down list is disabled if protection type is selected as **1+0**.
i) Check the **Record Route** check box to record the route.
j) (For ODU UNI) From the **Service Type** drop-down list, select an option. Service type values are populated based on the bandwidth selected.

k) (For ODU UNI) Check the **Open End** check box to get the values populated in the Destination drop-down list.
l) (For ODU UNI) From the **Source drop-down list**, choose a source port or controller. Source values are populated based on the service type or open end selected
m) (For ODU UNI) From the **Destination** drop-down list, choose a destination port or controller. Destination values are populated based on the service type or open end selected..
n) Click the**Path Option Configuration hyperlink** button.

Perform the following steps in the Create/Edit dialog box that appears.

- From the ODU Level drop-down list, choose an option. ODU Level values are populated based on the Destination. ODU level is one less than the Destination. If Destination is selected as ODU2, values in this drop-down list would be ODU1 and ODU0.
- Select a time slot highlighted in green color above, press Ctrl key and select the next time slot.
- Click **Channelize** to allocate the time slot to the lower order channelize controller. The lower order controller appears in the controller tree hierarchy.
- Click **OK**.

o) Click **Finish** to create the circuit.

Step 7 Return to your originating procedure.

Configure an OTN Circuit Using CTC

Purpose	This procedure configures an OTN circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	You can load the profiles from a file that has OTN extension.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the network view, click the **OTN** > **Circuits** tab.
Step 2 Click **Create**. The Circuit Creation wizard appears.
Step 3 In the **Circuit Type** screen of the wizard, choose **ODU TUNNEL** as the circuit type.
Step 4 Click **Next**.
Step 5 In the Circuit Attributes screen of the wizard:
a) From the **Source Node** drop-down list, choose a source node for the circuit.
b) From the **Destination Node** drop-down list, choose a destination node for the circuit.

c) Enter the circuit name. The length must not exceed 64 characters.
d) Check the **Diversity** checkbox and choose the circuit from the drop-down list whose diverse circuit you want to create.

Note
This step is applicable only when diverse circuit is created.

The drop down list will display <tunnel id>: <circuit name>

e) From the **Bandwidth** drop-down list, choose a bandwidth.
f) Click the **Bandwidth Configuration** hyperlink.

Note
This hyperlink is enabled when you select the bandwidth type as **ODUFLEX**.

Perform the following steps in the Bandwidth Configuration dialog box that appears.

- In the **Bit Rate** field enter the bit rate.
- From the **Framing Type** drop-down list, choose **CBR** or **GFP-F-Fixed** (for 10 Gigabit Ethernet).
- Click **OK**.

g) From the **Protection Type** drop-down list, choose an option **1+0**, **1+1**, **1+R**,**1+1+R** .

Note
Circuit diversity is supported only for 1+0 protection type.

h) Click the **Path Option Configuration** hyperlink. The Path Option Configuration screen appears.

Note
This hyperlink is disabled when the **Diversity** checkbox is checked.

Click **Add**. Perform the following steps in the Create Path Option dialog box:

- In the **Index** field enter a unique index . The valid range is from 1 to 1000.
- From the **Path Option Type** drop-down list, choose **Dynamic** or **Explicit**.

  Note
  For using the option Explicit, make sure that an explicit path is already defined. You can define an explicit path using procedure Add an Explicit Path Using CTC, on page 26.

- From the **Path Name** drop-down list, choose an explicit path name.

  Note
  The **Path Name** field is disabled, if the path option type is dynamic.

- From the **Affinity Attribute-Set Name** drop-down list, choose an affinity profile.
- From the **Protected By** drop-down list, choose a protected path option.

  Note
  The **Protected By** drop-down list is disabled for Restored or Protected path options.

- From the **Restored By** drop-down list, select a restored path option. If any of the working or protected path fails, restored path replaces the failed path.

Note
The **Restored By** drop-down list is disabled if you have selected path option as Restored.

- Click **OK**.

i) From the **Path Protection** Profile drop-down list, choose an option. The default option is **None**.

Note
This drop-down list is disabled if protection type is selected as **1+0**.

j) Check the **Record Route** check box.
k) Click **Finish** to create the circuit.

Step 6 Return to your originating procedure.

Discover a Circuit Using CTC

Purpose	This procedure provides instructions to discover a circuits from the list of OTN circuits using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* #unique_97
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Circuits** tab.

Step 2 Click **Query**. Perform the following steps in the OTN Services Query screen that appears.

a) From the **Existing/New Query** drop-down list, choose **New** or **Existing**.
b) Enter the tunnel IDs if you have selected **New Query**.

Note
For **Existing Query**, Tunnel IDs and Query Group fields are populated automatically.

c) Click **Query Group**. Perform the following steps in the User Query Group Chooser dialog box:

- From the **Group** drop-down list, choose an option.
- From the **Available Nodes** pane, choose a node.
- Click >> to move the selected node from the Available Nodes to the Grouped Nodes pane.

- Click **Save** to save this query group criteria. A dialog box appears, enter a name for the query group and click **Save**.
- Click **Apply All** to select all the available nodes. These nodes appear in the field next to the **Query Group** button.
- Click **Apply Selected** to select only the grouped nodes. These nodes appear in the field next to the **Query Group** button.

d) Click **Save** to save the query criteria.
e) Click **Run Query** to execute the query.

Note
The **Run Query** button gets enabled only when you enter a value in the Query Group field. The search result appears in the Query Matches pane.

f) Enter a search criteria in the field adjacent to the **Find Next** button.

Note
This button gets enabled only when you have a value in the Query Matches pane.

g) Click **Find Next**.

Note
The next value gets highlighted in the Query Matches pane based on the search criteria.

h) From the **Query Matches** pane, choose a **circuit**.
i) Click >> to move the selected circuit from the **Query Matches** pane to the **Selected Services** to Discover pane.
j) Click **Discover All** to display all the circuits of the **Query Matches** pane on the **Circuits** tab.
k) Click **Discover Selected** to display all the selected circuit of the Selected Services to Discover pane on the **Circuits** tab.

Step 3 Return to your originating procedure.

Edit General Parameters of a Circuit Using CTC

Purpose	This procedure provides instructions to edit general parameters of an OTN circuit using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Network View, click the **OTN** > **Circuits** tabs.

Step 2 Select a circuit and click **Edit**.

Step 3 Click the **General** tab. Perform the following steps in the Edit Circuit screen that appears:

a) Modify the parameters such as **Name**, **Bandwidth**, **Path Protection Profile**, **Bandwidth Configuration**, **Diversity** and **Source and Destination** client interfaces as needed.

Note
Details of source and destination client interfaces are editable only when you update UNI circuits.

Note
The **Path Option Configuration** hyperlink is disabled when the **Diversity** checkbox is checked or when diverse circuit of the selected circuit exists.

b) Click **Apply** to save the changes.

Note
CTC hangs for a minute when multiple edit circuit windows are opened with multiple pluggable OIR.

Step 4 Return to your originating procedure.

Edit ODU Configuration of a Circuit Using CTC

Purpose	This procedure helps to edit the ODU configuration of a circuit.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series* #unique_97 Discover a Circuit Using CTC, on page 21
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Circuits** tab.

Step 2 Select a circuit from the list.

Step 3 Click **Edit**.

For the procedure to view TCM parameters, see View TCM PM Parameters Using CTC

Step 4 Click **ODU Configuration** tab.

Step 5 From the left pane, click the **ODU Line Configuration** tab. Perform the following steps in the Edit ODU Line Configuration screen that appears:

a) Select a controller from the list.
b) From the **Admin State** drop-down list, choose **Automatic in Service**, **Maintenance** or **Normal**.

Note
This field displays the current status of a controller.

c) From the **Loopback** drop-down list, choose an option **Internal**, **Line** or **None**.
d) From the **GCC1** drop-down list, choose **Enable** or **Disable**.
e) Click **Apply**.

Step 6 From the left pane, click the **ODU TTI Configuration** tab. Perform the following steps in the Edit ODU TTI Configuration screen that appears:

Note
TTI configuration is not supported on HO ODUs.

a) From the **Controller Name** drop-down list, choose controllers for the **Source** and **Destination** pane respectively.

Note
The values that you enter in the **Transmit** area of the **Source** pane are displayed in the corresponding fields of the **Expected** area of the **Destination** pane. Similarly, the values that you enter in the **Expected** area of the **Source** pane are displayed in the corresponding fields of the **Transmit** area of the **Destination** pane. The values of the **Received** area of the **Source** and **Destination** pane must be the same.

b) In the **Transmit** area, click **ASCII** or **Hex (1 byte)** to specify the data type for the operator string.
c) Click **ASCII Mode**. The operator string is converted to ASCII data type.
d) Enter a new operator string. This string replaces the operator specific string when you click **Apply**.
e) Repeat steps (b) through (d) to select a data type in the **Expected** area of the **Source** pane.
f) Check the **Auto-Refresh** check box to refresh the received operator specific value automatically in every 5 seconds.
g) Click **Apply**.

Step 7 From the left pane, click the **TCM Line Configuration** tab. Perform the following steps in the Edit TCM Line Configuration screen that appears:

a) From the **Controller Name** drop-down list, choose a node.
b) From the **TCM Mode** drop-down list, choose a mode.

The available options are:

- Transparent - TCM data is passed through without any change , fault management and performance monitoring parameters are not enabled.
- Operational - fault management (the LTC-CA alarm can be enabled) and performance monitoring parameters can be enabled.
- NIM (Non-Intrusive Monitoring) - Performance monitoring parameters are enabled but are read-only. The LTC-CA alarm cannot be enabled.

c) Check the **Enable PM** check box to enable performance monitoring. This check box can be selected when the TCM Mode is either Operational or NIM.
d) Select the **LTC-CA** (Loss of Tandem Connection-Consecutive Action) check box to enable this alarm. This check box can be selected only when the TCM Mode is Operational.
e) Select the **TIM-CA** (Trace Identifier Mismatch-Consecutive Action) check box to enable this alarm. This check box can be selected only when the TCM Mode is Operational.
f) Click **Apply**.

Step 8 From the left pane, click the **TCM TTI Configuration** tab. Perform the following steps in the Edit TCM TTI Configuration screen:

a) From the **Controller Name** drop-down list, choose controller for the **Source** and **Destination** pane respectively.

Note
The values that you enter in the **Transmit** area of the **Source** pane are displayed in the corresponding fields of the **Expected** area of the **Destination** pane. Similarly, the values that you enter in the **Expected** area of the **Source** pane are displayed in the corresponding fields of the **Transmit** area of the **Destination** pane. The values of the **Received** area of the **Source** and **Destination** pane must be the same.

b) From the TCM drop-down list, choose TCM on the **Source** and **Destination** pane respectively.
c) In the **Transmit** area, click **ASCII** or **Hex (1 byte)** to specify the data type for the operator string.
d) Click **Hex Mode**. The operator string is converted to hexadecimal data type.
e) Enter a new operator string.
f) Click **Apply** to replace the operator specific string.
g) Repeat steps (c) through (e) to select a data type in the **Expected** area of the **Source** pane.
h) Select the **Auto-Refresh** check box to refresh the received operator specific value automatically, every 5 seconds.
i) Click **Apply**.

Step 9 From the left pane, click the **PM Thresholds** tab.

a) Click the **ODU Controller** tab. Perform the following steps in the ODU controller screen that appears:

Note
Performance monitoring should be enabled for ODU controllers.

- From the **Controller Name** drop-down list, choose a **controller**.
- From the **Layer Name** drop-down list, choose an option **Path** or **GFP**. The PM threshold values get populated in the table appears on the screen.
- Click either **15 Min** or **1 Day** interval to get the PM interval.
- Click **Refresh** to get the updated PM threshold values in the table from the legacy node.

b) Click the **TCM** tab. Perform the following steps in the TCM screen that appears:

Note
Permon should be enabled for TCM controllers.

- From the **Controller Name** drop-down list, choose a controller. The PM threshold values get populated in the table appears on the screen.
- Click either **15 Min** or **1 Day** interval to get the PM thresholds interval.
- Click **Refresh** to get the updated TCM PM threshold values from the legacy node.

Step 10 Return to your originating procedure.

Add an Explicit Path Using CTC

Purpose	This procedure provides instructions to create an explicit path using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* Configure OTU for OTN Controller Using CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Explicit Paths**.

Step 2 Click **Add**. Perform the following steps in the Create Explicit Path screen:

a) Enter a name of the explicit path.

Note
Strict path type is selected by default.

b) Click **Add**. Perform the following steps in the Add Node dialog box. Alternately, select a node from the map, and click **Add**.

- From the **Node** drop-down list, choose**node**.
- From the **Interface** drop-down list, choose an **interface**.
- Click **Apply**.

c) Click **Apply** to save the explicit path.

Step 3 Return to your originating procedure.

Store an Explicit Path Using CTC

Purpose	This procedure provides instructions to store an explicit path using CTC.
Tools/Equipment	None

Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* Add an Explicit Path Using CTC, on page 26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **Explicit Paths** > **Explicit Paths** tab.

Step 2 Click **Store**. Perform the following steps in the Store Explicit Path (s) dialog box:

a) Check the check box adjacent to a node name.

b) Click **OK** to store the explicit path.

Step 3 Return to your originating procedure.

Load an Explicit Path Using CTC

Purpose	This procedure provides instructions to load an explicit path using CTC.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* Store an Explicit Path Using CTC, on page 26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **OTN** > **Explicit Path**.

Step 2 Click **Load**. Perform the following steps in the Load Explicit Path (s) dialog box:

a) Check the check box adjacent to a node name.

b) Click **OK** to load the explicit path.

Step 3 Return to your originating procedure.

Link Management Protocol

The Link Management Protocol (LMP) is a protocol used in Generalized Multi-Protocol Label Switching (GMPLS) networks to manage and maintain the control channels and links between nodes. LMP is essential for ensuring the proper functioning of GMPLS by handling these tasks:

- **Link Verification**: LMP verifies the connectivity and integrity of data links between nodes, ensuring that the links are operational and free of faults.
- **Fault Management**: LMP detects and isolates faults in the network, allowing for quick identification and resolution of issues.
- **Control Channel Management**: LMP manages the control channels used for signaling and routing information between nodes, ensuring reliable communication.

Create an Local UNI LMP Using CTC

Purpose	Link Management Protocol (LMP) is used to manage Traffic Engineering (TE) links. It allows multiple data links into a single Traffic Engineering (TE) link that runs between a pair of nodes. Link Management Protocol (LMP) is used to support interoperability between the NCS 4000 node and the MSTP node. The LMP creation wizard allows you to provision the source and destination end-points of the LMP link, the optical parameters, and alien wavelength settings.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View**, click the **Provisioning**.

Step 2 Click the **LMP** tab.

Step 3 Click the **Create** button.
The **LMP Creation** wizard appears.

Step 4 In the **LMP Origination** screen, provision these parameters.

a) Select the source node of the LMP from the **Originating Node** drop-down list.

If the source node is NCS 4000, then the destination node must be MSTP.

b) Select any of these options to create a numbered or unnumbered LMP.

- Click **Unnumbered** if you want to create an unnumbered LMP.

The Interface IP field is disabled if this option is selected. and the DWDM node Router ID and Unnumbered IfIndex assigned to the local controller by the DWDM node identify the link.

- Click **Numbered** if you want to create an unnumbered LMP.

  A numbered interface will have an IP address at the two ends.

c) In the **Communication Channel** field, enter the router IP address.
d) Select UNI from the **Mode** drop-down list.
e) Select the port that is connected to the DWDM node from the **Port** drop-down list.

Step 5 Click **Next**.

Step 6 In the **LMP Termination** screen, provision these parameters:

a) From the **Terminating Node** drop-down list, choose the destination node of the LMP.
b) Rx Port Selection—Choose the card type from the **Type** drop-down list; choose a unit from the Unit drop-down list; choose a port from the Port drop-down list.
c) Tx Port Selection—Choose the card type from the **Type** drop-down list; choose a unit from the Unit drop-down list; choose a port from the Port drop-down list.
d) Enter the IP address of the destination node in the Interface IP field.

   The Interface IP field is disabled if the Unnumbered option was selected in the LMP Origination screen of the wizard.

e) Mode—Sets the type of revertive restoration to either UNI-C or UNI-N. If the mode is set to UNI-C, the reversion of the circuit from the restored path to the original path is triggered by the UNI client. If the mode is set to UNI-N, the reversion of the circuit is triggered by the DWDM network and can be either a manual revert or an auto revert.

Step 7 Click **Next**. Perform the following steps in the Optical Parameters screen that appears in the LMP creation wizard:

Step 8 In the **Optical Parameters** screen of the wizard, provision these parameters:

- Check the **Allow Regeneration** check box (optional).

  Note
  When checked, the computed path traverses through the regeneration site only if optical validation is not satisfied. If a transparent path is feasible, the regenerator is not used.

- From the **UNI State** drop-down list, choose **Enable** or **Disable**.

  Note
  The Enable state is used to configure the UNI interface for the circuits to pass through, between the router and DWDM node. In the Disable state, the interface is configured but not active and circuit activation is rejected. When the status is changed from Enable to Disable, all the active circuits on the interface are deleted.

- Description—Enter the description of the UNI interface. The description can be up to 256 characters.
- Label—Enter an alphanumeric string. This label is an unique circuit identifier.
- Validation—Sets the optical validation mode.
- Acceptance threshold—Sets the acceptance threshold value for the GMPLS circuit. The circuit is created if the actual acceptance threshold value is greater than, or equal to, the value set in this field.

- Restoration—Check this check box to enable the restoration of the GMPLS circuits on the UNI interface.
- Validation—Sets the validation mode during restoration.
- Acceptance threshold—Sets the acceptance threshold value for the GMPLS circuit. The circuit is restored if the actual acceptance threshold value is greater than, or equal to, the value set in this field.

Step 9 Click **Next**.

Step 10 In the **Alien Wavelength** screen of the wizard, provision these parameters:

- From the **Alien Wavelength** drop-down list, choose an alien wavelength class.

  Note
  Choose the 400G-XP-LC-CFP2 wavelength if the NCS4K-4H-OPW-QC2 card is used for creating the LMP between the NCS 4000 and MSTP nodes.

- From the Trunk Selection drop-down list, choose 100G or 200G

  Note
  Choose 100G or 200G if the port is provisioned as OTU4 or OTUC2 respectively.

- From the **FEC** drop-down list, choose the forward error correction (FEC) mode on the alien wavelength channel. The following options are available:
  - 15% Soft Decision FEC DE OFF
  - 25% Soft Decision FEC DE OFF
  - 15% Soft Decision FEC DE ON
  - 25% Soft Decision FEC DE ON

  Note
  Choose the FEC configuration that matches the one in use on the NCS4K-4H-OPW-QC2 CFP2 interface.

Note
This step is applicable when an LMP is created between NCS 4000 and MSTP nodes.

Step 11 Click **Finish** to create the LMP.

Step 12 Return to your originating procedure.

Create a Permanent Connection Using CTC

Purpose	This procedure enables you to create a permanent connection for NCS4K-20T-O-S, NCS4K-2H-O-K,NCS4K-24LR-O-S, NCS4K-2H10T-OP-KS, and NCS4K-4H-OPW-QC2 line cards, using CTC. Permanent connection allows to create a cross-connection.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the Node/Card View, double-click the line card.

Step 2 Click the **Circuits** > **Permanent Connection** tab.

Step 3 Click **Create**. Perform the following steps in the Create Permanent Connection dialog box that appears.

Note
User is allowed to create high order cross connection only. The high order being used should not be channelized. All the permanent connections (except high order connections) are read only.

a) Enter the **XConnect Name** of the permanent connection. The connection ID value ranges from 1 to 32655.
b) From the **End Point 1** drop-down list, select the ingress point of the permanent connection.
c) From the **End Point 2** drop-down list, select the egress point of the permanent connection.
d) Click **OK**.

Stop. You have completed this procedure.

Perform a Path Switch

Purpose	This procedure enables you to perform a path switch. The possible actions are: • Manual Switch Over • Force Switch Over • Lockout (available only on a working circuit)
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the **Network View** , click the **OTN > Circuits** tab.

Step 2 Select a circuit from the list. Ensure that the **Type** is 1+1.

Step 3 Click **Edit**.

Step 4 Click the **Protection** tab.

Step 5 The details of the selected circuit are displayed under the Source and Destination . The working circuit details are in green and the protect circuit details are in purple.

The same details are represented in a pictorial format, in the **File** section. To perform the switchovers, use this pictorial format.

Step 6 Right-click the port of the working circuit or the protect circuit.

The available options are:

- Open Port - opens the card view of the line card.
- Switch commands - displays the available switch over options.

Step 7 Select one of the options under Switch commands.

The available options are:

- Manual Switchover - to switch from the working to the protect circuit or vice-versa
- Force Switchover - to switch back to the working circuit
- Exercise - to check the protocol in use
- Lockout (available only for a working circuit)- the path continues to be on the working circuit (even if a failure is detected on the working circuit)
- Clear Lockout (available only for a working circuit)- the path can now use the protect circuit
- Clear - clears the manual switch option (not available when the path is in the lockout mode)

Step 8 Return to the originating procedure.

Configuring OTN Circuits Using Node Configuration Wizard

Purpose	This procedure configures the OTN circuits using Node Configuration Wizard.
Tools/Equipment	None
Prerequisite Procedures	
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Step 1 In the **Node View** or **Card View**, right-click anywhere and choose the **Node Configuration Wizard**

Step 2 In the **IP Configuration** pane, if you want to provision the Virtual IP, Management IP, EMS IP, Craft IP, Gateway IP and the corresponding mask, complete the following :

a) Enter the **Virtual IP Address** drawn from the management IP address pools that supersede the IP address of RP0 and RP1.

b) Enter the **Subnet Mask** for the Virtual IP address previously entered.

c) In the **RP0-Mgmt IP** and **RP1-Mgmt IP** areas, complete the following information:

- IPv4—Enter a unique IPv4 address assigned to RP0/RP1. It displays blank if not configured.
- IPv4 Mask—Enter the IPv4 subnet mask.
- Rp0 or Rp1 Service State - Select an option from the drop-down menu. The available options are IS, OOS.
- MAC Address—Displays the MAC address of RP0/RP1.
- IPv6 —Enter the IPv6 address assigned to RP0/RP1.
- IPv6 Prefix Length—Enter the prefix length for the provisioned IPv6 address. The value must be between 1 and 128.
- EMS Interface --- Displays the IP address of RP0/RP1 that connects to a device via serial or LAN port.
- EMS Submask --- Displays the subnet mask corresponding to the EMS IP.
- EMS Service State - Select an option from the drop-down menu. The available options are IS, OOS.
- Craft Interface --- Displays the IP address of RP0/RP1 that connects to a device via serial or LAN port.
- Craft Submask --- Displays the subnet mask corresponding to the Craft IP.
- Craft Service State --- Select an option from the drop-down menu. The available options are IS,OOS.

Note
If your node is having dual RP, then you must configure both the RP0 and RP1 to avoid discrepancy while performing switchover.

d) In the Gateway area, complete the following information :

- IPv4 --- Enter a unique IPv4 address.
- IPv6 --- Enter a unique IPv6 address.
- IPv6 Prefix Length --- Enter the prefix length for the provisioned IPv6 address. The value must be between 1 and 128.

Step 3 Click the **Next** button to save the changes and open the **OTN Topology** pane.

Step 4 Click **Close** to save the changes and close the Node Configuration Wizard.

Step 5 In the loopback interface area, complete the following :

- Interface Type/ID --- Displays the loopback0 and it cannot be modified.
- IP Address --- Configure the Loopback IP Address.
- Sub Net Mask -- Enter the Subnet Mask for the Loopback IP Address.

You cannot delete the Loopback information once configured.

Step 6 In the RSVP-Interface List area, the details include:

- Interface Name - displays the interface.
- RSVP State - choose an option from the drop-down menu. The available options are - Disable and Enable.

Step 7 If you want to create the controller, configure GCC interface, MPLS-TE, RSVP-TE on a particular card, complete the following :

a) In the Port Controller Configuration area, click the **Slot** to see the already configured ports with its corresponding data. The ports which are not configured on the node display the value None.
b) Displays the **Port** number.
c) Displays the **Service State** for the port. The states can be --- IS-NR, OOS-AU.
d) Select a **Service Type** from the drop-down list to create the controller.
e) Check the **GCC0/GCC1** check box if you want to enable GCC on OTU or ODU in each slot.
f) Check the **Unnumbered GCC0/1** check box to assign unnumbered loopback only on the enabled GCC interfaces.
g) Check the **MPLS** check box if you want to configure the specific controller as a part of MPLS configuration. Complete Configure an MPLS-TE Instance Using CTC, on page 11 as needed.
h) Check the **RSVP** check box if you want to configure the specific controller as a part of RSVP configuration. Complete Configure a RSVP-TE Instance Using CTC, on page 12 as needed.
i) Configure the value of **Admin weight** only if MPLS is enabled. This weight ranges from 0 to 65535.

   The default value of Admin weight is 0.
j) Configure the value of **TTI Mode** only if MPLS is enabled.
k) Configure the value of **Timer** only if RSVP is enabled. It ranges from 180 to 86400 seconds.
l) Configure the value of **Missed messages** field only if RSVP is enabled. It displays the number of refresh optical missed messages and ranges from 1 to 8.

Step 8 If you want to delete the controller, perform the following:

a) Click the **Next** button to save the current changes and open the **OTN Topology** pane.
b) Choose the **Service Type** as **None** to delete the already configured controller.
c) Click the **Previous** button to save the changes and display the previous configuration pane.
d) Click the **Close** button to save the changes and close the Node Configuration Wizard.

   Delete the controller manually from the MPLS or RSVP, If you have configured the controller as part of MPLS or RSVP configuration.

Step 9 In the **OSPF** area, Complete the following :

- OSPF Process ID --- Displays OTN and cannot be modified.
- Router ID --- Displays the virtual IP of the node.
- Enable NSR --- Displays the field as checked once the OSPF process ID and Router ID is created.
- Enable NSF --- Displays the field as checked once the OSPF process ID and Router ID is created
- Add --- Click this button to create an OSPF entry.
- Delete --- Click this button to delete a selected OSPF entry.
- Interface --- Choose the OSPF interface from the drop-down list.
- Area ID --- Displays area ID as 0.
- Cost --- Enter the cost used by OSPF routers to calculate the shortest path.

- Passive --- Choose the state of the OSPF interface from the drop-down list. The available options are True and False.

Step 10 Click **Previous** to save the current changes and display the previous configuration pane.

Step 11 Click **Close** to save the changes and close the Node Configuration Wizard.

Stop. You have completed this procedure.

Configure Interoperability Between NCS 4000 and MSTP Nodes

Purpose	Link Management Protocol (LMP) is used to support interoperability between the NCS 4000 node and the MSTP node. To support interoperability, this procedure provisions an LMP between an NCS 4000 node and MSTP nodes followed by the creation of an GMPLS OCH trail circuit between two NCS 4000 nodes.
Tools/Equipment	None
Prerequisite Procedures	"Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.*
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 To provision an LMP between an NCS 4000 and MSTP node, complete Create an Local UNI LMP Using CTC, on page 28.

Step 2 To provision a TE link, complete Enabling GMPLS Using CTC, on page 8.

Step 3 To provision a GMPLS OCH trail circuit between two NCS 4000 nodes, complete Configure GMPLS OCH Trail Between NCS 4000 Nodes, on page 35

Stop. You have completed this procedure.

Configure GMPLS OCH Trail Between NCS 4000 Nodes

Purpose	This task provisions a GMPLS OCH trail circuit between NCS 4000 nodes that are connected to MSTP nodes.
Tools/Equipment	None

Prerequisite Procedures	• "Login to CTC" in *System Setup and Software Installation Guide for Cisco NCS 4000 Series.* • Create an Local UNI LMP Using CTC, on page 28
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the network view, click the **DWDM Functional View** icon in the toolbar. The DWDM Network Functional View <Circuit Maintenance> opens.

Alternatively, you could perform the following steps in the network view:

- Click **Circuits** > **Circuits** tabs.
- Click **Create**. The Create Circuit dialog appears.
- Click **WSON**. The DWDM Network Functional View <Circuit Maintenance> opens.

Step 2 From the Change Perspective drop-down list in the toolbar, choose **Circuit Creation**. The Circuit Creation view opens.

Step 3 Select the source node from where the OCH trail circuit must originate.

Step 4 Right-click and select the originating port on the source node.

Step 5 Select the destination node where the OCH trail circuit must terminate.

Step 6 Right-click and select the terminating port on the destination node.

The GMPLS/WSON OCH_TRAIL Selection window appears.

Step 7 Specify a name and label for the circuit.

Step 8 Set the validation mode and acceptance threshold.

Step 9 Check the Wavelength Configuration check box to configure an explicit wavelength for the circuit.

Step 10 Check the IS checkbox to place the OCH trail circuit in service after creation. It is checked by default.

Step 11 Click **Create**.

All the configurations are applied to the circuit. The circuit appears in the Circuits tab in the Network Data pane.

Step 12 Return to your originating procedure.